Legally Authorized Telephone Surveillance: Problems and (Some) Solutions

Micah Sherr
Georgetown University

Joint work with
Adam Bates, Matt Blaze, Kevin Butler, Sandy Clark, Eric Cronin, Gaurav Shah, Clay Shields, Patrick Traynor, and Dan Wallach
What this talk isn’t about

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

at&t
Security analysis of the **legally authorized** domestic telephone wiretapping in the U.S. that is subject to U.S. law and scrutiny by U.S. courts.
Why study telephone wiretapping?

- Lots of prior “work” on illegal wiretapping and countermeasures
- No (public) security analysis of legally authorized wiretap systems
  - Closed-source “blackbox” systems
  - Only sold to law enforcement agencies (LEAs)
- Viewed with little skepticism by judges and juries
- Implications to the public:
  - Investigative intelligence
  - (Exculpatory) evidence in legal proceedings
Why study telephone wiretapping?

• Lots of prior “work” on illegal wiretapping and countermeasures

• No (public) security analysis of legally authorized wiretap systems

• Closed-source “blackbox” systems

• Only sold to law enforcement agencies (LEAs)

• Viewed with little skepticism by judges and juries

• Implications to the public:
  • Investigative intelligence
  • (Exculpatory) evidence in legal proceedings

© www.countermeasures.pimall.com
Is legal wiretapping **reliable?** **trustworthy?** **secure?**
Agenda

- Introduction and Motivation
- Loop Extender Wiretaps
- CALEA Wiretaps
- Recent work: “Accountable Wiretapping”
## Two Flavors of Legal Wiretaps

<table>
<thead>
<tr>
<th>Pen Register / Trap and Trace</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Record metadata (call-identifying information)</td>
<td>- Record content along with call-identifying information (e.g., call audio, text messages, etc.)</td>
</tr>
<tr>
<td>- Identities of caller/callee, time of call, duration, etc.</td>
<td>- Government must establish probable cause</td>
</tr>
<tr>
<td>- Not usually subject to judicial approval</td>
<td></td>
</tr>
</tbody>
</table>

---

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab

https://security.cs.georgetown.edu
Telephony 101

Subscriber → Subscriber's Central Office → verizon → Telephone Network → Callee's Central Office → verizon → Callee
The last mile: How your telephone works

- Telephone cable consists of 2 wires, forms closed loop with Central Office (CO)
- DC current loop detects hookswitch status
- During call, audio is carried via AC signal
- In-band audio used for other signals between phone and CO
  - Tone dialing (DTMF)
  - Dial tone, busy signal, audible ring
Loop extender wiretaps

Target

Target's Telco

Target Line

Friendly Line

Law Enforcement Agency (LEA)
Loop extender wiretaps

Target

Target's Telco

Target Line

Loop Extender

Friendly Line

Law Enforcement Agency (LEA)
Loop extender wiretaps

Target

Target's Telco

Target Line

Law Enforcement Agency (LEA)

Dialed Number Recorder

Friendly Line

Target extender wiretaps

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab
https://security.cs.georgetown.edu
Loop extender listening post at LEA
Acquiring loop extender wiretap equipment
Acquiring loop extender wiretap equipment

- In US, possession restricted to LEAs
  - Felony to own one otherwise (18USC2512)
  - Vendor won’t sell you one
Acquiring loop extender wiretap equipment

• In US, possession restricted to LEAs
  • Felony to own one otherwise (18USC2512)
  • Vendor won’t sell you one
• So you have to get them on eBay
  • (NSF grant makes this legal; don't try this at home)
Unilateral loop extender countermeasures*

- Manipulating captured digits
  - False digits logged in place of real number
- False call records
  - Insert nonexistent calls into log
- Recording suppression
  - Disable audio monitoring and recording at will

* Describes joint work with Matt Blaze, Sandy Clark, and Eric Cronin (IEEE S&P Mag, 2005)
Manipulating captured digits

- Telephone numbers dialed using *Dual Tone Multi-Frequency* (DTMF) or *TouchTone* signals
- DTMF tones decoded by Telco switch at CO
- ... and separately by DNR at LEA
- Acceptance of DTMF depends on frequency of tones, amplitude, twist, noise, distortion, etc.
- No two decoders are identical

<table>
<thead>
<tr>
<th>frequencies (Hz)</th>
<th>1209 Hz</th>
<th>1336 Hz</th>
<th>1477 Hz</th>
<th>1633 Hz</th>
</tr>
</thead>
<tbody>
<tr>
<td>697 Hz</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>770 Hz</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>B</td>
</tr>
<tr>
<td>852 Hz</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>C</td>
</tr>
<tr>
<td>941 Hz</td>
<td>*</td>
<td>0</td>
<td>#</td>
<td>D</td>
</tr>
</tbody>
</table>
Manipulating captured digits

Spectrum

Acceptable range of tone amplitudes – ISO Standard
Manipulating captured digits

Spectrum

Acceptable range of tone amplitudes – ISO Standard

Range accepted by Telco switch
Manipulating captured digits

Spectrum

Acceptable range of tone amplitudes – ISO Standard

Range accepted by Telco switch

Range accepted by wiretap decoder
Manipulating captured digits

Confusion:
Interpreted by wiretap but ignored by Telco switch

Acceptable range of tone amplitudes – ISO Standard

Range accepted by Telco switch

Range accepted by wiretap decoder
Manipulating captured digits

- Evasion: Interpreted by Telco switch but ignored by wiretap
- Confusion: Interpreted by wiretap but ignored by Telco switch

Acceptable range of tone amplitudes – ISO Standard

Range accepted by Telco switch

Range accepted by wiretap decoder
Manipulating captured digits

Confusion:
Interpreted by wiretap switch but ignored by Telco switch

Range accepted by Telco switch

Range accepted by wiretap decoder
Manipulating captured digits

Evasion:
Interpreted by Telco switch but ignored by wiretap

Range accepted by Telco switch

Range accepted by wiretap decoder
Recording suppression

- DC signaling used to convey (target's) hook status to CO
- Cannot relay target's DC signals over “friendly line” to LEA
- Loop extenders put a continuous “C tone” DTMF signal on the friendly line when the target line is not in use
  - Idle tone removed when target goes “off hook”
  - DNR activates when C-tone off, deactivates when C-tone on
Exploiting C-tone signaling

- DNR cannot distinguish “authentic” C-tone signal generated by loop extender from “fake” C-tone sent by subject on target line
  - In both cases the DNR detects, correctly or falsely, that the target line has been hung up
  - Turns off recording equipment, logs end of call
- Low amplitude C-tone (less than 1/1000 of normal signal) sufficient to disable audio monitoring and recording
• Alice and Bob, suspected of some kind of illicit activity, are subjects of Title III wiretap order.

• This short call was captured with a Recall NGNR-2000 loop extender system.
• Alice and Bob, suspected of some kind of illicit activity, are subjects of Title III wiretap order.

• This short call was captured with a Recall NGNR-2000 loop extender system.
• Their conversation was actually much longer
  • In fact, Alice and Bob run an illicit mattress-tag forgery ring
  • But the LEA never finds out...
• Their conversation was actually much longer
  • In fact, Alice and Bob run an illicit mattress-tag forgery ring
  • But the LEA never finds out...
FBI reaction

A spokeswoman for the F.B.I. said “we're aware of the possibility” that older wiretap systems may be foiled through the techniques described in the paper. Catherine Milhoan, the spokeswoman, said after consulting with bureau wiretap experts that the vulnerability existed in only about 10% of state and federal wiretaps today.

- NYTimes 11/30/2005
Agenda

• Introduction and Motivation
• Loop Extender Wiretaps
• CALEA Wiretaps*
• Recent work: “Accountable Wiretapping”

* Describes joint work with Matt Blaze, Sandy Clark, Eric Cronin, and Gaurav Shah (CCS09)
CALEA wiretaps

- CALEA represents 90% of deployed wiretap systems in U.S.
- Results based on analysis of architectural specifications
- No access to actual wiretap hardware
  (we couldn't find CALEA equipment on eBay)
• 1994 U.S. law requires Telcos to wiretap at the switch
• Originally applied to voice services
• Interpreted to also cover wireless data and VoIP
• Law does not specify wiretap mechanisms
  • Telcos and Law Enforcement Agencies (LEAs) develop voluntary standard:
    J-STD-025, also known as the “J-Standard”
  • Telcos that implement J-Standard deemed to be in compliance with CALEA
Legally Authorized Surveillance: Problems and (Some) Solutions

- Originally targeted at voice services
- “Patched” to cover data and VoIP

Wiretap requirements:
- Accurate
- Complete
- Undetectable

Conspicuously absent:
- Resistance to manipulation
- Security analysis or standards
Legally Authorized Surveillance: Problems and (Some) Solutions

- Originally targeted at voice services
- “Patched” to cover data and VoIP
- Wiretap requirements:
  - Accurate
  - Complete
  - Undetectable
- Conspicuously absent:
  - Resistance to manipulation
  - Security analysis or standards

Last modified August 2006
CALEA (J-Standard) architecture

Target

3G Data Service

Mobile Voice

Telco

Telco Switch

Telco Switch

Telco Switch

Delivery Function

LEA

3G Data Service

Mobile Voice

Telco Switch

Telco Switch

Telco Switch

Delivery Function

LEA
CALEA (J-Standard) architecture

Telco Switch → Delivery Function → LEA

- 3G Data Content
- Mobile Voice Content
- Landline Voice Content
- Multiplexed Call Metadata
CALEA (J-Standard) architecture

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab
https://security.cs.georgetown.edu
CALEA (J-Standard) architecture

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab
https://security.cs.georgetown.edu
CALEA (J-Standard) architecture

CAE (J-Standard) architecture

Telco

Telco Switch

Telco Switch

Telco Switch

Delivery Function

J-Standard

3G Data Content

Mobile Voice Content

Landline Voice Content

Multiplexed Call Metadata

LEA

DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab

https://security.cs.georgetown.edu
• Target's signaling actions relayed to Law Enforcement Agency (LEA) via LAESP protocol
  • CCOpen, CCClose: change in “hook status”
  • Origination: target dials outgoing number
  • Answer: called party answers call
Underprovisioning of wiretap resources
Underprovisioning of wiretap resources

- Bad: All subscribed Telco services multiplex metadata over same channel
Underprovisioning of wiretap resources

- **Bad**: All subscribed Telco services multiplex metadata over same channel
- **Badder**: Multiple wiretaps multiplexed over same metadata channel
Underprovisioning of wiretap resources

- **Bad:** All subscribed Telco services multiplex metadata over same channel
- **Badder:** Multiple wiretaps multiplexed over same metadata channel
- **Really Really Bad:** Recommended and highest bandwidth configuration uses 64 kbps ISDN B Channel

(Similar standards for VoIP specify bandwidth be allocated according to “statistical call models”)

Resource exhaustion of Call Metadata Channel

- Target controls when call metadata messages are generated
- Significant amplification factor
  - Change of hook status (1 bit) produces 100 byte LAESP message
- Target has ample signaling capacity to overwhelm resources of call metadata channel

- Effects of call metadata DoS:
  - Incomplete records of call-identifying information
  - Gaps in audio (content) recordings
  - Worse than vulnerabilities in loop extender wiretaps: DoS extends to other wiretaps sharing same call metadata channel
Example: IP Flows

- Each new TCP/UDP flow reported to LEA in 160B LAESP messages
- Call metadata channel can convey at most 50 new flows/second
- Experiment:
  Rapidly produce UDP flows using 3G modem on Sprint's data service

![Graph showing successful flows per second over time]
### Additional call metadata resource exhaustion techniques

<table>
<thead>
<tr>
<th>Technique</th>
<th>Bytes per signal/message on call metadata channel</th>
<th>Target signaling rate required to DoS wiretap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Flows</strong></td>
<td>160 bytes per new flow</td>
<td>50 flows per second</td>
</tr>
<tr>
<td><strong>ISDN “Feature” Keys</strong></td>
<td>82 bytes per “Feature” press</td>
<td>95 signals per second</td>
</tr>
<tr>
<td><strong>VoIP Call Instantiation</strong></td>
<td>393 bytes/call (pen register) 1293 bytes/call (content wiretap)</td>
<td>21 calls/second (pen register) 7 calls/second (content wiretap)</td>
</tr>
<tr>
<td><strong>SMS Flooding</strong></td>
<td>173 bytes/SMS (pen register) 190 bytes/SMS (content wiretap)</td>
<td>46 SMS/sec (pen register) 42 SMS/sec (content wiretap)</td>
</tr>
</tbody>
</table>

In all cases, target can flood wiretap using one service and communicate privately using another.
• Call forwarding enables incoming calls to be redirected to specified phone number

• Each “conversation” must be recorded in content wiretaps

22 available call content channels on a T1 line
Call Content Channel exhaustion

Target → Telco → Telco Switch → Delivery Function → Telco → Target

Department of Justice

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab
https://security.cs.georgetown.edu
Call Content Channel exhaustion

Target

Telco Switch

Delivery Function

Telco

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab
https://security.cs.georgetown.edu
Call Content Channel exhaustion

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab
https://security.cs.georgetown.edu
Call Content Channel exhaustion

Target

Telco Switch

Delivery Function

Telco verizon

IRS
Department of the Treasury
Internal Revenue Service

FBI
Federal Bureau of Investigation

Legally Authorized Surveillance: Problems and (Some) Solutions

Georgetown CS SecLab
https://security.cs.georgetown.edu
Call Content Channel exhaustion

Telco Switch

Delivery Function

Target

Telco

IRS

Department of the Treasury
Internal Revenue Service

Call Content Channel exhaustion
Disabling content recording with in-band signaling (again)
Telco switches convey “hook status” to Delivery Function using dual-frequency tone (852Hz+1633Hz)
Disabling content recording with in-band signaling (again)

Telco switches convey “hook status” to Delivery Function using dual-frequency tone (852Hz+1633Hz)
What can law enforcement do?
What can law enforcement do?

- Provision call metadata and call data channels according to target's **maximum** signaling capabilities
- Provision each wiretap with independent call metadata channel
- Disable in-band signaling features
- Reconcile pen register transcripts with billing records
What can law enforcement do?

- Provision call metadata and call data channels according to target's maximum signaling capabilities
- Provision each wiretap with independent call metadata channel
- Disable in-band signaling features
- Reconcile pen register transcripts with billing records

May require expensive changes to Telco infrastructure
Summary of wiretap systems

- Loop extender wiretaps inherently vulnerable
  - Wiretap must infer behavior of Telco switch
  - Hookstatus relayed via in-band signals
- J-Standard CALEA architecture susceptible to DoS
  - Modern services (e.g., 3G data) provide target with sufficient bandwidth to overwhelm wiretap
  - J-Standard re-introduces legacy attacks
- Unlike encryption,
  - Wiretap countermeasures block call content and call metadata
  - Wiretap countermeasures can be conducted unilaterally
- Some vulnerabilities can be mitigated via wiretap configuration; others are architectural
Lessons learned

Is legal wiretapping **reliable?**

**trustworthy?**

**secure?**

- Wiretap transcripts aren't infallible
- Implementations and standards should consider adversarial model
Agenda

- Introduction and Motivation
- Loop Extender Wiretaps
- CALEA Wiretaps
- Recent work: “Accountable Wiretapping”*

*Joint work with Adam Bates, Kevin Butler, Clay Shields, Patrick Traynor, and Dan Wallach (NDSS 2012)
Accountable wiretapping
Accountable wiretapping

- Existing CALEA systems lack accountability
  - who watches the watchers?
  - case in point: Vodafone Greece wiretapping scandal
Accountable Wiretapping

- Existing CALEA systems lack accountability
  - who watches the watchers?
  - case in point: Vodafone Greece wiretapping scandal

- Ideally, we want “auditable” wiretap systems
  - verify correctness (completeness, soundness) of wiretap transcripts
    - prevent some of the attacks previously discussed
  - ensure that wiretaps have been properly authorized
    - sheriff doesn’t get to wiretap his daughter’s boyfriend
  - avoid redesigning the telco infrastructure (assume we want to achieve the above without spending $1T)
Audit goals

• Security goals:
  • **Integrity**: identify modified or corrupted records
  • **Completeness**: identify gaps in wiretap record
  • **Date compliance**: determine whether wiretapping occurred outside of court-authorized dates

• Reporting goals:
  • **Reporting**: report number of new and expiring pen/trap wiretaps, and new and expiring content wiretaps
    • necessary for legally-mandated reporting requirements
    • extremely difficult to compile reports (federal and state and local wiretaps)
• Send encrypted copy of all wiretap information to offsite, third-party storage facility (the “Log”)
  • Lightweight “Encryptor” device sends encrypted wiretap events and chaff to Log
  • Untrusted Log cannot decipher legitimate messages nor distinguish wiretap events from noise
Wait a sec... we should send all wiretap data to a 3rd-party service?

- Actually, this is already done.
- We’re just going to do it better.
  - (I.e., we don’t trust the service.)
Audit types

• Log enables multiple audit types:
  • **court audit:** auditor asks for all records pertaining to a particular wiretap
    
    ![Diagram showing court audit process]
    
    (1) wiretap ID
    (2) wiretap records

  • **accountant audit:** auditor asks for summary wiretap statistics
    
    ![Diagram showing accountant audit process]
    
    (1) statistics request
    (2) statistics
### Court audits

- For each wiretap event $\tau_i$, Encryptor sends

$$M_i = \langle t_i \ || \ E_r(\tau_i \ || \ I_w \ || \ h(\tau_i \ || \ I_w)) \ || \ \beta_i \rangle$$

- $M_i$ is sent to the Log, where:
  - $t_i$ is a timestamp
  - $E_r(\cdot)$ is the encryption of $\cdot$ with a wiretap key $r$ provided by the court (and not known to the Log)
  - $I_w$ is an event counter
  - $h$ is a cryptographic hash function
  - $\beta_i$ is an aggregation block (explained later)

- In a court audit, the auditor requests all records between times $T_{start}$ and $T_{end}$

- Only auditors who possess the correct wiretap key (as provided by the authorizing court) can decrypt
Court audits

\[ M_i = \langle t_i \parallel E_r(\tau_i \parallel I_w \parallel h(\tau_i \parallel I_w)) \parallel B_i \rangle \]

- Integrity protection through standard techniques
- Omissions readily apparent by “skips” in the event counter
- Use of heartbeat messages “bookend” potential omissions
Accountant audits

\[ M_i = \langle t_i \parallel E_r(\tau_i \parallel I_w \parallel h(\tau_i \parallel I_w)) \parallel B_i \rangle \]

- Each wiretap record includes an **aggregation block**:
  \[ B_i = E_{G^+} (1 \parallel R_i \parallel R_{i-1} \parallel \text{newP}_i \parallel \text{newC}_i \parallel \text{expireP}_i \parallel \text{expireC}_i) \]
  where:
  - \( E_{K^+}(\cdot) \) is the encryption of \( \cdot \) using an additive homomorphic scheme (e.g., Paillier)
  - \( R_i \) is a random nonce
  - \( \text{newP}, \text{newC}, \text{expireP}, \text{expireC} \) are booleans, set to 1 iff the record corresponds to a new (or expiring) pen/trap or content wiretap

- In an accountant audit for statistics between times \( a \) and \( z \), \( \text{Log} \) computes and returns \( \bar{B}_{az} = \sum_{k=a}^{z} B_k \) and \( M_a \) and \( M_z \)

- Importantly, the \( \text{Log} \) does not have the decryption key
Accountant audits

\[ B_i = E_{G^+} (1 \ || \ R_i \ || \ R_{i-1} \ || \ \text{newP}_i \ || \ \text{newC}_i \ || \ \text{expireP}_i \ || \ \text{expireC}_i) \]

<table>
<thead>
<tr>
<th></th>
<th>X=R_i</th>
<th>Y=R_{i-1}</th>
<th>newP_i</th>
<th>newC_i</th>
<th>expireP_i</th>
<th>expireC_i</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
$B_i = \mathcal{E}_{G^+}(1 \ || \ R_i \ || \ R_{i-1} \ || \ \text{newP}_i \ || \ \text{newC}_i \ || \ \text{expireP}_i \ || \ \text{expireC}_i)$

<table>
<thead>
<tr>
<th></th>
<th>X=R_i</th>
<th>Y=R_{i-1}</th>
<th>newP_i</th>
<th>newC_i</th>
<th>expireP_i</th>
<th>expireC_i</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>34</td>
<td>39</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Accountant audits

\[ B_i = \mathcal{E}_{G^+}(1 \ || \ R_i \ || \ R_{i-1} \ || \ \text{newP}_i \ || \ \text{newC}_i \ || \ \text{expireP}_i \ || \ \text{expireC}_i) \]

<table>
<thead>
<tr>
<th>(i)</th>
<th>(X=R_i)</th>
<th>(Y=R_{i-1})</th>
<th>(\text{newP}_i)</th>
<th>(\text{newC}_i)</th>
<th>(\text{expireP}_i)</th>
<th>(\text{expireC}_i)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>34</td>
<td>39</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- Auditor compares difference in “nonce” columns in \(\overline{B}\) with difference based on values in \(M_a\) and \(M_z\)

\[ X - Y = R_z - R_{a-1} \]

- Any discrepancies reveal that the Log omitted entries
So what have we accomplished?

• (Untrusted) Log allows for more audit-friendly wiretap process
  • Court audits detect omissions in particular wiretaps
  • Centralized architecture aids legally-mandated reporting requirements via accountant audits

+ Additional accountability with minimal impact on existing telco infrastructure

- Accountable wiretapping architecture assumes trusted Encryptor and Delivery Function

• Would this prevent the Vodaphone Greece scandal?
Summary

• Wiretap evidence isn’t necessarily infallible
  • older loop-extender systems are inherently vulnerable to manipulation
  • newer CALEA systems suffer from inadequate provisioning

• Architectural issues:
  • Wiretap systems are architected around existing telco infrastructure
  • DoJ’s CALEA II proposals suggest mandating built-in wiretapping for Internet-based communication systems; is this a good idea?

• High-level takeaway: we heavily depend on legally authorized wiretap systems; they deserve more scrutiny