Accountable Wiretapping
-or-
I know they can hear you now

Adam Bates
University of Oregon

Kevin Butler
University of Oregon

Micah Sherr
Georgetown University

Clay Shields
Georgetown University

Patrick Traynor
Georgia Institute of Technology

Dan Wallach
Rice University

NDSS’12, San Diego, CA, USA
7 February 2012
When wiretaps go bad...

“Due to the improper minimization of calls, creating ‘gaps’ throughout the majority of calls, and preventing relevant conversations from being heard in their full context, Blagojevich requests that all wiretapped recordings be suppressed...”
Wiretapping, Unaccountably

• United States wiretaps cannot demonstrate correct behavior or detect incorrect behavior.

• Wiretap targets can take active countermeasures to obscure communication or corrupt wiretap transcripts.

• Violation of wiretap laws could render transcripts inadmissible in federal trials.

• In turn, defendants would have stronger assurance that wiretaps were legally authorized and employed.
Accountable Wiretapping

• Our work demonstrates that wiretap events can be safely logged in a privacy preserving manner.

• Our architecture assumes a potentially untrusted storage service that:
  (i) Never obtains access to plaintext wiretap records
  (ii) Cannot determine the number or scope of wiretaps orders

• In spite of this, our storage can prove to auditors that it has correctly recorded all encrypted data.
Background: Lawful Access

• Modern United States wiretaps were established by the 1994 U.S. Communications Assistance for Law Enforcement Act (CALEA) and implemented via the 2003 ANSI J-STD-025 (“J-Standard”) specification.

• Two forms of wiretap order: *pen registers* allow access to call metadata, *full audio interception* orders allow law enforcement to access call content.

• CALEA wiretaps lack audit features, complicating the process of generating the required annual wiretap report.
Background: CALEA Wiretapping

Wiretap target 1

Wiretap target 2

Telecommunications Service Provider (TSP)

Switch

Switch

Switch

Switch

Delivery Function (DF)

Metadata channel

Content channel 1

... Content channel n

Law Enforcement Agency (LEA)

Telephone Network
Background: CALEA Wiretapping

Wiretap target 1

Telecommunications Service Provider (TSP)

Wiretap target 2

Switch

Switch

Switch

Law Enforcement Agency (LEA)

Telephone Network

Delivery Function (DF)

Metadata channel

Content channel 1

...

Content channel n
Background: CALEA Wiretapping

Wiretap target 1

Wiretap target 2

Telecommunications Service Provider (TSP)

Switch

Switch

Switch

Switch

Delivery Function (DF)

Metadata channel

Content channel 1

... Content channel n

Law Enforcement Agency (LEA)

Telephone Network
Background: Can They Hear Me Now?

• **Call Data Channel (CDC) Resource Exhaustion:** wiretap targets can generate events at a rate that overwhelm the channel, preventing call data from being recorded.

• **Injecting Confusion & Uncertainty:** targets can deny reconstruction of traffic flows and craft packets that insert non-existent correspondence into wiretap transcripts.
Design: Overview

Telecommunications Service Provider

Wiretap target 1

Wiretap target 2

Switch

Switch

Switch

Switch

Delivery Function (DF)

LEA

Call Data & Content Channels

Telephone Network

(1) wiretap ID

(2) wiretap records

(1) statistics request

(2) statistics

Accountant
Design: Overview

Wiretap target 1

Telecommunications Service Provider

Switch

Switch

Switch

Call Data & Content Channels

Delivery Function (DF)

Encryptor

LEA

Remote Audit Log

Wiretap target 2

Telephone Network
Design: Overview

Telecommunications Service Provider

Delivery Function (DF)

Encryptor

Remote Audit Log

LEA

Court

Accountant

(1) wiretap ID
(2) wiretap records
(1) statistics request
(2) statistics

Telephone Network

Wiretap target 1

Wiretap target 2

Switch

Switch

Switch

Call Data & Content Channels
Design: Threat Model

• **Wiretap Target**: may attempt denial-of-service attacks (*Completeness*) on the wiretap resource channels.

• **Unauthorized Wiretapper**: may issue illegal wiretap orders (*Total Reporting*), or use a legal wiretap outside of the valid date range (*Date Compliance*).

• **Dishonest Log**: may attempt to read records (*Confidentiality*), discover the existence of a wiretap order (*Unlinkability*) or tamper with records (*Integrity*).
# Protocol: Event Logging

## Encryptor-to-Log Message (Signed)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Wiretap Event</td>
<td>Record Key</td>
</tr>
<tr>
<td>(2)</td>
<td>Event Count (per wiretap)</td>
<td>Record Key</td>
</tr>
<tr>
<td>(3)</td>
<td>Hash of (1), (2)</td>
<td>Record Key</td>
</tr>
<tr>
<td>(4)</td>
<td>Aggregate Block</td>
<td>Accountant Public Key</td>
</tr>
<tr>
<td>(5)</td>
<td>Event Timestamp</td>
<td>Cleartext</td>
</tr>
</tbody>
</table>
Wishing to receive the records associated with wiretap order $\omega$ from time $T_s$ to $T_e$, the court issues request:

$$
\text{Court Auditor} \rightarrow \text{Log} : \text{CourtAudit}(T_s, T_e)
$$

<table>
<thead>
<tr>
<th>Message</th>
<th>$M_i$</th>
<th>$M_{i+1}$</th>
<th>$M_{i+2}$</th>
<th>$M_{i+3}$</th>
<th>$M_{i+4}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>$t_s$</td>
<td>$t_{s+1}$</td>
<td>$t_{s+2}$</td>
<td>$t_{s+3}$</td>
<td>$t_e$</td>
</tr>
<tr>
<td>Key</td>
<td>$r_\omega$</td>
<td>$r_\nu$</td>
<td>$r_\nu$</td>
<td>$r_\omega$</td>
<td>$r_\omega$</td>
</tr>
</tbody>
</table>
Protocol: Court Audits

Wishing to receive the records associated with wiretap order \( \omega \) from time \( T_s \) to \( T_e \), the court issues request:

\[
\text{Court Auditor} \rightarrow \text{Log} : \text{CourtAudit}(T_s, T_e)
\]

\[
\begin{align*}
M_i & \quad M_{i+1} & \quad M_{i+2} & \quad M_{i+3} & \quad M_{i+4} \\checkmark & \quad \xmark & \quad \xmark & \quad \checkmark & \quad \checkmark
\end{align*}
\]

<table>
<thead>
<tr>
<th>Message</th>
<th>Time</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( t_s )</td>
<td>( r_\omega )</td>
</tr>
<tr>
<td></td>
<td>( t_{s+1} )</td>
<td>( r_{\nu} )</td>
</tr>
<tr>
<td></td>
<td>( t_{s+2} )</td>
<td>( r_{\nu} )</td>
</tr>
<tr>
<td></td>
<td>( t_{s+3} )</td>
<td>( r_\omega )</td>
</tr>
<tr>
<td></td>
<td>( t_e )</td>
<td>( r_\omega )</td>
</tr>
</tbody>
</table>
Protocol: Accounting Audits

The aggregation block is a set of counters encrypted with the Paillier system \( \mathcal{E}_{G^+}(Q) \) such that for messages \( Q_1 \) and \( Q_2 \),
\[
\mathcal{D}_{G^-}(\mathcal{E}_{G^+}(Q_1) \cdot \mathcal{E}_{G^+}(Q_2)) = Q_1 + Q_2.
\]

<table>
<thead>
<tr>
<th>Block</th>
<th>( B_i )</th>
<th>( B_{i+1} )</th>
<th>( B_{i+2} )</th>
<th>( B_{i+3} )</th>
<th>( B_{i+4} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit Set?</td>
<td>( \mathcal{E}_{G^+}(1) )</td>
<td>( \mathcal{E}_{G^+}(0) )</td>
<td>( \mathcal{E}_{G^+}(0) )</td>
<td>( \mathcal{E}_{G^+}(1) )</td>
<td>( \mathcal{E}_{G^+}(1) )</td>
</tr>
</tbody>
</table>
The aggregation block is a set of counters encrypted with the Paillier system $\mathcal{E}_{G^+}(Q)$ such that for messages $Q_1$ and $Q_2$, $\mathcal{D}_{G^-}(\mathcal{E}_{G^+}(Q_1) \cdot \mathcal{E}_{G^+}(Q_2)) = Q_1 + Q_2$.

\[ B_i \oplus B_{i+1} \oplus B_{i+2} \oplus B_{i+3} \oplus B_{i+4} = \mathcal{E}_{G^+}(3) \]
The aggregation block is a set of counters encrypted with the Paillier system $\mathcal{E}_{G^+}(Q)$ such that for messages $Q_1$ and $Q_2$, $\mathcal{D}_{G^-}(\mathcal{E}_{G^+}(Q_1) \cdot \mathcal{E}_{G^+}(Q_2)) = Q_1 + Q_2$.
The accountant can use aggregate block sequence numbers to confirm that no records were omitted.
The accountant can use aggregate block sequence numbers to confirm that no records were omitted.

\[
\text{Accountant} \rightarrow \text{Log} : \text{AccountingAudit}, T_1, T_4 \\
\text{Log} \rightarrow \text{Accountant} : M_1, \sigma(M_1), M_4, \sigma(M_4), \sum_{i=1}^{4} B_i
\]
The accountant can use aggregate block sequence numbers to confirm that no records were omitted.

Accountant $\rightarrow$ Log : AccountingAudit, $T_1, T_4$

Log $\rightarrow$ Accountant : $M_1, \sigma(M_1), M_4, \sigma(M_4), \sum_{1}^{4} B_i$

The accountant subtracts the sequence numbers from the sum of the previous sequence numbers.

Most cancel out, leaving the value $s_4 - s_0$. 

<table>
<thead>
<tr>
<th>Random seqno</th>
<th>Previous seqno</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s_4$</td>
<td>$s_0$</td>
</tr>
</tbody>
</table>
## Protocol: Message Type Summary

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Wiretap Event</td>
<td>Transmits legitimate wiretap data</td>
</tr>
<tr>
<td>(2) Wiretap Start, Stop</td>
<td>Sets counters in aggregate block</td>
</tr>
<tr>
<td>(3) Heartbeat Message</td>
<td>Bounds Log record omission</td>
</tr>
<tr>
<td>(4) Noise</td>
<td>Thwarts timing analysis of channel</td>
</tr>
</tbody>
</table>
Security Analysis

• Detecting Denial-of-Service: our architecture can detect lost messages through redundant storage and sequence numbering.

• Detecting Unauthorized Wiretaps: our architecture can detect unauthorized wiretaps whose data is relayed through the Encryptor.

• Handling a Malicious Log: wiretap records’ confidentiality and privacy are handled through encryption of call and aggregation data. If the LOG attempts to modify or omit records, it will be evident in the accounting audit.
Evaluation: Microbenchmarks

- We implemented our architecture using an Asterisk telephone softswitch.

- Our Implementation’s Encryptor throughput was 30.53 events per second with 1024-bit aggregate block size.
• Generated call events from the anonymized data of a major university (4/04/2011).

• Wiretapped call events from calls of the busiest 10 minute window of the day.

• On one desktop, our Encryptor accomplished this at less than 3.2% maximum throughput!
Evaluation: Additional Calculations

- In 2008, there were 21,000 pen registers. Our implementation would require three commodity machines to handle this load.

- In 2003, ATT handled 3,500 calls per second. Our implementation could handle 10% of this traffic on a single multicore machine.
In this work we have made the following contributions:

- Developed an attacker model for accountable wiretapping.
- Introduced new protocols to enable trustworthy wiretap auditing.
- Developed a minimal-impact retrofit for current interception systems.
- Demonstrated that all U.S. pen register traffic can be handled on a few commodity machines.
Questions?

Adam Bates

amb@cs.uoregon.edu
When wiretaps go bad...
When wiretaps go bad...
When wiretaps go bad...

The Athens Affair: A cellphone bugging scandal that targeted the conversations of highly-ranking Greek officials leading up to the August 2004 Olympic Games in Athens. The penetration remained undetected until January 24, 2005.
Evaluation: Implementation

Softswitch (Asterisk)
- PSTN
- SIP
- IAX
- Skype

Call Handling (Fast AGI script)

Noise/Heartbeat Generator

REMOTE AUDIT LOG

ENCRYPTOR

Telco
Design: Log Access Control

- **Court Audit**: a wiretap authority (e.g. court) queries Log for all records pertaining to a particular wiretap for which it granted access.

- **Accounting Audit**: an accountants may issue statistic requests to Log to discover the total number of wiretaps in a date range.
“With STAR-GATE, service providers can access communications on virtually any type of network, and query and deliver content and data in compliance with CALEA, ETSI, and other lawful interception standards and regulations...”