Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps

Micah Sherr, Gaurav Shah, Eric Cronin, Sandy Clark, and Matt Blaze
Dept. of Computer and Information Science, University of Pennsylvania
Philadelphia, PA USA
{msherr, gauravsh, ecronin, saender, blaze}@cis.upenn.edu

ABSTRACT

Although modern communications services are susceptible to third-party eavesdropping via a wide range of possible techniques, law enforcement agencies in the US and other countries generally use one of two technologies when they conduct legally-authorized interception of telephones and other communications traffic. The most common of these, designed to comply with the 1994 *Communications Assistance for Law Enforcement Act (CALEA)*, use a standard interface provided in network switches.

This paper analyzes the security properties of these interfaces. We demonstrate that the standard CALEA interfaces are vulnerable to a range of unilateral attacks by the intercept target. In particular, because of poor design choices in the interception architecture and protocols, our experiments show it is practical for a CALEA-tapped target to overwhelm the link to law enforcement with spurious signaling messages without degrading her own traffic, effectively preventing call records as well as content from being monitored or recorded. We also identify stop-gap mitigation strategies that partially mitigate some of our identified attacks.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Circuit switching networks; H.4 [**Information Systems Applications**]: Miscellaneous

General Terms

Legal Aspects, Reliability, Security

Keywords

CALEA, law enforcement wiretaps, wiretapping

1. INTRODUCTION

The United States Communications Assistance for Law Enforcement Act (CALEA), which became law in 1994, requires telecommunications service providers to incorporate various capabilities for law enforcement wiretapping (sometimes called "lawful access") into their networks. CALEA requirements first applied only to traditional voice telephone services provided by telephone companies (wireline analog, ISDN, cellular voice, etc). In recent years, however, the law has been interpreted to also cover many data services (such as 3G cellular Internet access) and non-traditional voice services (such as VoIP services offered by cable companies). Most service providers comply with CALEA by using equipment that provides a standard interface, defined jointly by the Telecommunications Industry Association (TIA) and Alliance for Telecommunications Industry Solutions (ATIS) in ANSI Standard J-STD-025 (often referred to in the industry simply as the "J-standard") [3] for transmitting intercepted traffic to a law enforcement agency[1].

CALEA was, and continues to be, controversial. Criticism of CALEA, and wiretap-capability mandates in general, has centered largely on questions of whether the provision of an explicit interface for wiretaps on every switch in a network inevitably makes the national communications infrastructure vulnerable to illegal, unauthorized abuse by the government or others [20][2].

In this paper, we focus on a different question: whether the standard interfaces used for most CALEA wiretaps are vulnerable to manipulation by wiretap *targets* in ways that prevent accurate *authorized* intercepts of their traffic from being collected.

In previous work, we found that wiretap subjects can manipulate *loop extender* wiretapping technology used by law enforcement to tap analog telephone lines, enabling the target to unilaterally disable content recording, cause incorrect dialed numbers to be recorded, and interject spurious records into the interception record [28]. Many of these vulnerabilities resulted from the use of in-band signaling in loop extender systems. By injecting spurious control signals, the target could manipulate the wiretap.

The newer CALEA architecture establishes a separate out-of-band channel to communicate signaling information between the telephone service provider (TSP) and the law enforcement agency (LEA). Surprisingly, although separating signaling information from call content removes (at least in

CCS'09, November 9–13, 2009, Chicago, Illinois, USA.

[1]This paper focuses specifically on *law enforcement* wiretaps. US intelligence agencies also conduct wiretaps, but the technologies used for them are beyond the scope of this paper. See e.g., [5] for a discussion of the technical aspects of the NSA's domestic wiretap technology.

[2]And indeed, these concerns appear to have been validated by, for example, a recent incident of large-scale wiretapping in a Greek cellular network [23].

principle) many of the previously discovered vulnerabilities, the CALEA design introduces several entirely new vulnerabilities. While our existing work suggested that CALEA systems may be less susceptible to manipulation than the loop extender technology they replaced [28], this paper shows that the opposite appears to be true.

Unlike traditional wiretapping countermeasures (e.g., encryption), the attacks outlined in this paper can be conducted *unilaterally* by individual wiretap targets, and affect the accuracy not only of the captured content, but also of the captured metadata record (who called whom and when). Although encryption obfuscates communication content, it does not conceal the identities of the communicating participants. Coupled with the results of our prior work [28], the vulnerabilities identified in this paper raise significant questions about the reliability of wiretap evidence and suggest that the bulk of the wiretapping technologies currently employed by law enforcement are largely incapable of reliable evidence collection in the face of relatively simple countermeasures.

In particular, we find that CALEA-based wiretaps of many current communications services are readily vulnerable to denial-of-service by a wiretap target. Perhaps most significantly, we found practical attacks that a wiretap target can employ to overwhelm the low-bandwidth signaling channel of the J-STD-025 interface. Signaling events generated by the target (such as taking a telephone off-hook) are encoded for transmission in a way that consumes far more bandwidth on the (low bandwidth) law enforcement signaling link than on the target's own link. A wiretapped subject can exploit this by generating a moderate volume of spurious signaling events that reliably exhausts the capacity of the signaling link to the law enforcement agency for *all* wiretap targets connected to a given switch, without significant degradation of service to the targets' actual traffic. This effectively prevents the law enforcement agency from accurately collecting or recording the true call metadata as well as the associated data traffic or audio content.

As we will see, these vulnerabilities largely arise from narrow engineering choices in the CALEA architecture rooted in assumptions about "average case" workloads. However, a motivated wiretap subject may intentionally violate these assumptions to overwhelm the resources of the wiretap. This is especially true with wireless telephone services (which account for the vast majority of law enforcement wiretaps [2]), where voice services are increasingly bundled with moderate- and high-bandwidth data services.

This paper has four main contributions:

- We provide the first (in the public literature) security analysis of the technical standards used for a large fraction of law enforcement telephone and data wiretaps in the United States (as well as in other countries).
- We identify practical attacks against systems that implement the standard that cause incomplete or incorrect interceptions, possibly without detection, in current implementations.
- We conduct experiments that demonstrate the feasibility and practicality of our attacks. In particular, we verify that common US telecommunications carriers provide consumers with sufficient resources to exhaust the capacity of CALEA systems that implement the J-standard's recommended wiretap configuration.
- We propose stopgap mitigation strategies that partially mitigate some of our identified attacks.

Any weaknesses in CALEA wiretaps, of course, represent a pressing problem for the many law enforcement agencies that rely on them. But the failures have wider implications as well. CALEA requirements are being adopted for an increasingly broad range of communications platforms. Yet there has been remarkably little published analysis of the effectiveness of the standards that are being mandated.

1.1 Wiretapping in the United States

The US laws governing electronic surveillance are arcane and complex; a complete discussion is beyond the scope of this paper. The law has its basis in the Fourth Amendment with specific rules codified in various federal and state statutes and case law interpretations that have evolved over many years. For our purposes here it is sufficient to note a few salient highlights of surveillance law as it applies to law enforcement wiretaps.

In the US, broadly speaking and in general, surreptitious third-party interception of telephone and network communication is illegal whether done by government or private individuals, with narrow exceptions for criminal investigations and similar matters. Even when allowed, law enforcement wiretaps must be conducted under court supervision, with different requirements and standards that must be met depending on the kinds of information being collected. The procedures and requirements for Federal law enforcement wiretaps are codified in Title III [33]; most states have essentially similar rules.

Different kinds of wiretaps have different legal requirements. The most stringent legal standards apply to wiretaps that intercept the *content* of communication (e.g., telephone call audio, text messages, etc.). These taps are permitted only if the court is convinced there is sufficient probable cause and that the interception is essential to an investigation. *Pen register*[3] intercepts, which seek only *metadata* or *call-identifying information* (a transcript of who communicated with whom and when) can meet a lower legal standard. All that is required, in general, for such taps is an assertion that the specific records involved are likely to be germane to a investigation, and pen registers requests are not usually subject to extensive case-by-case judicial approval. Most law enforcement taps are in this category, although it is not unusual for evidence obtained from a pen register to be used to support a request for a warrant for a content tap.

1.2 Wiretapping Technology

In principle, there are many possible approaches for third-party recording of analog and digital telephone and data communications, depending on the network topology and the access and other capabilities of the wiretapper. Interception might be performed at the wireline link between the target and the network (the "local loop" in telephony parlance), within the network itself, or by surreptitious "bugs" placed in the target's own hardware or software. Wireless devices, such as cellular phones, can introduce an additional option: capturing and demodulating the radio signals.

[3]Named after the (now historical) electro-mechanical chart recorders once used to conduct them. They are also called *dialed number recorder* taps.

Loop extenders: Tapping the local loop Historically, the favored approach for law enforcement wiretapping in the US has been to tap the target's local loop. For analog wireline telephone calls, relatively little special hardware is required at the tap point; it is sufficient simply to connect a second pair of wires leading back to the law enforcement agency's facilities. To make such taps less detectable and to ensure proper isolation and level equalization of intercepted content, however, law enforcement agencies use a small device called a *loop extender* at the splice point. The device copies the audio on the subject's line over to the law enforcement line, re-encodes signals, and performs level equalization. Collection equipment at the law enforcement agency decodes the dialed digit and other call processing signals and can record the audio contents of the calls.

Digital communications can often also be tapped at the local loop, but the interception equipment and techniques may need to be more sophisticated to capture accurately the complex, higher bandwidth signal encodings used in such modern systems. Tapping some services in this way can entail the use of highly specialized (and relatively expensive) equipment, and as bandwidth becomes greater and signal encodings become more complex, the loop interception can become correspondingly more difficult to perform.

CALEA: Tapping in the switch A newer wiretapping technology used by law enforcement agencies – and the subject of this paper – is based on the 1994 CALEA law. CALEA wiretaps are distinguished from loop extenders by performing the interception not at the subscriber's local loop, but rather within the switching equipment of the network provider, allowing more context-sensitive capture of digital as well as analog communications.

CALEA mandates a standard set of capabilities for wiretaps in telephone (and certain other communications) switches. In these taps, the switch (not the law enforcement agency) decodes the call signaling information and, when content interception is performed, segregates content on a separate channel from the signaling. As noted above, ANSI J-STD-025 standardizes a CALEA-compliant interface between switches and law enforcement agencies.

The J-standard architecture and messages are described in detail in the rest of this paper. Basically, a law enforcement agency conducting CALEA interceptions typically leases one or more telephone lines between the agency facilities and the target's telephone switch. The first of these lines carries a *Call Data Channel (CDC)* that reports the signaling events (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 or data stream of any active monitored lines for which content interception has been authorized. The CDC carries call data for every active target on the switch tapped by a particular agency. The CCCs, on the other hand, carry only one audio or data stream at a time, with their activity reported over the CDC.

While CALEA applies only in the United States, J-standard compliant switches and interception products are marketed in other countries as well.

Other approaches Law enforcement agencies in the US generally use either loop extenders or CALEA for wiretaps associated with criminal investigations. Intelligence agencies and other eavesdroppers (legal or illegal), however, may use other techniques. The range of *technically possible* approaches to surveillance on modern communications platforms is very wide. In this paper, however, we focus on the much more limited set of tapping techniques used by US (and other) law enforcement to gather evidence legally.

2. CALEA AND J-STD-025

In 1994, the *Communications Assistance for Law Enforcement Act* (CALEA) [34] was enacted to regulate telecommunications compliance with lawful surveillance of digitally switched telephone networks. The law was intended to protect consumer privacy in light of new communications services [35], to avoid encumbering the development of new communication technologies [35], and to clearly delineate the responsibilities of telecommunications carriers with respect to court authorized surveillance [11].

2.1 J-standard (J-STD-025)

While CALEA clearly defines the legal responsibilities of telecommunications service providers (TSPs), it does not provide technical specifications or protocols pertaining to wiretap configuration, data collection, or data delivery. Rather, the law specifies that a joint task force composed of representatives from TSPs and Federal and State Law Enforcement Agencies (LEAs) develop a *voluntary* industry standard. Consequently, the current standard has evolved as a result of compromise amid conflicting interests between the FBI, the telecommunications industry and interest groups.

Specifically, the Telecommunications Industry Association (TIA), the Alliance for Telecommunications Industry Solutions (ATIS), and various other industry organizations and interest groups developed the interim standard J-STD-025 [3] (the J-standard). The current revision of the J-standard, the J-STD-025-B, was adopted in 2006 and adapts the Standard in order to accommodate new wireless services. Additional adaptations of the J-standard add support for VoIP services [22, 15].

The vast majority of CALEA vendor equipment of which we are familiar implement the J-standard or a derivative of it. This architecture is the only currently fielded standard for complying with CALEA. Moreover, CALEA's "safe harbor" provision, stating that any wireline, cellular, and broadband TSP that implements these standards is considered to be in compliance with CALEA [34], further incentivizes its adoption.

2.2 Architecture of J-standard CALEA Systems

TSP subscribers (regardless of whether they are a wiretap target) interface with the TSP through a collection of network elements (e.g. telephone switches, home location registers) which together form the TSPs network. Each element is responsible for interpreting certain customer actions in order to provide service.

The J-standard mandates that some or all network elements be able to function as *interception access points* (IAPs) when authorized by a wiretap order. As shown in Figure 1, each IAP feeds information into a *Delivery Function* (DF), also located inside the TSP. IAPs forward *call-identifying information* and optionally, *call content*, to the DF. The DF serves as an aggregation point for the various IAPs and transfers call-identifying information and (when authorized)

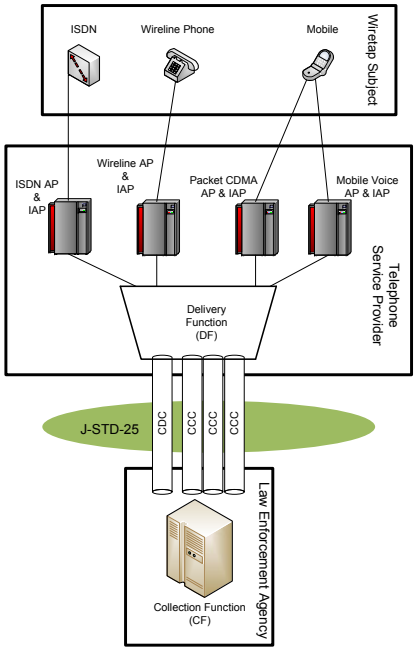

Figure 1: Example CALEA architecture for a wiretap subject with mobile, analog wireline, and ISDN services. The J-STD-025 standard covers the interface between the Delivery Function (DF) and the Collection Function (CF).

call content to a *Collection Function* (CF) located at the LEA.

The J-standard defines the interfaces between the DF and the CF. Call-identifying information is transmitted using the *Lawfully Authorized Electronic Surveillance Protocol* (LAESP), a message-based protocol that encodes actions taken by the TSP or the wiretap subject. (LAESP is described in detail in the following section.) LAESP messages are transmitted via a unidirectional (and somewhat confusingly named) *call data channel* (CDC) between the DF and CF. Importantly, LAESP messages from multiple wiretap orders may be multiplexed on the same CDC.

The CDC conveys call-identifying information for both pen register and content wiretaps. In the latter case, the DF also relays *call content* over one or more *call content channels* (CCCs). Each CCC is dedicated to relaying a particular *bearer service* (e.g., voice, packet data, etc.) for a single wiretap order between the TSP and the LEA. CCCs carry verbatim (i.e., unedited) copies of the wiretap subject's communications. The number of CCCs is determined by the LEA. CCCs may either be *separated*, conveying inbound (towards the subject) and outbound (away from the subject) traffic using separate channels, or *combined*, relaying bidirectional traffic on a single channel.

In particular, we note the following properties of the J-standard: (a) The J-standard requires neither reliable communication between the DF and CF nor the use of integrity checks for LAESP messages. Congestion on the CDC may therefore lead to message corruption and/or loss. (b) Since LAESP messages do not contain sequence numbers, message loss may be undetected by the LEA. (c) Furthermore, since LAESP messages delineate the beginning and end of calls, loss of LAESP messages may therefore cause recording equipment at the LEA to fail to capture call content.

2.3 Lawfully Authorized Electronic Surveillance Protocol (LAESP)

The J-standard specifies the semantics and wire format of the Lawfully Authorized Electronic Surveillance Protocol (LAESP) used to convey call-identifying information over the CDC. Like many telecommunications protocols, LAESP is defined using ASN.1 [18] notation, allowing a human-readable description to be compiled into routines for unambiguously marshalling of messages across a network. The J-standard defines 17 LAESP message types (summarized in Table 1), corresponding to classes of both high-level network events and low-level subject/network signals.

Due to the generality of the J-standard, LAESP messages contain "conditional" fields for parameters which are only present in certain technologies (e.g., IMSI for ISDN, ESN for wireless, or IP for VoIP), as well as variable-length fields filled in with human-readable strings for identifying equipment or locations. The size of a particular LAESP message can vary significantly based on the technology being monitored and the policies of the TSP performing the collection.

3. VULNERABILITIES IN THE J-STANDARD

The architecture of the J-standard is a poor fit for many current (and emerging) communications services. The evolved protocols no longer cleanly separate authoritative network signaling events from captured content (thereby moving away from one of the apparent original design goals of the system), and bandwidth is provisioned according to assumptions that no longer hold true. In this section, we show how these deficiencies can be exploited in practice by wiretap targets to suppress or inject uncertainty into the data stream delivered to law enforcement. The result is that targets subscribed to many of the most commonly wiretapped services (such as cellular telephones) can effectively prevent accurate records from being delivered to law enforcement, often without the possibility of detection.

Unlike more traditional eavesdropping countermeasures (in particular, encryption), the attacks identified in this section may be unilaterally deployed by the wiretap subject and do not require the participation of the other communicating party. Moreover, the attacks prevent not only call content from being recorded (in the case of call-content wiretaps), they additionally prevent accurate call records from being delivered to law enforcement, often without the possibility of detection. That is, unlike encryption that may be used to obfuscate the content of calls, the techniques described in this section may be used to additionally hide call records (who called whom and when) from wiretap transcripts.

Law enforcement agencies (and their vendors) do not, as a rule, reveal the precise equipment and configurations used to conduct wiretaps. Therefore, we did not attempt to test these attacks against specific implementations of the CALEA standards. Instead, we conducted experiments on various telecommunications services that we modeled as being wiretapped with the most generous (to law enforcement) CALEA configurations recommended in the J-standard. Our analytical and experimental results conservatively assume that wiretap systems are provisioned with the maximum resources described by the standard (i.e., a full T1 line between the TSP and the LEA). It is worth emphasizing that

LAESP Message	Causal Event
`CCOpen`	Delivery of circuit-based call content
`Origination`	Subject dials feature code or attempts a call
`TerminationAttempt`	Incoming circuit-based call to subject
`Redirection`	Incoming call is redirected
`Answer`	Circuit-based call has been answered
`CCClose`	End of circuit-based call content
`Release`	Resources previously used for circuit-based call are released
`PacketEnvelope`	Subject transmits ISDN, SMS, or IP packet (Used to transmit packet contents over the CDC)
`DialedDigitExtraction`	The subject dials DTMF digits after the call has been established
`NetworkSignal`	IAP transmits network signal (e.g., call waiting tone) to subject
`SubjectSignal`	Subject transmits control feature (e.g., switchhook flash or feature key) to TSP
`ServingSystem`	Subject's mobile device switches to another service area or TSP

Table 1: LAESP messages defined in the J-standard, excluding messages associated with conference party calling and cdma2000 data packets.

since the discovered vulnerabilities arise from the architectural design described by the Standard rather than from any particular implementation defect, any CALEA system and configuration that abides by the J-standard would be at least as vulnerable as our experiments and analyses suggest.

3.1 Call Data Channel (CDC) Resource Exhaustion

The *Call Data Channel* (CDC) transmits call-identifying information for pen register and content wiretaps from the Telephone Service Provider (TSP) to the Law Enforcement Agency (LEA).

The engineering aspects of the CDC do not appear to have been well explored either within the J-standard or in the public literature. J-STD-025-B contains a 24 page annex on proper CCC delivery, while the corresponding CDC annex is less than two pages. Neither determining adequate CDC capacity nor the potential consequences of an improperly provisioned CDC are included in the J-standard or its annexes. Additionally, although the capacity of the CDC between the telecommunications service provider (TSP) and law enforcement agency (LEA) is a variable which can be configured on a per-wiretap basis, the critical internal provisioning of a TSP's network for routing CDC messages to the Delivery Function (DF) is far more difficult to change.[4] While provisioning resources for the average case or based upon statistical traffic models of normal communication patterns may be sufficient if the target does not apply any countermeasures, a motivated wiretap subject (or any slightly paranoid individual) need not conform to the TSP's average customer profile.

Of particular concern, the "preferred" and highest bandwidth CDC configuration in the J-standard is a single ISDN B channel (64 kbps). When congestion occurs on the CDC, there is no preemption or notification – messages are silently dropped. While 64 kbps may be sufficient for "average" voice signaling traffic volumes, modern services allow the subject to generate events at a rate that will greatly exceed this, especially after they are encoded under LAESP. This, as we will see, provides a rich vector for attack on both the CDC and the CCC.

The CDC as currently designed is a low-bandwidth, unreliable, heavily multiplexed resource. All call-identifying information generated by intercept access points (IAPs) are transmitted via the same CDC to the LEA on a first-come-first-serve non-queued basis, allowing a single IAP element to consume the entire channel. If the CDC is occupied when an IAP needs to relay signaling information, the LAESP message is dropped without notification or retry. A single CDC is used between the DF and the LEA for a given wiretap, and this CDC may be further shared by other wiretaps between the same TSP and LEA.

At the time the J-standard was first developed, the technological landscape was relatively homogeneous. However, in modern networks, the same CDC may carry call-identifying information for voice calls, IP data, and SMS messaging. Because messages on the CDC come from so many sources and can relate to different investigations, a significant overhead of descriptive information is required which would not necessarily be needed on a less heavily shared channel.

The most obvious danger of an underprovisioned CDC is that call-identifying information will be irrecoverably destroyed. A more subtle danger arises from the use of the CDC as a control channel for the CCC. The Collection Function (CF) at the LEA depends on `CCOpen` and `CCClose` messages on the CDC to control capture of call content. These messages signal the respective start and stop of call content. If these messages are lost, then both pen register and call content data have been irrecoverably destroyed.

We use 64 kbps (the preferred CDC capacity) as a benchmark for the remainder of this section. While faster circuits may be possible between the TSP and LEA, the bottleneck may lie within the TSP network designed to this 64 kbps bandwidth upper limit. We observe that at the time the J-standard was originally developed, the difference between the average and worst case bandwidths was likely very small, particularly in the case of cellular telephony (the technology of most interest to law enforcement [2]). Today, in contrast, due to the rapid development of new services being shoehorned into CALEA and the J-standard, the worst case is unpredictable and likely several orders of magnitude greater than the average case.[5]

[4]The J-standard specifies only that this internal capacity be "adequate", while similar CALEA standards specify bandwidth resources allocated based on "statistical call models" [22].

[5]In many regards, this is very similar to another recently published telecommunications vulnerability, in which over the air signaling channels (designed for the requirements of voice calls) are overloaded for new data services [32]. These new services turn out to be excellent vectors for denial-of-service attacks, which disrupt not only the new service but

By the nature of surveillance, most LAESP messages are generated as a direct result of some action taken by the subject. This places the subject at an advantage by allowing her to reliably and precisely generate traffic on the CDC. Although LAESP uses a fairly efficient binary encoding framing protocol on the CDC (BER and X.25 respectively), the messages themselves contain a significant amount of information not present in the monitored channel to facilitate de-multiplexing at the LEA. Each message must contain (at a minimum) a timestamp, a case identifier, and possibly the identity of the IAP that intercepted the call-identifying information. Most messages also contain call and party identifying information. This often leads to a significant amplification factor, where, for example, the one bit of information necessary to encode whether a subject's phone is on- or off-hook requires nearly 100 bytes when expressed as a LAESP message. LAESP also transmits both raw user signals (e.g. "phone went on hook") and higher-level TSP network events (e.g. "call released"), causing further amplification.

The remainder of this section presents a number of different methods that the wiretap subject may utilize to exhaust a fixed capacity CDC. It should be kept in mind that when multiple technologies are being simultaneously monitored (e.g. wireless voice plus data), a successful attack on the CDC using any of these technologies prevents wiretapping of them all.

ISDN Feature Keys ISDN allows users to directly control supplementary features such as call forwarding, call waiting, and call holding through the Q.931 [17] signaling protocol. The protocol supports both a *stimulus mode* in which the terminal (i.e., phone handset) operates in a very simplistic stateless mode and a *functional mode* intended for more sophisticated devices such as computers. In stimulus mode, Q.931 messages are sent to the switch immediately whenever a function button is pressed on the handset, with no local interpretation or decision making. The J-standard requires that such "subject signals" be reported over the CDC as long as they are not made redundant by another LAESP message; it does not require the IAP or Delivery Function to interpret or validate the signal in any way.

The Q.931 feature key message is 6 bytes in length. In contrast, the generated `SubjectSignal` LAESP message conservatively requires 82 bytes – an amplification factor of nearly 14. To saturate a 64kbps CDC with `SubjectSignal` messages, the target must generate $64000/(8 \cdot (82+3)) = 94.11$ signaling messages per second (X.25 frames require 3 bytes of overhead). The capacity of a standard Basic Rate Interface (BRI) ISDN used by the target to signal the TSP is 16 kbps. Producing 6-byte signals at a rate of 94.11 per second requires 4.52 kbps of bandwidth (Q.931 messages require no additional framing), well within the capacity of the subscriber's signaling channel. The target can easily exhaust the resources of the CDC, preventing the wiretap from receiving call records and (in the case of content wiretaps) requests to open call content channels.

SMS Messaging In addition to traditional voice calls, the J-standard also covers messaging services such as the Short Message Service (SMS) available on nearly all wireless devices and plans. When a SMS message to or from a monitored subject is sent, a `PacketEnvelope` LAESP message is generated that specifies the sender and receiver identities and optionally the message contents. A conservative size for a `PacketEnvelope` is 173 bytes for an SMS with no message payload and 190 bytes for SMS messages with a 1 byte payload. An attacker would therefore need to generate at least 46 (pen register) or 42 (content) messages per second to saturate a 64 kbps CDC.

Although the J-standard does not specify the locations of IAPs within the TSP network, a logical position for capturing SMS messages is at the Short Messaging Service Center (SMSC) since all messages to or from the subject must pass through it [7]; product literature from several SMSC manufacturers supports this assumption [30, 31], touting CALEA support as a SMSC feature.

The SMSC is at a fixed location within the core of the wireless network, allowing messages to be accepted and queued even when the recipient's phone is offline or in use. In addition to messages originating with other mobile devices, most SMSCs also handle messages originating from external networks, permitting features such as mobile e-mail, travel or financial alerts, and search engine queries.

Previously, Traynor et al. [32] showed how these Internet-facing external network connections can be exploited to create DoS attacks on cellular networks. The same approach could be used by an attacker to simultaneously send many SMS messages to the target's phone number from multiple accounts and services. Since the publication of Traynor's attack [32], many TSPs have improved their defenses through rate limiting and attack detection at the SMSC and at submission interfaces like web and e-mail, reducing the practicality both of their attack against the cellular network and the SMS-based attack against CALEA wiretap systems. However, as the popularity of SMS messaging increases, TSPs will likely provision more resources to increase SMS capacities (and consequently, increasing potential profits). Since the capacities of CDCs are fixed, diminished SMS rate limiting will permit better service while concurrently increasing wiretaps' vulnerability to SMS-based CDC exhaustion attacks.

VoIP Signaling As a product of the traditional circuit-switched wireline and wireless telecommunications industry associations, the J-standard does not specifically address the requirements of other (competing) technologies such as Voice-over-IP (VoIP). The J-standard has, however, in practice served as a guide from which other industry associations have made minimal modifications to suit their differing technical requirements [22, 15]. We focus our evaluation of VoIP on the PacketCable™ Specification since it is the most recent and most referenced standard of which we are familiar.

Since consumer VoIP messaging traverses broadband connections, the target can dedicate a large fraction of his bandwidth to producing VoIP signaling data. Unlike analog wireline services, VoIP signaling data may be generated at broadband speeds. Moreover, routing policies that prefer VoIP data over non-VoIP IP traffic [6] further enhance the target's ability to saturate the 64kbps CDC.

To determine achievable signaling rates, we used the SIPp traffic generator tool [12] to rapidly place and immediately release SIP calls using a consumer broadband connection. We applied SIPp to two SIP destinations: the IPTel (a free SIP provider) echo test service and the TellMe SIP service.

also the basic voice signaling for which the channels are primarily used.

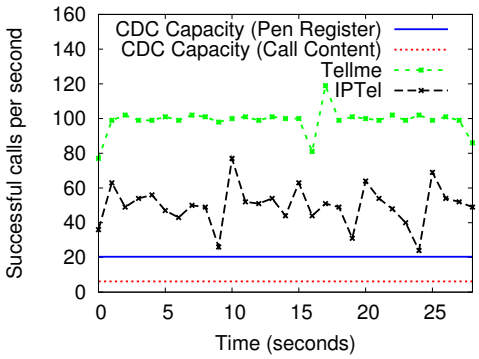

Figure 2: Achieved SIP VoIP call rates using residential broadband connections.

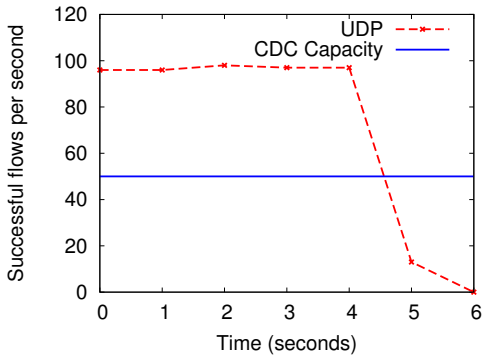

Figure 3: Number of flows per second, measured at the receiver, using Sprint's EVDO cdma2000 data service.

Requiring no SIP-to-wireline gateways, calls to the echo test server are analogous to calls directed towards an internal TSP destination (e.g., voicemail). Calls to TellMe reflect purely SIP-to-SIP communication. The achieved call rates, measured as the number of successful completed calls per second, is shown in Figure 2. To prevent our experiment from attacking the two called services, we capped our call rate at 100 calls per second (careful measures were taken to ensure that both services could easily tolerate such rates).

According to the PacketCable™ Specification, a completed subject-initiated VoIP call produces the following CDC message sequence: `Origination`, `CCCOpen`$^\flat$, `Answer`, `CCChange`$^\flat$, `CCClose`$^\flat$, and `Release`, with messages marked with $\flat$ sent only for content wiretaps. Thus, every completed call produces 3 or 6 CDC messages, depending upon whether call content is delivered to the LEA. The corresponding message sequences require 393 or 1293 bytes for pen register and content wiretaps, respectively. A 64kbps CDC can therefore handle 20.36 calls/second for pen register taps and 6.19 calls/second for content wiretaps. Hence, the signaling rate achievable using a consumer cable Internet connection is more than sufficient to overwhelm the CDC.

The above attack highlights the inadequate provisioning of VoIP CDCs. Other signaling attacks – for example, the rapid production of hold, transfer, or call forwarding signals – are likely also effective at overflowing the CDC. In general, allocating wiretap resources based on statistical call models (which likely differ little between VoIP and wireline services) does not take into consideration the resources available to a motivated adversary.

IP Flows Adopted in 2006, the J-STD-025-B revision of the J-standard added requirements for intercepting and reporting packet data (for example, mobile Internet connections made using cdma2000 or GPRS/UTMS). Reporting of connections over the CDC is performed at two different granularities. `PacketDataEstablishment` and `PacketDataTermination` messages are respectively generated each time the subject attaches to and disconnects from the Internet. Each network "flow" is indicated using a `PacketDataPacketFilter` message. For TCP, the start of a flow is recorded when a SYN packet is first intercepted and continues until a FIN or RST closes the connection. UDP flows begin when the tuple {source IP, source port, destination IP, destination port} is first seen, and expire after a timeout period has elapsed.

Several of the fields within a `PacketDataPacketFilter` messages contain objects whose exact encoding and size we were unable to determine. At a minimum, however, a message must be at least 160 bytes to contain the mandatory fields and addresses. A subject who can open (or close) 40 flows per second will fill a 64 kbps CDC, causing denial-of-service.

Sending 40 TCP SYN packets or empty UDP packets per second requires 16kbps of upstream bandwidth from the target's data connection, well within the advertised rates available on 3G and 2G+ data networks in the US. To evaluate whether this holds true in practice, we used a Sierra Wireless Compass 597 EV-DO Revision A cdma2000 modem provisioned for Sprint's wireless data service. This card connects to a computer using a USB2 connection, and data sessions are made by opening a PPP session over the device. We measured the maximum rate at which we could establish new UDP flows to a server in our lab, which is shown in Figure 3. The results show that for the first four seconds a steady rate of 100 connections per second was achievable, after which traffic shaping within the Sprint network kicked in and blocked new connections from being established to our server for several seconds. However, 4 seconds is more than sufficient to initiate a voice call in parallel, causing the `Origination` and `CCOpen` messages to be lost. For complete stealth, the CDC could be flooded again when terminating the voice call, leaving no record at the Collection Function.

3.2 Inbound Attacks

The previous section described attacks in which the wiretap target produces signaling information at a rate that exceeds the wiretap's capacity. We now consider wiretap countermeasures that may be carried out by parties other than the wiretap target.

Kampmeier *et al.* [19] speculated that Call Content Channel (CCC) resources may be exhausted if the target uses call forwarding (a service that redirects incoming calls to a destination selected by the service subscriber). The J-standard requires that a CCC be provisioned per call rather than per service, and hence each forwarded call must be allocated its own CCC. Since CCCs are a limited resource, a sufficient number of incoming forwarded calls will consume all CCC channels, causing subsequent calls to or from the target to be unmonitored.

We demonstrated the practicality of this attack by con-

figuring a mobile phone (the "target") to forward calls to a large call center. In the most generous scenario listed in the annex of the J-standard, LEAs may provision a T1 line to carry CCCs from the TSP. A T1 has 23 bearer channels for carrying voice or data traffic, one of which is used by the CDC, leaving 22 channels for CCCs. (The number of available CCCs may be even lower if the T1 line is shared between multiple wiretaps.) In our experiment, 29 callers using various cellular carriers were asked to simultaneously call the target's mobile phone number. When the target used AT&T's mobile service, 20 of the 29 calls were successfully forwarded. We repeated the experiment using T-Mobile as the target's service. Here, all 29 callers were forwarded to the call center, exceeding the capacity of the T1 link that carries CCCs between the TSP and the LEA.

An analogous (but perhaps less practical attack) is possible against the CDC. Each incoming forwarded call produces `TerminationAttempt`, `CCOpen`$^\flat$, `Redirection`, `CCClose`$^\flat$, and `Release` LAESP messages ($\flat$ indicates messages generated only for content wiretaps), consuming 482 or 736 bytes of CDC bandwidth for pen register and content wiretaps, respectively. Since the CDC is transmitted over a single 64kbps bearer line, the CDC may be exhausted if the rate of incoming calls exceeds 16.60 (for pen register) or 10.87 (for call content wiretaps) calls per second.

3.3 Injecting Uncertainty into Packet Traces

Wireless service providers regularly sell data plans that connect mobile devices to the Internet. The J-standard specifies that intercepted IP packets should be mirrored to law enforcement agencies (LEAs) without modification in content wiretaps. Below, we identify three techniques that prevent the reliable reconstruction of IP flows.

Confusion *Confusion* has been previously proposed as a method of injecting false information into the transcripts of Internet eavesdropping systems [8]. By injecting specially crafted IP packets that are intercepted by the eavesdropper but are never received by the receiving party (e.g., a web or email server), wiretap subjects hinder the accurate reconstruction of actual communication.

The eavesdropping subject may apply a number of techniques to cause spurious chaff to be accepted by the wiretap but dropped by the network before reaching the receiver. For example, she may use packet TTLs that are insufficient to reach the receiver, produce packets whose sizes exceed a hop's MTU, or specify IP options that cause packets to be dropped by intermediary Internet routers [8, 24].

Internet eavesdroppers can be located at various positions in the network: near the sender, near the receiver, at routers along the path joining the communicating parties, or in the case of colluding eavesdroppers, some combination of the above. Reliably confusing Internet monitoring systems is difficult since it requires precise knowledge of the locations of all interception points. Generally, such information is not known to the eavesdropping target.

By providing the subject with the location of the interception point, the wiretap architecture proposed in the J-standard makes it significantly easier to conduct confusion attacks. Given the wiretap's location, the subject can more accurately construct messages (e.g., with small TTLs) that will be recorded by the wiretap but dropped before reaching the receiver.

To verify the feasibility of conducting confusion attacks, we transmitted specially crafted confusion packets on Sprint's cdma2000 data network to a server running on our institution's network. Packets were constructed using the hping packet assembler tool [26] running on a laptop connected to Sprint's network via a Sierra Wireless Compass 597 EV-DO modem. We verified that the cdma2000 network routed packets with arbitrary TTLs and with the Congestion Window Reduced (CWR) and ECN-Echo (ECN) TCP flags set. By specifying sufficiently small TTLs, we were able to produce routable packets that did not arrive at the receiver but would be perceived by the wiretap.

Subject-Originated cdma2000 Timestamps Each IP packet is enveloped within a `cdma2000InterceptionofContent` LAESP message before being transmitted to the LEA. Along with the IP packet's payload, the LAESP message includes a timestamp of when the IP packet was intercepted. The timestamp is not required if the underlying protocol (the J-standard lists RTP [27] as an example) includes timing information in the protocol header.

CALEA systems that rely on application-layer protocol headers to convey timing information are vulnerable to manipulation. The subject can send messages with erroneous date information, aggravating LEA's ability to accurately reconstruct flows. Additionally, the subject may specify timestamps that are outside of the dates specified in the wiretap order, potentially forcing the disqualification of such records in court proceedings.

Loss of cdma2000 Direction Information `cdma2000InterceptionofContent` messages contain an optional field that indicates the direction of the IP packet (that is, towards or away from the wiretap subject). If cdma2000 messages do not use the direction field and are transmitted over a combined CCC (carrying both inbound and outbound packets), the LEA must discern the sender and receiver of intercepted messages using network addresses specified in the IP header. A subject could exploit the lack of directionality information and generate forged IP packets purportedly from another party to the subject, hence inserting arbitrary and non-existent communication into the wiretap transcript.

3.4 In-band Signaling within the Service Provider Network

As an optional feature, intercept access points (IAPs) may communicate *hook status* (whether or not the line is in use) to the Delivery Function (DF) using in-band signaling. When the subject's line is not in use, the IAP transmits a "C-tone" (a two frequency audio signal consisting of 852Hz and 1633Hz) to the DF. Upon detection of C-tone, the DF releases the CCC and transmits a `CCClose` message on the CDC [3], causing LEA equipment to stop recording.

A subject can exploit the use of in-band signaling and apply C-tones during her conversation to avoid being recorded. Since the DF cannot distinguish between C-tones produced by the IAP or by the wiretap subject, the subject can disrupt the wiretap at will by playing C-tones, even at low volume, over her conversations.

In a previous paper [28], we noted a similar vulnerability in pre-CALEA "loop extender" wiretap systems. In these systems, the telecommunications service provider (TSP) transmits hook status information to the LEA using in-band signaling over the same voice channel used to relay the content.

In loop extender systems, recording equipment located at the LEA stops recording (and mutes the speaker) whenever it detects the presence of C-tone, regardless of whether the C-tone originated from the TSP or from the wiretap subject [28]. In contrast, the design of J-standard CALEA systems should eliminate the use of in-band signaling between the TSP and the LEA (since signals are sent out-of-band via the CDC).

In CALEA systems, ironically, the problem appears to be much worse: in-band C-tone signaling may be used not just at the link between the TSP and law enforcement (where the vulnerability can be more easily mitigated on the law enforcement side), but also *internally* within the TSP's delivery network. That is, if a surveillance subject applies C-tone on a link tapped by CALEA equipment designed in this way, the CCC between the TSP and the LEA simply closes (as if the call terminated normally) and no content is delivered at all. Worse, nothing the LEA equipment does by itself can detect or mitigate such an attack; it can only be fixed at the TSP side.

3.5 Content Leakage

In the case of a pen register only tap, US law requires that *no* call content be delivered to the LEA. However, many telephony features make separating *call-identifying information* from *content* a non-trivial task. The problem is even murkier in IP telephone networks since both signaling information and digitized audio are sent over the same channel and often within the same packets.

Merely excluding CCCs from delivery in pen register taps does not necessarily remove all content delivered to the law enforcement agency. For example, content is delivered via the CDC when intercepting SMS messages. In the publicly available TSP literature [16, 1, 4] and in patents for wireless interception devices [9], the content of SMS messages is transmitted via `PacketEnvelope` messages on the CDC. Neither the J-standard nor any of the vendor implementations attempt to separate SMS content from SMS identifying information. If an LEA receives any information about an SMS message, it receives the entire message as well.

Additionally, the transmission of post cut-through dialed digits (i.e., digits dialed after call completion) via the CDC is another instance of content leakage. We are aware of no technology that can accurately discern whether post cut-through digits belong to another phone number or (for example) a bank account and PIN.

The communication of any content to LEAs over the CDC in the absence of a content warrant may be in violation of US law. In particular, while there is not yet a general consensus, courts are beginning to affirm that post cut-through digit extraction constitutes content and may therefore not be provided in pen register wiretaps [29, 21].

3.6 Legacy Attacks

For completeness, we briefly describe in this section the vulnerabilities in CALEA systems that have been previously identified in the literature.

Confusion and Evasion Dialing In pre-CALEA loop extender wiretap systems, separate DTMF decoders residing at the telecommunications service provider (TSP) and the law enforcement agency (LEA) are respectively used to route calls and record telephone numbers dialed by intercept subjects. Since the same analog DTMF tone is decoded by two distinct systems that inevitably have slightly different tolerances, a wiretap subject may generate DTMF tones at the edge of acceptable ranges that are interpreted by one decoder and not by the other. In previous work [28], we demonstrate that the wiretap subject can *confuse* the wiretap by generating DTMF tones that are accepted by the wiretap while being ignored by the switch (e.g., by varying pitch, amplitude, etc. of the tones). Similarly, the subject may *evade* detection by producing tones that are acceptable to the switch but are ignored by the loop extender system.

Post-loop-extender CALEA systems utilize intercept access points (IAPs) located within switching hardware to record the TSP's decodings of DTMF tones. At first blush, the J-standard architecture appears to thwart confusion and evasion dialing since LAESP messages contain the switch's interpretations of DTMF tones. However, a target of a CALEA wiretap can circumvent her TSP by using a third-party service (for example, a calling card service) to route calls. Typically, a user of such services specifies the called party's telephone number using post cut-through DTMF tones. Although the call is subject to wiretap, the TSP does not have direct access to the third-party's interpretation of the post cut-through DTMF digits.

CALEA attempts to mitigate such wiretap circumvention attempts by decoding post cut-through digits and reporting their interpretations via `DialedDigitExtraction` messages. As with loop extender systems, the device used to decode DTMF tones for the wiretap is independent of the system that interprets the tones to route calls, allowing the subject to use confusion and evasion techniques to insert false records into the wiretap transcript.

In-band Signaling on the CCC Pre-CALEA loop extender wiretap systems utilize in-band signaling to convey hook status. When the phone is on-hook (not in use), DTMF C-tone is applied to the connection between the TSP and the LEA. Loop extender systems stop recording when C-tone is detected, regardless of whether the DTMF tone is produced by the TSP or by the subject.

CALEA systems based on the J-standard do not use in-band signaling between the TSP and the LEA. Instead, call-identifying information is sent via a physically separate CDC channel. Provided that TSP switches do not relay hook status information using in-band signaling to the DF (creating the vulnerability described in Section 3.4), the subject should not be able to manipulate the CALEA wiretap by applying C-tones.

However, as noted in our original study [28], CALEA vendor literature and related patents describe C-tone on the CCC as an optional feature to control audio recording equipment at the LEA [10, 13, 14, 19, 25]. CALEA systems may apply C-tone to CCCs to inform LEA equipment that the subject's phone is on-hook. If the LEA equipment relies on the presence or absence of C-tone on the CCC to discern hook status, the subject can easily control the recording equipment and wiretap log seen by law enforcement.

4. PRACTICAL ATTACK SCENARIOS

Using easily obtainable equipment, a subject can conduct unilateral attacks against virtually all TSP services, causing either gaps in wiretap transcripts or the recording of inaccurate information. Below, we describe several practical attack

scenarios in which the wiretap target can evade monitoring and/or inject uncertainty into call records.

- A target with a mobile data service installs an application on his smartphone that continuously generates UDP connections to one or more Internet sites. The resultant `PacketDataPacketFilter` LAESP messages saturate the CDC. Since `Origination` messages that indicate subject-initiated calls consequently do not reach the LEA, the target may place calls that do not appear in the wiretap's call records. Similarly, `CCOpen` messages may be lost (in the case of content wiretaps), preventing the LEA from associating a CCC with the call, enabling the target to communicate via voice and data without being monitored.
- A wiretap subject with wireline and mobile services conducts the above UDP flow attack using his smartphone to saturate the CDC. Since the same CDC is used to convey signaling information for both the wireline and mobile services, the target may place unmonitored calls using his wireline phone.
- A VoIP subscriber wiretap target uses a scriptable softphone or call generation tool (e.g., SIPp) to rapidly place VoIP calls to his voicemail service. Operated by the TSP, the voicemail service does not require traversal of the traditional wireline telephone network. To maximize his signaling rate while limiting the resources required by the voicemail system, calls are immediately disconnected after they connect. Since the signaling capacity of the wiretap target vastly exceeds that of the CDC, the target exhausts the resources of the CDC connection. Call records and call content pertaining to the subject's legitimate incoming and outgoing calls are not recorded due to CDC congestion.
- A mobile data service subscriber installs an application on her smartphone that sends a superfluous packet with small TTLs before each legitimate packet. As most TCP reassemblers discard packets with previously seen sequence numbers (even if their contents differ) [8], the wiretap reconstructs the target's chosen chaff rather than the legitimate traffic. In contrast, since the receiver is located further from the sender than the wiretap, the receiver does not receive the chaff traffic with small TTLs. Manual inspection of wiretap logs may reveal the target's duplicity, but without knowledge of the precise network topology *at the time of interception*, the LEA cannot definitively reconstruct traffic flows.
- A wireline, mobile, or VoIP subscriber produces C-tones at low amplitudes during the duration of her calls. Due to the use of in-band C-tone signaling within the TSP, the TSP's Interception Access Point (IAP) produces `CCClose` LAESP messages and consequently the target's calls are not recorded in call-content wiretaps.
- A wiretap target enables call forwarding on her wireline or mobile phone, redirecting calls to a high capacity call center (e.g., an airline reservation system). Using an automated tool (e.g., SIPp), she places many concurrent calls from a subscribed Internet VoIP service to her phone, causing all calls to be redirected and forcing the TSP to delegate a separate CCC for every VoIP call. By placing 22 such VoIP calls, she exhausts the capacity of the T1 connection between the TSP and the LEA, enabling her to use her wireline or mobile phone to place unmonitored calls.

The above attack scenarios are by no means exhaustive of all possible wiretap countermeasures, and are intended only to highlight the architectural weaknesses in current-generation CALEA wiretap systems.

5. STOPGAP MITIGATION PRACTICES

In this section, we describe stopgap mitigations for several of the described vulnerabilities. These recommendations and best practices are intended to be used with currently deployed CALEA equipment. However, because many vulnerabilities arise from the architectural design of J-standard-based implementations and cannot therefore be remedied without significantly modifying the wiretap infrastructure, the recommendations presented below are intended to mitigate some (but not all) of the described attacks and do not necessarily result in a system that is impervious to manipulation.

- **Provision CDC and CCC resources according to the subject's signaling capabilities.** The LEA and TSP should ensure that bandwidth and other resources are properly allocated for the CDC and CCC to prevent exhaustion attacks. Rather than provision bandwidth according to estimated average-case signaling rates, bandwidth requirements should be derived from the subject's maximum possible signaling rate. Additionally, this same worst-case analysis should be performed on internal links connecting IAPs to the Delivery Function.
- **Do not trust the interpretations of third-party signaling.** The wiretap system should not be trusted to accurately estimate the interpretation of data by a third-party. For example, the decoding of post cut-through DTMF tones is subject to manipulation (see Section 3.6) and should not be considered accurate.
- **Disable in-band signaling features.** In-band signaling (e.g., the use of C-tones to convey hook status) allows the subject to control the behavior of recording equipment. In-band signaling should not be used between IAPs and the DF (see Section 3.4) or between the TSP and the LEA (see Section 3.6).
- **Provision each wiretap with its own CDC.** A CDC should not carry call-identifying information from multiple wiretap orders, preventing the manipulation of one wiretap from causing denial-of-service to another.
- **Clearly demarcate inbound and outbound messages in a CCC.** CCCs should always capture directionality. If a combined CCC is used, the directionality bit for packet data should be turned on.
- **Reconcile pen register information with other forms of evidence.** LEAs should examine billing records and other forms of evidence to reconcile pen register information. Although such data may not be available in real-time, the transmission of stored call records is not susceptible to resource exhaustion attacks.

Although several of the vulnerabilities described in Section 3 can be mitigated using the above stopgap procedures, there are many design characteristics of CALEA systems that make them inherently susceptible to manipulation. In particular, combining data from multiple IAPs into a single CDC, sending SMS and IP payloads via the CDC, and requiring a separate CCC for each call leg are intrinsic in CALEA designs based on the J-standard, leading to vulnerabilities that cannot easily be addressed by modifying the configurations of wiretap systems. Additionally, while

many of the resource exhaustion attacks identified could be best mitigated by modifying TSP equipment, rarely do these attacks on CALEA impact the operational stability of the TSP. Without such danger there is little motivation for TSPs to rate limit (potentially profitable) calls or messages.

6. CONCLUSION

This paper represents the first (in the public literature, at least) security analysis of the J-standard, the architecture currently used for the vast majority of law enforcement wiretaps in the United States [2]. Our results demonstrate that modern services, especially the wireless platforms that account for most of the wiretaps, render these systems vulnerable to denial-of-service and other attacks. Unlike traditional eavesdropping countermeasures (e.g., encryption), these attacks can be done unilaterally by a wiretap subject, are difficult to detect by law enforcement, and prevent the accurate collection not only of content, but of the metadata recorded in legal record.

Given that the J-standard appears to have been engineered narrowly based on outdated assumptions about communications platforms and has been "patched" several times to accommodate a changing environment, the presence of vulnerabilities in the architecture is somewhat unsurprising.

However, the scope and severity of the vulnerabilities embedded in the standard is both surprising and disturbing. It is especially dismaying that the CALEA standards – protocol specifications used for evidence gathering and investigative intelligence – fail to consider *any* attack model in which a motivated target deliberately attempts to evade the wiretap.

Instead, the standard notes (unwisely, as we have seen) only that resources should be provisioned according to statistical traffic models [22] (for VoIP services) or that law enforcement has expressed preferences for 64kbps ISDN channels [3] (for wireline and wireless services). The asymmetry of signaling resources between the target of the wiretap and the channel over which wiretap information is conveyed enables the target to overwhelm the wiretap at will. Moreover, because signaling information from multiple sources is multiplexed over the same low-capacity link to law enforcement, a target may use a high bandwidth service (e.g., his mobile network's data service) to saturate the wiretap in order to place unmonitored calls using a lower bandwidth service (e.g., a wireline telephone). Since multiple wiretaps at a given switch may share the same channel to law enforcement, the resource consumption attack applies to all wiretaps at the switch, not just those of the subject conducting the attack.

In addition to overwhelming the capacity of the wiretap's signaling channel, we discovered attacks in which a target of a content wiretap can inject spurious IP packets into wiretap transcripts, potentially causing the wiretap to interpret messages of the target's choosing rather than the messages received by the other communication party. Another attack, using call forwarding features, exhausts the wiretap's call content resources, allowing the target of a content wiretap to converse without being monitored. Finally, we note that the use of in-band signaling within the telephone network enables the target to suppress recording by producing low amplitude dual frequency tones.

The vulnerabilities in the J-standard represent a serious threat to the accuracy and completeness of wiretap records used for both criminal investigation and as evidence at trial. This has implications not only for investigators and prosecutors, but also for defendants, since exculpatory evidence might also be missed.

ACKNOWLEDGMENTS

The authors are grateful to Andrew Brennan for help with some of our experiments, and to the anonymous reviewers for their insightful feedback. This work is partially supported by NSF Grants CNS-0831376 and CNS-0627579. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the National Science Foundation.

7. REFERENCES

[1] 3rd Generation Partnership Project. Lawful interception architecture and functions. Technical Specification Group Services and System Aspects 3GPP TS33.107 v3.1.0, 2000.

[2] Administrative Office of the United States Courts. Wiretap report, 2007.

[3] American National Standards Institute. Lawfully authorized electronic surveillance. Joint Standard ANSI/J-STD-025B, TIA/ATIS, Aug. 2003.

[4] ANSI. UMTS handover interface for lawful interception handover interface for lawful interception. Standard ANSI T1.724-2004, Alliance for Telecommunications Industry Solutions, Jan. 2004.

[5] S. M. Bellovin, M. Blaze, W. Diffie, S. Landau, P. G. Neumann, and J. Rexford. Risking communications security: Potential hazards of the Protect America Act. *IEEE Security and Privacy*, 6(1):24–33, 2008.

[6] Cisco Systems, Inc. VoIP over Frame Relay with Quality of Service (Fragmentation, Traffic Shaping, LLQ / IP RTP Priority), February 2006. Document ID 12156.

[7] Communication Technologies, Inc. SMS over SS7. Technical Information Bulletin 03-2, National Communications System, Dec. 2003.

[8] E. Cronin, M. Sherr, and M. Blaze. On the (un)reliability of eavesdropping. *International Journal of Security and Networks (IJSN)*, 3(2):103–113, 2008.

[9] C. T. Dikmen and M. Karabatur. System for intercept of wireless communications. Patent No. 6, 577, 865, U.S. PTO, 2003.

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

[11] FBI CALEA Implementation Unit. AskCALEA frequently asked questions, Oct. 2008. http://www.askcalea.net/faqs.html.

[12] R. Gayraud and O. Jacques. SIPp. http://sipp.sourceforge.net/.

[13] R. M. Howell. Method of intercepting telecommunications. Patent No. 5, 920, 611, U.S. PTO, 1996.

[14] R. M. Howell. Telecommunications intercept system. Patent No. 5, 943, 393, U.S. PTO, 1996.

[15] International Packet Communications Consortium. Lawfully Authorized Electronic Surveillance for

Softswitch-based Networks, July 2003.

[16] IPFabrics. *DeepSweep VoIP Surveillance Modules User's Manual*, May 2007. http://www.ipfabrics.com/pdf/VoIP_SM_users_manual.pdf.

[17] ITU. ISDN user-network interface layer 3 specification for basic call control. Recommendation Q.931, May 1998.

[18] ITU. Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation. Recommendation X.680, November 2008.

[19] E. E. Kampmeier, D. B. Smith, and M. R. Smith. Utilization of communication channels between a central office switch and a law enforcement agency. Patent No. 6, 728, 338, U.S. PTO, 2000.

[20] S. Landau. Security, wiretapping, and the internet. *IEEE Security and Privacy*, 3(6):26–33, November 2005.

[21] Orenstein, James. In the matter of an application [REDACTED] of the united states of america memorandum for an order authorizing the use of a pen register and trap and trace device... United States District Court Eastern District of New York Case 1:08-mc-00595-JO, December 2008.

[22] PacketCable Electronic Surveillance Focus Team. PacketCable^{TM}Electronic Surveillance Specification. Specification PKT-SP-ESP-I03-040113, Cable Television Laboratories, Inc., January 2004.

[23] V. Prevelakis and D. Spinellis. The Athens affair. *IEEE Spectrum*, 44(7):26–33, 2007.

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

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

[26] S. Sanfilippo. Hping - Active Network Security Tool.

[27] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A transport protocol for real-time applications. RFC 3350, Internet Engineering Task Force, July 2003.

[28] M. Sherr, E. Cronin, S. Clark, and M. Blaze. Signaling vulnerabilities in wiretapping systems. *IEEE Security and Privacy*, 3(6):13–25, November 2005.

[29] Smith, Magistrate No. H-06-356M . In the matter of the application of the united states of america for an order authorizing (1) installation and use pen register and trap and trace device. United States District Court Southern District of Texas Houston Division Case 4:06-mj-00356, July 2006.

[30] TeleCommunications Systems. Lucent/TCS short message service center. http://www1.telecomsys.com/carriers/lucent_smsc.cfm.

[31] TeleDNA Inc. TeleDNA short messaging service center (SMSC), 2008. http://www.teledna.com/pdf/smsc.pdf.

[32] P. Traynor, W. Enck, P. McDaniel, and T. L. Porta. Exploiting open functionality in SMS-capable cellular networks. *Journal of Computer Security*, 16(6):713–742, 2008.

[33] United States Congress. Omnibus Crime Control and Safe Streets Act of 1968: Title III. Pub. L. No. 90-351, 82 Stat. 197, USA, June 1968. (codified as amended in 18 U.S.C. Sect. 2510-2522).

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

[35] United States House of Representatives. Telecommunications carrier assistance to the government. H.R. Rep. No. 103-827, USA, Oct. 1994.