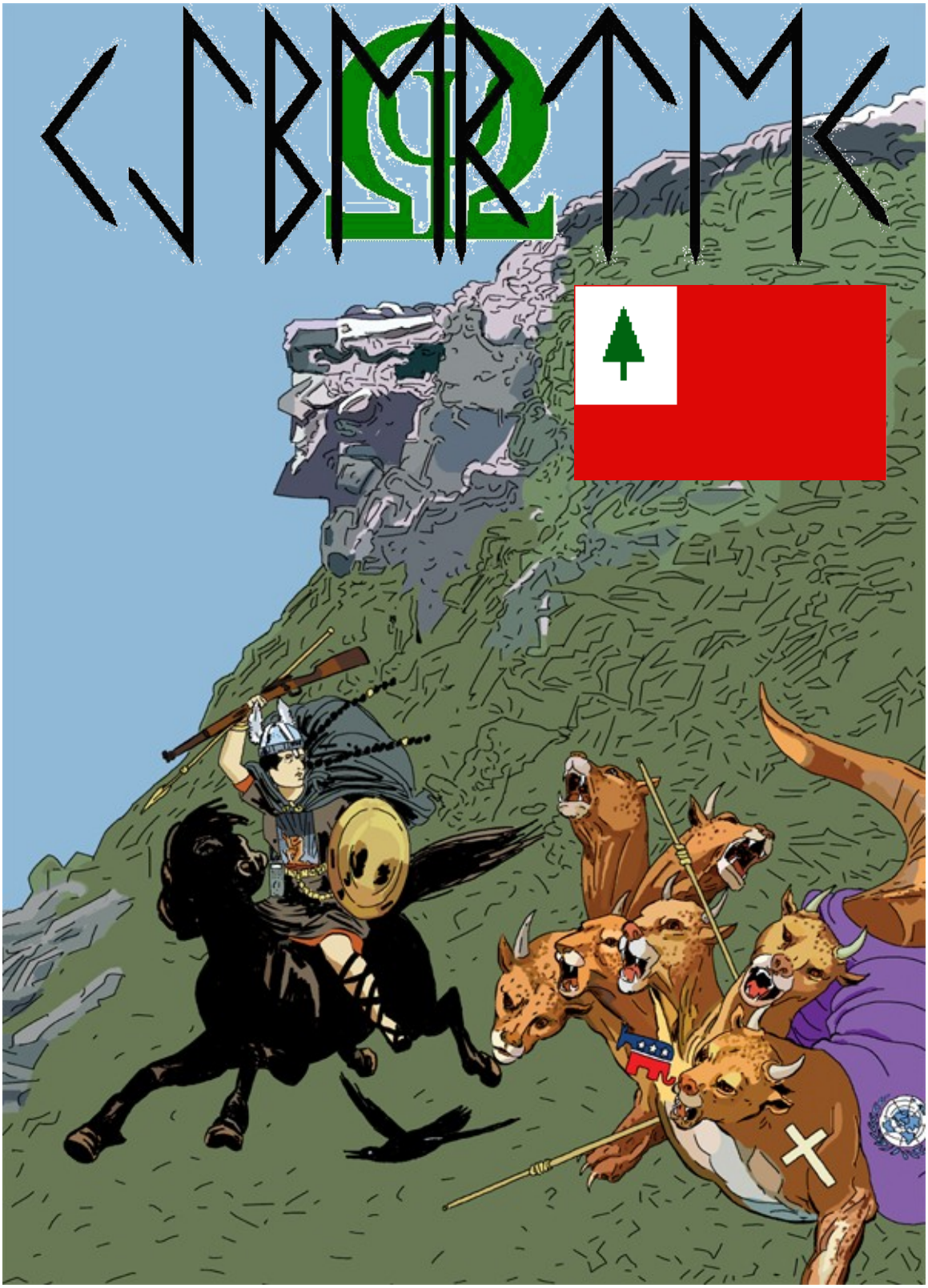
Cybertech Issue #23



Cybertech

The Cyberpunk Technological Survival Journal

Established 1990.

Issue Number 23, Released October 1st, 2007

Cover Art: **"Reason Slays the Beast"** by Stanley Lieber

Table of Contents:

Cybertech has been published since 1990. It is a tool intended to help freedom-loving individuals function in an increasingly unstable, dangerous, and totaltarian society. Cybertech is published for educational purposes only under the First and Second Amendments of the Bill of Rights, United States Constitution.

"If you are the type who likes to fantasize functioning under a totaltarian system which treats everyone like he was either a prison or a nuthouse inmate, you'll love this." - Kurt Saxon

Effective SSH Implementation

by Rightc0ast

I thought it would be good to have a plain language doc on using Secure Shell effectively to give to people just getting their feet wet in secure network communications. This is fleshed out version of presentation I gave at Melbourne LUG a few months back on SSH's common, and not so common uses. This is by far both the easiest and best way to do things like set up a VPN, automate encrypted backups, set up a secure ftp server for your network, and mount a secure file system you can interact with as if it were on the localhost. I use Debian and Ubuntu, so this file will be mostly geared to those distros. Most of the info is global to any ssh install however, and if needed, easily tweaked.

First if you don't already have it, install ssh:

apt-get install ssh-server

Now we will connect to a remote machine. To do this you type 'ssh hostname' on your local machine.

$ssh 192.168.1.103

You use the hostname or IP address of the remote machine that you want to connect to. By default ssh will authenticate as the same user you are using the local machine. To log in as a different user use remoteuser@hostname as the argument. Such as in this example:

$ssh rightcoast@192.168.1.103

After logging in you will be presented with a dialog asking to add the new machine to a list of known hosts. You can say yes here, or go the extra step and check the RSA fingerprint to ensure you are connecting to the machine you think you are. You're connected to the remote machine and can execute commands on it as if you sitting in front of it.

You can also run a command directly on the remote machine. Check running processes:
$ ssh 192.168.1.103 ps aux

Monitor a log:
$ ssh rightcoast@192.168.1.100 tail -f /var/log/syslog

Etc...

Securing the default install

Further hardening of the default install is easy. I think these following two steps harden just enough without sacrificing any functionality. First I like to edit the /etc/ssh/sshd_config file either uncommenting or editing the following.

Protocol 2
Ciphers blowfish-cbc,aes256-cbc,aes256-ctr
PermitRootLogin no
PermitEmptyPasswords no
IgnoreRhosts yes
StrictModes yes
LoginGraceTime 30
MaxStartups 6
MaxAuthTries 6
Subsystem sftp /usr/lib/openssh/sftp-server

I like Compression set to no. I like to compress and transfer backups with piped commands and what happens when it is set to yes is you basically make a redundant compression workload.

I also forward X sessions.

The second step to securing your ssh install is to configure tcpwrappers by editing the hosts.allow and the hosts.deny file in your /etc directory. Single addresses or whole ranges and tld's can be added. The following examples work well:

hosts.deny/hosts.allow example:
/etc/hosts.allow
sshd: ALL EXCEPT 123. .cn .pl .ru .in .my .ro .kr : ALLOW
/etc/hosts.deny
sshd: ALL : ALL

Here are some iptables rules you can use to accept/deny connections if you want to really restrict access to only other hosts on your LAN or whatever machines you want. Keep in mind these two rules are pretty restrictive and suitable if you don't forsee the need to connect from an unknown machine. Of course you can also use fwbuilder or whatever other firewall tool you use to configure this.

Permit connections from address 192.168.1.102 to SSH (port 22)

iptables -A INPUT -p tcp -m state --state NEW --source 192.168.1.102 --dport
22 -j ACCEPT

Deny all other SSH connections

iptables -A INPUT -p tcp --dport 22 -j DROP

Remember to save the rules: /etc/init.d/iptables save

Public/private Keys

I like to generate public/private keys for passwordless authentication. It is very secure and after configuring ssh-agent, easier than typing in a password every time. You first generate a key pair with:

$ ssh-keygen -t dsa

Which will output:

Generating public/private dsa key pair.
Enter file in which to save the key (/home/rightcoast/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/rightcoast/.ssh/id_dsa.
Your public key has been saved in /home/rightcoast/.ssh/id_dsa.pub.
The key fingerprint is:
42:**:**:**:**:**:bd:14:**:**:**:**:13:37:**:** rightcoast@mobileops

Then it asks for a passphrase. You should choose one that is long and not easily guessed like a sentence. Adding punctuation and digits makes guessing the passphrase even harder. Spaces are allowed. The private key ALWAYS stays on the local machine and you have to be sure not to lose it or allow it to be made public knowledge. You put your public key on the machines you want to connect to in a file called .ssh/authorized_keys. The public key is the one that is distributable and can be viewed by others.
After being sure you now know which is which you can move the proper (public) key to the remote machine on a floppy or using scp (I will cover this more later, cut and paste the following after replacing

my username@machine with yours if you don't know scp yet):

$ scp ~/.ssh/id_dsa.pub rightcoast@192.168.1.103:.ssh/authorized_keys

After asking for the user password it will begin transferring. Then you ssh to the remote machine, and should be asked for the passphrase. It is longer than your password, but don't worry, you won't be typing it much longer because we are going to automate this later. After connecting we are going to set the proper permissions on the directories:

$ sudo chmod 700 ~/.ssh
$ sudo chmod 600 ~/.ssh/authorized_keys

Now we want to do the automation part to make life easier. Having to type a password or passphrase every time is a real drag. Debian and Ubuntu which I use both start ssh-agent by default. You would need to start that if your distro does not start it when you start your session. You add your key by typing ssh-add at the prompt and entering your passphrase when asked. You might want to add the ssh-add program to your startup programs so it brings up a prompt in X to ask for your passphrase when you login initially. In gnome this can be done by adding ssh-add in session preferences under the startup tab. You also will need a variation of the askpass program. I did an apt-get install ssh-askpass-gnome.

SCP

The program most often used for copying to and from a remote machine is called scp. It is a replacement for rcp hence the name 'secure file copy'. The basic usage to copy a file from a remote machine:

$ scp rightcoast@192.168.1.103:~/docs/br407_ssh.txt ~/docs

To copy a local file to the remote machine you can use:

$ scp ~/docs/br407_ssh.txt rightcoast@192.168.1.103:~/docs

The times and modes of the file can be saved by passing -p. I should point out that the first two examples were longer just for clarity. A real transfer can be shortened (if I have the file in my home dir) to the following because /home/localuser is the default both locally and remotely as I mentioned before.

$ scp -p br407_ssh.txt 192.168.1.103:/tmp

You can also specify ports to use with (capital) -P:

$ scp -P 435 ~/docs/br407_ssh.txt 192.168.1.103:~/docs

SFTP

You can also use secure ftp transfers via the command line. You can also set up putty, gftp, etc to use secure ftp transfers if you want to. Connect using the CLI by typing:

$ sftp 192.168.1.103
$ rightcoast@192.168.1.103's password:
sftp>

You can then list commands with help. Common ones are ls, cd, put and get. If you are familiar with ftp commands, that is all they are. The commands are similar to Linux commands for the most part.

Encrypting X sessions

One of the more underused functions of ssh is encrypting remote X sessions. In order to save resources on

the laptop you can use this to run applications like Xchat and other gui programs on the remote server. This is done by using the -X switch:

$ ssh -X 192.168.1.103

A shell opens on the remote host which forwards X traffic to your machine. You can then open up any program that uses X (Gaim, xchat, xterm, Firefox, etc)

Piping commands over ssh

Any command, to my knowledge, can be piped over ssh. An example showing active connections to a remote apache server.

$ ssh 192.168.1.100 netstat -an |grep :80 |wc -l

Backups with rsync and tar
From Samba.org: "rsync is a file transfer program for Unix systems. rsync uses the "rsync algorithm" which provides a very fast method for bringing remote files into sync. It does this by sending just the differences in the files across the link, without requiring that both sets of files are present at one of the ends of the link beforehand."

Rsync needs the -e switch to specify the secure shell. Here is a simple example of off the remote machine onto the local one synched to my home directory.

rsync -ave ssh 192.168.1.103:~/br407_ssh.txt br407_ssh.txt

A period at the end saves the exact file to the current directory.

$ cd docs
~/docs$ rsync -ave ssh 192.168.1.103:~/br407_ssh.txt .

Copy a file from the local machine to the remote one in much the same way:

$ rsync -ave ssh br_407.txt 192.168.1.103:/home/rightcoast/

You can also mirror directories exactly. The --delete command will delete any files on the remote machine that don't exist on the local one. Like say you deleted a couple files, and want them gone on the server as well, since they are there too from the last rsync. Here is how I could mirror my ebooks directory and remove any deleted locally deleted books on the remote at the same time. The -z switch also compresses the data transfer.

$ rsync -az -e ssh --delete ~/ebooks 192.168.1.103:~/ebooks

There are some great examples of different uses at samba.org and the rsync man page is a good one.
http://www.samba.org/rsync/examples.html

You can tar really large directories or files too and send them securely. This is usually a lot faster than rsync if the directory/file is huge, and usually a good idea to do on your first backup. This is one variation on how to do that:

$ tar cf - /home | ssh rightcoast@192.168.1.103 tar xf - -C /home/backup/

Automating the Backup

Automating backups with ssh is a snap too. Once you've set up a keypair like we talked about above you can just use a small shell script and set it up with crontab to run at the desired times.

First set up the directory to put the backups in:
ssh 192.168.1.103 mkdir bkups

then make the script:
$ nano bkup.sh

and save the script like the following.

```
#! /bin/bash

# syncs the local home with the remote directory bkups preserving everything but
# hardlinks. If you need to preserve those and know what they are, don't forget to add the
# -H
rsync -rca -e ssh --delete-after ~/ rightcoast@192.168.1.103:bkups
```

make sure it's executable and fire up crontab:
$ chmod ug+x backup.sh
$ crontab –e

The crontab file, if the reader doesn't know, schedules tasks. If you aren't familiar with cron, of course rtfm (read the fine manpage :D) or paste in the following using your username of course to schedule nightly backups at 0200.

```
0 2 * * * rightcoast ~rightcoast/bkup.sh
```

rdiff is great for backups to, but for these purposes I went with the easiest way for just about anyone to do a couple Ubuntu installs and get this up and running with a couple cut and pastes.

Port forwarding and tunneling

You can forward traffic from local machines to remote machines and vice-versa. This is a great feature of ssh, though one I don't use that often. Traffic is tunneled from the localhost to a remote port with –L switch:

```
$ ssh –L 1234:localhost:23 rightcoast@192.168.1.103
```

You can forward in the opposite direction (remote to local) with the –R switch:

```
$ ssh –R 1234:localhost:23 rightcoast@192.168.1.103
```

I do use dynamic forwarding sometimes. This is a very useful tool that comes in quite handy when you need to access sensitive data on an untrustworthy network. The –D switch is what is used here.

```
$ ssh –D 1234 rightcoast@192.168.1.103
```

After doing this you can then go into your browser settings and set up your localhost as a socks proxy. Irongeek has a good flash tutorial on this topic at his site.
http://www.irongeek.com/i.php?page=videos/sshdynamicportforwarding. Hopefully this guide helps set some people up using ssh and allows anyone reading to set up basically unsniffable communications on the network. Coupled with an encrypted filesystem and fuse mounting remote sshfs encrypted systems (A Google exercise for the reader after setting the above up) the network is for all intents and purposes protected by the best cryptography available to you period. Of course if you typo and blow out your home partition, or if I typo'd and you blow out your home partition, don't come hollering at me. All of the above is use at your own risk yada yada yada.

```
.-------------------------------------------------------------------------.
|                                                                         |
|-------------------/ Secure Data Caching With OpenBSD /-------------------|
|                                                                         |
|               Practical Techniques For Remote Data Storage              |
|                                                                         |
`-------------------------------------------------------------------------'
```

azure@osuny.co.uk ============================== https://osuny.co.uk/~azure

These Kids Today

Time was, the gentleman computer enthusiast could expect to zero out and reformat his hard drive with the relative certainty that whatever data he had stored upon it would not come back to haunt him. As we are often resigned to acknowledge, times do change; and often with alarming swiftness. In this era of constant, bewildering flux, the proliferation of inexpensive computer forensics techniques has rendered even the thoroughly blanked hard disk an open book to law enforcement, paranoid employers, and nosy younger siblings alike.

What-Ever To Do?

One solution to our dilemma is never to commit unencrypted data to disk in the first place. Tools that ship with several of the popular open source Unix implementations make setting up an encrypted volume a trivial matter for the reasonably savvy user. The resulting filesystem, stored on the drive as an encrypted flatfile, may be manipulated as any other file on the system; including, but not limited to, being the subject of a remote back-up. This article will explore one method of setting up nested, secure storage, and then caching it at a distance.

For this text I have selected the popular OpenBSD[1] operating system. Other free Unices, such as Linux and FreeBSD, offer similar subsystems and utilities, which can be used to achieve similar results.

No Place Like Home

On most systems, the overhead from an encrypted volume is not a significant impediment to performance. Accordingly, it is often sensible to protect one's entire /home partition. OpenBSD, in particular, provides a kernel-level device driver for setting up such a volume, called *vnd(4)*[2]:

> The vnd driver provides a disk-like interface to a file. This is useful for a variety of applications, including swap files and building miniroot or floppy disk images. There are two variants, the traditional vnd that bypasses the buffer cache and thus is suitable for swap on files, but not for building disk-images, and the svnd (``safe'' vnd) variant that goes through the buffer cache, thereby maintaining cache-coherency after the block-device is closed which makes it suitable for creating disk images.

Additionally, when used with a passphrase, the svnd device utilizes Bruce Schneier's *blowfish(3)*[3] encryption algorithm.

Earlier implementations of svnd in OpenBSD faced various limitations, including an arbitrary maximum size and a lack of support for the *fsck(8)*[4] utility. As of OpenBSD 4.0, these limitations are no longer present. On my own systems, I fsck all svnd partitions on boot, some of which are in excess of 136GB.

Foundation (Or: Creating Your Home Partition)

In this example we will create both a secure /home partition, as well as a "portable" sub-partition (for the data we will back-up remotely), whose encrypted flatfile will be stored on the secure /home partition. OpenBSD's default kernel configuration allows for up to four simultaneous vnd pseudo-devices, and may be extended by re-building the kernel, or otherwise modifying the running kernel with the *config(8)*[5] utility.

First, select a location with enough room for the flatfile that will comprise your /home partition, and create the flatfile using the *dd(1)*[6] utility:

```
# dd if=/dev/zero of=/cryptfiles/crypt_home bs=1024 count=1024000
```

In this example we have created a 1GB partition. Adjust according to your own needs.

Next, the *vnconfig(8)*[7] command is used to associate /cryptfiles/crypt_home with an svnd device:

```
# /usr/sbin/vnconfig -ck -v /dev/svnd0c /cryptfiles/crypt_home
Encryption key:
/dev/svnd0c: 1048576000 bytes on /cryptfiles/crypt_home
```

You will be prompted to enter an "Encryption key." This key will serve as the passphrase needed to mount your volume. There does not appear to be any limitation to its length.

Use *disklabel(8)*[8] to create a partition on the svnd device:

```
# disklabel -E svnd0

Initial label editor (enter '?' for help at any prompt)
> a
partition: [a]
offset: [0]
size: [2048000]
FS type: [4.2BSD]
> p
device: /dev/rsvnd0c
type: SCSI
disk: vnd device
label: fictitious
bytes/sector: 512
sectors/track: 100
tracks/cylinder: 1
sectors/cylinder: 100
cylinders: 20480
total sectors: 2048000
free sectors: 0
rpm: 3600

3 partitions:
# size offset fstype [fsize bsize cpg]
```

```
a: 2048000 0 4.2BSD 2048 16384 16 # Cyl 0 - 20479
c: 2048000 0 unused 0 0 # Cyl 0 - 20479
> q
```

Use *newfs(8)*[9] to format your partition:

```
# newfs /dev/svnd0a

newfs: /dev/svnd0a: not a character-special device
/dev/svnd0a: 2048000 sectors in 20480 cylinders of 1 tracks, 100 sectors
1000.0MB in 13 cyl groups (1632 c/g, 79.69MB/g, 10240 i/g)
super-block backups (for fsck -b #) at:
32, 163232, 326432, 489632, 652832, 816032, 979232, 1142432, 1305632, 1468832, 1632032,
1795232, 1958432,
```

Mount your partition:

```
# mount /dev/svnd0c /home
```

Your protected /home partition is now ready for use.

Mounting And Unmounting In The Wild

Kyle Amon's original *OpenBSD Encrypted Virtual Filesystem Mini-HOWTO*[10] included a helpful shell script for mounting and unmounting encrypted partitions once they have already been created, called *cryptfs*[11]. This script can be modified to reflect your specific setup. It should be stressed here that entry of the actual encryption password should never be automated, as doing so would somewhat nullify the benefits of never writing sensitive, unencrypted data to the disk.

Portable Darkness

While the flatfile created aove is itself portable, the typical /home partition will be much too large to easily export for remote back-up. By creating additional, smaller encrypted partitions, one may easily categorize information and distribute it to diverse locations by means of portable media (such as a USB thumb drive) or via a network connection.

Such remote back-ups are easily managed with the open source utility *rsync*[12]. It is not necessary to unmount an svnd partition in order to copy its underlying flatfile to another location. A typical remote back-up script might look something like this:

```
#!/bin/sh

/usr/local/bin/rsync -v --rsh=/usr/bin/ssh --progress \
/cryptfiles/crypt_nude_pix username@remote.host.com:/home/username/backup/cryptfiles/
```

In the script above, your encrypted pr0n partition is safely tucked away on some other host. Anyone stumbling across your file will be unable to mot it unless they 1.) recognize what it is they're looking at, 2.) have an OpenBSD system handy, and 3.) know your passphrase.

Extraordinary Rendition

Even if an adversary gains physical access to your hard disk, an encrypted /home partition will be no good to them unless they have also acquired your passphrase. Since data is never written to the partition unencrypted, no amount of forensic knowledge or investigatory swagger will reveal previously deleted information; or for that matter, information that has yet to be deleted. In this way, even the worst-case scenario of having your hardware seized will likely not result in significant exposure of your data.

In Closing

This article offers no express warranty or implied warranty of any kind, including implied fitness for use or implied fitness of merchantability. I won't promise that you're not already under surveillance, in which case your keystrokes may already be subject to capture, and a passphrase of nigh-infinite length is still not going to do you very much good. If this is the case, you've got more important things to worry about anyway.

Good luck.

Bibliography

[1] http://www.openbsd.org
[2] http://www.openbsd.org/cgi-bin/man.cgi?query=vnd
[3] http://www.openbsd.org/cgi-bin/man.cgi?query=blowfish
[4] http://www.openbsd.org/cgi-bin/man.cgi?query=fsck
[5] http://www.openbsd.org/cgi-bin/man.cgi?query=config
[6] http://www.openbsd.org/cgi-bin/man.cgi?query=dd
[7] http://www.openbsd.org/cgi-bin/man.cgi?query=vnconfig
[8] http://www.openbsd.org/cgi-bin/man.cgi?query=disklabel
[9] http://www.openbsd.org/cgi-bin/man.cgi?query=newfs
[10] http://web.archive.org/web/20060110060446/http://www.backwatcher.org/writing/howtos/obsd-encrypted-filesystem.html
[11] http://web.archive.org/web/20060110060446/http://www.backwatcher.org/software/cryptfs
[12] http://samba.anu.edu.au/rsync

EOF

ΨΩΨ

An Evaluation of the Nigerian Pot-in-Pot Cooling System

by Rightc0ast

The Nigerian pot-in-pot system is a little known way of cooling food and medicine using evaporative cooling when no power at all is available. After coming across a submission to the 2003 California State Science Fair entitled "How Does the Nigerian Pot-in-Pot Refrigeration System Perform in Ramona, California?" I downloaded a PDF of the students experiment and set about testing it in the more humid climate of the east coast. I tested it in Central Florida on a day with a high of 75f and a relative humidity level hovering around 60%.

You don.t need much in the way of materials. All you need are sand, water, a large terra-cotta pot, the larger the better, and a smaller pot to set inside. It is essential the pots are a breathable terra-cotta. Plastics and kiln fired non-porous pots won.t work at all.

It is as simple as taking the large pot, and filling it with sand to where the base of the smaller pot can sit inside so that the tops of both pots are level with one another. Sit the smaller pot inside, centered, and then backfill the sides so there is an insulating layer of sand between the larger and smaller pots. I used the dish the terra cotta pot usually sits in as a lid. It was a snug fit and is undoubtedly a better insulator than the rags I saw placed over the pots in the Nigerian setup.

Place the items to be refrigerated inside the smaller, internal pot and pour water slowly into the insulating layer of sand. Backfill in the sand so that the level is once again at the top of the pots, since adding water settles the sand some. Add a little more water to moisten the top of the sand. It should be mentioned that you should take care adding water to the sand. You don.t want sandy food and medicine. You also are shooting for a wet sand insulator, not a sand soup or water with sand in it insulator. I also tried this experiment with a pot that barely fit within the larger pot, and it was no where near as effective as the one that allowed for a layer of sand a few inches thick. That is something to keep in mind when scouring for free pots.

The system was in place with no food or medicine inside the internal pot at 2100 hours. I put a mercury thermometer inside to check the internal temperature, wet the sand, covered it with foil and left it on the back porch where direct sunlight wouldn.t be a factor. At 2200 I checked it to soon, and the pot and the external air temp were both 70f. At 0210 the internal pot was at 65f and the external air temp was 67f. I forgot to check in the morning, but at 1145 the pot was working as advertised. The internal reading was 53f while outside the air temp was 76f. At 1500 the internal temperature was 55f and the external air temp was 81f. As you can see the temperature difference was 25-26 degrees Fahrenheit during the hottest part of the day.

I took a couple of pictures to help visualize the setup. You can see right after I put the water into the sand, it was already seeping its way out through the pot. The evaporative cooling takes place that way, allowing the warm air to be drawn out and leaving the inside between the cool temperatures of 53f and 55f.

WILDFLOWER'S NOTES 2007

FIRST WORD

First off, this year be of weirdness of all kinds of potential crap that will amaze or frighten one.s mind if not their sanity altogether. Be forewarned, things may occur that could change presently one.s view of any future into a sudden nightmare of survival against the odds as the situation develops. Consider if you don.t want to be prepared for the worst, you should at least acquire the skill of kissing your ass goodbye.

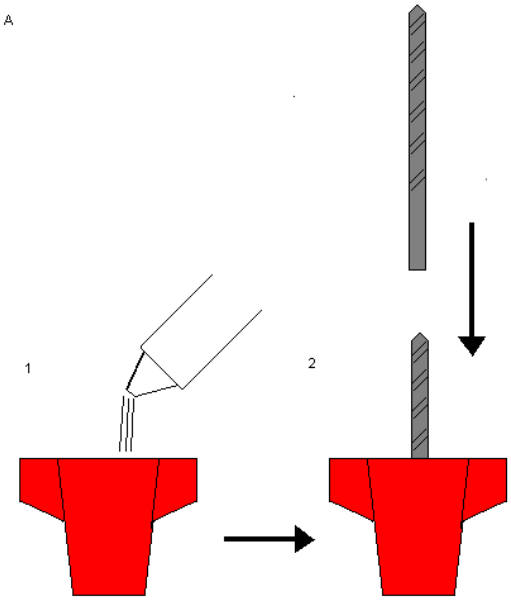
Now for the one.s whom want to survive, it may get real tough depending on your location and type of event that occurs there. Storms of any sort will be more intensive in duration and strength, incurring wind, water, and other stuff destroying homes, crops , and other infrastructure. Periods of higher daylight UV, drought seasons, and pestilence may become the norm. Last winter saw multiple types of flu emerging, sometimes "out of nowhere" taking sometimes a fatal direction for some. And of any note in February saw for a few weeks intense volcano activity occur worldwide. Interesting was the lack of media concern on such activities that been occurring, or even coverage of upcoming events.

What has also been noted spontaneous deadly acts by people harming or killing others on the increase in recent months, oh to wonder what summer going to be like as the general public struggles with the bills, the weather, the economy, and more. This may be the forerunners of a collapse within America that will affect everybody sooner or later worldwide. And that sadly be within your lifetimes, my dear critics, whether you like it or not, even in your "backyard".

Face it for real, the party is over, and guess whom is going to be billed for all this. If you think those same elected bozos are going to help you out of your mess, just remember back in the Cold War, to present day Homeland Security, the average American is expendable regardless of situation. The government al large will protect itself along with the banking and industrial empire, spending your taxes as they see fit. Unless you are part of their crowd, you are on your own unless its politically correct to aid you.

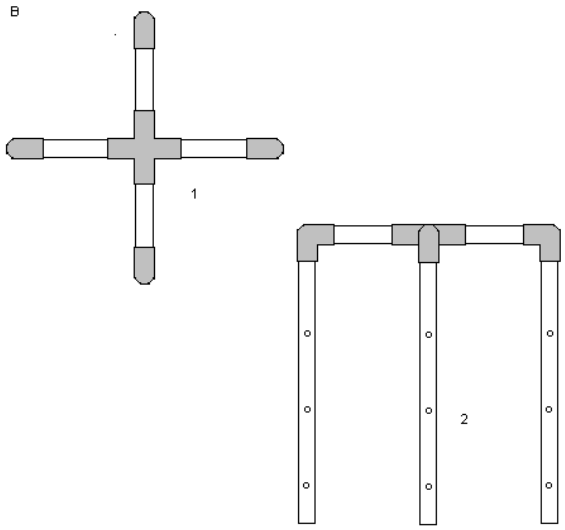
PROJECTS

Drill-bits are useful for drilling holes in wood, plastics, and metals. Even if needed just to start a hole, or ream one existing larger, one could use a pin-vise or pliers to hold the drill bit to "hand-drill" with. However there is another way, especially if a pin-vise is not available or if your hands cannot hold the pliers right.



In figure (A) a large electrical romex wire connector is filled (A-1) with hot glue then drill bit is inserted into the wire connector and held till glue cools straight, centered and upright (A-2). Glue in cap should be allowed to sit and harden for at least 8 hr to achieve a strong bond. I use "winged" wire connectors to make

"hand drilling" easier. This same method could be used with sharpened nails to make "awls" or with "saber saw " blades for small saws.



Staking up tomato or any other plants, people use all sorts of commercial to home-made contraptions. This variation shown in figure (B) can be constructed out of ¾ to 1 inch pvc pipe and fittings. I used the ¾ " pipe stock along with four 90 degree elbows, and one "four-way" cross.

First I cut four sections of ¾" pipe into 6 inch sections (can be longer if you need to). Then with solvent and glue inserted each section into each cross piece end. Then using a flat plywood section on a table solvent and glued each elbow so that all elbows pointed down the same way (B-1).

Now for the "stakes" , mine were sections of same pipe cut into 4 foot pieces (can be any length you choose), each drilled with string holes about "3/8" diameter, 6 inches apart along each length of those sections. This is so you can string thin cord the various plant branches off the ground better.

Take each stake and "press-fit" (do not glue!) into each elbow as in (B-2) then with a wood mallet or wood club insert whole structure into garden spot or growing container 6 to 12 inches deep where future tomato or other plant be growing.

As for stinging cord, I use a homemade needle made from a food can key as in figure (D). at end of season, the structure is removed, the stakes and cord is removed, rinsed off well then stakes and top section is put away till the next season.

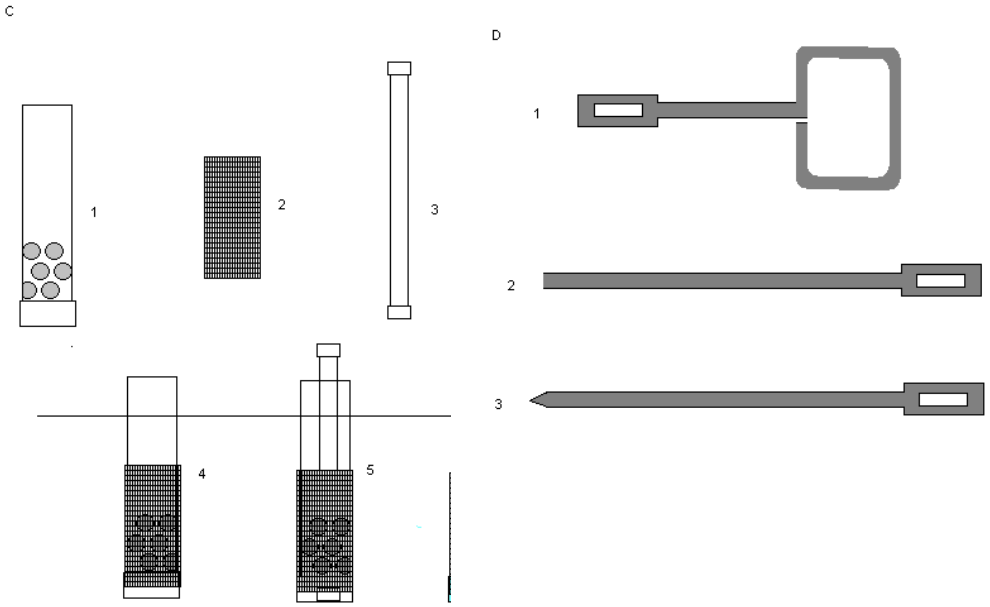
Watering one.s plants is part of your gardening skills. As long as your plants have just enough water, they do fine. However over-watering can lead to root rotting to "blossom rot" destroying your plant and its fruits, like those ugly dark spots on your tomatoes. But as a solution came up with a way to check if my garden containers had enough water or too much.

In figure (C) using 2 and ¾" PVC pipe and cap fittings constructed my own water level checkers. The following are as you choose in pipe lengths.

In (C-1) measure to bottom of your garden container to soil top plus 2 extra inches. Cut a section of 2 inch pipe to this length. Drill up 1/3 rd from bottom, holes with a step drill bit at least each ½ to ¾ inch diameter. Press fit 2 inch cap over bottom. Cut a section of plastic window screen (C-2), wrap over holes and secure with tape or plastic zip-ties, so when buried into soil looks like (C-4). The screen keeps the soil out of the pipe.

The float section is made by cutting to length of the 2 inch section (C-1) plus 2 extra inches a section of ¾ inch pipe, then ¾ inch end caps are solvent cleaned and glued (C-3). When fully dried can be inserted as in (C-5), later on will rise and fall to water level in garden container as in (C-6). If the level shows too much water, one can siphon pump the excess water out.

As a precaution, during skitter breeding season, remove the float and cap top of pipe with another 2 inch cap to prevent any water in pipe become a skitter nursery.



Making a home-made needle from a food can key can be tough as only with some imported can foods are still issued with such keys. However if you came across one you can do as in figure (D), the following instructions be of some help.

Take key (D-1) and using two pliers bend as best as one can straighten as possible. Heat with torch (holding end with pliers), pound with hammer the hot metal into a straight piece on a flat anvil or equivalent. Then place the cooled metal (D-2) into a vise and with flat metal file sharpen the non-hole end into cone head shape (D-3). Re-heat whole needle till hot, then let it cool. This is your homemade needle from a food can key.

If you got a four inch finishing nail, heat the head end, the pound into a flat section, then drill a hole(s) re-heat end , let it cool and use as a home-made needle.

LAST WORD

ZIPPO BRAND LIGHTERS are very hardy tools for lighting cigars, fires, melting glue sticks, lighting candles, melting rope ends, or as an oil lamp in the dark. Its fuel is made from naphtha, which is refined from the high octane aviation fuel. This is why in some survival fiction, the fuel is often several drops of gasoline as a substitute fuel. Rather than be forced to try that option, have stock away several pints of the "official fuel".

Good to have also stashed away are at least several packs or more of flints. However am also able to salvage butane lighter flints, (sometimes cutting them in half) to be reused in the Zippo. Replacement stuffing is salvaged cotton from aspirin bottles. Good to also stash away several replacement wicks. Wrapping the body with a bright color duct tape lets one find the lighter if dropped on the shop or forest floor a lot easier.

SEINE TWINE is a three stranded yarn cord used in chalk lines, mason stone line, making nets, or just trying up stuff. I also use it as a replacement wick for my Zippo lighter. Can also be used as a candle wick for home-made candles, but one should soak the wicks in a solution of borax (4 teaspoons to one hot pint of water) for several hours. Afterwards take the wicks out, hang to dry, then when dried, scrape the wicks of excess crystal borax before using in your candles.

CAYENNE PEPPER a real hot pepper has many other uses. One is that it can be a powerful pain relief for joint pains if mixed with a salve base before applying (ratio at 5 parts max pepper to 95 parts petroleum jelly) to skin. Two is that powdered cayenne pepper can be sprinkled into a bloody wound, it will clot the blood and stop the bleeding . Will have more on this pepper in a future article. Recommend you Google the subject to learn more yourself.

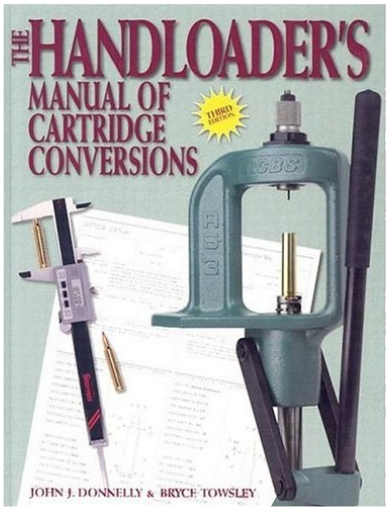
The Handloader's Manual of Cartridge Conversions

Many survival experts suggest acquiring firearms in “common calibers”, and this is generally considered good advice for the beginner. There are several instances however, where that might not be possible or desirable. Beginning survivalists on a budget may not be able to afford an AR-15, M1A, or FAL yet need something reliable and inexpensive. In such an instance it would be preferable to purchase a milsurp bolt action such as a Mauser or Enfield than a modern “sporting” rifle. In a similar vein, many pre-1898 “antique” guns available for purchase sans Big Brother paperwork are in “obsolete” calibers. If your group is lucky enough to have a designated marksman, he or she will most likely have a pet caliber they have been shooting for a long time, and have developed pet loads and ballistic data for it. In such an instance it would be foolhardy to make them switch to something else when they are already intimately familiar with their personal weapon and cartridge combination. These are a only few situations which you may encounter, and The Handloader's Manual of Cartridge Conversions, by John J. Donnelly and Bryce Towsley is your guide for them.

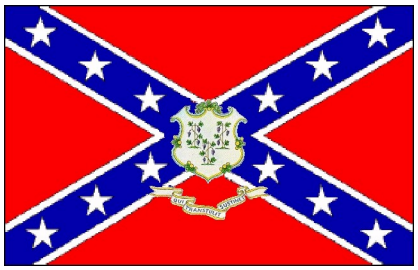
The Handloader's Manual of Cartridge Conversions (HMCC), represents the type of survivalist knowledge that is commonly available now, but probably won't be when it'll be really needed. The time to acquire such knowledge and tools is now while you still can. The HMCC contains information on how to make rare cartridge cases from common brass, substitute smokeless powder for black powder, fabricate 100-year old ammo with modern technology, build and equip a handloading shop, and other knowledge you'd need to keep your “obsolete” boomsticks fed. To provide a few examples, one of my favorite cartridges, the 6.5x55mm Swedish Mauser, can be made from .270 Winchester cases. The 8mmx57 Mauser, the caliber used in the Yugo and German Mausers that are coming into the country, can be made from either .30-06 or .270 Winchester brass. Have a 7.7mm Arisaka that your grandfather (or great-grandfather) brought back from World War II? You can make the brass from .30-06 cartridges. The HMCC contains conversion information on about a thousand cartridges. Along with the conversion information, it also has some basic loading data for each cartridge to get your started with developing your own handloads. The HMCC also contains a wealth of information on equipment, setting up your own handloading shop, and machining techniques for converting and making cartridges from brass stock. With the information provided in this manual you could set up a nice sideline business, or a post-TETOWAKI cottage industry.

The Handloader's Manual of Cartridge Conversions is a useful and fine addition to the gun enthusiast's book shelf. If you are a machinist-type, survivalist or aficionado of fine older firearms, then this book should be considered a must-have for your library. Even if ammunition were to be totally banned by jack-booted, Clinton-worshiping, UN flag-waving thugs intent on destroying the Republic and Constitution, you could take some tools, brass stock and the information in this book to help restore liberty. Knowledge is power, and this book has the knowledge.

The Handloader's Manual of Cartridge Conversions
by John J. Donnelly and Bryce Towsley
608 pages
Stoeger Publishing Company (February 2004)
ISBN-10: 0883172690
ISBN-13: 978-0883172698
List Price: $39.95



ΨΩΨ



Basic Operational Security (OPSEC)
The Unobtainable Goal?

By: CTsurvivalist/CSA

Trying to get people to implement OPSEC into their daily lives is about as easy as giving a tiger a bath. OPSEC, which is any process that identifies critical information to determine if friendly actions can be observed by adversaries intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

Implementing OPSEC is not an easy chore for those without a military mentality. It's hard to convince a mother of two in Wisconsin that she should be concerned about OPSEC. One of the most amazing things to our organization is the apparent apathy among so-called patriot groups and militia's when it comes to OPSEC.

Those with a conspiracy mindset especially make us laugh. They talk about "big brother" and the "new world order", but send communications in plain text. We have seen addresses, chat rooms, operational information, and IP addresses sent to us in unencrypted plain text format.

These individuals talk the talk, but don't walk the walk. Their idea of security is, "knock 3 times and say Bill Sent you". In this day of phishing and e-scams, their group's privacy is apparently not high on their priority list.

Many of my group's members came out of the hacking community of the eighties. These members have been called "well armed hackers" and "high-tech lowlifes". These portrayals are stereotypical of the liberal media. The benefit to the Connecticut Survivalist Alliance (CSA) was a vast amount of OPSEC knowledge and practices.

Basic OPSEC will not cost you a fortune nor will you need hackers to teach you; In fact it can be done for FREE!

Your first step in OPSEC, should be to obtain PGP.

What is PGP, you ask?

This is the most common question our organization receives in e-mail.

PGP (Pretty Good Privacy) is a public key encryption program originally written by Phil Zimmermann in 1991. You may already know that encryption is the process whereby codes are used to attempt to conceal the meaning of a message. PGP is a digital data encryption program. He created PGP to promote awareness of the privacy issue in a digital age. It has become more urgent today because of the ease with which digital data (information in databases, e-mail, and so forth) can be accessed, intercepted and monitored.

Even the former goat herders and sheep gynecologists of al-Qaeda have recognized this fact. If you are a regular reader of our Intel Blog, you may remember the March 15th, 2007 posting of

"Mujahedeen Secrets Download".

During the 1990s, the NSA was frequently in court trying to keep PGP off the market. In the 1980s, the NSA was trying to get the key length of commercial ciphers kept shorter than business wanted.

Although the NSA never admitted it, most cryptography experts believed the NSA wanted to keep longer keys out of use, because NSA did not have powerful enough techniques, or computers, to crack longer keys.

The security of an encryption system depends upon a lot more than the encryption algorithms used. It depends upon the user; Weak passphrases (passwords) are the most common weakness.

Using any passphrase that's ever been published is the inexperienced users first mistake. Some use Biblical quotes or passages from common books.

Cracking PGP is extremely easy if this is done.

The NSA as well as many organizations use dictionary attacks and can also bruteforce the “key”, which is a string of letters and numbers. The Connecticut Survivalist Alliance (CSA) uses a dictionary of Biblical and Quranic quotes in Arabic to intercept Islamic PGP e-mails.

Use an older version of PGP, (before the NSA interest) and use at least a minimum of a 2048 bit key generated by using a completely random passphrase (never been in any published book).

Currently there is no "invulnerable" encryption" method. Human apathy is the biggest weakness.

Pre NSA interested versions of PGP 6.5.8ckt can be downloaded for FREE at:

http://www.pgpi.org/cgi/download.cgi?filename=PGPFW658Win32.zip

Instant messaging has become a fast and convenient way for individuals to stay in touch. These messages are also easily intercepted and monitored. To protect yourself for FREE with the two most popular Instant Messengers you can go to:

AIM (AOL Instant messenger)
http://www.aimencrypt.com/

or

Yahoo

http://www.secway.fr/us/products/simplite_yahoo/getsimp.php

I will not digress into a long dissertation on these programs other tan to say that if you install these methods and would like to test your installation, contact me online.

IF YOU ARE NOT ENCRYPTED - I WILL NOT RESPOND!

AIM - ctsurvivalist

Yahoo - ctsurv

If you procrastinate on OPSEC, you only have yourself to blame.

The most common excuses are:

1. “It’s too inconvenient”
2. “They’ll just crack it anyway”
3. “It’s too complicated”

Our replies are:

1. Is prison or worse more convenient for you?
2. If you’re a moron and use a weak pasphrase. Is your traffic that critical to dedicate a competent mathematician and one of their systems to it?
3. If the former goat herders and sheep gynecologists of al-Qaeda can figure it, we think you can too.

For the “conspiracy freaks”, when "big brother" and the "new world order" kick your front door down, then you'll say, "I should have practiced OPSEC!” Unless you’re conducting a psychological operation (PSYOP), you have no reason not to be practicing OPSEC.

ΨΩΨ

Motorola DTR Radios

by “T”

Editors Note: This review was given to us by a long-time friend of the 'zine. It was originally submitted to a very well-known communcations hobbyist magazine who rejected it, saying “The only thing hip about our readers is the type that involved replacement.”

The first warning I heard was Rambo asking Jimmy Dean “Want me to play 'Bubba Shot the Jukebox'?” Looking like a more worn version of Willie Nelson, Rambo is a feral, slightly unhinged Army veteran of both Vietnam and Desert Storm. He's really useful at getting broken equipment working again in the field, and when you need a bodyguard when visiting such entertaining locales as Hartford and Bridgeport. At any other time he's best kept out of sight of the customers. He was in a foul mood today as he was getting sued by the families of a group of Norwalk youths who thought he was a homeless person when they tried to assault him. The police dropped the charges as it was five against one and self-defense, even if three of them are still in a coma. He was just finishing up his lunch with a copy of Edward Abbey's The Monkey Wrench Gang, and listening to The Doors on his Ipod at a volume that would bring Jim Morrison back from the dead. Having been exposed to too many loud noises while serving his country, Rambo needs to crank his Ipod's volume up full bore despite having the earbuds jammed so far into his auditory canal that Jacques Couesteau couldn't find them. Jimmy, not being the brightest of bulbs, made the mistake of telling Rambo “Yea, that's a good song.” That's when I dived over the workbench, as Rambo was in the process of pulling his .45 out from his toolbox in an attempt to silence Jimmy's annoying noise source. Afraid that the round would overpenetrate the boombox and fly off to hit some innocent person or piece of test equipment, I knock Rambo off his chair, and wrestle the .45 out of his hands while he's cursing at me in Vietnamese.

It started out innocently enough and with the best of intentions (much like a Warren Zevon song). How was I know what started as a simple exercise in boredom-induced technological funkenspiel would

introduce me to the next quantum leap in portable personal communications systems. That's one of the more interesting things about this hobby. I was at the shop and had just been asked to stop harassing my co-worker Jimmy Dean. Jimmy likes both types of music, and therefore keeps his radio tuned to the local FM station that plays his particular genre of acoustical entertainment. Sometimes he likes to play his music at excessively high volume, and his co-workers are forced to defend themselves. In this instance, the implement of defensive destruction was an Ipod playing Cruxshadows and E Nomine hooked up to a service monitor. After several loud inquiries of "What the heck is that?!", the boss comes in and asks me to play nice. I actually was playing nice, as I made sure all the songs from The Mentors were not on my defensive playlist.

So I soon found myself on this slow day surfing Motorola's product website when I came across ***them***. I'm always keeping an eye out for neat exotic communications equipment at hamfests, and when I saw the Motorola DTR portables I thought to myself "I have to check these things out!". The DTR series are one watt license-free handhelds operating on the 902-928 MHz band along with other Part 15 and ISM devices. Unlike other license-free radio services such as FRS, MURS,and CB that operate on a single analog FM or AM frequency per channel, the DTR series use digital frequency hopping spread spectrum modulation (FHSS). This means they are less susceptible to interference, can't be received by police scanners, and have a longer communications range than analog single-frequency radios running a watt. Motorola in fact claimed a two-mile range with these units. FRS radio manufacturers claim a 2 mile range with their little half-watt 460 MHz handhelds, and anyone who has played with them knows that at best you get a half-mile to mile tops under most circumstances. How well would the DTR handhelds operate under a variety of circumstances? I would soon find out. After a few inquiries and a trip into the back storeroom, I soon found myself in possession of a pair of Motorola DTR650s. Jimmy went back to playing both of his favorite types of music. As I walk out into the shop floor, I hear someone with a Texas accent sing about the differences between divorces and horses, Jim Morrison telling everyone "This is the end. My only friend, the end." and Rambo asking Jimmy "Want me to play 'Bubba Shot the Jukebox'?"

Frequency hopping spread spectrum is nothing new. The military has been using it for years with their SINCGARS (Single Channel Ground/Air Radio System) radios. Instead of staying on one frequency when transmitting, the radio "hops" through a number of different frequencies in a pseudo-random sequence. This reduces the vulnerability of the communications to interference and interception. Frequency hopping is also used on the ISM bands such as 902-928 MHz for telemetry and control aka "SCADA" (Supervisory Control and Data Acquisition) systems. Many cordless phones operating in the 902-928 and 2.4 Ghz. bands also use FHSS. In the latter two instances it is used for spectrum efficiency as well as interference reduction. You may also find certain cutting-edge amateur radio operators experimenting with spread spectrum communications on UHF and microwave ham bands, and the ubiquitous 2.4 Ghz. Wifi systems use spread spectrum as well. While spread spectrum communications are commonplace in industrial, government, military, and wireless networking applications, until the release of the DTR series radios there simply was not a unit that offered spread-spectrum voice communications in an inexpensive license-free package.

These radios are comparatively priced with less expensive portable radios and give a significant measure of privacy over handhelds operating on a "dot" frequency. If you were putting together a new portable radio system from scratch, it would be worth your while to invest in DTR radios. From a management standpoint these radios have some neat features not found in similarly priced conventional portables that will enhance your communications system. These features will be addressed later in this article. These radios are license-free and truly plug and play. Their operation is uncomplicated. Scanning receivers cannot monitor them, and it is extremely unlikely that will change anytime soon. The DTR is an FRS radio on steroids, and just like FRS, MURS and CB does not require an FCC license. Until now there was really no way to inexpensively experiment with spread spectrum voice communications. A pair of DTR410s cost less than a digital trunk-tracking scanner.

Motorola makes three models of DTR radios for the US market. The basic entry-level Model is the DTR410. This features six "public talkgroups". For the purposes of keying-up and talking consider them the same as a channel on an FRS or CB radio. The other two are the DTR550 and DTR650. The DTR550 and DTR650 can operate in a private "unit-to-unit" mode, and the DTR650 can act as a supervisor radio

enabling the user to do remote monitoring and disabling of other DTR units. Other than these firmware differences, they are all the same 1 watt 900 MHz FHSS radio.

The first thing I absolutely had to do with these things is try a scanner on them. Ok, I used more than a scanner. To be more specific I used a Signal Stalker scanner, frequency counter, spectrum analyzer and old Optoelectronics R-10 Interceptor on them. I started with the Signal Stalker. This little $100 scannist's friend has since its appearance on the scene totally changed the way hobbyists look for frequencies. I turned it on, made sure the 800/900 MHz band was selected, and keyed up the DTR. Nothing. Nada. Zip. I then did a more traditional frequency search of 902-928 MHz I found a donut shop's drive-through, a couple baby monitors and some ham radio operators on a local 927 MHz repeater. No test transmission from the DTR though. Neat! Next in line was the Optoelectronics R-10 Interceptor. Finally I head something. Yes, this deceptively capable piece of intercept gear masquerading as an innocent piece of test equipment heard something! What did it hear? A popping "digital" sound that sounded nothing at all like audio. Not only is the DTR a frequency hopper, it also uses digital audio! After that test the frequency counter and spectrum analyzer results were anticlimactic. They confirmed what I already knew about the units. The frequency counter attempted to lock on the signal, but didn't have a quick enough gate time and just gave readings around 900 MHz The spectrum analyzer gave me a nice view of a FHSS signal.

One aspect of operation I noticed about the units was that they needed a fellow unit on the same "channel" in order to key up. Otherwise they give an error message when you attempt to key up. This is a neat feature as if the radio keys up you can generally be assured that at least one person you are talking to is within range. It also allows you to do solo communications range tests if you're lacking a fellow hobbyist to play with you. In this case, I had help from a number of friends with these units. First among them was Hank Frost. Hank is a fellow veteran with a similar interest in electronic communications who is my usual co-conspirator in playing with things technological. Hank is much like a technological spider sitting in a big electronic web (that is if you can imagine the spider looking like an Alaskan Brown Bear). Hank has the disturbingly cool ability of taking common consumer electronics equipment and modifying them into interesting pieces of what refers to as "test gear". It makes me wonder what he actually did in the Army, but when I ask him he just shrugs and says "Oh, this and that." After running the gauntlet of electronic security that separates his residence from the rest of the world, I present a DTR unit for his examination. He breaks out this piece of equipment that looked like it was put together from spare parts found in a TV shop. I ask him what it was and he replies "It was originally a satellite receiver." Further questions as to the "test equipment's" origin only elicit that it was originally from "a dude in Green Bay." After checking out the DTR for a few minutes, he hands it back to me and says "Nice for something off-the-shelf". I ask him if he wants to help evaluate it, and he replies "New Hampshire sounds good about now." The next Saturday, we're in a two-vehicle convoy heading up Interstate 91 on our way to Keene and parts beyond. This is a well-known route to us, being the way to get to the famous and now-defunct Hosstraders Hamfest that was held in Hopkinton, NH. Talking car to car, we were able to achieve about a two mile range between radios, thus living up to Motorola's claims about range. Bouncing around the towns of Southern New Hampshire, the units consistently gave us a range of about a mile to a mile and a half. Hiking in the region's mountainous terrain, that range went down to about a half to three-quarters of a mile.

After playing with them a while up North, I gave The Lone Gunmen a call. The Lone Gunmen are a group of three friends and fellow electronics hobbyists who share my interest in exotic communications equipment. We decide on the most RF-intense, interference-plagued, radio-unfriendly proving ground that's equidistant between the two of us: New York City. If they can perform *there*, they'll perform anywhere. With Frank Sinatra crooning in the Ipod I hop a train south and meet them at Grand Central Terminal. Soon were walking down Park Avenue looking for a suitable place to do a distance test. Motorola claimed an in-building range of 25 stories, and we wanted to see how they actually stacked up. There are few if any tall buildings in Manhattan you can just walk into and start ascending in order to do a radio test. We notice the tallest thing on the New York skyline, and figure "Why not?" I would have loved to take one of these up to the observation deck and attempted a 33cm band DX record, but the line to the observation deck was oppressively long and we were carrying way too much interesting shit on our persons to deal with a security checkpoint. We walk into the "office" entrance and look around. Despite being one of New York's premier tourist attractions, the Empire State Building has a more mundane function of being home to thousands of law offices, accounting firms, and other businesses. Langely asks me for one of the radios and

goes in. A few minutes later he keys up from the 25th floor with perfect audio quality. Then he keys up from the 30th floor with perfect audio quality. After the 51st floor the audio was getting "digitized" and unreadable. Impressed by the performance so far, we went on to have some fun. By this time it was getting close to 5 O'Clock, and it was first Friday.

For those of you who are unaware, a very well-known and infamous hacker magazine has held get-togethers on the first Friday of the month in New York City since 1987. The location is Citicorp Center on Lexington Ave. At this get together you get computer hobbyists of all stripes, including a contingent of radio ninja wannabes with dual-band ham handie-talkies that like to screw with the security guards. The last time The Lone Gunmen and I were there, we sported VHF Saber handhelds and ran DES-XL on 151.88 Mhz. The wannabe radio ninjas thought we were Feds as their Optoelectronics frequency counters could lock onto our signals, but all they heard was the open-squelch noise of an encrypted signal. We figured that tonight would be no different, and we were correct. We walked in with these radios on our hips, and the intrepid group of hamsters in training reach for their Signal Stalker police scanners. Their smug looks changed to that of utter confusion when they discovered that this time they couldn't lock on our signal. Brohike yells at them "Try a spectrum analyzer!", to which they reply "What's that?" Soon the word spread around the meeting that "The Feds are back!" Our mission of inducing paranoia completed, we proceed to sit down at a chair and loudly talk about our other favorite subjects: firearms and alcohol. And they all moved away from our table.

Why would you be interested in a proprietary frequency-hopping radio when there are other license-free radios available that cost less? From a hobbyist standpoint, these radios offer a very inexpensive means to play with practical spread-spectrum communications. Since these radios are still relatively new, experimenters have yet to work with them. Much like hobbyists have done with WiFi and other electronics gear, I expect to see a whole host of "mods" to become available for these excellent little radios. From the point of a group of individuals looking to implement a small portable radio system, the cost of these radios is the same as any medium-grade business band radio, but with the superlative quality that Motorola products are known for. Their use of FHSS provides a high-level of privacy than a handheld operating on a "dot" frequency, and the added features of the higher-end units offer better functionality for a small business. In a similar vein, the higher privacy level would be valuable for such users as CERT, search and rescue, and disaster response teams for relatively private communications when mobile phone service is unavailable for whatever reason. A few years ago, communications at this level would have been out of reach of most individuals and small businesses. The Motorola DTR series represents the next step on communications, and are a good value for a small group wanting some extra privacy and management ability for their communications or a hobbyist wishing to experiment with the new generation of wireless communications. If you fall into this category, the DTR series radios are highly recommended.

While scanner hobbyists may as expected decry the advent of such technology as the end of their voyeuristic hobby, the advantages of such technology as represented by the DTR series of radios outweigh such fatalistic rants. The communications hobby is a beautifully diverse pastime represented by intelligent and forward thinking individuals. Such individuals will see the DTR series of radios as having the potential to add new excitement to their hobby, and embrace it with open arms much the same way 802.11 wireless networking was embraced. Individuals and groups with a need for inexpensive private communications will likewise see the DTR radios as a useful tool for whatever their mission happens to be. As crowding becomes more of an issue on the RF bands, I expect to see more equipment utilizing spread spectrum communications. So no matter where you might be in the wide world of radio, I would recommend you take a look at these radios. They are the future.

ΨΩΨ

The Story of Johnny Hack

Part I

by Ticom

Johnny was a hacker, and there was no doubt about it. His parents bought the family a computer when he and his sister were in junior high school. His sister used it for schoolwork and chatting online with her friends, but really had no interest in it other than as a tool. Johnny was a different story, however. In short order he became proficient in writing his own web pages in HTML and then Javascript. After that he started tackling C++ and came to the realization that his parents' system was crippled as it was running Windows XP. He wanted a system of his own that he could run Linux on, especially since Johnny was getting into the dark side of computing. There were certain places in the grungy hidden corners of cyberspace where Johnny was known as "The Titanium Ferret", his handle inspired by Harry Harrison's Stainless Steel Rat sci-fi series. He would have called himself "The Stainless Steel Rat", but some guy during the 1970s and 1980s already used that handle and Johnny wanted something original and more modern-sounding. He also had a ferret and thought it was the coolest pet in existence. Johnny was particularly excited about this summer. He just turned 15 in February, and was now able to work at a real job. He cleaned tables, washed dishes, and cleaned floors at Goodfellas Pizzeria and Italian Restaurant. This not only meant more money to fund his hobby, but also a source for free pizza. Being a hacker, Johnny of course existed on pizza and Chinese food whenever possible. Johnny was pretty much a lone-wolf hacker. There were a couple online acquaintances he chatted about hobby stuff with, but he never met them in real life. The nearest 2600 meeting was about an hour's drive away. He went there, but he wasn't impressed with all the posers that strutted around, dressed like they just walked off the scene of some vampire movie and really didn't do anything interesting at all.

There was another "hacker" in his school, but he avoided him whenever possible. Dan had some "issues" and did way too many recreational chemicals for Johnny's comfort. Johnny was a notorious caffeine addict but that was for mental enhancement, not for turning his brain off. Dan was sitting in some institution after deputy sheriffs and federal agents paid his parents' house a visit one morning. Dan had found out about "wardialing" and proceeded to have his computer call every single number in his phone exchange over the course of a few days, apparently not aware of or caring about this thing called "Caller ID". He also had a habit of shoulder-surfing the payphone down at the local gas station/convenience store and jotting down people's calling card numbers so he could talk all night to girls he met online without it showing up on his parents' phone bill. When the cops raided Dan they not only took his computer, but also his stash of weed. Fortunately the judge was a compassionate sort and dropped the charges if Dan got treatment for his issues. That meant being locked up in a private hospital for the children of parents with money, and taking society-approved chemicals that did the same thing as the weed he smoked until some doctor thought he had enough "treatment".

Johnny being a smart young man wanted to avoid those hassles and therefore not only stayed away individuals who already had them, but also didn't do anything sketchy on a phone line traceable to him. This imperative of avoiding phone lines traceable to him was at the forefront of his mind lately as he was beginning to get into the realm of phone hacking or "phreaking". "Phone phreaks" were hackers who specialized in the Phone Company. With a steady income now at his disposal, he would now be able to implement certain techniques to enable him to safely phreak with minimal risk. Today was Johnny's day off. He just received his paycheck and cashed it. It was now time to take the bus down to "the strip", the place in any town where all the retail establishments were, and do a little shopping. Over the past few months of saving up his cash, Johnny had assembled a list of items he'd need to safely engage in this new aspect of his hobby. Now it was time for The Titanium Ferret to implement his plan. His first stop was the local Goodwill. After a couple minutes rummaging through the electronics section he found a fairly recent model 900 MHZ. cordless phone that used a 12V wall-wart transformer for its base unit for $5.00, an old one-piece corded phone for a dollar and an old VHS camcorder for $20. His next

stop was at Radio Shack where he picked up a package of .01 uMfd capacitors, alligator clips, a miniature slide switch, and a 12v gel-cell battery. After Radio Shack he went down to the local hardware store where he picked up cut-off wheels and other assorted bits for the Dremel Tool he received last Christmas, and a can of dark green spray paint.

When Johnny got home later that afternoon, he first tried the camcorder. It worked fine except for the tape drive mechanism. This was no problem. He'll be going to Wal-Mart with his parents later and get the rest of the parts he would need. He then looked at the cordless phone. The battery on the handset was hosed, but he was expecting that. It was a fairly recent model so he should be able to get a replacement battery for it. He then disassembled the base unit and took the case outside with his can of Krylon. Five minutes later the white base unit was now a nice dark green. While it dried he took a look at the one-piece phone. He took it apart and set aside the electronics of the phone. Using his Dremel Tool and recently purchased cutting wheel he cut a notch out of the side of the phone's case to fit a small toggle switch. He then took a look at the electronics. Breaking out his soldering iron (a recent birthday present), he de-soldered the green wire going from the phone cord to the circuit board. He then soldered the switch in series with the green wire and a .01 uFd capacitor across the switch contacts. Satisfied with his work, he then put the one-piece phone back together, fitting the switch in the notch he cut previously. Looking at the modular cord again, he cut the plug off with his Leatherman Tool's wire cutters and soldered two alligator clips in its place on the red and green wires. He now had a functional equivalent of a lineman's "butt set". He'll buy a nice Harris Dracon when he has the cash to do so, but for now this will work. Going under his desk, he unscrews the cover from the modular phone jack, makes sure the switch is set to "off" or "monitor", and clips in. Sure enough his sister is on the phone talking with a friend, he blows into the microphone and is satisfied to note that she can't hear him, flipping the switch to "on" or "talk", his sister hears the click and yells "I'm on the phone!" Johnny replies with a quick "Sorry." and goes back to monitor mode. After listening to about 15 seconds of his sister talking about whom likes whom at their school he becomes bored and disconnects.

By this time it was getting close to dinner and the paint had dried on his cordless phone case. He brought the case inside, and ate dinner with his family. After dinner, his parents asked him if he wanted to go to Wal-Mart with them. After telling them yes he went upstairs grabbed his jacket, and before leaving jotted down the make and model number of the cordless phone and its battery in his "hacking notepad" that he buys at the dollar store a couple blocks from his school. Once at Wal-Mart he goes over to the home electronics section and notes with satisfaction that the battery for his phone is still available. He picks one up, a 50-foot roll of dark Grey telephone phone wire, and a video patch cord. Going over to the automotive section where he finds his dad (after discretely caching his acquisitions), he notices with delight that Wal-Mart sells some nice alligator clips at a half-dozen for a buck. Much cheaper than Rat Shack. Going a couple aisles over to the sporting good section he finds this really neat Rayovac headlamp with red LEDs. He remembered reading in a hacking magazine called Ethertech about how red flashlights are better for night use because they don't mess with your night vision and aren't as visible at a distance. While his parents were still shopping, he paid for his items and took them out to the family's minivan where he stuffed them under a seat; opening the vehicle with an "extra" key he had made from the spare his parents kept on the mud room key rack for emergencies.

With everything together, Johnny needed a phone line that wasn't traceable to him. He also needed to make sure that his number scanning wouldn't raise too many flags. After Christmas last year, Johnny took the gift money he received from relatives and visited some pawnshops that specialized in electronics looking for a police scanner. A lot of people were offloading their old scanners because the local sheriffs department went to a digital radio system. After checking out a few, he found a Radio Shack PRO-2006. The PRO-2006 was the classic scanner for the serious hobbyist during the 1990s. It could be modified for full 800 MHz. coverage to receive the old AMPS cellular phone band, and there were several modifications available to enhance its performance. Sure enough the unit was already "modded" by the scanner dweeb (or one of his technically competent friends) who owned it previously. Johnny needed a better

antenna that would work over a wide frequency range, so he went to Radio Shack and picked up a Discone antenna. He cable-tied the antenna to a scrap piece of 1 1/2" wood dowel he found in the basement, and then cable tied the dowel to the bedpost closest to the window. Tuning from 902 MHz. to 928 MHz. he hears a couple baby monitors, some ham operators on a repeater around 927 MHz., and a few cordless phones. He'd like to put the antenna on the roof and his parents probably wouldn't mind, but that would be advertising something he didn't want known.

Johnny's parents had upgraded the family's entertainment center and replaced the old VCR with a DVD player. Instead of letting the old VCR get thrown out, Johnny instead kept it thinking he could use it in a project. Now it was time. Johnny was at school or work during the day and could not keep an eye out for phone company repair activity during that time. He thought that by putting surveillance on the b-box outside his house he might catch a lineman dialing in certain test numbers. Johnny set the camcorder on a table in front of the window, hooked it up to the VCR, and aimed it down at the b-box with the zoom at its highest setting. Later on that evening, he went out to the b-box and wedged a used match in the corner of the b-box's door to show when it was opened. When he left in the morning he hit "record" on the VCR with the record speed set to its slowest setting. A few days later he noticed the match he wedged into the door was missing. Checking the day's video coverage, an hour into the recording there was a technician at the box. Watching the video, he notices the technician dial a number: 234-9970. The next day before going into work, Johnny tries the number at a payphone. A male voice answers with the name of the town his central office is located in. "Is Susan there?" Johnny asks. "I think you got the wrong number" the voice replies. Johnny says "Sorry." "No problem." The voice says before disconnecting. From reading various old phone phreak text files, Johnny knew that phone companies often used the 99NN range in an exchange for test numbers. His area apparently followed that guideline. Now all he needed was an untraceable phone line.

Over the course of a few weeks, Johnny had identified a likely prospect. There was a retired couple who lived a couple blocks down the road. They still owned an analog 900 MHz. cordless phone and never seemed to hit the "channel" button. They had relatives across the country, and liked to go on frequent trips to visit them. Johnny guessed that they would be useful for what he had in mind. Their frequent long distance calls indicated they probably had a flat rate phone service plan, and it would be an easy enough to find out. Due to his sister's frequent phone use calling her friends his parents had a flat rate service and he knew how much it cost. When the next phone bill came in, he'd be ready. When he saw his parents' phone bill come in, he watched the elderly couple's mailbox. On the same day the husband went out that afternoon, placed some envelopes in the mailbox, and lifted the flag. Later on that evening, Johnny went out to the mailbox with a can of electronic cleaning spray. The chemical in the spray turns envelopes transparent and then dries without leaving a trace. Looking at the bill through the envelope, he noticed that their phone bill was the same flat rate amount as his parents. Johnny had his PRO-2006 scanner attached to a VOX tape recorder and tuned to the frequency of his target. His surveillance informed him that around Labor Day they would be going on a trip out of state to visit some relatives for three weeks. Their subscription to a flat rate service plan would ensure there would be no anomalies on their phone bill.

Johnny had cut the wall-wart off the cordless phone's power cord and replaced it with a 12V gel-cell battery. That should power the phone for a few days. Placing the base unit on the back porch, Johnny walked down the block to the neighbor's driveway and turned on the handset. He was out of range. He'd need to use an antenna with higher gain. Surfing the Net that evening, he found a few sites selling yagi and log periodic antennas for extending the range of wireless LANS. After finding who had the lowest price, he ordered a 900-2600 MHz. PCB log periodic antenna. After this project he was sure he'd find some other purpose for it. In the meantime, he needed to do some research. While his initial focus was going to be on local Telco test numbers, if his first limited endeavor in number scanning worked out he was going to scan the exchange for interesting numbers. Unlike his institutionalized acquaintance however, he was going to do it in a more intelligent manner. Johnny was already implementing one means of anonymous dialing with his modified cordless phone. More technical means will have to be developed so he won't be

limited to phone lines in his immediate neighborhood, but that will wait for now. As Johnny observed, straight-out sequential dialing of every phone number in an exchange was very noticeable and attracted unwanted attention. It was also very efficient. The dialed number sequence would have to be at random and residential lines could be ignored, as they would probably not have anything of interest on them. Johnny acquired a phone directory CD program from the local consumer electronics retailer. He had to do some research, but he discovered which brand would be the easiest to export data into a "do not call" list. He would use the residential listings for that. He would also be able to search addresses of industrial and business parks for potentially interesting targets, and make an educated guess as to what number ranges he should scan for them. Businesses are often assigned numbers in sequential blocks by the phone company, and by knowing the main number one can make an educated guess as to where to scan for a business' more interesting numbers.

While waiting for antenna to come in, Johnny did a little more research. While he could get anything he wanted via mail order, he would rather find local sources beyond Goodwill and Radio Shack he could visit and pay for things with cash. Cash is untraceable, and he would be yet another anonymous face among hundreds visiting a business during the course of a day. He could browse aisles and perhaps discover something he was previously unaware of that he could use in the pursuit of his hobby. Buying local would also reduce the number of packages arriving at his house, and keep his parents from getting suspicious. He found what appeared to be a well-stocked electronics supply house in a city about an hour away. There was a commuter train line that went there. On his next day off he'd go take a trip, but he'd want to do some more research to see what other opportunities awaited him in the big city. The city was the same one that had a 2600 Meeting, so maybe he'd take a Friday off to see if the situation there had changed any. His last visit to the 2600 meeting left him unimpressed, but that was a little over a year ago and things might be better this time around. In the meantime, he'd probably have to find another source of income, or a better job. The hobby was getting more expensive as he went further into things. While his boss at the pizza place was very good to him, he was going to check some of the local computer stores to see if he could find something that paid more.

Johnny visited his local computer stores, but didn't have any luck. They were either single proprietor establishments that weren't looking for any help, only hired people over 18, or were looking for someone with "certifications". He'd have to look into getting some IT industry certifications if he wanted that particular career route, but for now it looked like the possibility of a 15 year-old working in a computer shop was slim to non-existent. He went into work this afternoon, and his boss was complaining about the brand-name PC they bought. It was having problems. All they kept getting when they called the help line was someone from Pakistan telling them in broken English to "reinstall Windows", and how it would cost $75 an hour for a technician to come out and look at the computer with a one-hour minimum charge. Johnny's boss came to him in desperation and said "Johnny, you're into computers. Do you think you can fix this fucking thing?" About 15 minutes later, Johnny had the machine working. When he left, Johnny's boss slipped him a $50 bill along with a hearty "Thank you. You saved me a lot of hassle and money." His boss also asked him if he could move the phone line for the credit card machine. When Johnny said he could, his boss told him he'd no longer be cleaning up and bussing tables all the time and he'd be getting a raise.

ΨΩΨ