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

Micah Sherr, Gaurav Shah, Eric Cronin, Sandy Clark, and Matt Blaze - CCS'09

By Hassan Shahid Khan

CS 598 - COMPUTER SECURITY IN THE PHYSICAL WORLD

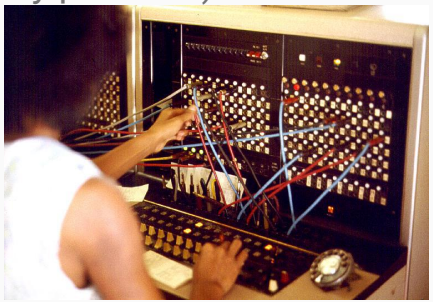
Brief History

- The United States Communications Assistance for Law Enforcement Act (CALEA) became law in 1994 forcing telecom operators to incorporate capabilities for law enforcement wiretapping into their networks.

- Done via a standard interface, in ANSI Standard J-STD-025 (J-standard) for transmitting intercepted traffic to a law enforcement agency (LEA).

Background: Wiretapping Technologies

- **Loop extenders: Tapping the local loop**
  - Interception might be performed at the wireline link between the target and the network (the “local loop” in telephony parlance)



-

CALEA: Tapping in the switch

- Perform interception within the switching equipment of the network provider (telephone switches), allowing more context-sensitive capture of digital as well as analog communications.

Introduction

- Previous work explored vulnerabilities which resulted from the use of in-band signaling via ***loop extender*** technology.

- Question: Is the J-standard for most CALEA wiretaps vulnerable to manipulation by wiretap ***targets*** in ways that ***prevent*** accurate authorized intercepts of their traffic from being collected?

- New CALEA architecture establishes a separate out-of-band channel to communicate signaling information. Separate call content from signaling information.

Is CALEA more secure?

- Unfortunately not. CALEA systems found to be MORE susceptible to manipulation than the loop extender technology.

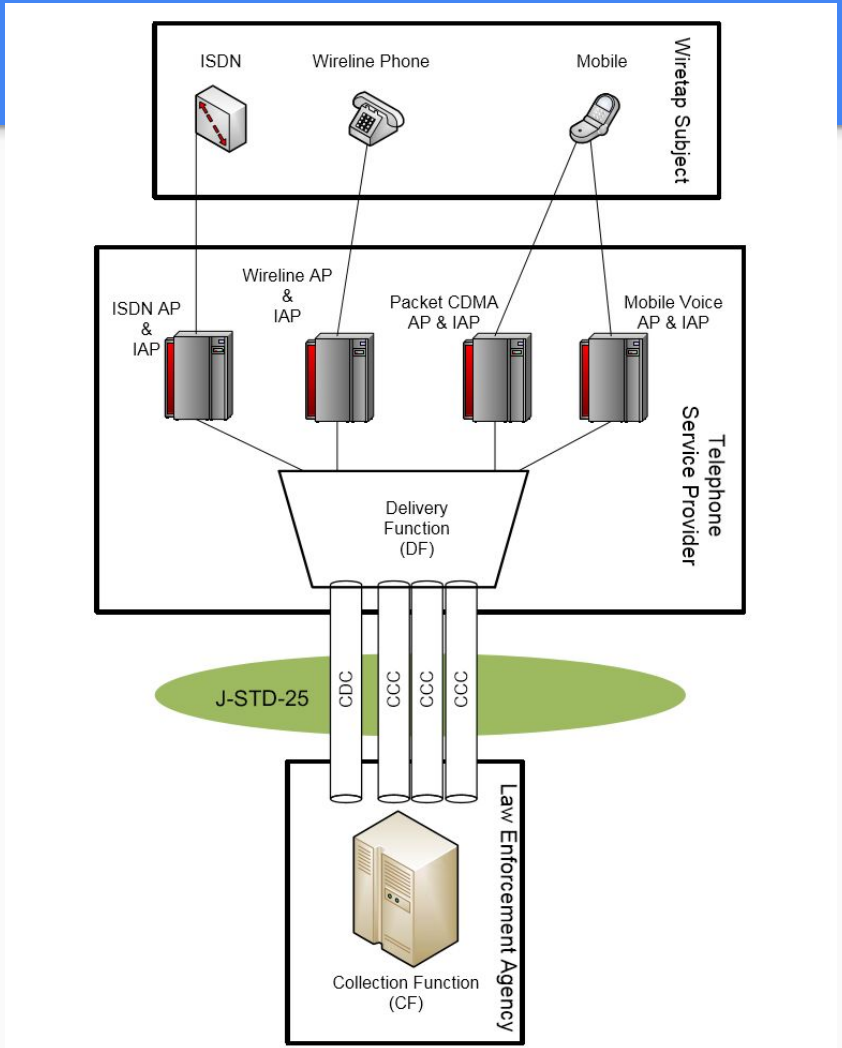
Findings

- Wiretaps are vulnerable to denial-of-service by a wiretap target.

- Found practical attacks that a wiretap target can employ to overwhelm the low-bandwidth signaling channel of the J-STD-025 interface.

J-Standard Architecture

-



J-Standard in a nutshell

Intercepting party leases multiple telephone lines b/w switch and self

- 1) The first of these lines carries a Call Data Channel (CDC) that reports the signaling events (call times, numbers dialed, line status, etc.) for lines being monitored.

- 2) 22 Additional lines, Call Content Channels (CCCs), carry the unedited live audio or data stream of any active monitored lines.
    - Each CCC is dedicated to relaying a particular bearer service (e.g., voice, packet data, etc.) for a single wiretap order

- The CDC carries call data for every active target on the switch tapped by a particular agency. The CCCs **only** carry one audio or data stream at a time

Lawfully Authorized Electronic Surveillance Protocol (LAESP)

Call-identifying information on the CDC is transmitted using a message-based protocol that encodes actions taken by the TSP or the wiretap subject

- 17 messages corresponding to a mix of high and low level network events.
  - Raw user signals (e.g. “phone went on hook”) and higher-level TSP network events (e.g. “call released”)
  - Message sizes can vary depending upon the technology being monitored (variable length fields and conditional fields)
  - 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.

LAESP Messages

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

Observations

(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.

1. Call Data Channel (CDC) Resource Exhaustion

- Highest bandwidth CDC configuration in the J-standard is a single ISDN B channel (64 kbps). When congestion occurs on the CDC, messages are silently dropped.

- Produce signaling information at a rate that exceeds the wiretap’s capacity

- All signalling information may be multiplexed on a single CDC (!)

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.

1. Call Data Channel (CDC) Resource Exhaustion (Cont)

1. ISDN Feature Keys
    a. Each Q.931 feature key message is 6 bytes in length. The generated **SubjectSignal** LAESP message requires 82 bytes. Create 94.11 signalling messages per second.
2. SMS messaging
    a. Each SMS generates a **PacketEnvelope** message (173 bytes). 46 messages per second.
3. VoIP Signaling
    a. A completed subject-initiated VoIP call produces the following CDC message sequence: **Origination, CCCOpen , Answer, CCChange, CCClose , and Release**. 1293 bytes. *6.19 cps*
    b. Used the SIPp traffic generator tool to rapidly place and immediately release SIP calls
4. IP Flows
    a. **PacketDataEstablishment/PacketDataTermination** messages generated upon connecting to Internet. Network “flow” indicated using a **PacketDataPacketFilter** message.
    b. Min 160 bytes needed for the filter message. A subject who can open (or close) 40 flows per second will fill a 64 kbps CDC, causing denial-of-service.

2. Inbound attacks

- J-standard requires that a CCC be provisioned per call rather than per service. Use call-forwarding to consume all CCC channels, subsequent calls will be unmonitored.

Practical Attack Scenario

- 29 callers using various cellular carriers were asked to simultaneously call the target's mobile phone number. In case of T-Mobile all calls were successfully forwarded, congesting the T1 link.

- If these messages are lost, then both pen register and call content data have been irrecoverably destroyed.

3. Injecting Uncertainty into Packet Traces

- Inject specially crafted IP packets that are intercepted by the eavesdropper but are never received by the receiving party.
  - E.g packet TTLs that are insufficient to reach the receiver, produce packets whose sizes exceed a hop's MTU

- Authors crafted packets on Sprint's cdma2000 data network using hping
  - Each IP packet is enveloped within a **cdma2000InterceptionofContent** LAESP message. Timing information parsed from the protocol header.
    - Manipulate packet fields so timestamps that are outside of the dates specified in the wiretap order, making them inadmissable in court
  - Manipulate the **'direction'** field of the LEASP message. (that is, towards or away from the wiretap subject). Insert arbitrary and non-existent communication into the wiretap transcript by generating forged IP packets.

4. In-band signalling within the Service Provider Network

- IAPs can communicate hook status (whether or not the line is in use) to the 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, causing LEA equipment to stop recording.

- DF cannot distinguish between C-tones produced by the IAP or by the wiretap subject

- **Attack Scenario**: subscriber produces C-tones at low amplitudes during the duration of his/her calls

Practical Attack Scenarios

- Continuously generates UDP connections to any website. The resultant **PacketDataPacketFilter** messages saturate the CDC. Subsequent **origination** or **CCOpen** messages may be dropped preventing the LEA from associating a CCC with any calls made in the future

- Use an application to craft superfluous packet with small TTLs before each legitimate packet. TCP reassemblers discard packets with previously seen sequence numbers, the wiretap reconstructs the target's chosen chaff rather than the legitimate traffic.

- Using an automated tool (e.g., SIPp), place many concurrent calls from a subscribed Internet VoIP service to subject's phone, exhausting resources.

Mitigation Strategies

- Provision CDC and CCC resources according to the subject's signaling capabilities.
  - Requirements should be derived from the subject's maximum possible signaling rate.
- 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.
- Provision each wiretap with its own CDC.
- Clearly demarcate inbound and outbound messages in a CCC.
  - Directionality bit should be turned on at all times
- Reconcile pen register information with other forms of evidence.
  - Billing information?

Discussion Points

- What are the key contributions of the paper?
- Limitations of the paper?
- Vulnerabilities arise from the architectural design rather than from any particular implementation defect.
  - This is different to stuff we have seen earlier
- No technical spec was provided for J-standard
  - To avoid encumbering the development of new communication technologies
  - To clearly delineate the responsibilities of telecommunications carriers with respect to court authorized surveillance
- How practical are the attacks described in the paper?
  - Should a target take precautionary measures forever?
- What do you think about backdoors being enforced in other technology?