

CYBERTECH

Technological Survival Newsletter
10th. Anniversary Issue, Spring, 2000
P.O. Box 641, Marion, CT 06444

"It was 20 years ago today...." - The Beatles

It really was 10 years ago, but nevertheless, on the first weekend of January, 1990 a zine called Cybertek was conceived. Two months later, with the help of Necross Sinister (Sin), The Omega Man, a TRS-80 Model II computer provided by The Datamaster, and a 9-pin dot matrix printer the first issue of Cybertek: The Cyberpunk Technical Journal was released for public consumption. We had something like 10 subscribers, and a few copies on the rack of Malcolm Tent's store Trash American Style (a/k/a "Trash" in Danbury, Connecticut). Cybertek has been gone for 2 years now, and the realization of this weekend's significance hit me

when I was driving down to Trash to visit Malcolm and see what new stuff they had. This has caused me to look back over the past decade to see how far things have come since we first started spreading the message of freedom through technological knowledge. The end result of this rumination was the release of a special 10th Anniversary issue of Cybertech. We had to change the spelling due to trademark conflicts with a company in Texas who'd been using it as a trademark since 1974. It took them 8 years to notice, by the way. Whether it's spelled with a "ch" or a "k", it's still the same Cyberpunk Technical Journal! In the tradition of the original issues we've included not only high-tech

(Continued on page 2)

Data Transmission Techniques: Hardware

by Ticom

Every good techie should keep a few different types of ICs on hand to take care of common applications they might encounter. Devices such as 555 Timers and 741 Op-Amps always quickly find a use in the shop. If you, at some point, need to establish a telemetry or other data link, you will want to keep on hand MAX-232, XR-2206, and XR-2211 ICs. Consider these devices a staple for any techie's hardware stock. The MAX-232 is an RS-232 to TTL level converter. Many serial interface devices such as PICs, microcontrollers, and data communications ICs use TTL (5V) level voltages in their serial communications lines. In some instances this causes difficulty when talking to a computer's RS-232 (+- 12V) serial port. The MAX-232 converts the voltage levels back and forth to the proper levels each device needs to communicate with. You will need a MAX-232 to have an RS-232 port communicate with the XR-2211 and XR-2206 ICs. You can get the full specs on the MX-232 off of

Maxim's Web Site. The XR-2211 and XR-2206 are AFSK deodulator and modulator ICs respectively. They are the heart of many ham radio AX.25 packet radio TNCs (Terminal Node Controller: a radio modem). Full specs on these ICs are available at Exar's Web Site.

Phone Sources

For phone line communications I always keep a couple old modems handy. Hayes compatible 2400 baud (and slower) modems are found at hamfests for \$5 or less if you can't find someone throwing them away. You can use them as straight autodialers with DTMF signaling to call a pager for status/condition reports, or you can have them dial a remote computer system to report. With some of the more advanced microcontrollers you can program a simple script to dial into an ISP shell account, telnet to a remote system, and leave a status message. You could also just simply email one to you if real-time reporting is not required. Old modems also have a wealth of interesting parts for experimentation; typically a power supply, telecom

(Continued on page 2)

Cybertech 10th Anniv. Issue

(Continued from page 1)

articles, but also low-tech survivalist-type ones as well.

The first big thing has been the sheer increase in computing power available to the average person. Cybertek was born on a 64K Z80 computer with 8" floppy drives. That was replaced quickly by an AT&T PC6300 with 640K and 8086 CPU that cost us \$500 (in 1990 currency) used from the local computer store. The second was The Internet. Back in 1990 you had Bulletin Board Systems (BBSes). Some were connected together by a message and email network called "Fidonet", but it didn't have the real-time connectivity and bandwidth available today. A 9600 baud modem was considered state of the art. The libertarian possibilities as a result of this technological explosion are incredible! The average individual now has the capability for cryptography, desktop publishing, and inexpensive, almost instant, multimedia communications across the globe. What was once the domain of large establishment entities is now within the reach of the average person. This is a beautiful thing, as it enables people to have secure communications amongst each other, and to become their

own media outlet. Unfortunately, it is estimated that only 25-40% of American households are on The Internet.

I feel the number one priority of technological enthusiasts and Libertarians should be to get computers and Internet service into more homes, so as to more effectively bypass traditional establishment media outlets and bring our message to more people. Many individuals are disgusted with the whole two-party system in this country, but due to establishment media censorship are unaware that alternatives exist. Consequently, they drop out of the political process and give the Republicrats and Demopublicians more strength. Remember that our last "president" won the election with 24.75% of the popular vote. If half of the 55% who decided not to vote instead voted Libertarian, we could quite possibly have had a third-party candidate in The White House! A presidential election is coming up this year. You can be rest assured that the third-party alternative will be ignored and/or misrepresented by the mass media. We have the technology to deal with them, and make sure the truth gets out. We should endeavor to do so.

(Continued from page 1)

interface ICs (more on those in a later article), RS-232 to TTL level converters, and other datacomm-related stuff.

You should try to add as many old modem manuals to your documentation collection as possible. Some of them are very educational and even contain schematics. The old Hayes Smartmodem 1200 manuals had a section detailing how to hook up the modem to a transceiver for ham radio use. There were different brands of "smart" modems, such as Digital and Ven-Tel, that didn't use the Hayes command set, but the manuals give full details on how they work. Non-Hayes compatible modems are dirt cheap at flea-markets and ham-fests, since people don't know how they work. Back in the days when BBSes were not only common, but 200 baud, I used a Ven-Tel 212 smartmodem for BBSing. The Ven-Tel provided you with a menu of options when you communicated with it, and was really user-friendly. It also, unlike the Hayes, had an auto-redial feature built into the modem. Alas, one day it died from an electrical

surge through the phone line, and I replaced it with what was the best non-Hayes modem in existence; the Western Electric/AT&T Dataphone 1200. This modem was dumb. You had to rig an interface adapter to the DB-25 connector on the back that hooked up to the phone set you were told was needed to use the modem. The modem was so dumb it would work with anything: Atari, Apple, Commodore, IBM PC, TRS-80, or even a VT-100 terminal. Considering the compatibility problems with some of the systems and "Hayes compatible" modems of the times, this was a godsend. It also had the most sensitive carrier detect, loudest carrier tone, and best noise resistance of any modem I've worked with. In the 80s when the quality of local loops and analog trunks often sucked, this modem communicated. Why, in this day of 56K modems, should you keep such an antique? It's auto-answer, and it works when nothing else will. 1200 baud is adequate for modeming in a command line or shell environment, and the Dataphone will run forever without problems. I've seen Dataphones still working after 15 years of continuous, 24/7 use. Set one

(Continued on page 3)

(Continued from page 2)

up for a low speed dial-in telemetry application in an area where the phone lines suck, and you'll have no problems communicating. Even in some not-so-remote areas, you might have phone line problems. If you've ever lived in Auburndale, MA you'd know what I am talking about.

Wireless

The best way to get good cheap wireless equipment for data commo is to subscribe to Nuts & Volts, and attend hamfests. Wireless equipment is expensive when purchased new, but sells for pennies on the dollar when you buy it used or surplus. Those of you who would like to use packet radio for your link can acquire a used transceiver and a TNC (radio modem) starting at about \$100 for the pair at a hamfest; if you do a little looking around. There is one company which you will find interesting. Abacom sells wireless RS-232 transceivers, with modules starting at \$25, and complete transceivers starting at \$140. Transfer rates peak at 40Kbps, and range is about 640 feet. You will also want to keep a couple Ming RF Transmitter and Receiver modules from Digikey. The transmitter is part # TX-99V3-ND, and the receiver is RE-99V3-ND. They only run at 1200 baud, but cost \$10 apiece. There was an excellent article in the May 1998 Nuts & Volts entitled "Naked Data", by Ryan Sheldon that went into excellent detail on the Mng units.

Sources:

Maxim - <http://www.maxim-ic.com/>

Exar - <http://www.exar.com/>

Abacom Technologies
67 Hamptonbrook Dr.
Weston, ON M9P 1A2
Canada
416-242-3120

Digikey - <http://www.digikey.com/>
1-800-DIGI-KEY

Survival Barter Items

by Douglas P. Bell

Many people are looking for a way to make a living "after the day" and barter looks like the only way it is going to be done for quite some time. This is nothing new of course, barter goes on all the time now and has been around since there were two or more people. But what would make a good survival barter item? Everyone has their own ideas about that, but many don't make much sense when looked at rationally. First off the "gold bugs" tell you gold will be KING. When you ask why, they really can't back up why except to say that it will. While there is a government that will back gold, or an industry that needs it, gold will do all right, but in a survival situation where you are looking for your next meal and there is no government or industry, gold will be just another shiny, soft metal and is fairly easy to make. The same goes for silver and jewels too, with no practical use and without a government or industry to use them, there will be no demand and fake "silver" or "precious" stones, which are easy to ake, will be rampant.

The other item that most people or books recommend for survival barter are guns and ammunition. The reason for this is simple, all through history and all over the world, fine weapons have been in demand. In any bad times, guns and ammunition will be literally worth their weight in gold. Don't believe it? If you have all the gold, and I have all the guns, in short order I'll have both and there is nothing you could do to stop me. However that is exactly the problem many people see with guns and ammunition, the chance that they might be used against the seller or to terrorize the countryside. This is a valid point too, so instead of high powered rifles, you might look at such items as inexpensive .22 rifles and .22 ammunition or gun parts such as springs and magazines (clips). Cleaning gear would be (and is now) like money in the bank, it being a safe bet that cleaning rods, rod tips, bore solvent, gun oils, patches, etc. will be in great demand.

Along these lines would also be reloading gear. Obviously powder and primers will top the list. A set of reloading dies in the ten most popular calibers along with the various military calibers

(Continued on page 4)

Cybertech 10th Anniv. Issue

(Continued from page 3)

would also be a good survival investment so as to be able to trade loaded ammunition for other goods, or to be able to use any firearms that you trade for. Always get carbide dies where available, especially in straight-walled pistol cartridges. as they last much longer and normally don't need the case to be lubed when resized. While the exact top ten cartridges might change from year to year due to a new cartridge coming out and making the top ten that year, most years include the following: .38 Spec./357 Mag. (use the .38 Spec. dies for both), .308, .30-06, .223, .30-30, .270 Win., .45 ACP, .243 Win., .44 Spec./44 Mag. (use the .44 Spec. dies for both), 9mm, etc. The .30 M1 Carbine, .380 ACP, .45 Colt, all make the top 20 each year as well, so it might be a good idea to include them as well. The military cartridge would include the 7.62x39 Russian Short, 7.62x54 Russian Rimmed, .303 British, 8mm Mauser, 7mm Mauser, 7.65 Mauser, 7.35 Carcano, 7.5x54 MAS, 7.7 Jap, and the various 6.5s like the Jap, Swedish, Carcano, and Mann. Schoenauer. Other reloading gear would include reloading die lubricant to lubricate the cartridge cases before reloading so they don't stick in the reloading dies, spare decapping pins in case you break them, bullet lubricants for cast bullets, shell holder kits, and possibly bullet casting equipment such as molds for the calibers you reload for. Inexpensive single stage reloading presses, such as the Lee or Lyman presses would also be in demand and are cheap enough to buy several without busting the bank. Don't forget the priming tool attachments that go on the presses either. Hand held priming tools are very handy as well.

Next on the list is food, or more generally seeds. This is a good idea, but too many people seem to think all they have to do is go to the local garden store and buy some seeds, put them away and that is that. Well the problem is the seeds you normally buy are hybrids that will not bred true. That is they will be OK for the first year, but after that they will not be like what was planted or hoped for. What you need is the standard non-hybrid plant or seeds and to keep the seeds from each year's planting so you can grow more next year. Also keep enough seed back so if you have a crop failure you can either replant if early enough in the season or have enough to plant the following year.

Other food items that are currently fairly

cheap and will keep literally forever include salt, pepper, honey, sugar, flour, baking powder, baking soda, powdered milk, and the various spices. Dried fruits, fruit leathers, and the like will also keep for more years than you are likely to need them. Grains or other dried seeds such as corn, wheat, rice, beans, peas, etc. will last for centuries if properly stored. Coffee, tea, and cocoa, if kept sealed, should last quite a while as well. The various high grade liqueurs should also be in demand, but rot-gut is rot-gut no matter how long it has been bottled and can be made at home fairly easily so it probably won't be worth much then either.

While at least one "survivalist" had pinned all their hopes on being the Survival Soap King, soap will only be a short term investment while things are up in the air and then everyone will be making their own out of lye (wood ashes) and animal fat (grease). Other than that soap might be a good specialty item in such items especially gentle/baby soap, shampoo, or scented soaps and shampoos.

A quick look around will point out a number of items that are used every day, but most are not even made in this country, or can't be made without some sort of industry. These items are such simple items as safety pins, sewing needles (not made in the US anymore), thread, pencils, pens, hand tools, etc. To expand on the hand tool list, just about anything needed to rebuild, such as axes, shovels, picks, hammers, files, pliers, locking pliers (a/k/a Vice-Grips), screwdrivers, jewelers screwdrivers for those who wear glasses, tap and die sets, drills, drill bits, and saws would be in great demand.

Medical items such as scissors, gauze bandages, adhesive tape, petroleum jelly, tweezers, syringes, needles, catheters, elastic bandages, snake bite kits, rubber gloves, burn or other salves, etc. will also be in great demand. Don't forget the teeth either, and get toothbrushes and toothpaste. get some Oil of Cloves and Zinc Oxide to make temporary fillings, or better yet, Intermediate Restorative Material (IRM) for longer lasting fillings. For pulling teeth, you will need a probe, elevator, upper universal forceps, and Lower bicuspid forceps if you would like to be the "Painless Pete" in your area.

Basic Phone Security - Making and Breaking It

By: Mob Boss <mafia_man777@ureach.com>

The other day I was sitting in class and I was bored out of my head so I picked up a dictionary. I was curious to see how a hacker was defined, considering that seems to be one of the most passionately fought arguments, good against evil, hackers against crackers. I found the definition to be "A computer enthusiast, someone who breaks into computers". Not surprising but when I went to look for "Phreak" and "Phone Phreak", low and behold, it was not there. This seems to be common these days. Everyone is shaking in their boots about big, bad, evil hackers and what might happen to their home or business computer, but no one ever stops to think about the phone system. This article is not geared towards anyone specific, in fact this is just an abstract to guide all those who are interested in general security, privacy, and H/P. Whether your a small business owner, a homemaker, or an executive, there is something here that you should know, if you don't already.

Phone Phreaking can be loosely defined as the exploration and exploitation of the phone system and everything that goes along with it. Back in the 60's and 70's there was blue boxing, back in the eighties and early nineties there was red boxing, but nothing compares to the things that are here now, in the early part of the 21st century. Seems everything is hooked up to the phone system one way or another these days.

People are sporting voicemail, pagers, cell phones, home answering machines, fax machines, computers hooked up to the internet, cell phones hooked up to the internet, and there are plans to have cars on the internet pretty soon as well, (i.e. 2600 issue 16:4, I OWN YOUR CAR).

1984 is here, just a little late .

Now considering all that why would someone ignore learning about the phone system considering the whole backbone of telecommunications is the phone system. That's a mistake a lot of companies and individuals make. Besides theft of phone service, as there are so many legal ways to make a free call these days, but how about privacy. How

would you like someone monitoring your business via the voicemail system or maybe monitoring your house by using the remote access feature on your answering machine to actually listen in on what's going on. How about someone tapping your analog cell phone or old cordless phone?

Now from the attackers point of view, what better way to watch a target?

You want to break into a computer network, monitor the voicemail systems for possible technical information and logins. You want to break into a house, listen to messages on the answering machine to find out the patterns of those who reside there. Want to blackmail, extort, and steal, well then there are tons of possibilities for you.

Lets start at home. What communication devices do you own? Cordless phone, PC, Fax machine, answering machine? I'm willing to bet you have at least one or all of those items in your home. First I will touch on answering machines, personally I could live without it. Most people hate talking on answering machines , and when its not meant to be its not meant to be. But I still own one and the first thing I did when I learned about breaking into answering machines was to check my manual to see if my machine had remote access. As it turned out, it did have remote access but lucky for me it has a strong security policy, two bad tries will boot you off, plus the code is a good one. Now machines I have encountered in businesses and homes were as easy as dialing 123 after the tone.

So what you say? You have nothing to hide? Well privacy is privacy and either way I don't want some thug hearing when I'll be at the dentist or vacation. This is twice as bad if you're a business and you have customers leave orders on the phone after hours. Credit card fraud has been booming since the 1980's and two decades later its still a problem, and its a safe bet that it always will be a problem. Here is an easy to follow system for getting into an answering machine, out of the many techniques I have read, tried, or heard of this one is the most rewarding...

after the tone start dialing this sequence,

(Continued on page 6)

Cybertech 10th Anniv. Issue

(Continued from page 5)

9876543210000123456789 then 2000, 3000, till you hit 9000, then 1111, 2222, and so on till you hit 9999.

21	46.770	49.830
22	46.830	49.890
23	46.870	49.930
24	46.930	49.990
25	46.970	49.970

That technique will break into answering machines in the homes of government officials, mail order stores, and places that should be more secure. Try that on your machine or a friends (with his permission of course) and see how secure that answering machine really is.

Obviously you want to listen into the base frequencies so that you hear both sides of the conversation. Now you may say well I don't have an old phone, "I have a brand new cordless phone that runs on the 900mhz band and scrambles the conversation".

Another problem that has been around for many years is that of people tapping cordless phones with simple frequency scanners. Now this problem has been dying out but when I flip on the Ol' Bearcat I still hear morons yacking away on there old, ten dollar, garage sale, cordless phones.

The only thing I have to say to that is, what if your business partner, mistress, and/or accomplice are using a old cordless phone, then your security measures mean nothing and its out there. That's why you have to analyze security from afar, missing the big picture will really screw you up.

These aren't wholesome conversations either. Drug deals, phone sex, and fights. I guess it all depends on where you live but just the same there are a lot of possibilities here. Like I said, this is not a new problem, but its still wide spread even though a whole decade of cordless terror has gone by.

Are you running a dialup server at your residence or small business? If you think its safe because no one but you had the dialup then you my friend are dead wrong. For years people have been using programs called war dialers (i.e. ToneLoc) to scan exchanges looking for computers and just because times have changed and the internet seems to dominate all doesn't mean that people have stopped looking to their local exchanges either. In fact much can still be found by having a war dialer go for a few hours and attackers know this. A company can have a big fancy firewall but a dialup sticking out like a sore thumb a few numbers up from their main switchboard number. That kind of ignorance can be very, very costly and it would be wise to see how your computers are set up. If a dialup server is necessary be sure to pick strong passwords and keep up with a good policy for protecting that data, physically and remotely.

By programming the following frequencies into your scanner you'll here many conversations:

	Base	Handset
1	43.720	48.760
2	43.740	48.840
3	43.820	48.860
4	43.840	48.920
5	43.920	49.000
6	43.960	49.080
7	44.120	49.100
8	44.160	49.160
9	44.180	49.200
10	44.200	49.240
11	44.320	49.280
12	44.360	49.360
13	44.400	49.400
14	44.460	49.480
15	44.480	49.500
16	46.610	49.670
17	46.630	49.845
18	46.670	49.860
19	46.710	49.770
20	46.730	49.875

Lets move on to your small (or large) business.

Most businesses worth anything at least have a small PBX and voicemail system, plus the kind of stuff you may have at home, as all the same of rules of home security apply at the office as well. Its very important that a person takes his sweet time with setting up the phone system, baby it just as much you would the computer network because leaving the phone system open will lead the path to your precious network.

(Continued on page 8)

Injun Jessie's Notes: "Random Ideas"

by Injun Jessie

This article is made up of random thoughts and ideas on living outside the system; full or part time. We all need some way to keep ourselves and our loved ones fed and sheltered in a way that the predatory parasites of the self-serving gangster government can't steal from us. Everything discussed here will be low cost (or no cost), easily made or procured, and off the books. Before you turn up your nose at my plans for gear made from recycled junk, stop to think:

Does it perform the same function as the expensive article?

Who's gonna see it anyway?

How much will I save and how much more gear will I have?

I try to remember how as kids my buddies and I used to build almost anything from material scrounged and adapted from scrap and nature, and how in the '60s we furnished our apartments with tables made from old cable spools and bookshelves made from milk crates or cinderblocks and scrap boards.

The true survivalist is not a purist. You know the type, "It's gotta be authentic Special Forces Issue... It's gotta be authentic mountain man era gear... Ya gotta make it with stone tools and yer bare hands... Etc." Use any and everything available!!!

Basics

Here is a checklist for putting together a kit:

Necessities - These you can't do without!

1. Good boots such as hiking or combat boots - The majority of your outdoor transportation will be your feet. Dependable footwear is essential.
2. A good knife - 6" blade bowie type of good quality.
- 1 The rest of the kit you can tailor to your needs. Here are some suggestions:

1. Earth tone clothing to match season and terrain. Keep to minimum.
2. Insect Repellent. My formula: 1 part rose geranium oil, 1 part eucalyptus oil, 3 parts citronella oil. Blend into cheap sunblock or mix with water in a spray bottle. (If mixed with water shake well before using.) Excellent against wood ticks.
3. Slingshot and ammo
4. Multi-Tool (Such as a Leatherman or clone)
5. Machete
6. Folding saw
7. 10'x10' tarp (Exact size unimportant. Can substitute construction plastic.)
8. Trash bags and ziplock bags.
9. Carpenter's cord
10. Power Shears (Those scissors that cut pennies in half.)
11. Tomahawk
12. Packs to carry/store everything - When living out of car, boat or camp I have found it convenient to store everything in backpacks.
13. Canteens (Make them from plastic soda bottles.)
14. Entrenching tool

Desert Canteen

An excellent desert canteen can be made from recycled materials.

Materials list:

1. Plastic 2 liter soda bottle
2. Cap from bottle of dishwashing liquid
3. Old bluejean leg.
4. Old blanket, towel or other heavy cloth scraps

Procedure:

1. Wrap several layers of cloth tightly around bottle. Sew in place.
2. Turn bluejean leg inside-out. Sew one end shut.
3. Slide bottle into leg. Adjust for fit. Sew side of leg to tight fit.
4. Remove bottle. Turn leg rightside-out. Put bottle back in.
5. Sew tight around shoulder of bottle.

(Continued on page 8)

Cybertech 10th Anniv. Issue

(Continued from page 7)

6. Thread on cap.
7. Tie thong around neck of bottle.

This canteen will keep water cold by evaporation when outer wrapping is soaked and canteen is hung in shade.

Slingshot

The slingshot is a very versatile and inexpensive weapon. With it you can hunt small game with shot or arrows, bow fish, launch a fishing weight with a line attached over a tree limb to haul up a heavier climbing line, or use it as a silent combat weapon. Slingshots are perfect companions to black powder firearms, using the same lead balls for ammo. It is much easier to adapt a slingshot to fire arrows (by adding an arrow rest if necessary) than it is to make a primitive bow. It is also much easier to carry (in your hip pocket) than a bow. To make an arrow rest, cut a "V" in the end of a strip of cardboard, sheet metal, or plastic and tape it to your slingshot so the "V" is level between the power bands. A permanent rest can be made from coathanger wire and attached. Marbles, pistol balls, fishing sinkers, arrows (primitive or modern), ball bearings, or even pebbles can be used for ammo.

I have an old Whammo slingshot which I converted to a sling bow. I don't know if they still make these, but they came with a detachable arrow rest. The only problem was that they were made with low power flat bands. (Easily replaced with modern tubing.) These antiques were wood, crude, and clunky, but are excellent candidates for sling bows if you can find one.

Chinese Crossbow

You've seen them everywhere: gun shows, flea markets, mail order catalogs. There's just no way about it. I had to try one of them Chinese pistol crossbows. At 45 lb. prod weight this puppy can do some hurt. There is an 80 lb. model which I haven't tried yet, but I'm told is quite good. These mini-weapons cost \$10 to \$20 for the 45 lb. (\$12 being average), and \$28 for the 80 lb. Be wary of buying an 80 lb. before looking inside the box. Many are mispackaged with 45 lb. prods. (The prod is the bow.) The 45 lb. prod is steel. The 80 lb. prod is

fiberglass. The body of the bow is plastic on the 40 lb. and metal on the 80 lb.

There are dress-up kits with quivers, telescoping stocks, and cocking stirrups available. (At \$16 I figured "What the hell?" and dressed one up.) These bows can be taken down and carried in an attache case, but you will need a friend to help you string it when you put it together. Bolts (arrows) are available in plastic or aluminum with steel target heads. You can make bolts from pencil diameter dowel (or pencils) fletching them with masking tape vanes and pointing them with a pencil sharpener. This is a silent, short-range, off-the-books weapon which could be an asset to your battery. Be sure to get extra bowstrings and prod nocks as I have found that the nocks wear through and I am told the strings break after a lot of use.

(Continued from page 6)

If someone gets into your phone system what do you have to lose? Privacy, valuable information about customers (credit card information), use of your lines to call Europe and what not.

I must say that PBXs are more challenging now than they were ten years ago but considering most voicemail systems run hand in hand with the PBX, having weak passcodes on your voicemail system can lead to exploitation of your PBX services. Meridian Mail, which is put out by Nortel (www.nortel.com), for instance has a nice little feature where you can set the operator assistance number, which in what I have seen is local numbers, just the same it can be useful for bouncing through to avoid tracing. I don't think anyone wants their phone system used as a jumping off point for attack against something big. The same rules of breaking into answering machines applies to voicemail, but one can get more creative here.

There is usually multiple accounts on a system so if you can't get into one, move onto another. 999 or 9999 is usually an administrators box and 100 or 1000 is usually a general delivery box. Its been my experience that the general delivery box can be the most influential as that's where your general information can be obtained and that's also a very easy box to get into, a lot of the time the passcode is just 1000. In general though some passcodes to try

(Continued on page 9)

Cybertech 10th Anniv. Issue

(Continued from page 8)

are the number of the box as the passcode, 1234, 1111 to 9999, 1000 to 9000, the name of the person or company in DTMF, and the last four digits of the phone number. Knowing that, its possible to use these private phone networks for a lot of different things and I think its very clear why someone should take this into consideration.

Ok now that its clear that your everyday conversations are at risk lets talk about some of the ways we can insure that our distant party is the only other person to hear the conversation. Remember the only secure conversation is one in person, free of any monitoring. Getting back to the point, one must consider what level of security is needed for a conversation before they begin to put security measures in place. For instance I doubt you need to encrypt a voice conversation with your grandmother (unless she works for a three letter agency) nor do I think you want to be on that old cordless phone while buying arms from third world terrorists (not that I'm advocating that). Lets say you are interested in securing voice communication, here are some ideas on what you can do to protect your privacy. The first method is accomplished through PGPphone, a nice little program from the makers of PGP (Pretty Good Privacy). This program allows for secure modem to modem or tcp/ip based voice communication. Using PGP keys at the strength preselected the conversation can be encrypted and secured from prying ears. Only drawback is that there is a little bit of lag and the stronger the key, the more static and breakup you will get. Another idea for shaking any taps on your phone line or your counterparts phone line is through the use of a number of payphone. If you keep a good list of payphone numbers in your area that allow for incoming calls you can be at a certain payphone at a preselected time to receive that call. If its busy you can always have a backup payphone not too far away or your contact will simply try back every two minutes. In my area at least there are still some neighborhood COCOTs (customer owned coin operated telephone) that still take in calls. Your best bet is to call a voicemail number that has ANI every time your at a payphone. When you get home call all the payphone numbers you accumulated and see which ones take in calls. Some owned by the Telco will not allow the call to go through, some COCOTs will have a modem pick up. As another approach you could always invest in

one of those expensive communication devices that hook up to the telephone and allow you to call another telephone with the device. The price is definitely a drawback (\$500 area) so using one of the less expensive methods is most likely the best way to go). Be creative and use your common sense, doing that you'll come up with many creative ideas.

This was meant simply as a primer to phone security. Yes these are old problems but they needed to retouched on because it seems many people are still mystified by simple phone phreaking techniques. There are other phone risks, such as beige boxing and social engineering, but those topics have been covered already in some very well detailed articles that are available on sites all over the internet and fine BBSs like Ripco. I hope this has opened your eyes to the dangers out there or at least refreshed your memory. And to cut off all those flames that I ripped this information off and what not, I have spent many hours on the phone testing and perfecting these techniques, there is nothing here that I don't have first hand knowledge of. I'd like to leave off with these words that good friend recently told me, "When you take from one its plagiarism, but when you take from many its research."

Appendix

PGPphone

<http://web.mit.edu/network/pgpfone/>

Phreaking Info

<http://come.to/mobdomain>

<http://www.phonelosers.org>

<http://www.hackersclub.com/km>

-The Mob Boss; <http://come.to/mobdomain>

Voicemail and fax: 1-877-203-3043

Special Thanks To...

Deo

Ryan

Websulker (<http://www.websulker.com>)

and anyone else I left out...

Cybertech 10th Anniv. Issue

FINAL WORDS

With this issue, I'm sure many of you are wondering if there will be further issues of Cybertech released. The Internet, for the time being, makes publishing a print zine for the sake of providing information pretty much a labor of love thing. During the height of Cybertech's (then spelt "Cybertek") run we had 500 subscribers. After soliciting all the articles, and laying out the zine, it took a day to drive down to Staples for photocopies, and then stuff, label, and stamp the envelopes for mailing. That was then. As I write this, I check the stats for The IIRG's web site' where the Cybertech archives are kept. The site averages 1200 visits a day. The simple fact is that more people are seeing Cybertech now via the Internet than when we were mailing out the zine, and with less effort on the part of the publisher.

The expenditure of effort for article solicitation, production, and mailing for a non-profit print periodical make electronic media look very attractive. With the state of the art in desktop publishing software one can download a copy right off the net. Electronic media, however, doesn't have the physical feel that an old-fashioned zine has. It's fun to take a trip over to the Post Office, and check one's PO Box for neat stuff, and hold a copy of a zine in one's hands. That's why I did a 10th Anniversary Issue.

My friends at The International Information Retrieval Guild (IIRG), of which I have been a member since 1992, have been publishing an e-zine called Phantasy since 1990. (The same year I started Cybertek incidentally.) After a short hiatus, we have released two issues this year and plan on continuing to do so on a regular basis. If you want a great hacker/survivalist zine, I recommend you surf on over to our website and download copies of Phantasy. Any articles which I write in the future will be published in Phantasy, and those of you would have liked to contribute something to Cybertech, please send it to Phantasy instead. Mercenary, the editor, can be reached via email to <iirg@iirg.org>.

International Information Retrieval Guild (IIRG) - Phantasy Magazine
<http://www.iirg.org/>

My wonderful, beautiful wife and soulmate Vivian Hecate is going to be doing a print zine for pagans called The Greymorie. I'll be doing a column on technopaganism in it. The address is Greymorie, P.O. Box 641, Marion, CT 06444 if you're interested.

Finally, fellow technological hobbyist (scanner enthusiast actually) Alex Blaha is doing a magazine for all you scanner enthusiasts called Scanning USA. This excellent magazine dedicated to VHF/UHF Communications monitoring is published monthly, and subscriptions are \$24.95 a year. Their address is Scanning USA, 2054 Hawthorne, Joliet, IL 60435 or you can subscribe by calling 1-800-651-0922. They also have a web site up at <http://www.scanningusa.com/>.

UPDATE: Jan. 2002 - Cybertech is back in full production on a bi-monthly schedule. Subscriptions are \$12/year. Send cash or "payee blank" money order (which makes them freely negotiable) to:

Cybertech
P.O. Box 641
Marion, CT 06444
Email: ticom@ticom-tech.com
<http://www.ticom-tech.com/>

We also accept Paypal on our web site.

Until next time, take care of yourself, and keep on hacking! - Ticom