SCANNERS

SHORTWAVE

# The Urban DX'er

Vol. 1 No. 4
April 15, 1997

Established 1984

## *Code Set Up to Shield Cellular Calls Breached*

*By JOHN MARKOFF*

*SAN FRANCISCO* -- A team of well-known computer security experts will announce on Thursday that they have cracked a key part of the electronic code meant to protect the privacy of calls made with the new, digital generation of cellular telephones.

The announcement, intended as a public warning, means that -- despite their greater potential for privacy protection -- the new cellular telephones may in practice be little more secure from eavesdropping than the analog cellular phones in use the last 15 years. It was such eavesdropping, for example, that caused trouble for House Speaker Newt Gingrich when a Florida couple listened to his cellular phone conversation in December about the congressional ethics inquiry.

Now that digital wireless networks are coming into use around the nation, the breaking of the digital code by the team of two computer security consultants and a university researcher confirms fears about privacy that were raised five years ago when the communications industry agreed under government pressure to adopt a watered-down privacy technology.

According to several telecommunications industry officials, that pressure came from the National Security Agency, which feared that stronger encryption technology might allow criminals or terrorists to conspire with impunity by cellular phones.

But independent security experts now say that the code is easy enough to crack that anyone with sufficient technical skills could make and sell a monitoring device that would be as easy to use as a police scanner is.

Such a device would enable a listener to scan hundreds of wireless channels to listen in randomly on any digital call within a radius ranging from 1,000 feet to a number of miles. Or, as with current cellular technology, if a specific person was the target of an eavesdropper, the device could be programmed to listen for any nearby digital call to that person's telephone number.

Other possible transgressions would include using the device to automatically harvest all calling card or credit card data transmitted with nearby digital wireless phones. And, because of a loophole in the Communications Act of 1934, making and selling such devices would not be illegal, though actually using one would technically be against the law.

These monitoring devices are not yet available, but security experts said that a thriving gray market was certain to develop. And with technical details of the security system already circulating on the Internet, instructions for cracking it will almost certainly make their way into the computer underground, where code breaking and eavesdropping are pursued for fun and profit.

Technical details of the security system were supposed to be a closely guarded secret, known only to a tight circle of industry engineers. But the researchers performed their work based on technical documents that were leaked from within the communications industry and disseminated over the Internet late last year.

"The industry design process is at fault," said David Wagner, a University of California at Berkeley researcher who was a member of the team that broke the code. "We can use this as a lesson, and save ourselves from more serious vulnerabilities in the future."

Communications industry technical experts, made aware of the security flaw earlier this year, have been meeting to determine whether it is too late to improve the system's privacy protections. Already the digital technology is in use in metropolitan areas, including New York and Washington, where either the local cellular networks have been modified to support digital technology or where new so-called wireless personal communications services are being offered.

***The Urban DX'er***

*The Urban DX'er is published monthly through the cooperative efforts of Bob Kozlarek, WA2SQQ and Charlie Hargrove, N2NOV*

*Any information contained is considered public and can be copied, distributed or otherwise electronically distributed provided that proper credit is given..*

*Contributions of information for future issues is always welcomed and greatly appreciated. Please send your E mail to wa2sqq@hili.com..*

"We're already in the process of correcting this flaw," said Chris Carroll, an engineer at GTE Laboratories, who is chairman of the industry committee that oversees privacy standards for cellular phones.

But Greg Rose, a software designer for the Qualcomm Inc., a leader in digital cellular systems, said that fixing the flaw would be "a nightmare." Tightening the security system, Rose said, would involve modifying software already used in the computerized network switching equipment that routes wireless digital telephone calls, as well as the software within individual phones.

Currently, about 45 million Americans have cellular phones, though most of them so far are based on an older analog standard that offers no communications privacy. But cellular companies are gradually converting their networks to the new digital standard, and the new personal communications services networks going into operation around the country also employ the digital-encryption system. Nearly a million PCS phones have been sold in the United States, according to cellular industry figures.

Besides Wagner, the other researchers who cracked the code were Bruce Schneier and John Kelsey of Counterpane Systems, a Minneapolis consulting firm. Schneier is the author of a standard textbook on cryptography.

The new digital wireless security system, which was designed by cellular telephone industry engineers, was never intended to stop the most determined wiretappers.

But because digital calls are transmitted in a format corresponding to the 1's and 0's of computer language, they are more difficult to eavesdrop on than conventional analog calls, which are transmitted in electronic patterns analogous to sound waves. And digital calls protected with encryption technology -- basically a mathematical formula in the software that scrambles the signal -- would be all the harder for a third party to listen to surreptitiously.

Because the encryption system that the industry adopted in 1992 was deliberately made less secure than many experts had recommended at the time, privacy rights advocates have been warning since that the code could be broken too easily. An announcement Thursday that the code has indeed been cracked would seem to bear out those concerns.

"This should serve as a wake-up call," said James Dempsey, senior staff counsel for the Center for Democracy and Technology, a public interest group. "This shows that government's effort to control encryption technology is now hindering the voice communications industry as well as the data and electronic communication realm." Industry executives acknowledged that steps must be taken to address the problem.

"We need strict laws that say it is illegal to manufacture or to modify a device which is designed to perpetrate the illegal interception of PCS telephone calls," said Thomas Wheeler, president of the Cellular Telephone Industry Association, a Washington-based trade group.

Wheeler said the weaker privacy technology had been adopted not simply to appease the government but because makers of wireless communications hardware and software had wanted to embrace a technical standard that would meet federal export regulations. Those rules, based on national security considerations, sharply curtail the potency of American-made encryption technology.

The three computer researchers who broke the code belong to an informal group of technologists who believe strongly that powerful data-scrambling technologies are essential to protect individual privacy in the information age.

These technologists, who planned to release their findings in a news release on Thursday, argue that the best way to insure that the strongest security codes are developed is to conduct the work in a public forum. And so they are sharply critical of the current industry standard setting process, which has made a trade secret of the underlying mathematical formulas used to create the security codes.

"Our work shows clearly why you don't do this behind closed doors," Schneier said. "I'm angry at the cell phone industry because when they changed to the new technology, they had a chance to protect privacy and they failed."

Carroll, head of the industry's privacy committee, said it planned to revise the process for reviewing proposed technical standards.

## *AR8000 URL's*

Here's a list of some good reference URL's if you own an AR8000!

****Please not: All links are active to your browser!**

AR8000 Digest Archives
http://www.rpmdp.com/lists/ar8000digest.archive/

AR8000 HOMEPAGE WITH DIGITAL SOUND
http://www.clark.net/pub/designer/vhealey/ar8000.homepage.html

AR8000 Serial Link Info
http://www.hollis.co.uk/john/ar8000sl.html

AR8000 ToolKit for Macs
http://www.mich.com/eddy/works/

Computer Aided AR8000s
http://www.scancat.com/ar8000.html

Home Brew Interfcaes for AR8000
http://www.capecod.net/tcpip/ARMod.html

LESS AR8000 LINKS
http://www.cris.com/Lsbutler/p3.html

Woodys AR8000 Page
http://homepage.daveworld.net/woody99/aor/aor.htm

## *SWL & RADIO URL's*

AirNav: Links to other WWW sites
http://www.cc.gatech.edu/db1/fly/links.html

Brys Shortwave Radio Links AF4K / G3XLQ FREE
http://www.mnsinc.com/bry/swllynx.htm

CLUBE DXISTA DO PAR
http://www.geocities.com/CapeCanaveral/6731/

Daily FCC Activity
http://www.lantz.com/cbs/

FUNKENHAUSERS Home Page under construction
http://Home.InfoRamp.Net/funk/

Ham Radio Online FCC Preempts TV Antenna Restrictions
http://www.hamradioonline.com/1996/aug/fccanten.html

LW BEACON LOGGINGS/A
http://funnelweb.utcc.utk.edu/jtdybka/beacon.htm

MicroWINGS Airport/Navaid/Fix Info and Maps
http://www.microwings.com/mwaptnav.html

Navagation Beacon Search
http://www.cc.gatech.edu/db1/fly/v1/navaidinfo.html

NTIA/Office of Spectrum Management
http://www.ntia.doc.gov/osmhome/osmhome.html

Satellite Tracking Prediction Form
http://acsprod1.acs.ncsu.edu/scripts/HamRadio/sattrack

Shortwave/Radio Catalog Radio Services
http://itre.ncsu.edu/radio/RadioCatalogRS.htmlSWSoftware

The Internet Guide To International Broadcasters
http://www.informatik.unioldenburg.de/thkoch/

The WUN URL List
http://www.cybercomm.net/slapshot/wunurl.html

URLS to Radio Resources on the Internet
http://www.clark.net/pub/designer/vhealey/sources.html

What Do NAVAIDS Look Like
http://204.242.42.20/7Edaled/navaids/

WZ2B NAVAID SEARCH TOOL
http://www.mdsroc.com/navaid

## *Scanner URL's*

Amtrak Radio Frequencies
http://www.trainweb.com/travel/freq.htm

DANS FEDERAL FREQUENCIES
http://www.geocities.com/Heartland/6095/FED.HTM

Jamess Internet Links For Scanner Listeners
http://www.primenet.com/confused/scan.html

Joe Cardanis South Jersey Scanner Page
http://www.voicenet.com/jcardani/sjscan.htm

KC5KTOs Radio Page
http://w5gb.nmsu.edu/kc5kto/mods

Radio Shack Scanner Modification Page
http://w5gb.nmsu.edu/kc5kto/mods.html

Mikes South Florida Scanning and DXing Page
http://www.shadow.net/mikef/

NJ State Police Radio Info
http://www.voicenet.com/jcardani/np00.htm

NY / NJ Fire Photos Links
http://www.njfmba.com/njmfpa/1.html

Pager Programming Monitoring and Applications
http://www.l0pht.com/radiophone/pager/pager.html

POCSAG Decoder HomePage

http://huizen.dds.nl/pocsag/

Province Of Ontario Scanner Frequencies
http://www.iaw.on.ca/sstdenis/ont.htm

Radio Manager for Windows Home Page by Ben Saladino
http://www.interplaza.com/bensware/rm.htm

Radio Monitoring Products
http://www.designeq.com/radio.html

Rod N2RMVs Home Page
http://www.hili.com/rod/index.html

Rutgers Univeristy Radio Frequency List
http://wwwns.rutgers.edu/thayes/freqlist.html

Scan Star Home Page
http://www.best.com/sdunham/homepage.htmlwinreq

SCANCAT Home Page
http://www.scancat.com/

Scanner Freqs
http://www.iaw.on.ca/sstdenis/links.htm

Scanning Reference
http://www.panix.com/clay/scanning/scanners.html

Scanning Upstate New York
http://www.ggw.org/nf2g/nys.shtml

South Brunswicks Trunked Radio System
http://mars.superlink.net/jcr1434/scanner/sb800mhz.html

Southeastern Wisconsin Monitoring Page
http://www.execpc.com/ghahn/

State by State Frequency Links
http://web.idirect.com/dkwood/links.htm

The Monitoring Post The Pro2006 Home Page
http://home.ptd.net/pro2006/

Trunked Radio Systems Users Page
http://members.aol.com/wwhitby2/trs.html

TV FREQS
http://users.deltanet.com/rbarron/same.html

UHF Log Periodic Antenna Design Page
http://www.globalnow.com/nightlife/UHF.html

## *UNIDEN TRACKER UPDATE*

I came across this on one of the news groups and I thought it might be of interest....

"Someone here asked last week if anyone could confirm the rumor that Motorola has sued Uniden to block the release of the Trunk tracker. The answer is no! At least, not yet.
I called Motorola's press relations folks yesterday and asked. They called back this morning and said "we are aware of the (Uniden) radio, and we are studying our options at this time. We have no further comment."0
I then asked if she was clearly stating that no lawsuit has been filed. She said none has been filed.

As an aside, Harold Ort, editor of Popular Communications magazine, told me yesterday that he spoke with Jill Prince, Uniden's media and trade show director on Monday, and she told him then that the first shipments of production model 235XLTs are expected either late this week, or early next week.

Of course, samples will have to be tested for quality control and such, so it will probably take another week or two to actually get them to the dealers.

## *POCSAG MONITORING WITH POC32ENG.EXE*

In a previous issue I commented about a Windows based program that allowed monitoring of most POCSAG paging systems. Despite several attempts, I couldn't get it to work using the serial port described in the scanty docs that were provided. I finally tracked the author down and downloaded the newest version. As it turns out, running the program under NT and / or some pentium boards will present some limitations. In my case the solution was to use the sound board as the interface, feeding the audio taken from my 2006's discriminator to the line input of the Sound Blaster. This program allows you to actually look at certain pagers, or exclude certain pagers. Listed below are a few actual pages just so you can see what kind of things are actually passed along!

```
3/30/97 5:38 PM      CH1    2400    0410267       0
(Alpha) HABLA PACO, FINALMENTE HE LLEGADO A
MI CASA, YA REGRESA, PARA QUE TE CUENTE
TODO LO QUE ME HA PASADO.

3/30/97 5:40 PM      CH1    1200    1044845       3
(Alpha) MAR 30 at 21:50 TEST PAGE SEQUENCE
NUMBER 5721 (THE QUICK BROWN FOX JUMPED
```

OVER THE LAZY DOG)

3/30/97 5:41 PM CH1 1200 1491689 2
(Alpha) are you O.K. i didn't get your message it cut out i love you if you need me call

3/30/97 5:45 PM CH1 1200 0771541 3
(Alpha) PLEASE COME HOME ASAP - I'M HORNY FOR YOU - KRIS

## URL DE WI2Q

http://www.martin-lynch.co.uk/start.htm

## POTPOURRI DE N2NOV

455.6125: Simplex for WABC-TV news camera/microwave control
450.975/455.9875: WFM WNYC-FM audio feedback in stereo
450.7875: Simplex with traffic report taping/cuing (WALK-FM?)
450.2875R: WCBS-TV audio feedback
450.3875R: WNBC-TV audio feedback
450.8125R: Metro Traffic
450.2375R: Spanish? Greek? Arabic? Too fast a voice/not too many words to decipher
450.7750R: "Set-up on 33rd Street"; "Unit 15 to Desk"; "ENG 2 to Desk" (ABC Sports?)
450.1375R: WEAK! (NBC News?)

## AM BCB DX NEWS

AM 1205 Radio Cayman (Note...this operation is NOT an endangered station contrary to previous reports. Demand to keep the facility on the air has been great enough to justify needed equipment repairs and upgrades.)

## HF FAX STATIONS YOU CAN HEAR !

USN Cutler NAA: 10865 (1) up till midnite 8080(2) 3357(3)
USN Keflavik NRK: 9318.5 (1) fades rapidly after 2200z.
USCG Boston NMF: 9110(1) usually OK at nite
USN Rota AOK: 7595(1)nite 9050(2)nite 10542 (3) day.
USAF Rosie Roads (day) 15781(1) 19363(2) 11622(3)
USAF Rosie Roads (nite) 7398(1) 7870(2) 4855(3)
Madrid Met 6918.5 (1) now becoming less usable at nite.
Halifax Metoc CFH: 10536(1) slow fade past midnite 4271(2)
Bracknell GFA / GFE: 8040(1)day 2618.5 (2) nite. 4610 nearly always multipathed.
Northwood GYA: 6452.5(1) daytime 4307 (2) nite 3652 (3) 8331(4) daytime
Melbourne Met AXI / AXM: 5110(1) around 1900z.
Moscow Met 53.6(1)
Hamburg 7880(1) multipath after dark!

## ANARC Shortwave Search On The Web!

http://www.anarc.org/naswa/swlguide/

## ANONYMOUS NYPD INFO

The following is a list of frequencies used by the NYPD Narcotics Buy N Bust Unit?? not too sure of the unit name. but here goes... they are probably very low power.. @ 1/2 watt all PL is 173.8 simplex

| | |
|---|---|
| *Channel 1* | *473.9375* |
| *Channel 2* | *473.7125* |
| *Channel 3* | *473.6875* |
| *Channel 4* | *470.9375* |
| *Channel 5* | *470.1375* |

Bust and buys have also been monitored on 470.7875 and the Queens portable freq.(sorry can't remember it off the top of my head at the moment.

## TIME MAY CEASE TO EXIST IN AUSTRALIA !

VNG, Australia's HF Time and Standard Frequency Service that operates on 2.5, 5, 8.638,12.984 and 16 Megahertz may close due to a lack of Funds. It is very unlikely that enough donations from the public will be found to save the station.
Stephen VK5VKA

## DE Eddie Muro, KC2AYC

1) I heard the Omaha 67 copter on Wed night at about 6:30PM on 165.240.

2) There is a club that I have been writing for now for 2 years. It's the All Ohio Scanner club. Don't let the name fool you we cover states from Main to Virginia and then West to Ohio. We put out a 50 page newsletter 6 times a year and have tables set up at both the Winter SWl Fest in Kulpsville PA and the Dayton Hamvention. We also attend the Virginia Beach Hamfest and the open house/air show at the Oceana Naval Air Station in Virginia Beach. I write both the New York and New England Columns, while a fellow named Bob Scull writes the NJ column. Our web page URL is: http://aosc.rpmdp.com

3) A company called Quest Systems is manufacturing and marketing a fleet racking/management system called Questrack II.

Using a Motorola G.P.S. receiver and the Questrack software the system can be configured to meet a variety of fleet requirements. In addition, secondary vehicle systems such as Sirens, warning lights, and panic alerts can be monitored by the dispatch center.

Another outfit called Transportation Management Solutions is marketing their version of a fleet tracking system called AVL Secure-Trac. This system utilizes both G.P.S. and Cell phone technology to offer similar features.

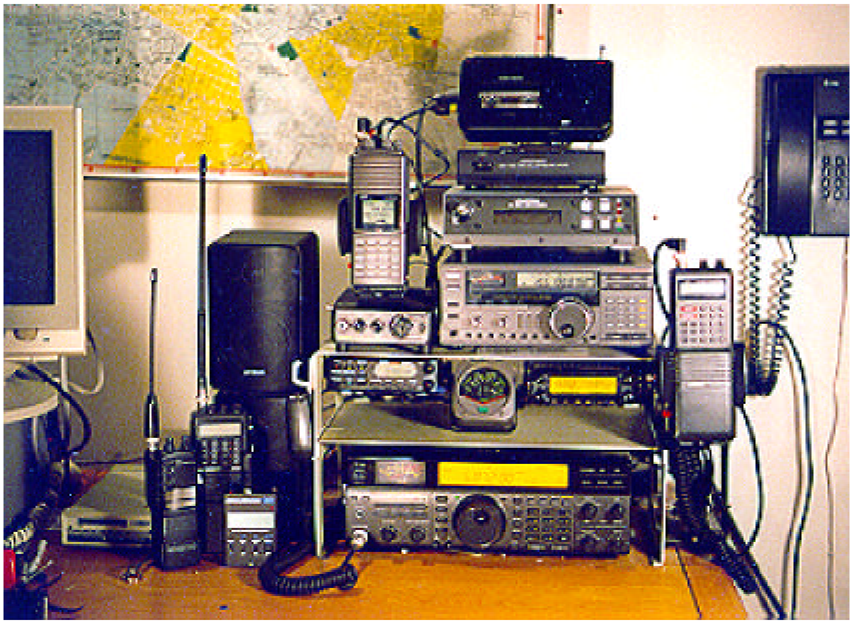
Standard Communications has introduced two new data-ready mobile trunked transceivers. The two new units will be compatible with both Motorola's Privacy Plus and E.F. Johnson's LTR trunking formats. The units can be programmed for either system with the use of a standard PC and the proper software.

Maxon has introduced a new mobile trunked radio, the TM-4800. This 15 watt unit is compatible with LTR systems and features both trunked and conventional compatibility.
The unit also offers both CTCSS and DCS.

73, Eddie Muro KC2AYC
E-mail: edmuro@sprintmail.com

## *AS I SEE IT de KB2SGJ*

Last issue I asked if some of you could share a picture of your shack / listening post with us. John Griffin, KB2SGJ of Hillsdale, NJ promptly sent me a photo of his shack. Here’s a good example of the efficient use of space!



KB2SGJ’s Listening Post