Signaling vulnerabilities in wiretapping systems

Micah Sherr, Eric Cronin, Sandy Clark, and Matt Blaze

Kyo Kim

Introduction

Law enforcement agencies use wiretapping to collect intelligence and evidence.

Growing reliance in wiretapping.

Wiretapping

Dialed Number Recorder

- Only record the number that the target dialed

Full Audio Interception

- Also records the communication content

The target should not be aware that the communication is being eavesdropped

Loop Extender

- POTS telephone line
- Another line is spliced into the target wire which extends to the tapper.
- Requires physical proximity
- Splicing may result in observable change in line characteristic

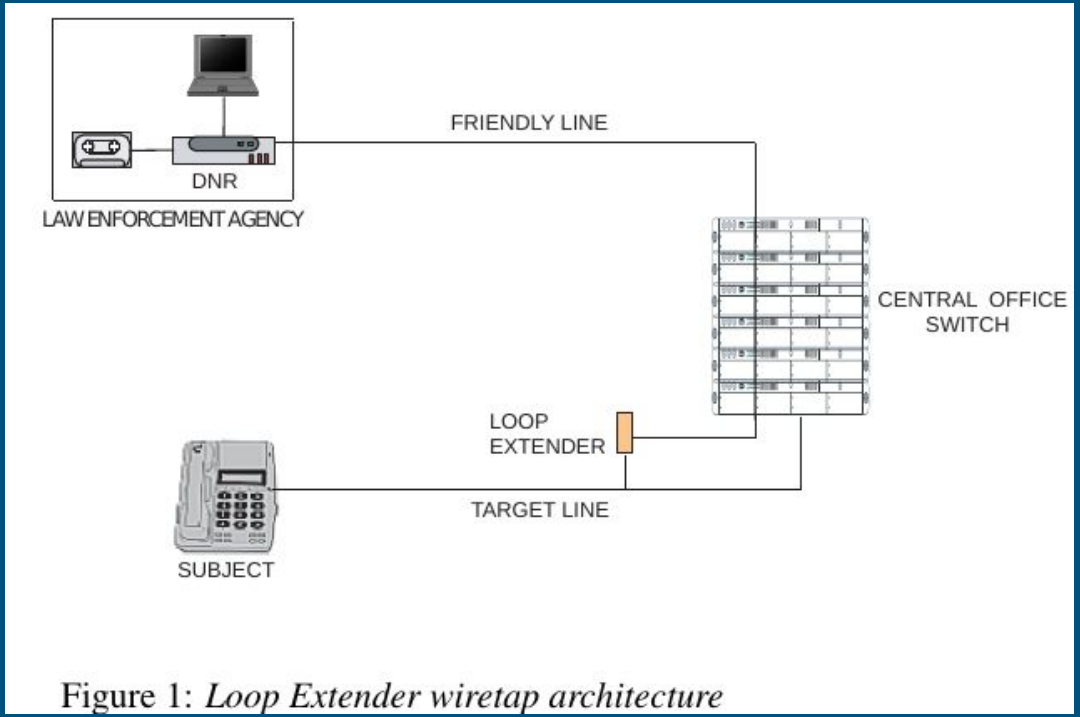

Figure 1: *Loop Extender wiretap architecture*

CALEA taps

- Telephone company provides an interface which law enforcement agency can use.
- CDC contains data about the number dialed
- CCC contains the communication data

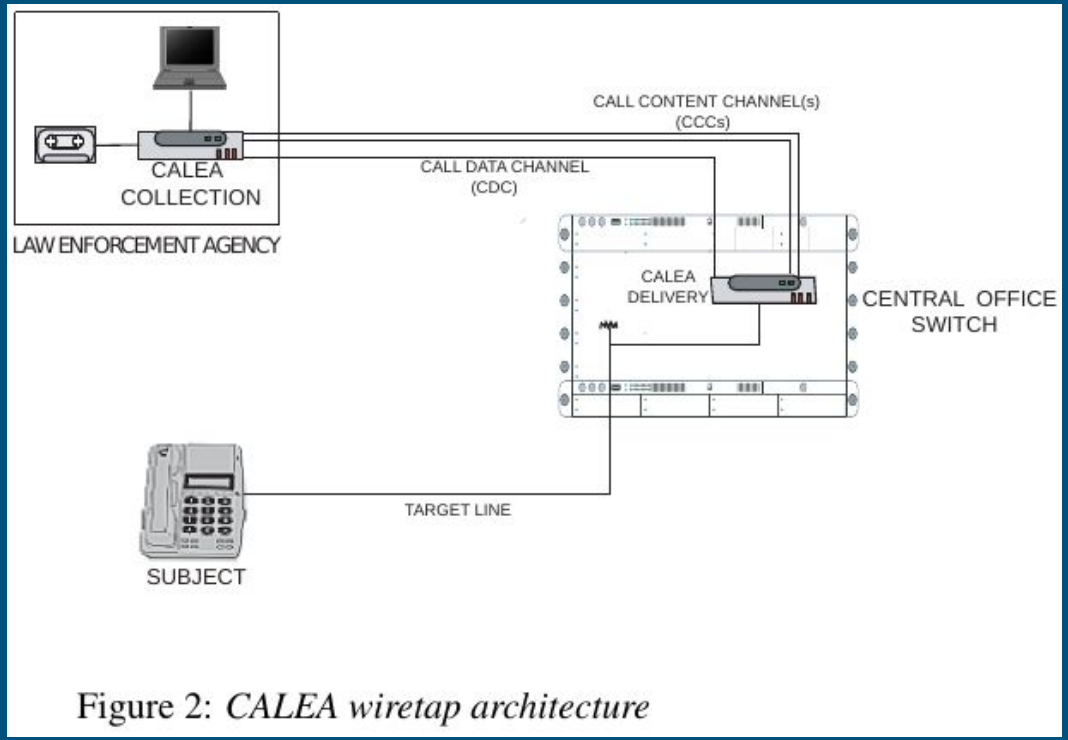

Figure 2: *CALEA wiretap architecture*

DTMF

Dual-Tone Multi-Frequency

Each key produces a “high-tone” and a “low-tone”

There are four more keys

Analog

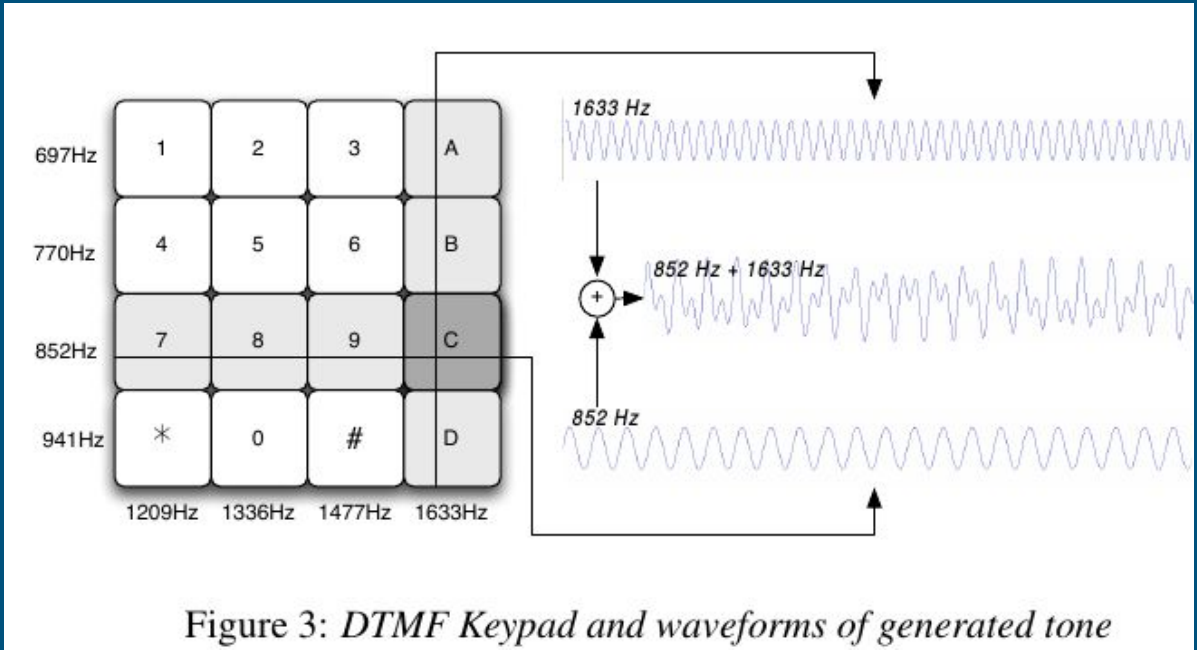

Figure 3: *DTMF Keypad and waveforms of generated tone*

C-tone

De facto standard for idle tone signal.

Motivated by backward compatibility with loop extender.

Voice communication can still occur under the presence of C-tone.

Eavesdropper’s Dilemma

- If the tapping equipment is too conservative, it might not recognize numbers decoded by the switch.

- If the tapping equipment is too liberal, it might recognize numbers that was not decoded by the switch

Method

Slightly change the output signal so that the switch is able to decode correctly while the tapping equipment cannot

Put signals that the switch cannot decode

- Use the switch response as the oracle
  - Use binary search to find the limits
- The tapping equipment is now in eavesdropper ‘s dilemma

Use C-tone to spoof the line status

Experiment

Computer uses the modem to seize the line (taking the line off-hook).

Use the sound card to evade and confuse the tapper.

Used actual telephone switches and simulated telephone switches.

Introduced C-tone to spoof the line to on-hook

Result

Took 30-120 minutes to probe the limits

Correct interpretation is 19876543210

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

Result

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

Correct interpretation is 19876543210

Result

What the tapping equipment observes:

http://www.crypto.com/papers/wiretapping/observed.mp3

What is actually happening:

http://www.crypto.com/papers/wiretapping/unobserved.mp3

Blue Box

2600Hz “idle” signal

Long distance calls are done by connecting to other switches in the path to the destination

Each connection is made by ending the idle signal

Billing is processed at the caller’s switch

Leading to “out-of-band” long distance signaling

Mitigation

Do not stop recording after hearing C-tone, use only on CDC to determine when to stop

Check with the communication company to see if the dialed number decoded in the law enforcement agency is consistent with that of the company.

Discussion

What are the key contributions of this paper?

Was the proposed countermeasure practical?

How relevant is this today?