Researchers Warn Against Potential Flaws in Wiretapping Technology

December 1 2005

As part of a federally funded program on electronic security, engineers at the University of Pennsylvania have discovered flaws in wiretapping technology that could allow parties being wiretapped to disable the recording and monitoring of their calls.

The Penn researchersfindings will enable law-enforcement agencies to detect and compensate for the flaws. Using publicly available information and surplus interception devices including enregisters that record dialed numbers, the researchers were able to reverse-engineer wiretapping protocols and devise several means of confounding them. According to the researchers, a simple tone transmitted over the phone line by the monitored party can trick wiretap devices into believing that the tapped phone is still on the hook, thereby disabling recoding equipment.

"If we could figure out these flaws so easily, it stands to reason that motivated wiretap subjects have as well," said Matt Blaze, a professor in Penn's Department of Computer and Information Sciences and lead researcher in the project. "Fortunately, these flaws can at least theoretically be fixed in the more recent wiretap systems. Those that are vulnerable may be able to be re-configured to prevent such countermeasures."

The researchers are part of the Trustworthy Network Eavesdropping and Countermeasures project at Penn, funded through the National Science Foundation's Cyber-Trust program. Their findings are to be published

Dec. 1 in the journal IEEE Security and Privacy.

"Legal wiretaps are widely-used tools for both law enforcement and national security. Thousands of federal, state and local agencies conduct wiretaps," Blaze said. "If they are to be truly useful, we need to find any exploitable flaws in the systems currently in use and create ways to fix them.According to Blaze and his colleagues, it is not just the law enforcement community that has a stake in the security of wiretapping technology.

ny questions about the reliability of information obtained by wiretap has implications for both the legal and technological communities,Blaze said. iretap evidence introduced in court, for example, may need to be examined for any telltale signs of signaling countermeasures before it is accepted.There are two general types of wiretap technologies used by U.S. law-enforcement agencies. The first are called loop extender taps and the second, more modern, types are known as CALEA taps.

Loop extenders are the most basic and oldest form of wiretap technology. They involve a direct connection between the subject's phone line and the law-enforcement agency.

The CALEA tapping technology named after the federal 1994 Communications Assistance for Law Enforcement Act mandates a standard interface between telephone-service providers and law enforcement. In CALEA taps, the telephone company decodes the signal and, when authorized, separates the call to a channel accessible by law enforcement.

Among the vulnerabilities Blaze and his colleagues noted, the loop extender taps are easily confounded by a simple two-frequency audio tone that phone systems use to determine if a particular line is idle that is, when the phone is on the hook. Automated recording equipment then

assumes that the line is not in use and therefore does not record. They also noted techniques to manipulate dialed-number recorders that make false or incorrect numbers appear in call logs. Such logs should be examined for discrepancies, the researchers said.

While at first glance, CALEA seems secure against these manipulations, many of the vulnerabilities can extend there as well. The CALEA system involves two separate channels: one for data signaling and the other for voice content. Some CALEA systems are configured, however, so that they also respond to the two-frequency idle tone over the voice content channel.

"While there is relatively little that can be done to make the loop-extender technology more secure, it may be possible to configure some CALEA systems to better withstand these countermeasures," Blaze said. "It is a matter of programming them not to shut off when the voice channel hears the idle tone. Instead, the system should rely only on the data channel for that information."

Blaze and his colleagues recommend that law-enforcement agencies and telecommunications companies confirm settings of CALEA equipment withvendors.

Co-authors of the paper include Micah Sherr and Eric Cronin of Penn and Sandy Clark of Princeton University.

More information is available at www.crypto.com/papers/wiretapping/

Source: University of Pennsylvania