Signaling vulnerabilities in wiretapping systems[*]

Micah Sherr[†], Eric Cronin, Sandy Clark[‡], and Matt Blaze
University of Pennsylvania
Contact: Matt Blaze, blaze@cis.upenn.edu

8 November 2005

Abstract

Telephone wiretap and dialed number recording systems are used by law enforcement and national security agencies to collect investigative intelligence and legal evidence. In this paper, we show that many of these systems are vulnerable to simple, unilateral countermeasures that allow wiretap targets to prevent their call audio from being recorded and/or cause false or inaccurate dialed digits and call activity to be logged. The countermeasures exploit the unprotected in-band signals passed between the telephone network and the collection system and are effective against many of the wiretapping technologies currently used by US law enforcement, including at least some "CALEA" systems. Possible remedies and workarounds are proposed, and the broader implications of the security properties of these systems are discussed.

1 Introduction

Voice telephone interception systems are used by law enforcement agencies in the United States and elsewhere to collect "wiretap" evidence and intelligence against criminal and national security subjects. Such systems provide a legal record of the digits dialed by the subject and, in some cases, the audio contents of the calls themselves. Wiretapping is often credited as an essential tool in the investigation and prosecution of serious crime, especially where complex criminal enterprises and conspiracies are involved.

Unfortunately, however, many of the telephone interception technologies that law enforcement depends upon for evidence collection are less reliable than previously thought. We found that the design and implementation of these systems often render them vulnerable to simple, unilateral countermeasures that allow wiretap subjects (or their correspondents) to prevent accurate and complete capture of their call data and contents. The countermeasures exploit the "in-band" signals passed between the telephone network and the law enforcement agency.

In particular, the evidence collected by virtually all interception systems based on traditional "loop extender" technology, as well at least some systems based on the newer "CALEA" interfaces, can be manipulated by the subject using practical techniques and readily available hardware. We found one countermeasure, requiring only a standard personal computer, that prevents the accurate recording of dialed telephone numbers

[*] © 2005; all rights reserved. A version of this paper appears in *IEEE Security and Privacy*, November/December 2005. The current version of this paper can be found at http://www.crypto.com/papers/wiretapping/.

[†] Authors listed in reverse alphabetical order.

[‡] Visiting from Princeton University

and line status signals. Perhaps more seriously, we also found simple countermeasures that effectively and selectively suppress the recording of call audio with only modest degradation of call quality.

Unlike traditional wiretap countermeasures (such as encryption), our techniques are entirely unilateral – they do not require active cooperation between subjects and their associates – and they obscure not only the content but also the "meta-data" that indicates the presence of communication and that identifies the communication endpoints, in a way that is sometimes difficult to detect. This has implications not only for the accuracy of the intelligence that can be obtained from these taps, but also for the acceptability and weight of legal evidence derived from it.

The analysis in this paper was based entirely on information obtained from published sources and equipment purchased openly in the retail and surplus markets. It is therefore possible (and perhaps even likely) that these techniques have already been discovered and actively employed by motivated wiretap targets, e.g., in organized crime. We recommend that currently fielded telephone interception systems be evaluated with respect to these vulnerabilities and re-configured or modified where possible to reduce their susceptibility. In addition, the possibility of these or similar countermeasures should be considered in analyzing previously collected wiretap evidence and intelligence.

Despite law enforcement's growing reliance on wiretaps, little attention has been paid in the open literature to their reliability. This paper, in fact, may represent the first analysis of the security of modern telephone wiretap systems by the computing and communications research community. Drafts of this paper have been made available to the law enforcement community.

1.1 Wiretapping and US law

Broadly speaking, there are two categories of telephone wiretaps that can be authorized for use by United States law enforcement agencies under Title III [7] and FISA [8] (the federal laws governing electronic surveillance for criminal and national security investigations, respectively).

The first category, called a *Dialed Number Recorder (DNR)* or *Pen Register,* records the digits dialed and other outgoing signaling information, but not the call's audio. DNR taps, which provide "traffic analysis" information but not the call contents or speaker identity, must pass only relatively modest judicial scrutiny to be authorized. A related investigative technique, called a "trap and trace," provides analogous information about incoming calls.

The second category, the *Full Audio Interception* (sometimes called a *Title III* or *FISA* wiretap depending on its legal context), records not only the dialed digits and signaling but also the actual call contents. Legal authorization for full audio interception taps entails a higher standard of proof and greater judicial scrutiny. These taps are also more expensive (and labor intensive) for the law enforcement agency than DNR taps because they generally require continuous real time monitoring by investigators.

In practice, although the legal requirements for, and information collected by, the two kinds of legal wiretaps varies widely, the same equipment can be used to implement both, with audio capture features that can be disabled for DNR-only taps. There are two wiretapping technologies commonly available to law enforcement agencies: *loop extender taps* and *CALEA taps*.

1.2 Wiretapping technology

Communication evidence is not produced exclusively by wiretap interceptions; some investigative functions are served by examining telephone accounting and billing data collected by the carrier. Law enforcement agencies occasionally subpoena telephone records and use them as a source of intelligence or evidence. These are not, strictly speaking, "interceptions" for the purposes of this paper; they are distinguished from the wiretaps considered here in two ways. First, they are inherently "retrospective" – they report on the subject's *past* telephone activity rather than on future activity. Second, they are not ordinarily available to the law enforcement agency until sometime after the activity has actually occurred. DNR and full audio wiretaps, on the other hand, are "prospective," reporting communication occurring *after* their installation, and typically in real time or near real time.

Real time interceptions, as noted above, may collect either signaling data or full audio, but either of the modern tapping technologies discussed below can be configured for either kind of tap.

1.2.1 Loop extender taps

The most basic, and oldest, wiretap technology involves a direct electrical connection between the subject's telephone line and a second line terminating at the law enforcement agency. Such a connection (literally a "tap") can be made anywhere along the length of the "local loop" serving the subject, in the telephone switching office, or in the subject's premises. In principle, no special hardware is required for such interceptions at the tap point; it is sufficient simply to "splice in" a pair of wires leading back to the law enforcement agency's facilities. To ensure proper isolation and level equalization of intercepted content, however, current law enforcement practice for such taps uses a small device, called a *loop extender* or *dialup slave,* at the splice point. The device sends any audio on the subject's line to the law enforcement line, re-encodes signals, and performs level equalization. DNR equipment at the law enforcement agency decodes the dialed digit and call activity signals and, when configured for a full audio interception, also records the voice contents of the calls.

To tap a line with a loop extender, a voice-grade telephone line (either a dedicated leased line or regular dialup line), controlled by law enforcement and terminating at the law enforcement agency, is provisioned in such a way that it shares at least one cable splice point with the subject's line. (In wiretap parlance, the subject line is called the *target line* and the law enforcement line is called the *friendly line.)* See Figure 1. The target line is physically tapped and connected to the friendly line through a loop extender (or dialup slave) device[1]. Any detected signals (and audio content when authorized) are decoded and logged by the law enforcement agency equipment at the other end of the friendly line.

Because loop extenders can intercept only wireline ("POTS") telephone lines, the technology has been largely supplanted in the United States by the *CALEA* systems described in the next section. However, analog loop extender systems remain on the law enforcement market, and some agencies still rely on them for some or all of their interceptions.

1.2.2 CALEA taps

The second, newer, wiretap technology was designed to comply with the U.S. 1994 Communications Assistance for Law Enforcement Act (CALEA) [1]. CALEA mandates a standard interface between telephone service providers (including wireline and cellular services) and agencies that perform wiretaps. In CALEA taps, the telephone company (not the law enforcement agency) decodes the signaling information and, when a full audio intercept has been authorized, separates out the call audio to its own channel. The law enforcement agency connects to the telephone company through a standard interface, defined in J-STD-025A [27], in which the signaling information (including dialed digits, on-hook/off-hook status, and so on) and call

[1] The terminology is not completely standardized, but most vendors use the term "loop extender" to refer to a device that uses a leased line for the friendly line and the term "dialup slave" when the friendly line is a regular telephone line. For simplicity, we will use the term "loop extender" to refer to either arrangement.

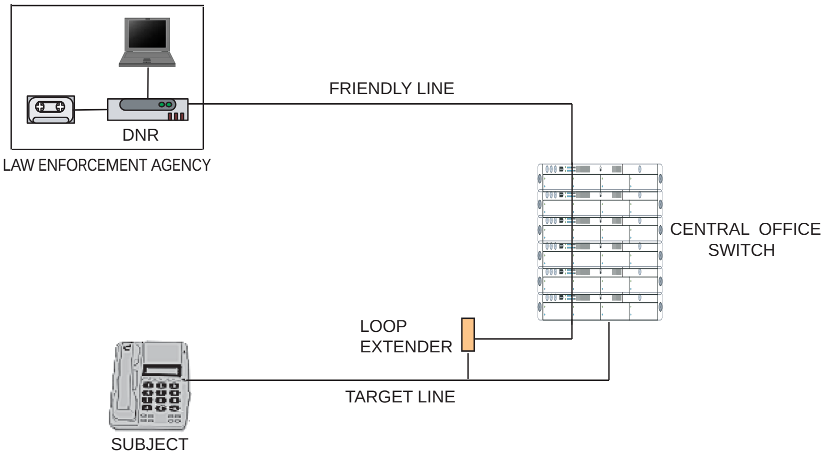

Figure 1: *Loop Extender wiretap architecture*

audio are sent to the agency over separate channels. While CALEA applies only in the United States, J-STD-025A-compliant switches and interception products are marketed in other countries as well.

Each law enforcement agency conducting a J-STD-025A interception leases one or more telephone lines between the agency facilities and the target's telephone switch. See Figure 2. The first of these lines carries a *Call Data Channel (CDC)* that reports the signaling data (call times, numbers dialed, line status, etc.) associated with all lines being monitored by the agency at that switch. Additional lines to the law enforcement agency carry *Call Content Channels (CCCs)* that contain the live audio of any active monitored lines for which a full audio interception has been authorized. The CDC may carry call data for more than one active tap, and although a single CCC can carry only one call's audio at a time, a particular CCC may carry audio for different subjects at different times, with CCCs dynamically assigned as lines become active (with the assignment reported over the CDC).

The J-STD-025A standard specifies the messages sent on the CDC as well as a several different delivery formats for CDC and CCC channels. The simplest (and, we understand, most widely deployed at this time) CDC and CCC arrangement is via standard analog ("POTS") telephone lines or 56Kbps ISDN bearer channels. However, the CCC and CDC may also be delivered with IP packets over a secure VPN.

Once a CDC (and, when needed, one or more CCCs) has been provisioned between a switch and a law enforcement agency, installing a tap on a new line is simply a matter of configuring the CALEA delivery system at the switch to report activity on the target line. Although telephone companies are free to implement the J-STD-025A interface any way they wish, in many systems no special physical connections to the local loops of the target lines are required.

1.3 Previous work and wiretap threat models

Perhaps surprisingly, there does not appear to be a widely agreed upon threat model against which law enforcement wiretap systems are measured.

Most scientific and engineering research in communication security views the *eavesdropper* as the adversary and is therefore concerned with guaranteeing that an abstract and powerful eavesdropping attack will fail. This perspective, while generally useful, does not readily apply when the threat is reversed to make

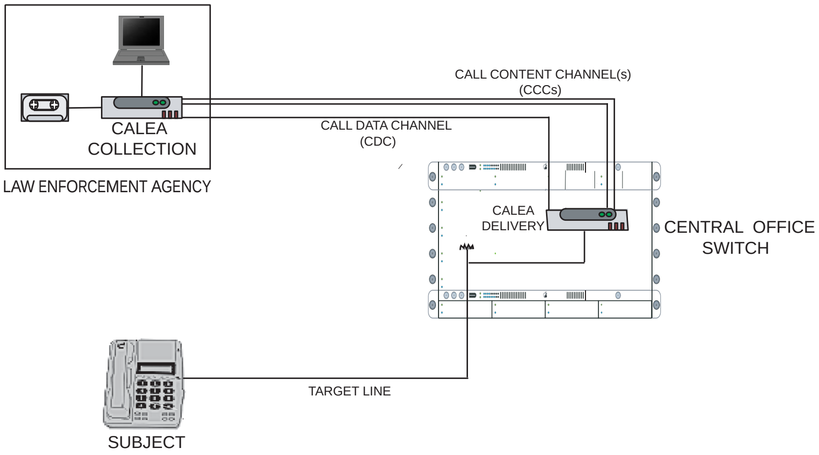

Figure 2: *CALEA wiretap architecture*

the communicator the adversary.

The most mature area of existing work that examines the effectiveness of eavesdropping does so from the perspective of digital network intrusion detection. There, the focus is on thwarting eavesdropping countermeasures such as *evasion* and *insertion* [19, 24, 16]. However, unlike network intrusion detection systems, telephone wiretaps aim to capture data about *all* communication, both normal and anomalous.

1.3.1 Detection

Perhaps the most prominently considered threat against eavesdropping systems is *detection.* Surreptitious interceptions are thought to produce better intelligence than those that are not. There is a vibrant, if occasionally somewhat disreputable, "technical surveillance and countermeasures" (TSCM) industry fueling both sides of a bugging and bug-detecting arms race.

Wiretap systems that depend on direct metallic connection to the local loop (such as loop extender systems) are potentially susceptible to detection by a range of means. A tapping device that is installed at or near a subject's premises might be noticed in a physical inspection. Depending on the circuitry used, taps that change the transmission characteristics of the line can sometimes be discovered electronically, e.g., through sensitive loss measurements or time domain reflectometry. Taps might also be exposed through penetration of telephone company information systems or facilities, e.g., via rogue insider access, computer compromise, or physical burglary. Loop extenders marketed to law enforcement agencies usually have an relatively innocuous physical appearance and high impedance circuitry, although, depending on how and where they are installed, an expert may still be able to detect their presence.

J-STD-025A has specific requirements that switch-based CALEA monitoring be undetectable to the subject and that the computing systems that provision and maintain interceptions be adequately secured. However, specific security mechanisms are not prescribed by the standard, and no special protection or authentication is required for the CCC and CDC traffic or links.

1.3.2 Encryption and content obfuscation

The most well-understood countermeasures against eavesdropping involve the use of cryptographic techniques, and modern cryptosystems are thought to provide very good end-to-end security when implemented properly. However, voice encryption is not widely used by wiretap subjects. Digital voice encryption systems for analog telephones are not yet readily available on the commercial market, and require the participation of both parties to be effective. Also, end-to-end encryption protects only the content, not the dialed numbers and other signaling (because the endpoint of the signaling is the phone network itself, not the called party).

1.3.3 Denial of service against CALEA CCCs

At least one practical countermeasure against CALEA / J-STD-025A call content collection has already been discovered by the law enforcement community and the telecommunications industry. The countermeasure prevents the collection of subject call content on systems with dynamically assigned CCCs and exploits the fact that the number of different voice channels associated with a monitored line is potentially unbounded if the subject subscribes to a "call forwarding" service. First, the target and target's correspondents "flood" a monitored line with unrelated calls that are forwarded elsewhere. (The number of forwarded calls is bounded only by the switch's call forwarding limits.) Each additional call is assigned its own CCC, eventually leaving no CCCs open for monitoring significant calls.

Although CALEA was motivated partly by new services such as call forwarding, this countermeasure was apparently not considered in developing the original CALEA interfaces. The problem was first publicly suggested in recent patent disclosures [12, 18] for systems that allow the law enforcement agency to disconnect superfluous CCCs. (This capability is not addressed in the J-STD-025A standard.) The published literature says little about whether wiretap subjects have actually employed CCC flooding countermeasures, or whether currently fielded CALEA systems incorporate the defenses described in the patents.

CALEA systems might also fail if the telephone company provisions the tap to monitor the wrong target line. A recent report from the US Department of Justice reported that there were instances of recorded traffic from FISA taps later discovered to have originated from incorrect sources[14].

1.3.4 Evasion, confusion, and the eavesdropper's dilemma

In a previous paper [4], we formalized the concepts of *evasion* and *confusion* as eavesdropping countermeasures, and identified the "eavesdropper's dilemma" as a fundamental tradeoff in certain interception architectures. Briefly, evasion occurs when a target can prevent legitimate traffic from reaching the interception system, and, conversely, confusion occurs when spurious traffic can be directed at it. If a system is susceptible to either countermeasure, the fidelity of the intercepted traffic can be arbitrarily degraded, either by the target or, in some cases, by a third party. The architecture of many eavesdropping systems allows defending against evasion or confusion only at the expense of increased exposure to the other; hence the "eavesdropper's dilemma."

An interception system is subject to the eavesdropper's dilemma whenever it has incomplete knowledge of how traffic is processed by the network and by the receiver, or if it destroys information processed at low layers of the protocol stack.

Although confusion, evasion, and the eavesdropper's dilemma were introduced in the context of digital network interception, they can be applied readily against the analog law enforcement wiretap systems described in this paper.

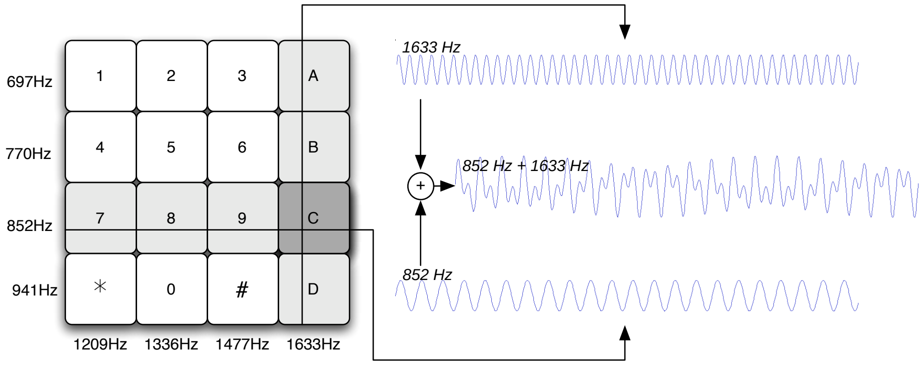

Figure 3: *DTMF Keypad and waveforms of generated tone*

2 Signaling countermeasures against loop extender taps

Loop extender taps rely heavily on in-band signaling, with an architecture that makes them especially vulnerable to manipulation by the target. We found three kinds of practical countermeasures against systems that use these taps. The first masks the dialed digits of outgoing calls. The second obscures incoming caller-ID signals. The third, and perhaps most serious, disables audio monitoring and recording by the agency.

2.1 Dialed digit spoofing

A fundamental weakness in the loop extender tap model arises from the way dialed digits and other audio signals are decoded by the tapping equipment. Telephone number signals, although they represent "digital" information, are transmitted on telephone lines in analog form. The most common dialing system uses audio *Dual-Tone Multi-Frequency (DTMF)*[23, 11] signals. DTMF is also popularly known by its original AT&T trademark, *TouchTone.* The analog DTMF signals are decoded and converted to digital form at the telephone company switch.

DTMF digit signals consist of two audio frequency tones, a "low" tone corresponding to the horizontal "row" position of the digit on the keypad and a "high" tone corresponding to the "column" position. While the familiar consumer telephone DTMF keypad has 12 digits (0 through 9, * and #) arranged in four rows and three columns, the DTMF standard specifies a fourth column, giving four additional tone signals, usually called "A," "B," "C," and "D." The "C" button, for example, is conceptually located to the right of the "7," "8," and "9" buttons. See Figure 3. (The forth column tones will be important to us in Section 2.3.)

Although most telephone instruments produce tone signals well within the "standard" acceptable range of properly operating DTMF decoders, signals at the edge of the standard will be accepted by some decoders but not by others. Many parameters affect whether a given tone signal will be recognized as a valid dialed digit by a given decoder, including the precise frequencies of the two tone components, their overall power level, the relative amplitude of the tones, signal duration, waveform distortion, external noise, and so on.

Two observations follow directly from the analog nature of DTMF signals and their decoding by telephone switches.

Observation 1 ("The Analog Eavesdropper's Dilemma"): Because DTMF transmission and decoding are analog processes, for any given parameter (frequency, amplitude, etc.), no two DTMF decoders will use precisely the same threshold to determine whether a given signal is accepted or rejected.

Observation 2: By completing or not completing dialed calls, a telephone switch is an oracle for determining whether DTMF signals sent to it have parameters within its tolerances.

We found that by systematic DTMF dialing with selectively degraded parameters, analog telephone subscribers can discover the thresholds of their switches' DTMF decoders efficiently and with sufficient accuracy and precision to construct signals likely to be treated differently by other decoders.

In a loop extender wiretap system, two different DTMF decoders process each dialed digit on the target line independently: one at the law enforcement agency (to determine the dialed number that is logged) and another at the telephone company switch (to determine the number used for actual call processing by the telephone network). This means that for each tone parameter of each digit, either there are tone encodings that are accepted as valid by the switch but not the wiretapper or there are encodings that are accepted as valid by the wiretapper but not the switch.

Note that this property is inherent to *any* interception system in which a separate DTMF decoder is used at the tap; it does not depend on the failure of any equipment to operate within standard specifications.

In our experiments, a simple, automated binary search (involving about 30-120 minutes of unattended experimental dialing and analysis with a laptop computer) could discover the precise threshold characteristics of a given telephone switch's DTMF decoder with sufficient accuracy to distinguish it from other decoders. Spurious digit encodings can then be constructed that are just *outside* the accepted parameters of the switch's decoder (such that they would have no effect on the actual number dialed) but that will be accepted with high probability by an external law enforcement tap. These signals thus attempt to "confuse" a tap. Conversely, non-standard digit encodings can be constructed that are just *within* the parameter range accepted by the switch but that will be ignored with high probability by an external law enforcement tap. These signals thus attempt to "evade" a tap.

Of course, this probe discovers nothing about the limits of the *wiretap's* DTMF decoder (or even if a wiretap is present), but it does not need to. Because of the analog eavesdropper's dilemma, and as our experiments confirm, a wiretap's decoder will always be either more *liberal* or more *conservative* than the switch in handling signals at the edges of acceptance. When a wiretap is conservative, digit signals accepted by the switch evade detection by the tap. When a wiretap is liberal, it accepts extraneous confusion digit signals that are ignored by the switch.

Complete telephone numbers can be dialed with a combination of evasion digits and confusion noise, such that the complete, correct number will be received as intended at the switch but where some or all of the digits recorded by the tap are incorrect. (Depending on the exact hardware at the switch and the tap, the tap will predominantly tend to either ignore evasion digits or accept confusion digits. Whether confusion or evasion dominates cannot be predicted by the subject without access to the tap hardware, but incorrect numbers are logged by the tap in either case.) The software to perform the probing and the dialing can be quite simple, and only modest computer, sound card and modem hardware are required.

A wiretap can never reconstruct evaded digit signals that it ignores by being too conservative. The obvious defense against evasion is therefore to use a more liberal decoder at the tap.

Unfortunately for the wiretapper, an interception system that is too liberal becomes susceptible to confusion. Although an overly liberal decoder might seem intuitively a "lesser evil" than one that is overly conservative (since fewer potential digits are discarded), in fact confusion can achieve perfect secrecy under ideal conditions. See the Appendix A for a perfect secrecy scheme based on confusion.

Confusion and evasion dialing are effective against any eavesdropping system that performs its own DTMF decoding and commits to a single interpretation of the digits. In a full audio tap, it may be possible to later conduct offline forensic analyses of recorded tone signals and reconstruct evaded or confused digits. However, such an analysis would depend on the precise tolerances of the local central office and the transmission characteristics between the tap and the subject at the time of the call. Deriving these parameters requires active probing from the tap, similar to that performed by the subject. Current wiretapping technology has no mechanism for performing such probes, and so precludes such analyses.

Of course, a subject cannot be sure whether an eavesdropper's DTMF decoder will be more conservative or more liberal than that of the switch for any given parameter, and so cannot be sure whether confusion or evasion will be more successful at masking dialed numbers. There is no need to make a choice between the two, however; confusion and evasion dialing can be used in concert with one another across an entire string of dialed digits.

Here, the subject intersperses n random noise digits in random positions among the l "true" digits to be dialed The true digits are signaled using evasion and the noise digits are sent using confusion.

This combined dialing technique is effective to the extent that *either* confusion or evasion dialing succeeds often enough to mask the actual dialed number. This, in turn, depends on the effectiveness of confusion and evasion dialing in practice. Our experiments with standard law enforcement loop extender tap hardware, as well as with taps we constructed based on laboratory and diagnostic DTMF signal analyzers, suggest that these countermeasures are both practical and reliably effective at hiding the true dialed number.

2.1.1 Dialing experiments

To test the practical effectiveness of confusion and evasion dialing, we conducted experiments under a variety of simulated network conditions and with a range of tapping hardware. Our results support our analytical hypothesis that confusion and evasion are effective at preventing DTMF digit recording in taps (such as loop extenders) that rely on their own DTMF decoders.

Our experimental setup is depicted in Figure 4. A central office (CO) switch simulator interprets DTMF tones from the "target" line (the simulated subject's phone line), generates call progress, ringing and caller ID signals, and switches calls. The subject line is equipped with both a normal telephone and a Pentium laptop computer with a modem, sound card and telephone audio interface. The laptop modem is used to seize the line, while confusion and evasion dialing signals are generated by the sound card. The telephone set is used for the actual voice communication.

To account for different telephone line and central office conditions, we ran our experiments with several simulated and actual telephone switches, including Teltone TLS-5C and Ameritec AM-7 simulators and the Western Electric / Lucent 5-ESS switch that serves one of the authors' homes. (The Teltone and Ameritec devices simulate most aspects of a telephone switch, decoding and generating all loop signals and providing voice paths; we simulated the loss and distortion of the local loop with Telebyte Model 453 variable length 26 gauge cable simulators.) Results were similar under all setups; data shown here used the Teltone simulator.

The primary tapping device in our tests was a Recall Technologies model NGNR-2000 (a current law enforcement loop extender DNR and audio collection system). We also constructed our own taps using various laboratory and diagnostic DTMF decoders. In all setups, every tap was able to correctly reconstruct all dialed digits when no countermeasures were employed.

The first step is determining the switch's limits. Although many parameters are defined for proper DTMF tones [11, 26], we concentrated on six: the amplitude of the high tone component (recall that a DTMF signal consists of a high frequency tone mixed with a low frequency tone), the amplitude of the low tone, and the positive and negative frequency skews of the high and low frequency tone components. Our probe software used a simple binary search for each parameter's limits. In each trial, a nonexistent number (say, `555-010X`) is dialed, with the parameter under test (e.g., the high tone frequency) varied on the last digit. If the entire dialed number was recognized by the switch (as indicated by a call completion signal) then the parameter was within the switch's tolerance. However, if the switch did not attempt to route the call

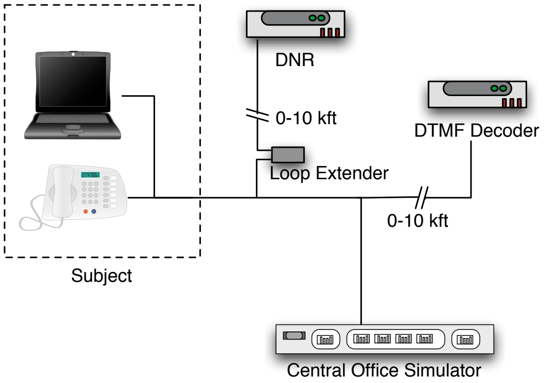

Figure 4: *Experimental wiretapping configuration*

(as indicated by a lack of response), then the parameter was outside of the switch's tolerance. The binary search narrows a pair of differentiating values for each parameter and each digit. Signals with the parameter value within the switch's tolerance can be used for evasion, while tones outside the tolerance can be used for confusion. This search is performed for all six parameters and for each DTMF digit (0 through 9). The entire automated probing process takes approximately 30-120 minutes to complete; it is re-run as needed to compensate for drift in the switch decoder hardware and changes in the transmission characteristics between the subscriber and the central office.

After probing the switch, we tested evasion and confusion dialing. Figure 5 shows the effects of evasion dialing alone. Here all digits were transmitted with evasion parameters, causing the tones to be barely recognized by the switch. As shown in the figure, although the switch received the full number and completed the call, only one of the wiretaps correctly captured all dialed digits.

Device	**Interpretation in the presence of evasion**
Recall model NGNR-2000 (DNR device)	`18753210`
Ameritec model AM8a	`1976541`
DSchmidt model DTMFLCD-2	`1976543210`
Harris model 25D	`19876543210`
Metro-Tel model TPM32MF	`1976541`
Metro-Tel model VNA70A	`19765421`

Figure 5: *DTMF reconstruction in the presence of evasion. The correct interpretation (as dialed by the subject and interpreted by the Teltone TLS-5C CO simulator) is* `19876543210`.

In this case, evasion was moderately successful; it prevented most of our taps from capturing at least one digit of the dialed number. Adding confusion, however, makes the eavesdropper's job even harder. In our next experiment, confusion signals were inserted uniformly at random among the evasion-dialed digits. For readability, we show here an experimental run in which the target sends 20 confusion digits along with the 11 digit number; more confusion digits would ordinarily be sent in actual countermeasures use.

The results of using both confusion and evasion are shown in Figure 6. As before, the switch correctly processed the desired number. All tested DTMF decoders were susceptible to both confusion and evasion, and not only failed to record some evaded digits, but also accepted some confusion signals. Confusion was particularly effective against the Ameritec AM8a, which recorded a total of 22 dialed digits. The number of possible 11 digit reconstructions of this string is approximately $\binom{22}{11} = 705,432$, and we note that not a single one of these interpretations is the actual dialed number, since some of the digits were evaded.

Device	**Interpretation in the presence of evasion and confusion**
Recall model NGNR-2000 (DNR device)	149876465642392120
Ameritec model AM8a	1346676649919555432610
DSchmidt model DTMFLCD-2	1497645432120
Harris model 25D	139876419556432610
Metro-Tel model TPM32MF	1476411543210
Metro-Tel model VNA70A	14876411543210

Figure 6: *DTMF reconstruction in the presence of evasion and confusion. The dialed number is* **1**734**9**66**87**6**6**4991695555**5**6**4**2**3**9**2**6**1**20**0**, *where* **bold** *digits were sent using evasion parameters and* light *digits were sent using confusion. The Teltone TLS-5C CO simulator received the correct number,* 19876543210.

2.2 Incoming Calling-Number ID spoofing

Calling-Number ID (CNID – sometimes referred to as “Caller ID”) is an optional feature offered by local exchange carriers that allows a subscriber to screen incoming calls. If CNID service is enabled on the called party’s line, the central office transmits the caller’s telephone number and, if available, the name associated with that account. The CNID information is relayed using in-band signaling between the first and the second ring signals. Special devices display the incoming calling number to the subscriber.

When CNID service is active on a target’s line, any wiretap device can also decode and record the source of incoming calls. Note that if CNID is not present, then loop extender taps must learn the caller’s number through some other mechanism (e.g., billing records).

Since the central office transmits the CNID data, evasion is not possible. However, a subject may trivially confuse the capture of the CNID transmission by injecting “counterfeit” signals on the line.

To confuse a wiretapper’s recovery of incoming CNID, we simply replayed periodically (through the sound card) a forged CNID audio signal while the target’s phone was on-hook. (We used a single static number for this purpose, but a more sophisticated subject could generate new signals each time.) In every case in our experiments, the wiretap decoded the forged signal instead of the legitimate CNID transmission when incoming calls were received (see Figure 7).

2.3 Line status spoofing and recording suppression

In-band signaling makes full audio loop extender taps especially vulnerable to countermeasures. It is possible for a subject to remotely disable any audio recording equipment (and cause the system to log line inactivity) for arbitrary periods during a call by spoofing the “on-hook” signal generated by a loop extender.

In loop extender systems, all signaling data and audio are sent to the law enforcement agency over a single channel (the friendly line), entirely in the analog, voice band domain. Any call progress and line status signaling data from the target that is to be processed or recorded by the law enforcement system must therefore be sent over the same channel that carries the target audio (“in-band”). This, as we shall see, is a rather fragile arrangement rich in potential for exploitation by the target.

Device	**No confusion** (baseline)	**With confusion**
Recall (model NGNR-2000) (DNR Device)	(987) 654-3210 Tony Soprano	(215) 898-5000 Matt Blaze
RadioShack Trim Phone with Caller-ID (model 43-3909A)	987-654-3210 TONY SOPRANO	215-898-5000 MATT BLAZE
Tempo (model ID'R Plus)	(987) 654-3210 TONY SOPRANO	(215) 898-5000 MATT BLAZE
US West Call Waiting ID (model CI-98)	987-654-3210 TONY SOPRANO	215-898-5000 MATT BLAZE

Figure 7: *Using confusion to forge CNID (caller-ID). The caller's actual telephone number and name are* 987-654-3210 *and "Tony Soprano", respectively. The forged CNID signal, introduced by the subject (the called party), is* 215-898-5000 *and "Matt Blaze".*

An intercept collection system must record several kinds of call processing signals from the target's telephone line. Some of these signals (including DTMF-encoded dialed digits, incoming calling number ID, and audible call progress signals such as dial tones, busy and audible ringing signals) are already encoded in the voice band audio domain as part of the standard telephone interface. These signals simply pass through the normal audio interface of the dialup slave and can be decoded entirely by the law enforcement hardware (although, as noted above, not always correctly). Other telephone signals, however – most notably the on-hook/off-hook state, rotary "pulse" dialed digits, and incoming call ringing signals – are not encoded in the audio domain on the target line but instead depend on the (DC) voltage and current on the wire between the central office switch and the target's telephone instrument. While these signals can be detected relatively easily by the dialup slave unit by observing the line voltage, they cannot simply be relayed back over the friendly line in the same form for processing by the agency (since that line's voltage and current maintain the connection through the telephone network between the loop extender and the agency itself). These signals are therefore encoded as special audio tones superimposed on the friendly line audio, and recognized and decoded as such by the law enforcement equipment.

The most important signal that is not already in the voice band audio domain (and from whose state many of the other DC signals can be derived) is the on-hook/off-hook status. Ordinarily, when the line is "on-hook" no target audio or other signals would be present on the line. This gives rise to a simple (and indeed, as we shall see, too simple) audio encoding of line status: an "idle tone" is sent continuously on the friendly line whenever the target line is detected in the "on-hook" state and removed when the line goes to the "off-hook" state. Most loop extender (and dialup slave) systems marketed to law enforcement use this scheme.

In fact, not only do virtually all loop extenders indicate line status with an idle tone, they almost all use the same *de facto* standard idle tone signal: the DTMF "C" digit (a two frequency audio signal consisting of 852Hz and 1633Hz). (Some literature mentions the use of the "A" tone for this purpose, but all current vendors of which we are aware use "C".) This is the only audio signal added to the friendly line by some dialup slave and loop extender products. (Other models also provide additional signals to indicate incoming ringing and periodic "keepalive" off-hook status signals, usually also using fourth column DTMF tones.) Because the on-hook/off-hook status signal is sent by the loop extender over the same channel that carries the target audio, legitimate indications of changes in target line status cannot be distinguished from an identical-sounding signal generated by the target while a call is in progress.

2.3.1 New call spoofing

Loop extender systems, which depending on in-band signals, can be manipulated by a wiretap subject. At any time during a call, the subject (or the subject's correspondent) can signal the end of the call and introduce a false new call record by sending the 852Hz+1633Hz DTMF "C" signal on the line during a call for long enough for the wiretap to detect an on-hook condition and register (incorrectly) that the current call has ended. At this point the subject can send additional DTMF and audible ringing signals to simulate a new call being placed (presumably to a different number), all the while maintaining the connection with the original correspondent.

Of course, sending a brief burst of C-tone does not by itself prevent the capture of the call content[2], but it does allow the target to introduce spurious call records into the wiretap logs and to associate captured call content with false telephone numbers and to create false links to innocent or uninvolved parties.

2.3.2 Recording suppression through C-tone spoofing

The use of the in-band C-tone idle signal has even more serious consequences for full audio wiretaps: the subject can suppress content recording for arbitrary periods.

Loop extender systems turn off audio recording when the C-tone signal is detected. Naturally, subjects cannot easily converse while a spoofed C-tone is sent at full volume over the target line (unless they employ special narrow-band filters to eliminate it). However, there is no need for the subject (or the correspondent) to send the tone at full volume.

We found that even under conditions very unfavorable to the target (in which the law enforcement equipment was attenuated by 10,000 more feet of 26 gauge cable than the total connection length between the target and the correspondent), it was possible to falsely indicate an on-hook condition and turn off the recording equipment with a continuous C-tone sent at very low amplitude. False signals of as little as -40dBm total power on the target line were sufficient for this purpose. We found it to be readily possible to carry on an intelligible, even comfortable, conversation over this tone, with the audio completely evading wiretap collection because the recording was turned off and muted.

Observe that vulnerability to this countermeasure is a fundamental property of the in-band signaling architecture used between the loop extender and the interception recording system. It could be prevented only by the loop extender filtering out DTMF C-tone signals from the target audio stream sent over the friendly line; we are not aware of any loop extenders or dialup slave products that perform such filtering, however.

Audio examples (in MP3 format) of this countermeasure can be found at `http://www.crypto.com/papers/wiretapping/`.

[2] Unexpected use of the idle signal, however, can trigger bugs in some loop extender equipment. At least one system that we tested (a Recall Technologies NGNR-2000) would become distressed if a DTMF-C idle signal was not immediately followed by new call setup signals; this apparently caused the device to conclude that it lost the connection with the slave unit, disconnect the friendly line, and initiate a new connection. Under best case conditions, it required more than 30 seconds to reestablish the connection to the loop extender or dialup slave. It was very easy to exploit this vulnerability; we simply sent the DTMF-C signal for three seconds. This would cause the collection function to stop recording audio for the 30-45 seconds required to establish the connection. Sending the DTMF C tone on the target line for 3 seconds every 30 seconds would allow no audio to be recorded by the wiretap with this hardware. We cannot speculate on the performance of other DNR and recording devices in this regard without testing them, of course.

3 Signaling countermeasures against J-STD-025A (CALEA) taps

At first blush, the J-STD-025A CALEA interfaces seem to effectively neutralize in-band signaling countermeasures; separate channels deliver the target's signaling (the "Call Data Channel" (CDC)) and voice traffic (the "Call Content Channel" (CCC)), and allow decoding of DTMF tones at the switch (instead of at a second unit at the law enforcement agency). Because the telephone company is responsible for DTMF decoding before sending the data to the agency, it is likely that the reported digits are derived directly from the switch's call processing system, and because the line status is reported over a separate signaling channel, such systems need not be vulnerable to in-band spoofing of the line status. Nevertheless, some CALEA implementations fall short of achieving the level of robustness that their architecture would appear to allow.

Many CALEA configurations may indeed be more reliable than traditional loop extender systems with regard to susceptibility to confusion and evasion dialing. However, we note that CALEA and J-STD-025A specify only a standard interface between the telephone company and law enforcement; they do not require or assume any particular implementation of these interfaces, and do not require effectiveness or performance beyond that which was achieved with pre-CALEA systems. In other words, although many CALEA-compliant telephone switches may report the true decoded digits processed by the switch for call processing, there is no explicit requirement that they be implemented this way, and thus there is no guarantee that the dialed numbers reported to law enforcement accurately reflect those processed by the switch. Also, "post-cut-through" DTMF digits reported on the CDC, which are processed not by the switch but rather by a remote endpoint (e.g., a voicemail system), can still be confused or evaded.

A more serious potential vulnerability in CALEA implementations is recording suppression via an in-band "continuity tone" signal that some collection system implementations recognize on the call content channel. Configurations that process this signal are vulnerable to exactly the same content evasion countermeasures that can be used against loop extender systems.

3.1 Recording suppression in CALEA implementations

Although the J-STD-025A standard appears to eliminate the possibility of in-band signaling countermeasures by providing the law enforcement agency with call content and signaling in separate delivery channels, actual implementations sometimes blur this distinction. In particular, the DTMF C-tone signal is used by some CALEA implementations to indicate that a call content channel (CCC) is in the "idle" state. Recall that this is the same signal used to indicate line status in loop extender systems. The C-tone is processed by some CALEA CCC collection systems in much the same way – as a signal to disable the recording equipment.

This mechanism may have been motivated by a desire for backward compatibility with loop extender collection systems. Law enforcement agencies and telephone companies may construct any of variety of CALEA collection system architectures. The CDC and CCC may be delivered to the agencies directly over separate telephone lines, they may be delivered via an IP VPN, or they may employ the services of a intermediate "CALEA service provider" such Pen-Link[17] or Xlence[25]. Some CALEA collection systems are designed to accept CDC and CCC channels directly, while others adapt "legacy" loop extender recording systems. The FBI and Justice Department explicitly requested that "continuity tone" on idle CCC channels be a required CALEA feature in a "punch-list" of proposed improvements to the original J-STD-025A specification[3, 2]. Although the FCC did not ultimately adopt the continuity tone as a requirement[3], it has become a common optional feature cited in CALEA vendor literature and system patents[6, 9, 10, 12, 20]. In particular, C-tone on the CCC is often specified in product literature as a mechanism to control the collection system's audio recording equipment. That is, when the C-tone is present, the CCC is assumed to be idle (regardless of the call status as reported on the CDC) and the collection system may automatically mute audio monitoring and stop the recording equipment. C-tone is also used internally by some switch-side CALEA delivery systems.

Just as with loop extender systems, such configurations (sometimes called "C-tone supervision") permit subjects to unilaterally disable content recording by sending a continuous C-tone at an amplitude sufficiently high to trigger the recording suppression mechanism but low enough to allow intelligible conversation. Since the same tone is also used to suppress recording in loop extender systems, the target need not know whether CALEA or loop extender taps are used by the agencies he or she wishes to evade.

Not all CALEA implementations support C-tone supervision signals; it is an optional feature not required by the standard. However, C-tone appears to be a relatively commonly available option among current CALEA system that use analog or ISDN bearer channels for CCC delivery and in CALEA products designed for output to legacy collection equipment.

4 Discussion

The signaling protocol failures described in this paper are of significance to a broad range of communities and for a variety of reasons. First, of course, is the immediate problem of conducting reliable lawful interception without evasion or manipulation by the subject. In fact, this is a more subtle problem than it might first seem to be. Someone who believes that he or she is being wiretapped can reliably evade interception simply by refraining from using the suspected telephone line for incriminating conversations or by using a voice encryption system for such calls. However, history suggests that "telephone silence" may not be a satisfying solution for many wiretap subjects, since apparently many criminal enterprises rely extensively on telephone communication. Neither does end-to-end encryption provide widespread practical cover for many law enforcement targets. Encryption requires advance planning for the use of special hardware by both peers, and reliable voice telephone encryption systems are still not widely available on the commercial market in any case. The signaling countermeasures in this paper, on the other hand, not only require less sophisticated equipment than encryption (and only unilateral action), but can be used to actively *mislead* an investigator with incorrect or incomplete interception records.

Whether signaling countermeasures are attractive to or likely to be employed by subjects depends on how they perceive the threat. Since wiretaps are usually secret, a subject can never be sure that he or she is actually being monitored or whether monitoring is conducted with a susceptible system. However, law enforcement procurement practices coupled with the relative lack of diversity among wiretap implementations may make it possible for a target to make an educated guess as to whether the agencies that might be expected to conduct an investigation are using vulnerable equipment. Federal and local agency procurement contracts for wiretap equipment are often publicly available. We were able to discover the vendors and even model numbers of the equipment used by several agencies in various jurisdictions with a simple Internet search.

There is evidence (albeit indirect and inconclusive) suggesting that signaling countermeasures might sometimes be employed by sophisticated targets. For example, law enforcement agents have noted (in trial testimony) unexplained audio gaps in wiretap recordings, with specific reference to C-tone signals[28].

More broadly, the existence of signaling countermeasures suggests that the wiretap technology used by law enforcement should be critically evaluated against a wider range of threats than perhaps it has been. The scope of our analysis was deliberately restricted to information and materials we obtained from public sources and was limited to the narrow problem of confusion and evasion countermeasures. We made no attempt to be exhaustive or comprehensive, and yet quickly discovered practical attacks that seem rather obvious in hindsight. Some of the potential vulnerabilities in modern CALEA systems arise directly from features (e.g., the CCC continuity tone) that were requested by the law enforcement community itself. It seems at least plausible that there are as-yet undiscovered weaknesses in the J-STD-025A specification (and the systems that implement and support it). A systematic effort to discover or rule out vulnerabilities would improve confidence in these systems.

Finally, the protocol failures and signaling weaknesses in voice wiretaps provide a case study in computer and communication security generally. Well-established principles of secure system design appear to have been violated in the loop extender and CALEA tap architectures, with interfaces subject to multiple interpretations and complex interacting features and options that strain to maintain backward compatibility with "legacy" systems.

The problem of in-band signal abuse in particular has a long history in communication security, most famously exposed in the US and international long distance telephone network of the 1960's and 1970's (see Appendix B). And yet vulnerable systems that depend on unprotected in-band signals for critical functions continue to be designed and fielded, suggesting that the risks inherent in such designs are not adequately understood or appreciated by many security practitioners and system designers.

5 Conclusions and Recommendations

There is unfortunately little room to make conventional analog loop extender interception systems more robust against these countermeasures within their design constraints; the vulnerabilities to dialed digit confusion and evasion and to on-hook/off-hook state spoofing arise from inherent properties of their architecture and design. Audio recording of dialing signals may provide limited opportunities for subsequent forensic analysis of confused or evaded dialed digits (assuming the characteristics of the central office and transmission line can be accurately estimated later), although legal constraints generally preclude agencies from making such recordings on DNR-only taps.

CALEA systems, on the other hand, may be able to be made more robust against these specific countermeasures with relatively minor configuration changes. In particular, the law enforcement equipment that processes the CCC should be configured *not* to shut off when a C-tone is present on the channel. Instead, such systems should rely only on the CDC to determine when recording should commence or stop. Agencies should confirm the behavior of their CALEA equipment with their vendors.

Wiretap evidence, whether collected by loop extender or CALEA systems, should be evaluated for signs of signaling countermeasures. In particular, records of dialed numbers and call times should be examined for discrepancies against telephone company call detail records. This reconciliation should be performed routinely and as soon as possible after the records become available.

We strongly urge that J-STD-025A and other interception standards and practices be evaluated critically against countermeasures such as those discussed here and, more generally, against a broader threat model. The relatively simple signaling countermeasures in this paper became quickly apparent even from our somewhat cursory analysis. It appears that a systematic search for vulnerabilities under a threat model that includes subject-initiated countermeasures was not a part of the development process for either the J-STD-025A standard or many of the systems that implement it. As wiretap systems become more homogeneous and standardized, the consequences of vulnerabilities become increasingly serious. Any weaknesses in J-STD-025A systems may have the unintended and somewhat ironic consequence of degrading law enforcement's ability to conduct wiretaps on the advanced digital and mobile systems that CALEA envisioned. J-STD-025A standardizes the delivery of intercepted content to law enforcement across many different communications services. Any countermeasures against these systems therefore threaten law enforcement's access to the entire spectrum of intercepted communications. We suggest that the law enforcement community develop and articulate security and assurance requirements for interception systems against which existing and future standards and technologies can be measured.

Acknowledgments

We are grateful for insights from Steve Bellovin, Bill Cheswick, Will Enck, Susan Landau, Patrick McDaniel and Fernando Pereira. The Trustworthy Network Eavesdropping and Countermeasures project at the University of Pennsylvania is funded by the NSF Cyber-Trust program under contract NSF-0524047.

References

[1] Communications Assistance for Law Enforcement Act. Pub. L. No. 103-414, 108 Stat. 4279, United States of America, 1994. (codified as amended in 18 U.S.C. and 47 U.S.C. Sect. 229, 1001-1010, 1021).

[2] Communications Assistance for Law Enforcement Act. Third report and order. CC Docket No. 97-213, Federal Communications Commission, 1999.

[3] Communications Assistance for Law Enforcement Act. Order on remand. CC Docket No. 97-213, Federal Communications Commission, 2002.

[4] E. Cronin, M. Sherr, and M. Blaze. The eavesdropper's dilemma. Technical Report MS-CIS-05-24, University of Pennsylvania, 2005.

[5] M. Eleccion. Beating the blue-box bandits. *IEEE Spectrum*, 9:52–58, August 1972.

[6] EWSD Product Line Management. EWSD integrated CALEA with dial-out capability. Bulletin 02PB-CALEA01, Siemens, 2002.

[7] Federal Wiretap Act. Title III, United States of America, 1968. (codified as amended in 18 U.S.C. Sect. 2510-2522).

[8] Foreign Intelligence Surveillance Act of 1978. Pub. L. No. 95- 511, 92 Stat, United States of America, 1978. (codified as amended in 50 U.S.C. Sect. 1801-1811, 1821-1829, 1841-1846, 1861-62).

[9] R. M. Howell. Method of intercepting telecommunications. Patent No. 5,920,611, U.S. Patent and Trademark Office, Sept 1996. *Issued July 6, 1999.*

[10] R. M. Howell. Telecommunications intercept system. Patent No. 5,943,393, U.S. Patent and Trademark Office, Sept 1996. *Issued August 24, 1999.*

[11] International Telecommunication Union. Multifrequency push-button signal reception. Recommendation Q.24, Telecommunication Standardization Sector of ITU, 1988.

[12] E. Kampmeier, D. Smith, and M. Smith. Utilization of communication channels between a central office switch and a law enforcement agency. Patent No. 6,728,338, U.S. Patent and Trademark Office, Nov 2000. *Issued April 27, 2004.*

[13] North American Numbering Plan Administration. North American numbering plan. `http://www.nanpa.com`.

[14] Office of the Inspector General Audit Division. Federal Bureau of Investigation's foriegn language translation program follow-up. Audit Report 05-33, U.S. Department of Justice, July 2005.

[15] R. Oklahoma. Regulating the phone company in your home. *Ramparts Magazine*, 10:54–57, Jun 1972.

[16] V. Paxson. Bro: a system for detecting network intruders in real-time. *Computer Networks (Amsterdam, Netherlands: 1999)*, 31(23–24):2435–2463, 1999.

[17] Pen-link, Ltd. Whats new, pen-link version 7.0 enhancement / fix list. Product manual, Pen-link, Ltd., 2004. `http://www.pen-link.com/downloads/pl7/whatsnew.txt`.

[18] L. Prieur. Automatic monitoring service for telecommunications networks. Patent No. 6,470,075, U.S. Patent and Trademark Office, Jun 1999. *Issued October 22, 2002*.

[19] T. Ptacek and T. Newsham. Insertion, evasion, and denial of service: Eluding network intrusion detection. Technical report, Secure Networks, Inc., 1998.

[20] Recall Technologies, Inc. R2801 Line Latch/Slave Controller. Product specification, 2005. `http://recallt3.com/products.htm`.

[21] A. E. Ritchie and J. Z. Menard. Common channel interoffice signalling: An overview. *Bell Systems Technical Journal*, 57:221–250, Feb. 1978.

[22] R. Rosenbaum. Secrets of the little blue box. *Esquire Magazine*, 76:117–125,222–226, Oct 1971.

[23] L. Schenker. Pushbutton calling with a two-group voice frequency code. *Bell Systems Technical Journal*, 39:235–255, Jan 1960.

[24] U. Shankar and V. Paxson. Active mapping: Resisting NIDS evasion without altering traffic. In *Proc. of the 2003 IEEE Symposium on Security and Privacy*, pages 44–61, May 2003.

[25] Xlence Technologies. Bartec/Xlence COPS server. Product manual, Xlence Technologies, 2001. `http://web.archive.org/web/20010702072944/http://bartec.com/content/whatshotCOPS.html`.

[26] Telcordia Technologies. Telcordia Notes on the Networks. Special Report SR-2275 Issue 4, Telcordia Technologies, Oct 2000.

[27] TR-45. Lawfully authorized electronic surveillance. J-STD-025A, ANSI, 2003.

[28] United States District Court, Southern District of New York. United States of America v. Ahmed Abdel Sattar, Lynne Stewart, and Mohammed Yousry. Trial transcripts, United States District Court, Southern District of New York, Oct 2004. Testimony of Special Agent Michael Elliot, 7392–7399.

Appendix A: Formal treatment of confusion, evasion, and dialing secrecy

Using the algorithm in Procedure 1, a target of a wiretap can achieve perfect secrecy. Here, we assume that confusion is always effective (that is, the wiretap must consider all confused DTMF tones).

```
for $digitnum \leftarrow 1, digitnum \leq length(number), digitnum \leftarrow digitnum + 1$ do
  for $digit \leftarrow 0, digit \leq 9, digit \leftarrow digit + 1$ do
    if $number[digitnum] = digit$ then
      Transmit $digit$ without confusion
    else
      Transmit $digit$ using confusion
    end if
  end for
end for
```

Procedure 1: *Perfect secrecy using confusion*

Definition: The *confusedtext* captured by a tap is the string of all reconstructed DTMF digits. It may include both legitimate DTMF tones and noise. In the context of confusion, *Perfect secrecy* is achieved when the probability that an adversary reconstructs the legitimate DTMF tones after capturing the confusedtext (*a posteriori* probability) is equal to the probability that the adversary reconstructs the legitimate DTMF tones without observing the confusedtext (*a priori* probability).

Theorem: Procedure 1 achieves perfect secrecy if all confused digits are interpreted by the DTMF decoder.

Proof. Let $Pr(i)$ be the *a priori* probability of selecting the ith legitimate digit. In round i of the protocol, all possible digits (0 through 9) are received, and hence no digit can be eliminated. Thus, the *a posteriori* probability of selecting the ith digit is also $Pr(i)$. □

In practice, however, not all confused noise will be interpreted by the wiretap. Although perfect secrecy may not be achievable, the number of possible interpretations of the dialed telephone number may suffice to mask the true dialed number. If the probability of a confused digit being interpreted by the eavesdropper is c, then the number of possible interpretations for a l-digit phone number is $(1 + (9 \cdot c))^l$.[3]

A more efficient confusion and evasion algorithm is given in Procedure 2. Here, the caller randomly intersperses n noise digits among the l legitimate digits. Noise digits are chosen uniformly at random and are transmitted using confusion (i.e., in a manner such that they are ignored by the switching equipment but may be interpreted by the wiretap). The legitimate digits are sent using evasion techniques.

```
Input: $tel$: legitimate telephone number, $l$: length of $tel$, $n$: number of confused digits
$len \leftarrow l + n$
**for** $i \leftarrow 0; i < len; i \leftarrow i + 1$ **do**
    $noise[i] \leftarrow rand(10)$ # choose random noise digit
    $legitlocation[i] \leftarrow 0$
**end for**
$j \leftarrow 0$
**while** $j < len$ **do**
    $r \leftarrow rand(len - 1)$ # choose random locations for legitimate digits
    **if** $legitlocation[r] = 0$ **then**
        $legitlocation[r] \rightarrow 1$
        $j \leftarrow j + 1$
    **end if**
**end while**
$legitidx \leftarrow 0$
**for** $k \leftarrow 0; k < len; k \leftarrow k + 1$ **do**
    **if** $legitlocations[k] = 1$ **then**
        Dial $tel[legitidx]$ using evasion technique
        $legitidx \leftarrow legitidx + 1$
    **else**
        Dial $noise[k]$ using confusion technique
    **end if**
**end for**
```

Procedure 2: *Using confusion and evasion to mask dialed digits*

[3] The number of plausible telephone numbers is slightly less than this, of course, since not all telephone numbers are equally likely (e.g., `000-0000`) [13].

Let $p_{e_i}, 1 \leq i \leq l$ be the probability that the ith digit of the called telephone number successfully evades the wiretap. Let $p_{c_i}, 1 \leq i \leq n$ be the probability that the ith noise digit is interpreted by the wiretap. We can define the average evasion probability as $\hat{p_e} = \frac{\sum_{i=1}^{l} p_{e_i}}{l}$ and the average confusion probability as $\hat{p_c} = \frac{\sum_{i=1}^{n} p_{c_i}}{n}$. The expected length of the interpreted telephone number is therefore $(l \cdot (1 - \hat{p_e})) + (n \cdot \hat{p_c})$, and thus the number of possible interpretations is approximately $\binom{(l \cdot (1-\hat{p_e}))+(n \cdot \hat{p_c})}{l}$.

Appendix B: In-band signal abuse in the long distance telephone network

In the late 1940's, the AT&T long distance telephone network added features for "direct distance dialing" of long distance subscriber calls without the need for manual operator assistance. These features required new protocols and mechanisms to support the automated signaling of trunk status and transmission of telephone numbers and other routing information between switching centers in different cities. Although local subscriber dialing had been available for many years, the signals and protocols used in the local loop were not directly applicable to the long distance trunk circuits used between switching centers. Subscriber signaling used (and still uses) a DC current loop, which, for various reasons, is inappropriate for circuits more than a few miles long or for wide-band inter-office trunks. The new long distance system instead used audio signals in the voice band to signal line status and dialed numbers. A 2600Hz "idle" signal was placed on trunks when they were inactive; other tone signals (similar to DTMF but using different frequencies) were associated with individual number digits. To route a long distance call, a switch would select an idle trunk to the next switch in the path, remove the idle tone, transmit the desired number, and connect the calling subscriber's local loop to the trunk. The remote switch would then route the call to the next switching center in the same way, until it finally reached the local switch of the destination number. Billing records for long distance calls were maintained at the originating subscriber's switch.

This arrangement had the significant advantage of allowing individual subscribers to use their existing equipment to perform long distance dialing, since the new trunk signals were intended to be encoded and decoded by the internal network switching equipment, not by the end-user telephone instruments. The signals, although in the audible voice band frequency range (hence "in-band"), were largely transparent to the end user. By the late 1950's the system was fully deployed in most of the U.S.

Within just a few years technically inclined telephone users had found ways to exploit the system to make fraudulent long distance calls. The fraud technique used a specially constructed signal generator, which became popularly known as a "blue box," to spoof the in-band long distance signaling tones. A race condition in the way idle trunks were handled allowed an end user to briefly send the 2600Hz idle signal during a long distance call, which would be misinterpreted by the remote trunk as signaling the end of the current call. The remote trunk then disconnected the call in progress and became ready to accept tone signals for a supposedly new call, which could be similarly spoofed by the caller. The accounting system at the caller's switch would continue to record the original call as if it were still in progress. It was therefore possible for subscribers to defeat the billing system by starting the process with a call to an inexpensive or toll-free long distance number and spoofing the idle signal and routing tones for what would otherwise have been a more expensive call.

By 1971 the in-band signaling flaws came to national attention[22, 15], bringing about an "arms race" of sorts between blue box users ("phone phreaks") and telephone companies seeking to protect their billing revenue (and prevent unauthorized access to the internal signaling network in general). AT&T eventually developed an out-of-band "common channel" long distance signaling architecture[21] that defeated the blue box by eliminating in-band inter-office signaling. The new system was not fully deployed in the U.S. until the mid 1980's, however.

The vulnerabilities in loop extender and CALEA wiretap systems – and the methods for exploiting them – are strikingly reminiscent of the weaknesses of the 1960's telephone network. It is notable that even though CALEA primarily uses out-of-band signals, the C-tone idle signal mechanism (when present) remains in-band and vulnerable to exploitation by the target.

Unfortunately, although the weaknesses themselves may be similar, the response of the telephone industry to the problem may not be as directly applicable as might be hoped in forming a response to wiretap countermeasures. A contemporary article[5] suggested a "three pronged" approach to mitigating the effects of the blue box. The first prong was user education on the ethical pitfalls of telephone fraud, the second was vigorous detection and prosecution of those committing fraud, and the third was migration to out-of-band signaling. Note that the first two prongs aimed for deterrence, not prevention. In retrospect this strategy was at least partly effective. Defrauding the telephone company is itself a serious crime. Fraud detection technology was deployed selectively throughout the network to aid in identifying suspected blue box users, who were subject to widely publicized criminal prosecutions. The prospect of detection and prosecution presumably dissuaded many otherwise law-abiding would-be blue boxers in the years before the vulnerability was fixed.

Deterring exploitation of wiretap countermeasures seems to be a much more difficult problem than deterring toll fraud, not least because many of those most motivated to deploy such countermeasures are already criminals (and, in any case, the use of wiretap countermeasures is generally not, in and of itself, a crime).