

Advertisement



GCN IT Leadership Conference
Learn Successful Strategies for
Deploying IT in Service of the Mission

May 24, 2006
Washington Post Conference Center

REGISTER NOW


[Login](#) | [Register](#)
 Search GCN GCN Quickfind

GO

[Current issue](#) | [▼ Subscribe](#) | [▼ Blogs](#) | [Events](#) | [eSeminars](#) | [White papers](#) | [RSS/XML](#) | [PostNewsweek Tech Media](#) | [▼ Visit our sites](#)
[GCN Home](#) > [web stories](#)

04/17/06 -- 04:04 PM

Wiretaps vulnerable to phreaking

You can't always believe what you hear

By [William Jackson](#), GCN Staff
[Story Tools](#): [Print this](#) | [Email this](#) | [Purchase a Reprint](#) | [Link to this page](#)

Researchers at the University of Pennsylvania have found that it is not at all difficult for bad guys to outwit law enforcement wiretaps on their phone lines.

A team of graduate students working with a National Science Foundation grant set out to determine just how trustworthy the most common types of telephone wiretaps used by police and intelligence agencies are, said Professor Matt Blaze.

The results of these taps are accepted uncritically by courts, Blaze said at the 2006 International Conference on Network Security being held in Reston, Va.

"It turns out, it can fail in all sorts of unexpected ways," he said. "Either party can disrupt a wire tap or introduce misleading information into the legal record."

The techniques exploit vulnerabilities in the single signaling and audio channel used in analog telephone systems.

Blaze said the project was an attempt to establish some baselines for network security by assessing how easy it is to conduct reliable eavesdropping on the century-old protocols used in analog voice phone systems. End-to-end cryptography often is seen as the most certain way to secure a communications channel. But almost nobody uses that for voice conversations because of the complexity. And, as it turns out, it is not necessary.

The most common technology for tapping a phone line is a loop extender, which is a one-way bridge from the target subject's local loop to the phone line of the listening station. The great majority of wiretaps are pen register taps, which record only the telephone numbers dialed by the target and when the calls are made. Only about 10 percent of taps actually record the content of calls. Both types use the same equipment.

But the caller can game the police equipment by using a notebook computer to fine-tune the pulse tones generated to dial a number. By tuning them properly, the correct numbers will be accepted by switching equipment at the caller's central telephone office, but tones often will be misinterpreted on the police equipment, producing meaningless numbers.

Techniques similar to the old phreaking tricks used to steal long distance service can be used to turn off a wiretap recorder remotely. A signaling tone can be sent on the line that will fool police equipment into thinking the

Advertisement



THE RELIABLE HP PROLIANT
BL20P G3 BLADE SERVER

featuring the Intel® Xeon® Processor
and HP Systems Insight Manager.





Now with \$250 in instant savings.

» STORAGE INFO » SAVE NOW

Most Read Articles on GCN.com

[Past 24 hours](#) | [Last 7 Days](#) | [Last 30 Days](#)

- **Enterprise Application Software: For Web development projects, Studio MX is the stuff of dreams**
- **Toot your horn, and increase traffic to your Web site with portals**
- **Army announces ITES2 awards**
- **Army issues statement of work for ITES-2**
- **Homeland IG takes FEMA to task**

[Go to complete list](#)

Most E-Mailed Articles on GCN.com

[Past 24 hours](#) | [Last 7 Days](#) | [Last 30 Days](#)

- **EXECUTIVE SUITE: CIOs — Be true to your name**
- **Streaming desktops: Don't call them thin**
- **Hacking Bluetooth**
- **A menu of Bluetooth attacks**
-

[Go to complete list](#)

Advertisement

You can't always believe what you hear

phone is back on the hook, causing the recorder to shut off. Blaze played a demonstration tape in which the participants were able to continue a conversation after the police equipment had "hung up." The same technique can be used to block police equipment from recording the number being dialed and to inject a phony number later.

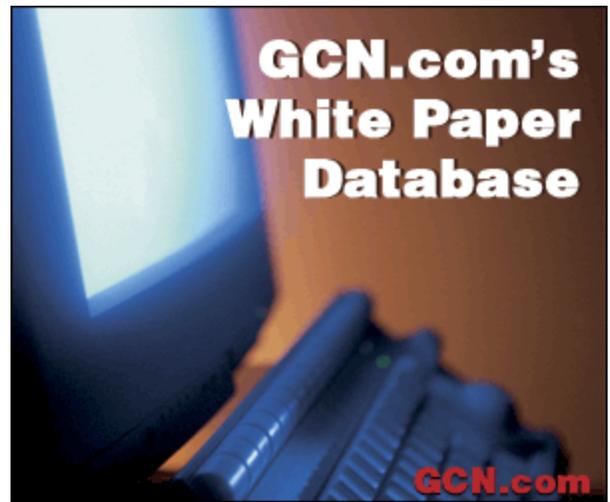
The 1996 Communications Assistance for Law Enforcement Act required vendors to include a wiretap interface in telephone switching equipment, which would theoretically thwart these tricks. But most vendors made their switches backward compatible to work with legacy loop extender equipment that police continue to use. This reintroduced the same vulnerabilities when using a CALEA interface.

This is an object lesson for software developers, Blaze said.

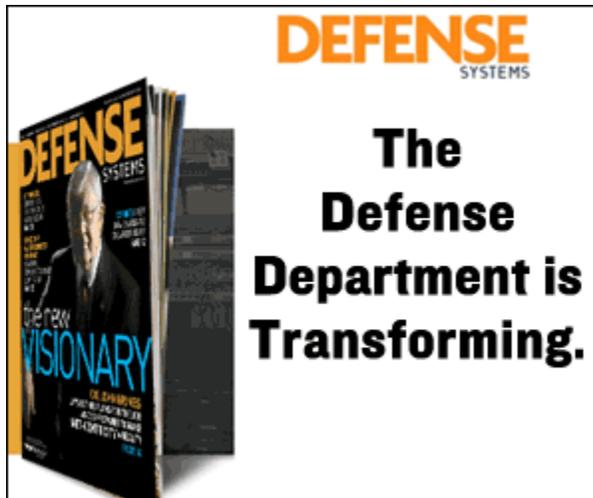
"We have to [be] careful about how backward compatibility can mean compatibility with old bugs," he said.

Blaze said there is no concrete evidence that these techniques have been used to thwart legitimate wiretaps. But he said court records show that anomalies in recorded conversations often are accepted as inevitable by police and the courts, leaving open the question of how trustworthy those recordings are.

More news on related topics: [Communications / Networks](#), [IT Security](#), [Homeland Security](#)



Advertisement



MARKETPLACE

Products and services from our sponsors

■ Security Within - Configuration based Security

Configuration and policy based security systems are a pro-active way to defend against IT security attacks. Click here to request our white papers, "Security Within - Configuration based Security" and "Policy Management vs. Vulnerability Scanning".

■ System Management for new Enterprise environments

Request white paper which outlines the case for an IT Portal architecture to meet the new requirements placed on IT management. These requirements include IT security; FISMA compliance; managing outsourcing contracts; and more.

■ Automating the FISMA process

Click here to request our white paper, "Automating the FISMA Process", which describes how automated systems such as BelSecure can help U.S. Federal government agencies comply with the FISMA security process.

■ Software License control, Windows XP/2000 Upgrades

Use your Intranet to manage Software Licenses, plan for Windows XP/2000 upgrades, do Security Audits and more. Click to try and ask for our white paper - PC Management for the Internet Age.

■ Policy Management vs. Vulnerability Scanning

You can't always believe what you hear

Which is right for you? Vulnerability scanning products test for known vulnerabilities. Policy management products are pro-active by locking the doors in advance of a possible attack. Click to request our white paper.

[View more products and services...](#)

[Buy a link now](#)

[Home](#) | [About GCN](#) | [Contact GCN](#) | [Customer Help](#) | [Privacy Policy](#) | [Careers](#) | [Editorial Info](#) | [Advertise](#) | [Link policy / Reprints](#) | [Site Map](#)



© 1996-2006 Post-Newsweek Media, Inc. All Rights Reserved.