Cyber `Zine

Issue
•10
Volume
•2

YOU NEVER SAW US COMING!

Cover By: IRIEMAN

The Ultimate Cordless Phone Antenna

The dipole antenna is one of the easiest and cheapest antennas to build. Its basic principle is a wire cut to a desired wavelength, cut that in half and add a feed line. Its design is portable and easy to build in emergencies. These are the same types of antennas used by emergency teams and ham operators during national emergencies.

LIST OF MATERIALS

- A piece of wire 22 feet long (This is the wavelength for cordless phones, other frequencies require different lengths)
- An insulator (use a paper towel roll for indoor use or whatever you can find)
- A piece of RG-58 coax cable (this works best for the low cordless frequencies)
- A wire stripper
- Some string
- Electrical tape
- Silicone sealer (for outdoor use)

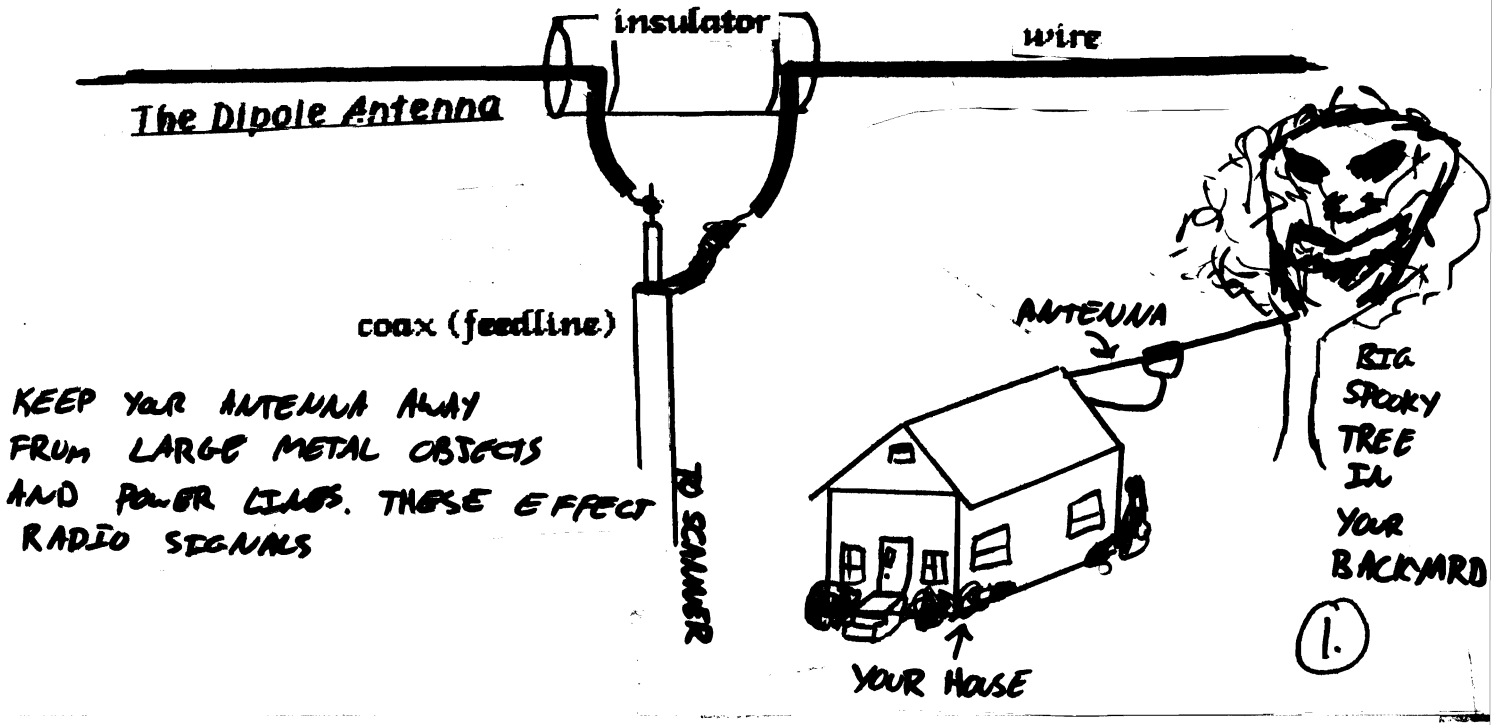
CONSTRUCTION

1. First, take the 22 foot piece of wire and cut it in half to get two 11 foot lengths.
2. Strip one end of each length of wire.
3. Take the paper towel roll and cut it in half, the size doesn't matter.
4. Punch a hole in each end of the paper towel roll and route the wire through it's enough through so you can easily hook up the coax (See Figure 1)
5. Use electrical tape to wrap the wire to the insulator (paper towel) this will protect the wire and make the insulator stronger.
6. Strip your coax, be careful not to cut the copper braid inside. Stripping coax is kinda hard with out the proper tools so you may want to practice on a piece before hand.

Your dipole has two elements, one on each side of the insulator. What you need to do is solder or tape the braid of the coax to one element, and the center wire to the other element. Wrap this entire hook up with electrical tape or the silicone sealer.

Tie the string to the other end of the elements and prepare to hang it.

Find the highest point possible to hang your antenna. Make sure you use the string to hook up the antenna to prevent any injected signals. If you can, mount the antenna vertically



SIMPLEX LOCKS

Simplex locks are some of the most popular security locks around. They can be found almost anywhere. From Federal Express boxes to telephone central offices. Their combination code is only three digits long, but their security relies in the way you put it in.

To open a Simplex lock, push the first two digits AT THE SAME TIME. Then press the third. Turn the handle to the right (on some older models you must turn the handle and press the third button at the same time). The lock will the open. These locks are all mechanical. There are no electronic alarms in them. I there is an alarm warning sign near the lock it means the alarm is inside the door (usually magnetic).

To clear out an invalid entry, turn the knob to the left. For more informationon them go to a locksmith, or call Top Notch Distributors at- 1-800-722-4210 or 1-800-233-4210.

The codes are:

121	122	123	124	125	231	232	233	234	235
341	342	343	344	345	451	452	453	454	455
511	512	513	514	515	131	132	133	134	135
141	142	143	144	145	251	252	253	254	255
241	242	243	244	245	351	352	253	354	355

Please Note- Since the first two digits are pressed at the same time, the firs two digits in our code may be reversed.

Example- If the code is 4-2-5, 2-4-5 would be the exact same.

See pictures on page 5

1-393 TEST NUMBERS

1-393 numbers are inter-office and corporate service numbers used by the phone company, like all their other stuff, so they don't have to pay. Many interesting offices are on these trunks, but you'll have to find most of them yourself. These numbers are toll-free so you can call them from pay phones, just dial 1-393-**** and the last four digits to that office. A long time ago, about eight years, they used to have computers on these numbers. For instance- 1-393-3900 used to be the Packet Switching Network universal access number! My, how things have changed.

Here is a small list of numbers:

1-393-2600	Coin Public Alert, Waukesha
1-393-2978	Network Switch Services T-Carrier
1-393-2448	Recent Change Center, Appleton
1-393-3131	Ameritech Headquarters
1-393-1718	Green Bay Jefferson CO, Relief #

Since you people are smart you'll have to demon dial the rest. I would advise doing it from a pay phone if you plan on doing any major social engineering. You can call from your home on certain numbers because some of them are available to the public. (Look around in the phone book)

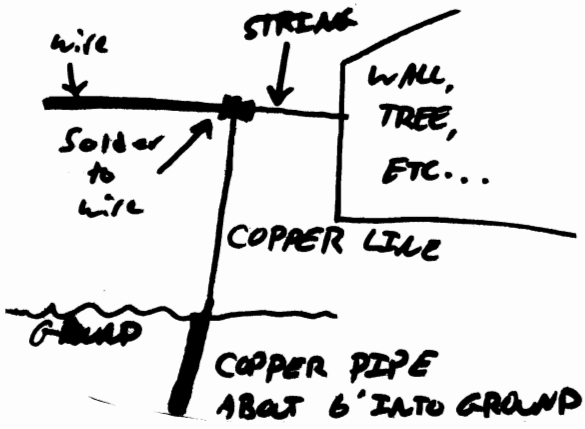
Here are some of the cellular carriers for Green Bay:

NXX (first three of phone number)	Company Name	Type
366	McCaw Cellular	CMC
399	Metro Media Paging	RCC
*493	RSA #10	CMC
556	Ameritech Cellular	RCC
*559	ACC of Madison	CMC
621	New Cell	CMC
664	Mega-Tell	CMC
665	All City Comm	RCC
995	Fromm Svc	CMC

*- Independant Telco exchanges
CMC- Cellular Metroplitan Carrier
RCC- Radio Common Carrier (paging company)

From page 1

ADDING A GROUND



ALWAYS UNPLUG YOUR ANTENNA DURING A STORM!

The Platform War

Yeah, I know your problem. The reason you're not out phrackin' right now is `cuz you're reading the `**Zine.** But there are other reasons. You can't decide which computer to buy. You also have extreme lack of cash to do that very thing, or you would have got off your ass and bought a damn scanner before they took the 800-900mHz range off. Here is a little insight (I may be biased against slow, stupid, retarded, user-friendly Macs, but I own both an Amiga 4000, and an IBM 486, so don't burn this article with any less than 3 gallons of gas.)

PC... System: Dell Dimension XPS - $2,799
With all the other crap - $6,304 {justa note, you are ***not*** going to spend that much unless you are a video, sound, and\or modem junkee like me. The "other crap" includes a sound board and lots of other video junk and software.}

Mac... System: Quadra 800 - $3,200
With other crap - $6,112 {No other hardware and alot less software}

Amiga... System: Amiga4000\040 - $2,300
With other crap - $3,615 {Includes DSS8+, lots **more** cool software}

As you can see, the Amiga platform is not that competitive, but when you load these machines up with cool, but practically useless stuff, it smokes the other machines. I used the top of the line stuff in my report so no one could complain that they really aren't similar.

The PC is a 486 based system mini-tower, and is quite impressive. But it is still an IBM sublet and it scares me to even think about backslashes.

This Mac is top of the line (Ha!) and has a lot of horsepower to waste on a Mac.

I *like my Amiga* its pretty cool for Video phreaks like me. Its software is what keeps the Amiga competitively priced. And I mean all software.

I used the top of the line here, but you can buy the cheaper stuff, you'll just inherit more technical problems. I hoped that this was informative as well as persuasive.

Oh, yeah! I almost forgot! Last week, the new RAPTOR was introduced for the Amiga 4000 that will make it over twenty times faster! True, it costs $15,999; but if you need a super computer...

Gotta Go! Bye!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Iriaman

The Canary Trap

The CIA, the FBI, the SAS, the SIS, and even the Secret Service use a ploy that is sometimes referred to as the "Canary Trap". This is a new use of the old ploy that used misplaced commas and other typos to trace intelligence leaks. The idea is that when the document is published illegally, the the writer of the article or whatever is bound to use a qoute or two. All the agencies have to do is find that document, and using the typos, trace the article to the person they sent the foresaid document to. Pretty soon the papers got wise to this, and started editing the the *qoutes.*

Which brings us to the Canary Trap. All you need is a thesaurus and an imagination. The first paragraph of the document is written in a livid form with many colorful adjectives and gory details. Just find synonyms for a few words, rearrange some sentences, and make copies of each one, with information as to who got which one.

In just the opening paragraph, there are virtually over **three-thousand** possible combinations, but considering the information is classified enough to have the Canary Trap, probably not more than a few hundred will be sent out. The language in the first paragraph should be so good that the press can't help but qoute a few lines. The rest of it is up to the Government (which totally defeats the purpose of a counter-intelligence tracking system).

Iriaman

SECURITY FEATURES OF THE #5 ESS

As you know the #5 ESS switch is replacing the current analog switches. The #5 is a digital switch that has all the advanced features that anyone could ever want. It is one large computer that can handle thousands of calls a second. Here are the security features of the Remote Office Test Line (ROTL).

To prevent unauthorized remote locations from taking trunks (lines) out of service, several conditions must be satisfied prior to affecting the condition of the trunk. First, the remote location must identify itself as being on an authorized list. The identification digit, supplied in the priming, must correspond to a valid entry in the office dependent data (ODD) relation "ROTLCB". Second, the #5 ESS switch must place a call to a prestored directory number and connect the tone detector to the callback circuit. Third, the remote location must transmit the unlocking frequency of 1004 Hz (the 958-0016 test number) to the ROTL over the callback circuit. Fourth, the ROTL (tone detector) must recognize the unlocking frequency and must declare that authorization has been established. The authorization list states whether a particular test center is authorized to exceed the automatic maintenance limit (AML). Currently, only manual test centers are allowed to exceed the AML. The AML limits the total number of trunks in a trunk group which can be in an out-of-service condition at one time. Once a security callback is performed, it is effective until the caller disconnects.

TRUNK CONDITIONING

The CAROT Test Center can preform the following functions

- Perform a security callback
- Remove trunks from service
- Restore trunks to service
- Request the status of a trunk or group of trunks, [in-service or out of service (locked out or disabled)]

These functions are requested by the test center via multi-frequency (MF) commands.

On the two malls, the first frequency is the repeater, scan this one to here all conversations. The second is the frequency used by their handsets. The same is for JJ. The 464 frequencies are the repeater frequencies.

Ah... Not even close

Rent-A-Cop Frequencies

Port Plaza Mall.....	464.875/469.875 MHz
Bay Park Square.....	464.975/469.975 MHz
JJ Security.....	464.8
	464.5
	464.55
	469.5

LOCAL AMERITECH CENTRAL OFFICES

De Pere
CLLI- DEPRWI11
Address- 119 S Michigan St.
Phone (voice)- 728-0022

Green Bay Cardinal Lane
CLLI- GNBYWI13
Address- 1936 Cardinal Ln.
Phone (voice)- 434-0022

Green Bay Huth
CLLI- GNBYWI12
Address- 155 Huth St.
Phone (voice)- 468-0020

Green Bay Jefferson (It is also a radio site)
CLLI- GNBYWI01
Address- 205 S, Jefferson
Phone (voice)- 433-4186

Green Bay Ridge
Address- 703 S, Ridge Rd.
CLLI- GNBYWI11
Phone (voice)- 497-0022

We have the complete list of all the Ameritech CO's in Wisconsin (there is around 240) if you need more information on them just contact us.

****

A Little Gift From Hallmark

What we are talking about are those new talking greeting cards offered by Hallmark. What these consist of is minature Analog-to-Digital and vice versa recorders. After removeing them from the cardboard holder, you get an extermely small recorder. If you hook them up to a small 6-volt battery you get a circuit that can be hid inside a film canister or lighter.

You can use the recorder for an improvised Red Box (record the tones off tape), an auto-dialer. There are hundreds of uses, and the best part about them is there only $8.00, and concealable! (Use battery Radio Shack part #- 23-469)

Automatic Number Identification on 1-800 Numbers

800 numbers are actually lines rented out to other companies from their local Regional Bell Operating Company (RBOC). Since all the lines run through a Bell central office, their switches record the number that you are calling from. Then, for a small fee the RBOC will sell a list of the numbers that called that company's 800 number. You will sometimes expirence this by receiving mail from a company that you called, but never gave your name.

Cellular Phones

The insides of cellular phones has been the recent scene for the underground hacker world. People have been experimenting with the hardware in cellular phones. No, we are not talking about the cloning or burning used by crazed drug dealers to make free phone calls to their parole agents. we are talking about the hidden diagnostics tests and advanced technology used by these phones.

To do anything with your cellular phone, you must first get ahold of a service manual. These will tell you how to fix your phone and may even give you schematic diagrams. Right now, they are hard to find because the cellular industry is telling the technicians not to reveal their secrets.

Here is some stuff we already know. The EPROM, *Erasable Programmable Read Only Memory. This chip is easy to find because it will have a small glass window on the top, and a number usually starting with 27 on the top. This large IC contains the operating information (not the* ESN *or* NAM*.) for the phone to use. This information is stored permanently and can't be changed unless you read the chip (in an* EPROM *reader), and then re-write the code to your own likening. (you could use it to control a coffee maker if you wanted)*

*The actual serial number (*ESN - *Electronic Serial Number) is in a different chip. This varies from manufacture to manufacture, but is usually stored in an* EEPROM *(Electronically Erasable you know the rest). This is the thing people read then re-write to get free phone calls. The* ESN *is transmitted digitaly in front of the number you called. A central computer receives this* ESN, *and then routes your call through the switch and billing computers, but only if the* ESN *comes up valid on the computer.*
If you use someone else's ESN, *they get the bill.*

You can even unmute the audio on a specific channel, even if your not talking on the phone. This feature can be usually done from the handset, and will let you listen to who ever is talking on that channel at that particular time. There are 666 channels to do this on, but you can only program one at a time. The technicians use this to test the phone to see how good the sound quality of it is, yeah right.

identifies your your phone in the cellular system.

NAM- Number Assignment Module. It consists of a telephone number, system ID, initial paging channel, access overload class, and group ID mark. All this along with the ESN

How to identify a sellout

The first thing you should notice is that 95% of the population at west high are sellouts the true one to the realm know what I mean but for the one just starting or the sellouts reading this zine here are six ways to identify if the person is a sellout.

1. The person walks around in a big group and they all do the same things, say the same words, and are as dumb as the dirt they walk on.

2.They always ask for help and relay on other people to figure thing out for them. They logical thinking skills are at zero.

3. Their vocabulary consists of the following words: SWEET, COOL, THAT'S REAL, BABY, CLEAN, and other words said in a sarcastic manner.

4.They don't understand what the purpose of hacking is because they are too dumb. All they do is try to get you mad by saying the words listed above and resorting to violence when you don't care what they do.

5. Sellouts always get mad and sometimes even pissed off at you because you are smarter and you don't give a rats ass if they existed at all.

6.They also can't fight their own battles. They call one their other sellout buddies and have them hold you down while they take your lap top, acoustic coupler,modem and all of your ESS dial-up's.

Total Random Chaos

What to do on your Summer Vacation

I just took a "business" trip to the Luxembourg-Casco area. They are obviously very organized there, but obviously don't have too many hackers. It is GTE territory and the payphones accepted slugs. I found this increasingly interesting as I had never come upon a payphone that would accept them. Alas, my curiosity got the better of me and I spent several hours inspecting it. I came up with these conclusions:
A: the buttons were one-third the height of Bell buttons, resulting in the fact that the numbers and letters were engraved *above* the buttons.
B: the phone gave a loud, single ping every time I put a slug in, hung up, or picked up.

There were many other things, but I will spare you the details. I have compiled a list of things <u>you</u> can do over the summer:

1. Keep in touch with us. We will hopefully keep printing through the summer and you won't want to miss this stuff. Give your name, address, some money, and some stamps to your dealer, and we'll send you the `Zine.
2. If you go on vacation, keep your eyes and ears open and take notes. Contact us when you get back and tell us what you found out. Better yet, write an article, we may either publish it, add it to our own stuff and give you credit, or burn it in disgust if we think you're clueless.
3. Dumpster Dive every night (not for the weak at heart)
4. Get a job and buy some cool equipment
5. Screw around with electronics until you burn your house down.

{Not that we suggest this stuff}

*(**Editor's Note**: Most GTE pay phones have test numbers is the 11x or x11 range. Where x is a digit between 0 & 9)*

Satellite Recon

Okay, here's some stuff on those annoying peeping toms that fly at 18,000 mph in the outer stratosphere.

*From 30 miles away, they can tell if your sholace is tied.

*They can identify someone by hairlength, height, weight, and bust size (no faces are ever clear). Yes, that's right! They determine who a girl is by the size of her breasts. They have to have at least C-cup sized breasts for her cleavage to show up on the photographs. I am not kidding you. Someone at Langley (CIA H.Q.) actually worked out the math.

*All pictures taken at night are thermal.

This is where the tax money goes.

Irieman 8.

Ameritech Commercial Service Internet dial-ups

906-225-0411
906-487-9007
906-632-3261
906-774-0585
906-789-2010
906-932-3219

LAST PAGE

Who ever has the phone # of 391-1239 we have to talk.

Cryptanalysis II

It has been called to my attention that not everyone understood my article on cryptanalysis. I shall have to hold off on the other things like scytales and such until I have enlightened those, to which I endeavor to with the greatest ferocity in the following text. (I'm going to make it simple for you if you didn't understand the last sentence). Here's an explanation of the words I will use:

Encode - to put a message into code
Encipher - to put a message into cipher
Decode - translate a message from code to English
Decipher - translate a message from cipher to English
Cryptographer - a man who works with codes or ciphers
Cryptanalysis - the process of breaking a secret code or cipher
Null - a meaningless letter in a ciphered message, placed there either to fill out the number of units in the message, or to confuse the enemy if he tries to decipher the message
Codes and Ciphers - the difference between a code and a cipher is that codes have a symbol or word that stands for another word. The good thing about them is that they are unreadable without a code book. The bad thing is the code book. You need at least two of them. One for the sender, one for the receiver, and one for each other person who you will send messages to.

Ciphers are different. They have a symbol, letter, or number stand for each *letter*. They are very easy to use and you need no code book. However, they are very orderley, and therefore relatively simple to break.

Srieman

Green Bay Police Back-up Frequency

Sunday, May 8 at around 1:30 P.M. anyone listening to the Green Bay Police on their scanner would have heard something unusual. The main dispatcher tried to dispatch a call about a security alarm going off at some business on Main St. Half the cars on patrol during that shift received the call. This prompted the dispatcher to switch to a channel called "800 Conventional" This is a back-up emergency channel, at **855.2125 Mhz**, listed to the Green Bay Police. This channel is not trunked, so the disposition, dispatch, fire-rescue, and teletype operators all had to use one frequency. It hardly ever gets used so you don't have to scan it all the time.

Since the end of the school year is coming up, you have to ask your local distributor about a three month subscription for around five dollars. This will cover you for the three month summer vacation. You can then start purchasing issues again normally. If we are not going to see you again, give us your name and address and we will mail issues to you. Thanks

Liars-

The article on home-made nightvision equip will be in Issue #11

Sorry