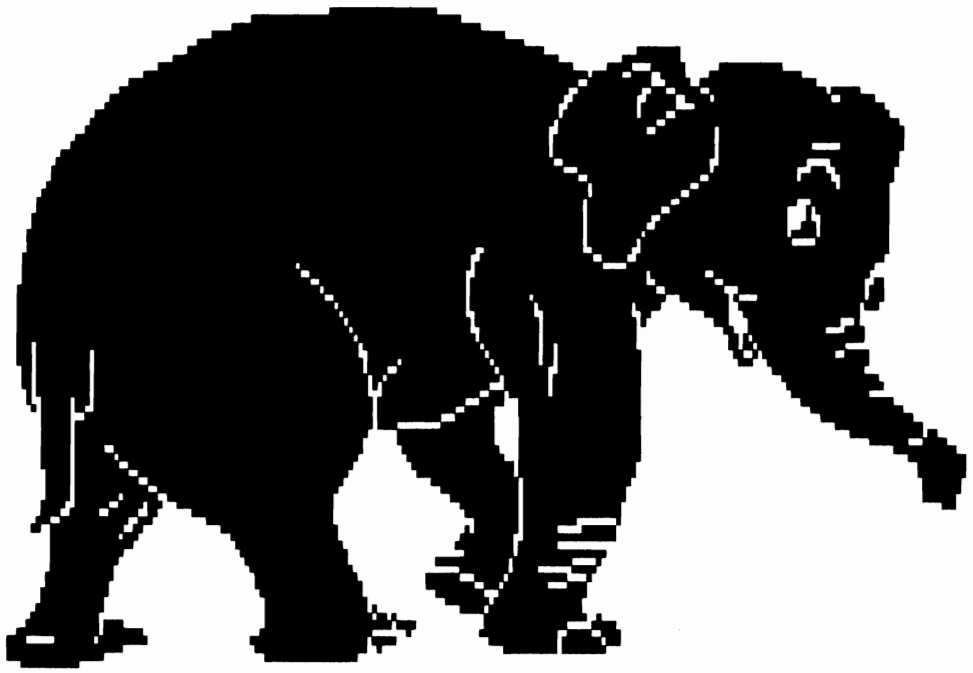
Cyber Zine

ANAC 330-4321

Ameritek's new trunk signaling system.



ISSUE # 9

Cover By:JOJON JANJOM

AMERITECH SECURITY BULLETIN

Ameritech has started a program that will secure all network elements by 1995. They are going to remove all the dial-up ports to every network element in the region. They are also going to the top 100 Central Offices by June 1, 1994. For more information you can contact:

Craig M. Granger/Area Manager
Distributed Security
23500 Northwestern Hwy. Room A-250
Southfield, Michigan, 48075 (810) 424-2500

They also have a secured Fax at (810) 424-2550.

Here is a list of the dial-ups for the Ridge Rd. Central Office here in Green Bay.

CLLI: GNBYWI11CGO
Office Type: #1/1A ESS (Electronic Switching System)
SCC (Switch Control Center) Name: Fox Valley SCC
SCC Telephone #: 735-3475 (voice)
Office Manager: Mark Schweiger, phone- 497-0020 (voice)
Other Manager: Gerald Weidemeir, phone- 497-0022 (voice)

COMPUTER DIAL-UP	TYPE	PURPOSE OF CIRCUIT
414-494-2439	SWITCH	AMA MAINTENANCE
414-494-2668	SWITCH	AMA HOST
414-494-0394	SWITCH	AMA MAINTENANCE
414-494-3286	SWITCH	AMA HOST
414-432-0043		ESS DIAL-UP

Please note that these are only for the 703 South Ridge Rd. Central Office. The other Central Offices (Huth St., Jefferson St., and Cardinal Lane) may have different types of host and maintenance computers.

**AMA- Automatic Message Accounting: An arrangement of apparatus for automatically recording and processing the data required to compute charges on certain classes of calls. (i.e. your phone bill)

You can also call the Ameritech Security Hotline although they may get mad. (810) 424-7751.

Another note: Ameritech USERID's are the person's first initial and last six digits of their social security number. For instance-

Redd Box, SSN- 345-67-5426 would have a USERID of R675426.
Their passcodes have also been known to be 14 characters long.

Have fun while it lasts. CZ9

1.

Alarm Symbols

These are the Industry Standard Symbols used by alarm dealers/installers on their blueprints.

Access Control Symbols

- Access control unit
- Card reader
- Digital keypad
- Digital keypad and card reader
- Door bolt
- Door strike
- Parking gate

Burglar Alarm Symbols

- Bell
- Buzzer
- Cash drawer money clip
- Contact switch, balanced
- Contact switch (flush)
- Contact switch (surface)
- Control unit
- Dual-technology device
- Emergency power supply/battery
- Floor mat
- Foil tape
- Foot rail
- Glassbreak detector
- Hold-up/panic button
- Hold-up/panic device
- Horn/siren speaker
- Laced wire
- Light/strobe
- Microwave receiver
- Microwave transceiver
- Microwave transmitter
- Passive infrared detector
- Photoelectric beam path
- Photoelectric receiver
- Photoelectric, self-contained
- Photoelectric transmitter
- Remote control—digital keypad
- Remote control—keyswitch
- Remote control—toggle/ pushbutton
- Remote zone annunciator
- Signal processor
- Signal processor—listen-in
- Signal processor—microwave
- Signal processor—passive infrared
- Signal processor—sound detector
- Signal processor—ultrasonic
- Signal processor—vibration/ shock
- Slave digital communicator
- Slave tape dialer
- Slave zone board/control/ annunciator
- Sound detector/discriminator
- Space protection device
- Supervised wireless receiver
- Supervised wireless transmitter
- Transformer
- Ultrasonic receiver
- Ultrasonic transceiver
- Ultrasonic transmitter
- Vibration/shock sensor
- Wireless receiver
- Wireless transmitter
- Zoned control unit

CCTV Symbols

- CCTV camera
- CCTV camera with zoom lens
- Film camera
- Manual switcher
- Monitor
- Pan and tilt control unit
- Pan and tilt unit
- Pan control unit
- Pan unit
- Remote control unit
- Sequential switcher
- Video tape recorder
- Zoom lens control

Letter Key

A: Police/Fire Connect
AL: Access Control
B: Direct (Central Statio Connect
C: Digital Communicator
D: Digital Keypad
E: Emergency Power/batt
F: Flush
G: Glassbreak detecto
H: Capacitance/proximity Sensor
I: Passive infrared
J: Multiplex
K: Keyswitch
L: Tape dialer
M: Microwave

Symbols Continued

Fire Protection Symbols

- Automatic detection and supervisory services
- Bell (gong)
- Buzzer
- Door holder
- Emergency light, battery powered (one lamp)
- Emergency light, battery powered (two lamps)
- Emergency light, battery powered (three lamps)
- Fire alarm control panel (FACP)
- Flame detector (flicker detector)
- Flow detector/switch
- Gas detector
- Heat detector (thermal detector)
- Horn with light
- Illuminated exit sign
- Illuminated exit sign with direction arrow
- Level detector/switch
- Light (lamp, signal light, indicator lamp)
- Manual alarm box (pull station and pull box)
- Manual station (call point)
- Pressure detector/switch
- Projected beam smoke detector
- Single stroke bell
- Smoke detector
- Speaker/horn (electric horn)
- Tamper detector/switch
- Telephone station (telephone call point)
- Valve with tamper detector/switch
- Vibrating bell

Letter Key Cont.

W: Wireless

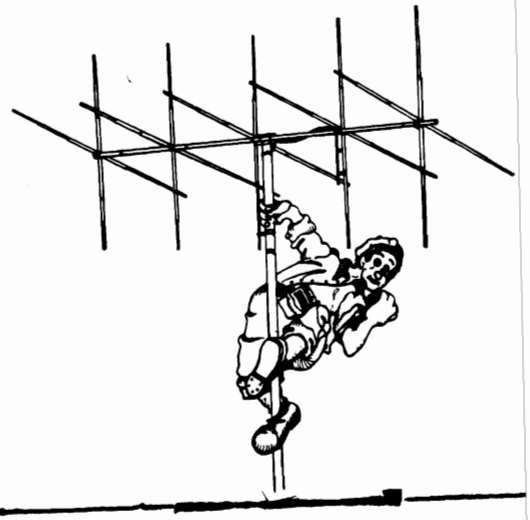
X: Transformer

Y: Supervised Wireless

Z: Zone

ZM: Zoom

n: number



Letter Key Cont.

O: Outdoor/weatherproof

P: Photoelectric

PN: Pan

Q: Listen: In

R: Remote

S: Sound detector/discriminator

SQ: Sequential

T: Toggle/pushbutton

TL: Tilt

U: Ultrasonic

V: Vibration/shock

Basic Programs

Here are some BASIC programs that will help you convert hex to decim
and decimal to Hex. To write these programs you must have The BASI
Programming language. If you have a IBM or compatible you already h
BASIC. Just go to your dos prompt and type BASIC and then you can wi
the program. But if you have one of these dumb, slow, retarded, user
friendly, Macintosh's then you have to buy the BASIC program disk for
apples or go to a friends house who has a real computer.

Type it as you see it here:

```
10 ' COVERT HEX TO DECIMAL
20 '
30 INPUT "ENTER A HEX NUMBER ", X$
40 PRINT "THE DECIMAL EQUIVALENT IS "; VAL ("&H"+X$)
50 GOTO 30
```

To terminate the program just press CONTROL + PAUSE at the same tim

```
10 ' CONVERT DECIMAL TO HEX
20 '
30 INPUT "ENTER A DECIMAL NUMBER ", X
40 PRINT "THE HEX EQUIVALENT IS "; HEX$ (X)
50 GOTO 30
```

If you want to make the programs shorter eliminate number 10 and num
20 from each program their only purpose is to identify what it does.

Have fun and experiment always. If you have any BASIC programs that
think we would like you can leave them in my email on metly world.

By: Foton Fem

NEXT ISSUE:

- CORDLESS PHONE ANTENNAS
- 1-393 #5
- SECURITY FEATURES ON THE #5ESS TEST/ACCESS PORT
- CELLULAR PHONES
- SIMPLEX LOCK CODE
- NIGHTVISION, MAKING YOUR OWN
- AND MORE!!

CRYPTANALYSIS

Deciphering by hand is a very simple process that is widely used, or at least it was before encrypting came along. It was very important during the Civil War, but it is almost obsolete now, except for several isolated instances (i.e. Naval ships, Third World countries, Amish country, etc.). Despite the view I'm establishing as an ancient, primitive process, it is very effective. You can use it on any kind of cipher. The best way to crack long messages is with a **Frequency Table.** The complete Frequency Table is:

E T A O N R I S H D L F C M U G Y P W B V K X J Q Z

* This system is almost foolproof with messages over 3 pages long
* The first five letters of the Frequency Table make up 45% of the letters used in the English language
* The first nine letters of the Freq. table make up 70% of the English language

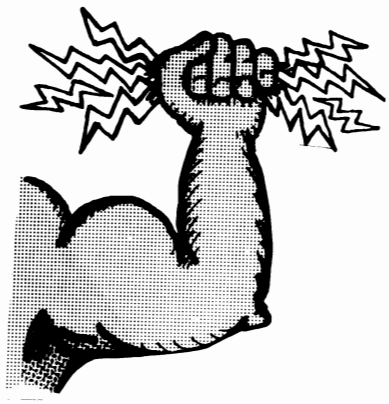
The most common combinations are:
(reading down the columns)

TH	EN
HE	OF
AN	TE
RE	ED
ER	OR
IN	TI
ON	HI
AT	AS
ND	TO
ST	WH
ES	

The letters that are most commonly doubled are:

LL	FF
EE	RR
SS	NN
OO	PP
TT	CC

There are two one-letter words, **A** and **I.**



The most common two-letter words are:

OF	HE
TO	BY
IN	OR
IT	ON
IS	DO
BE	IF
AS	ME
AT	MY
SO	UP
WE	AN

Hints:

1. Check for a signature, if there is one, and you know who it's from, you've got those letters.

2. Copy the message in large print on a seperate sheet of paper. At the bottom of the paper, write the alphabet. When you <u>think</u> you know a letter, but aren't sure, put it beneath the corresponding letter in the alphabet. When you're <u>sure,</u>

CONTINUED ON PAGE 11

Hacking Traffic Lights

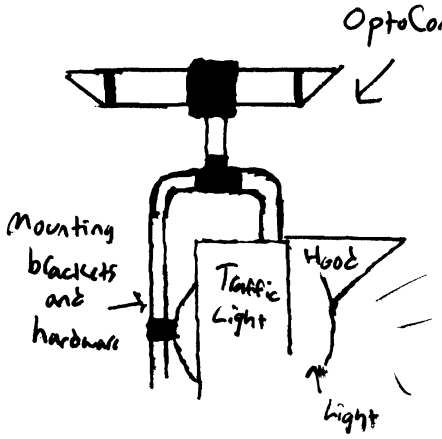
If you have ever noticed those little tubes that extend off of traffic lights, then you should know what we are talking about. Those tubes are part of a system called "OptoCom" that has been around for about four years now..

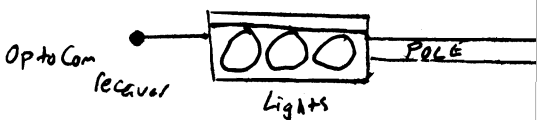
Those tubes are optical receivers that are triggered with pulses of light or infared energy. If you ever noticed the strobe light on top of a ambulance then you know were the light pulses come from. When the OptoCom receiver gets these pulses of light, it changes the light green!

It is normally used at busy intersections to allow rescue personal through with out causing a traffic jam. If an ambulance comes upon a red light, their OptoCom transmitter (strobe light) will change the red light to green, and the green light will go from green to red without going to yellow. Obviously, this could cause some major traffic problems.

In some areas the OptoCom can be triggered by infared. This is cool because you can't see infared so there is less of chance of getting caught. All you have to do is get a hand-held strobe light (available at Radio Shack for around $15) at stick it out your window when you come to an OptoCom served traffic light. You may have to adjust the flash rate to get the right flash rate. This can be done by adjusting the knob on the back or changing the main capacitor rating. (smaller microfared will cause it to flash faster) If you want to try the infared signalling, go to a photo developer and get a peice of unexposed, Kodak Ektachrome film. This film will transmit infared energy while blocking visible light.

Green Bay does have OptoCom. Go to just about any major intersection and look at the top of the traffic lights. There will be a tube that extends from it an kinda looks like a gun site. This is the OptoCom receiver. From what I know, the Green Bay area has a steady flash rate so the handheld Radio Shack strobe light will work but, in some citied they have a flash pattern (example: In California some cities have a flash pattern of two flashes then a pause and then two more flashes). I know your not stupid, so don't cause any major accidents.





This is how they look on overhead lights.




Federal Bureau of Investigation

The FBI is the principle investigation arm of the justice department. Recently, the FBI has been working to get their entir radio system in compliance with their new national radio plan. In a nutshell, the FBI is switching the old 163 MHz repeater outputs and the 167 MHz repeater input/simplex frequencies. The new frequency plan calls for repeater inputs in the 162 and 163 MHz range. all repeater output and simplex frequencies will be in the 164, 165, and 167 to 173 MHz ranges.

Here is a list of known FBI frequencies in the HF/VHF/UHF spectrum.

HF (All USB) in kilohertz

2810	4030	4617.5	4992.5	5014
5060	5390	5913	6594	6800
6954	7905	9015	9185	9240
9311.5	9313	10500	10550	10915
11075	11210	11490	13660	14460
14495	14453	15955	16376	17405
17602.5	18173	18668	22345	23402
23675	23875	27740		

The FBI tests their communications system on Monday mornings in USB and RTTY. Try 5060, 7905, and 14495 kHz.

VHF/UHF in megahertz

162.6375	162.7375	162.7625	162.7875	163.8375	163.8500	163.8625
163.8750	163.8875	183.9000	163.9125	163.9250	163.9500	163.9625
163.9750	163.9875	164.0500	164.1625	164.2500	164.3500	164.4250
165.5875	165.7125	185.8375	165.9000	165.9250	167.1500	167.2125
167.2375	167.2500	167.2625	167.2750	167.2875	167.3000	167.3125
167.3250	167.3375	167.3500	167.3625	167.3750	167.3875	167.4000
167.4125	167.4250	167.4375	167.4500	167.4625	167.4750	167.4875
167.5000	167.5125	167.5250	167.5375	167.5500	167.5625	167.5750
167.5875	167.6000	167.6125	167.6250	167.6375	167.6500	167.6625
167.6750	167.6875	167.7000	167.7125	167.7250	167.7375	167.7500
167.7625	167.7750	167.7875	167.8250	170.9000	411.0000	411.0500
411.1500	412.3500	412.4250	412.4500	412.4750	412.5000	412.5500
412.5750	412.6750	414.0000	414.0250	414.0500	414.0625	414.0750
414.0875	414.1000	414.1250	414.1500	414.1750	414.2000	414.2250
414.2500	414.2750	414.3000	414.3250	414.3500	414.3750	414.4000
414.4250	414.4375	414.4750	414.5000	414.5250	414.5500	414.5750
414.6000	414.7000	414.7500	417.1000	417.1500	417.3250	419.0750
419.1750	419.2000	419.2250	419.2500	419.2750	419.3000	419.3250
419.3500	419.3750	419.4000	419.4250	419.4500	419.4750	419.5000
419.5250	419.5500	419.5750	419.6000			

167.5625 Nationwide common
165.5375 Input 163.8625 Output- F.B.I. SWAT Teams

SPEECH SCRAMBLERS AND VOICE ENCRYPTION

The voice scrambler is a small box inserted between the transmitter and the microphone. On some newer types of radios, it is built into the actual hardware. There are many types around today but these are how most of them operate.

Inverters

Normal speech consists of many different frequencies each having different amplitudes. An inverter acts by reversing these amplitudes and making the speech sound like a poorly tuned radio.

Figure 1 shows a block diagram of a simple inverter. The input signal consists of speech sounds having components in the frequency range of 250 to 2750 Hz. These signals are fed to a modulator were they are heterodyned (mixed) with a signal from a 3,000 Hz oscillator. Two different sets of signal are produced in the modulator- the sum of the speech frequencies and the 3,000 Hz signal and the difference between the 3,000 Hz signal and the speech frequencies. A low-pass filter in the output lets only the difference frequencies pass. Thus, the output frequencies are between 250 and 2750 Hz, but the spectrum is inverted. For example, an input component having a frequency of 2750 Hz will beat the 3,000 Hz signal to produce a component of 3,000 - 2750, or 250 Hz. Similarly, a 250 Hz input signal will produce a 2750 Hz output signal.

Note that if the input were an inverted spectrum, the output would be plain speech. This means that the same equipment can be used for both scrambling and descrambling.

Although the simple circuit in Figure 1 is used in some scramblers, it has several disadvantages. The 3,000 Hz signal is difficult to completely remove allowing a small amount of speech to pass through and making the message somewhat legible.

Improved Inverter

A scrambling method that is easier to filter is shown in Figure 2. This method uses double modulation. In the first modulator, the speech is heterodyned with a high frequency signal, for example 13,000 Hz. only the high frequency components are passed on to the second modulator, which operates exactly 3,000 Hz higher in frequency than the first modulator. Here, a filter selects the low-frequency, or difference, components. In this arrangement, if the input signal has a frequency of 2750 Hz, the output of the first modulator will be a frequency of 15,750 Hz. The output of the second modulator is then 16,000 - 15,750, or 250 Hz. It produces the same output as the above method but maintenance and adjustments are easier.

The main disadvantage of the simple inverter is the fact that their signal can be descrambled by using an signal generator, together with a regular receiver. If, using the frequencies in the previous examples, a signal generator is tuned exactly 3,000 Hz below the carrier frequency and fed into a receiver, together with the inverted signal, the output will contain plain speech. There should be a 3,000 Hz beat to the speech but it will be legible. □

Figure 1

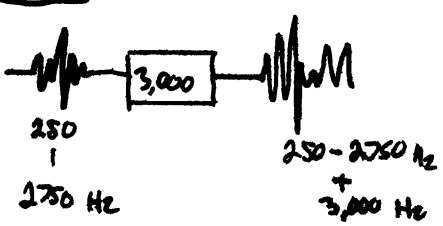
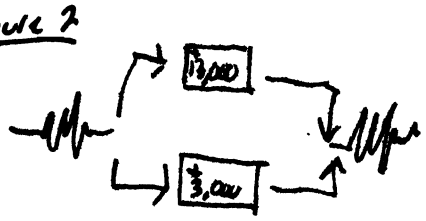


Figure 2



Remote Provisioning Procedures for SLC Series 5

The SLC (Subscriber Loop Carrier) carrier system 5, also referrred to as a digital loop carrier, is a small hut located away from a central office. Inside this hut, is a multplexing system that digitalizes communications and sends them down a line to the central office. What a multiplexer does is compress and transmit data with out interference. For example, ten lines may go into the SLC 5, but only one may go out. This allows for communication developments away from any central offices line. (i.e. out in a forest) It does this by converting the signals into digital radio frequencies and transmitting them trough a fiber optic or copper line. Sometimes this system may be wireless ans transmit the data direct to a central office with out any lines.

This article will cover a new software package developed by AT&T called Centralized Operations and Provisioning (COP). The phone company uses an AT&T 6386 shared PC system located inside Special Service Centers (SSC) that are available in Milwaukee, Madison, and Appleton.

Features of COP

- It provides the capability to provision (prepare) SLC series 5 channel units and channel bank memory.

- Provides status reports of the carrier channels, channel types, protection to the channels, and inventory of the channel bank is the carrier system.

The COP system does not support any test access or upgrading capabilities. It only supports activities with the preparing of channel units and channel bank memory.

Equipped Offices

The following offices have SLC series 5 with Feature package C with COP, the Dial-ups are underneath the SSC name.

more #'s on 11

Milwaukee (414 area code unless noted)

281-4212	*271-7285	*351-1349	251-0831	*789-7569
258-6837	354-0641	*781-0568	*481-0764	*764-0256

Madison

715-832-1207	608-231-1349
715-386-0637*	608-221-0364*
608-752-2502	608-267-4715*
608-251-1688*	608-277-0984*
608-241-3482*	

Milwaukee cont.

375-0374
367-2389
248-1541*
552-7069
632-0194
549-0922*
567-0064

* - **SARTS**, **COT** (central office terminal), and remote test access (RT) are also available.

The phone company accesses COP software through their special terminals located at a SSC. They have all of these special function. Their terminals are set to:

vt200 emulation, 7 bit controls
7 bit, odd parity
application keyboard
normal cursor keys
color on
enable XOFF
unlocked userdefined keys
9600 baud
no parity
Interpret control characters

Chances are your computer doesn't have all of these functions, so you will have to use a dumb mode. Anyway, after you figure everything out and call the system you'll get a welcome screen that says this.

1. Response:
Welcome to the AT&T 386 Unix system
login:

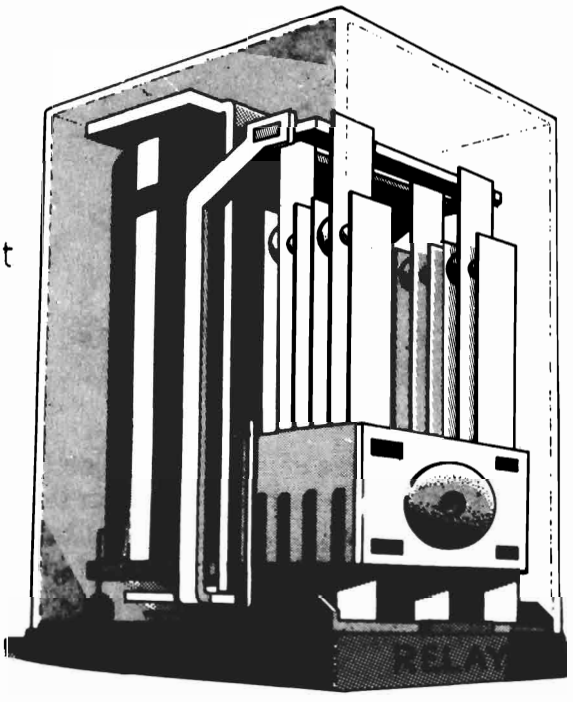
2. Type: cop

3. Response: Password:

4. Type: a valid password, this is up to you to get

5. Response: Enter your initials

6. Type: Your initials (first, middle, last)



The soft keys for COP are:

Attn= F1	Erase= F6
Clear= F2	Print= F7
CMD= F3	Play= F8
Cursor= F4	□= F9
ChgSc= F5	WS Ctrl= F10

7. Response: Setup Active

F1 = Port Select	F6 = Send Break
F2 = Exit to DOS	F7 = Modem Dial
F3 = Hang Up	F8 = Provision

THIS IS BASICALLY WHAT A #1/1A ESS IS. JUST GO UP TO ONE AND ASK FOR A TOUR. MOST OF THE TIME YOU'LL GET IT WITH NO PROBLEMS. G.

THROUGH THE APSN, SO THERE MAY BE A BACK DOOR.

This system is cool because you can dial out of it and call other system like Network Access Servers, AMA hosts, Packet networks. This will provide you with a good route to attack from. It may also help bypass any systems that have callback security, or ANI (Automatic Number Identification) checks.

I you unfamiliar with the system, the sellouts at the help desk will tell you to check the COP User Guide. I know you don't have one so here are a few of the commands you will probably use (you can figure some out yourself):

Change hosts: ALT/CTRL and CMD keys
Exiting: F3 from the Set Up screen
Exiting to the Help Desk. at login:, hit Shift and PF5, then ALT, CTRL, and CMD keys. Go to CH (Change Host) and hit enter twice.
Response: Wisconsin Bell Data Network Help Desk....

Here are the Channel Unit Types identified by the Status Summary Report

Identified by CLEI:

5SCU69	5SCU6A	(E Spots)
5SCU7C	5SCU7B	5SCU7D (4 Wire)
5SCU38	5SCU48	(DDS)
5SCU54	5SCU57	(Multiparty)
5SCU23	5SCU26	(Coin)
5SCU9E	5SCUPF	(DID)
5SCU50	5SCUT0	(FSR)

Identified as POTS, SPOTS, or POTS-SPOTS:

POTS-SPOTS	(RT)	AUA51	5SCU50
		AUA58	5SCU1H0
		AUA59	5SCU1L0
		AUA25	5SCURP7

Here is a little info on the Data Encryption Standard (DES) and SkipJack. SkipJack is a new chip (Clipper Chip) that was developed by the government to increase our privacy, but allow Feds to spy on us.

	DES	SKIPJACK
*Designer:	IBM	National Security Agency
*Year introduced:	1976	1993
*Formula:	Public	Classified
*Law enforcement access:	No	Yes
*Key chosen by:	User	Government
*Number of keys:	One	Two

start

PHONE NOTE: THE HMEKITECH PACKET SWITCHING NETWORK (APSN), DOES NOT HAVE AN EXTERNAL DIAL-UP. EACH CENTRAL OFFICE HAS A PACKET MODE BUT IT MUST BE ACCESSED THROUGH A MAINTENANCE SYSTEM LIKE COSMOS/TIRKS. THEIR E-MAIL ALSO