UNIVERSITY OF OREGON

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...

UNIVERSITY OF OREGON

"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

UNIVERSITY OF OREGON

- 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

UNIVERSITY OF OREGON

- 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

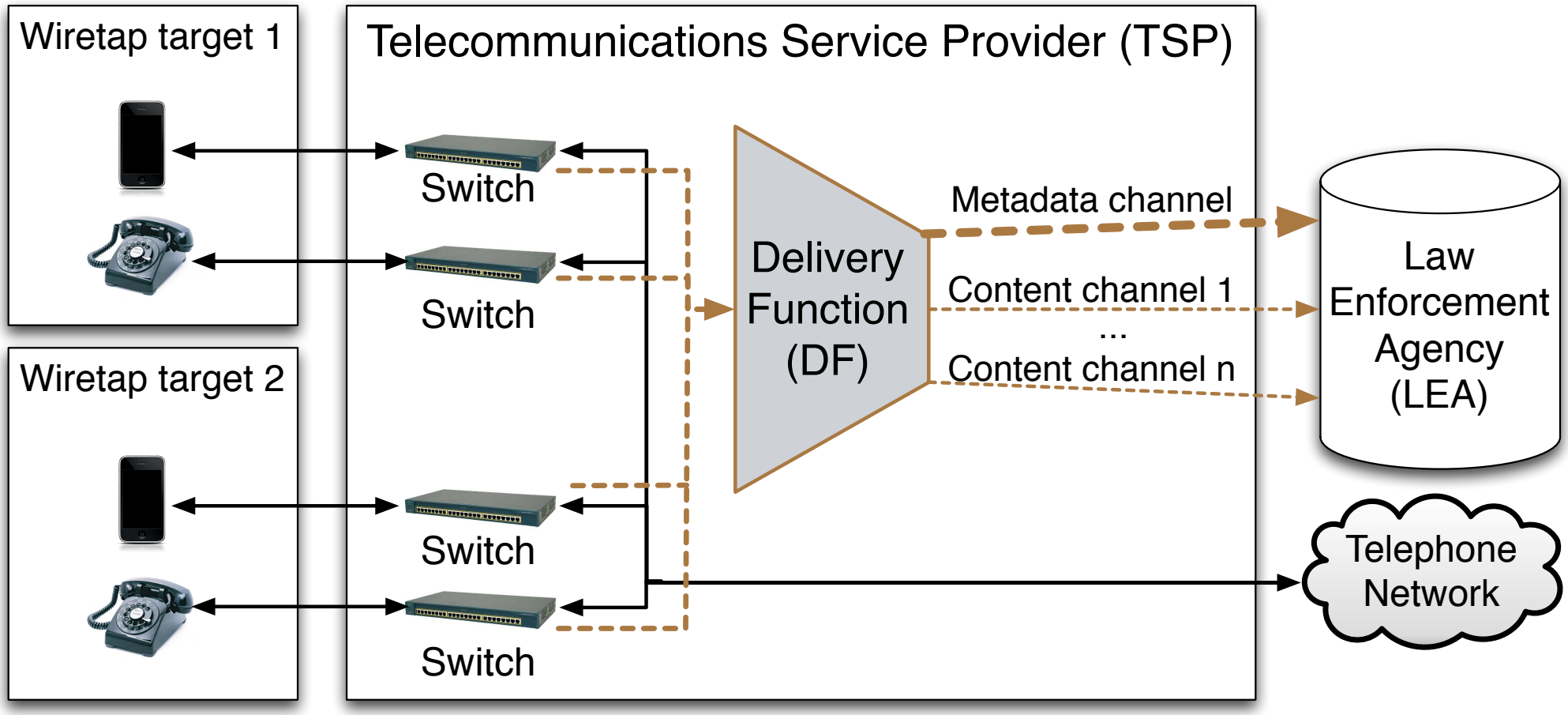
  (ii) Cannot determine the number or scope of wiretaps orders
- In spite of this, our storage can prove to auditors that it has correctly recorded all encrypted data.

Background: Lawful Access

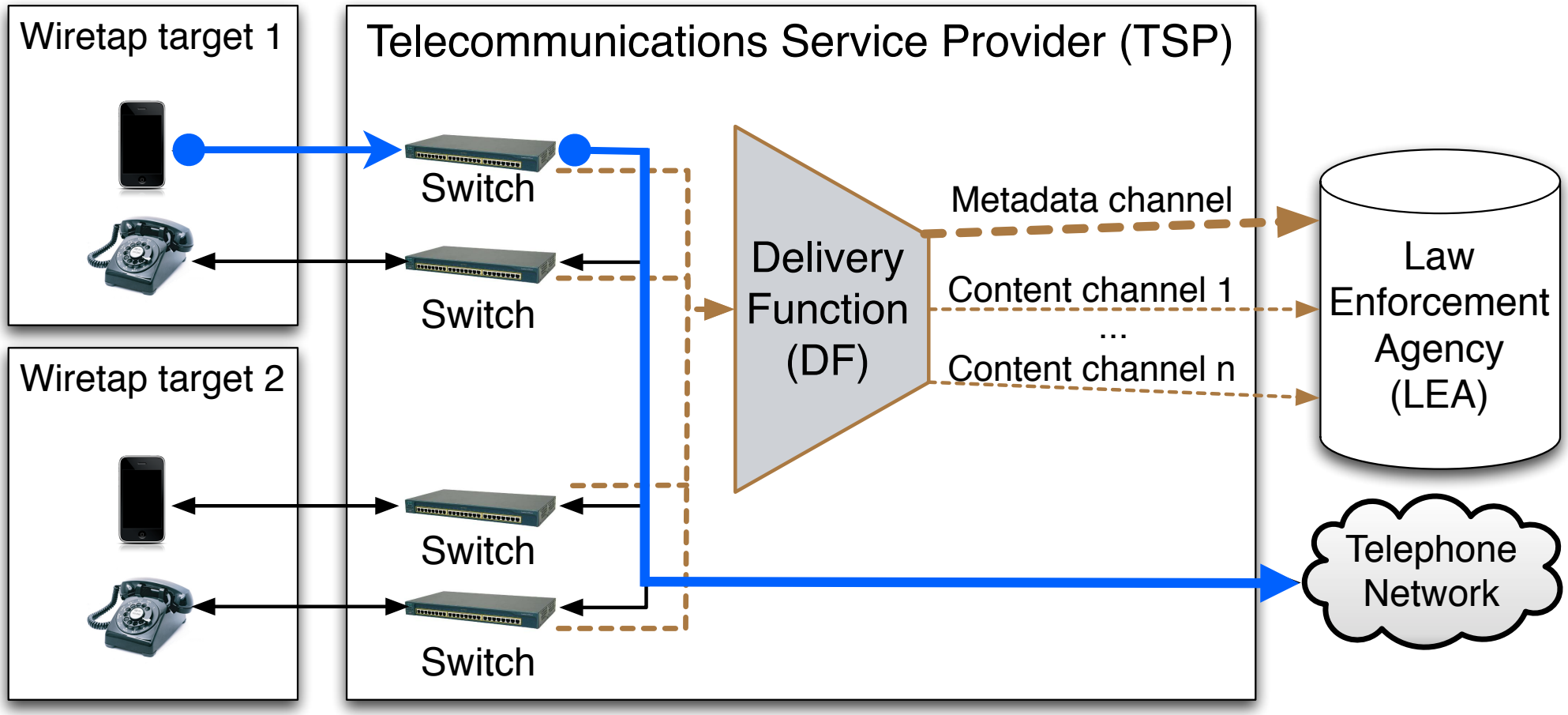
UNIVERSITY OF OREGON

- 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.

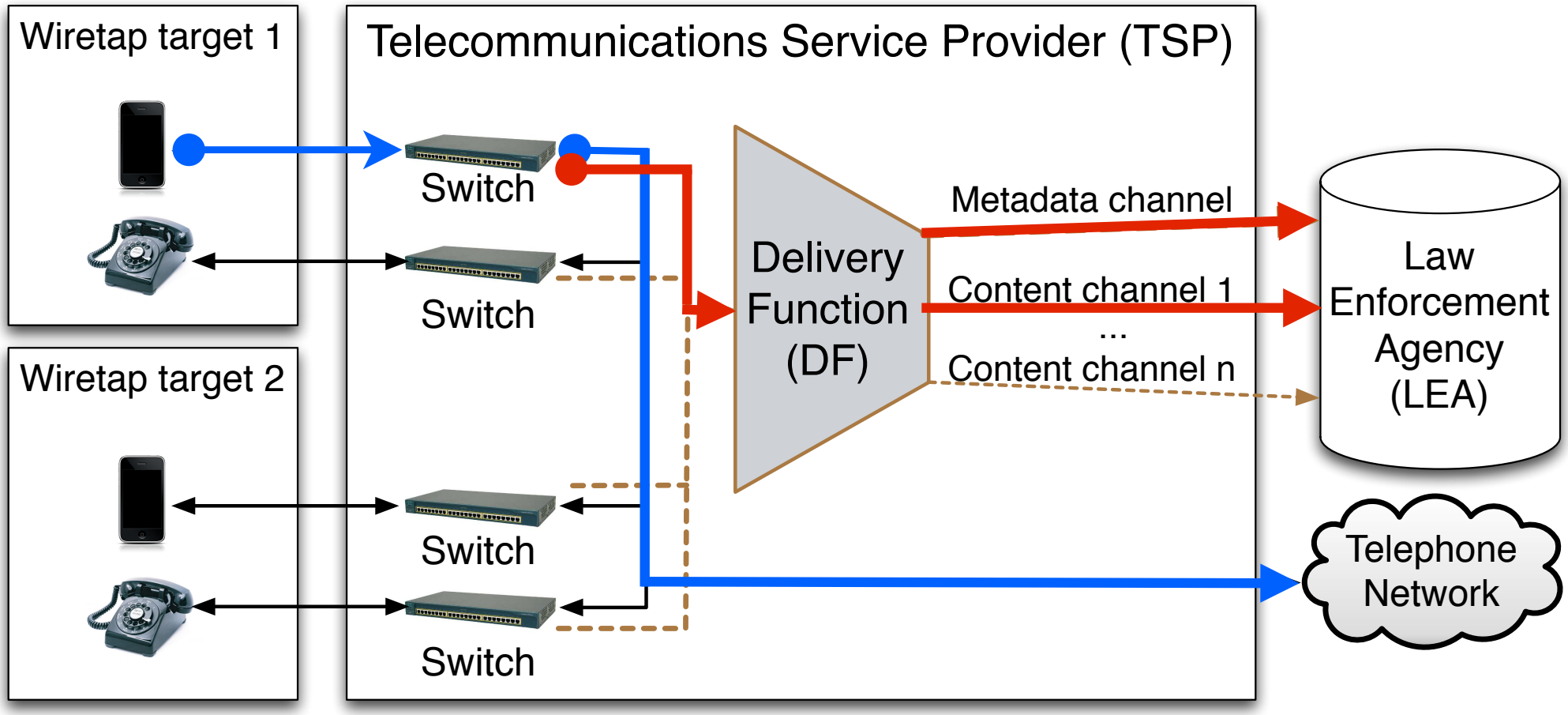
Background: CALEA Wiretapping



Background: CALEA Wiretapping



Background: CALEA Wiretapping

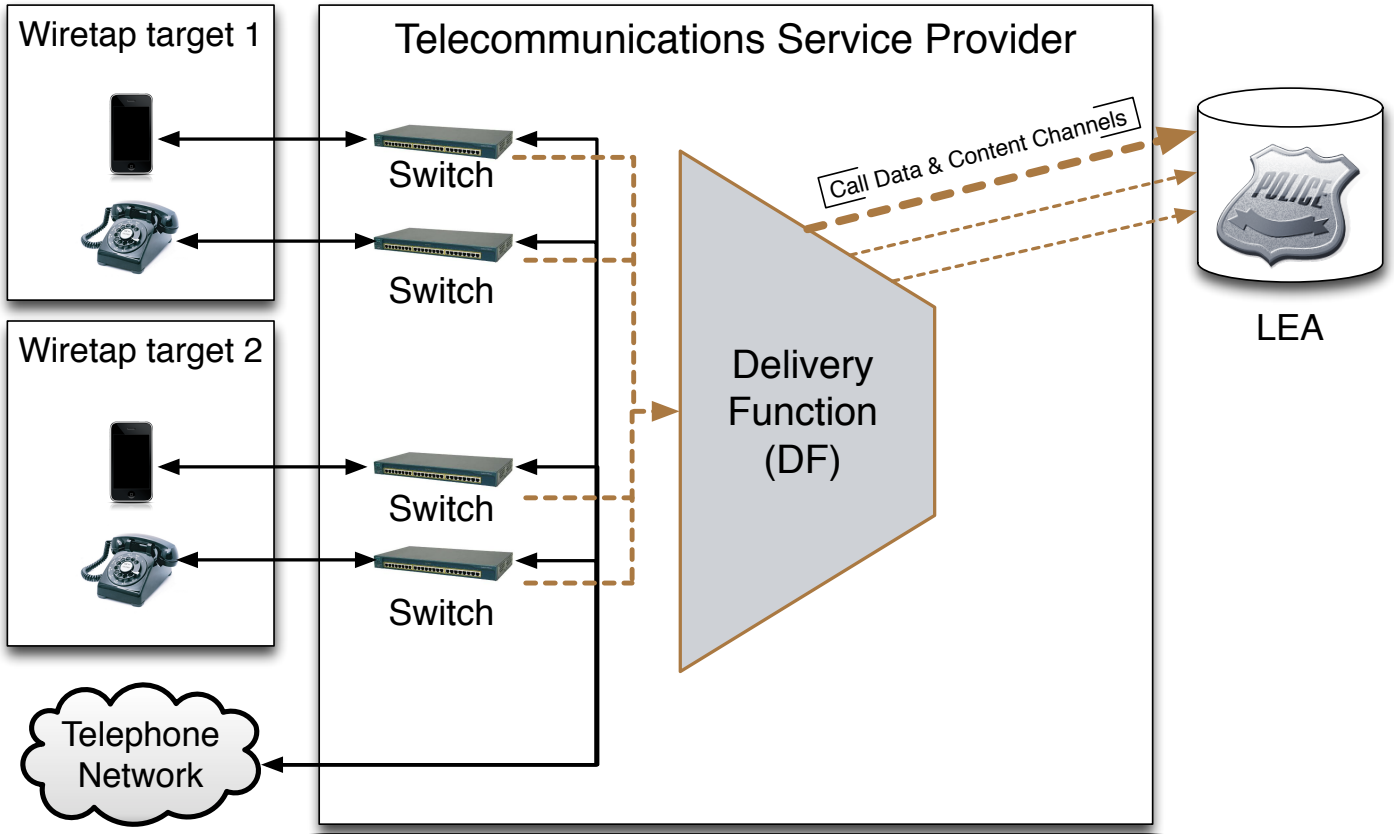


Background: Can They Hear Me Now?

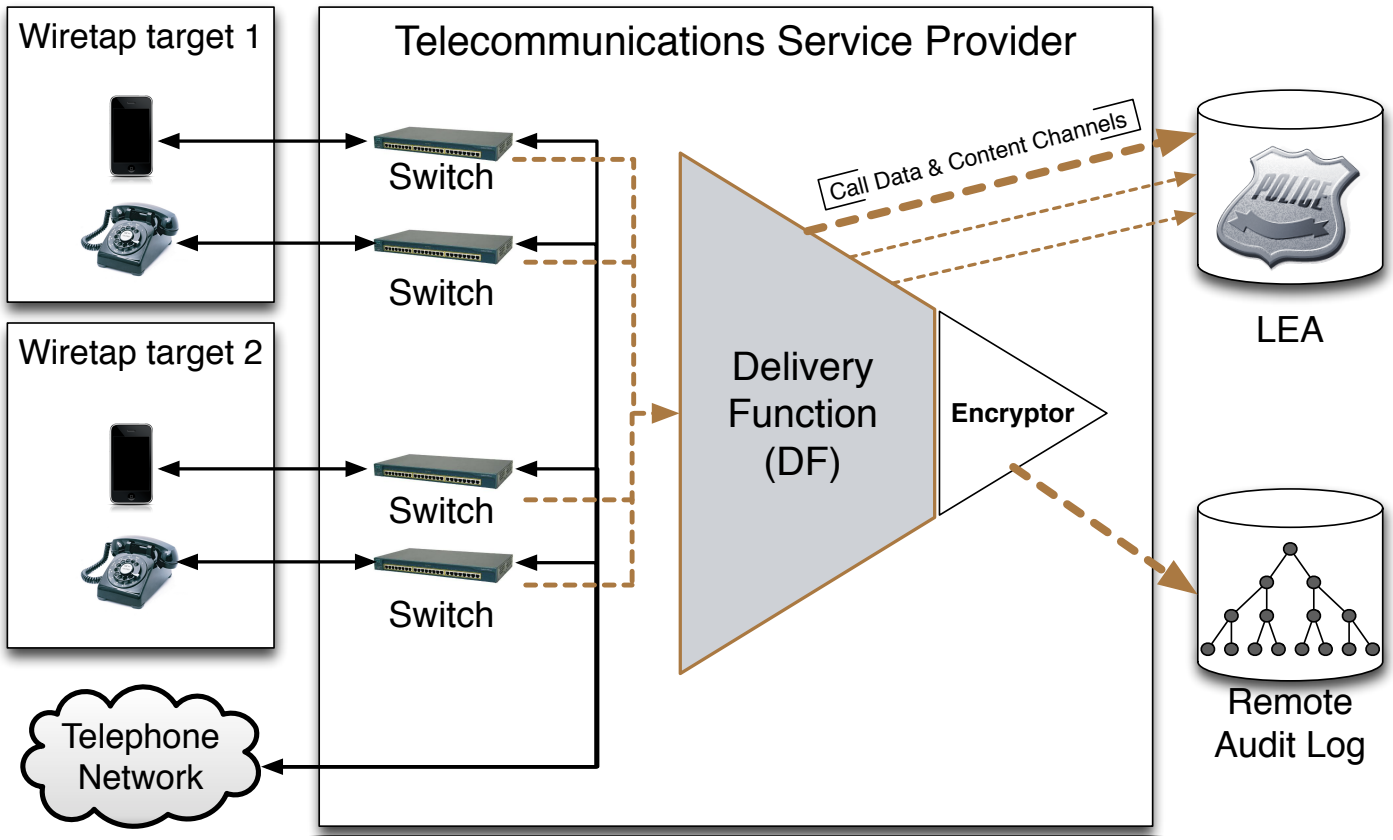
UNIVERSITY OF OREGON

- 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.

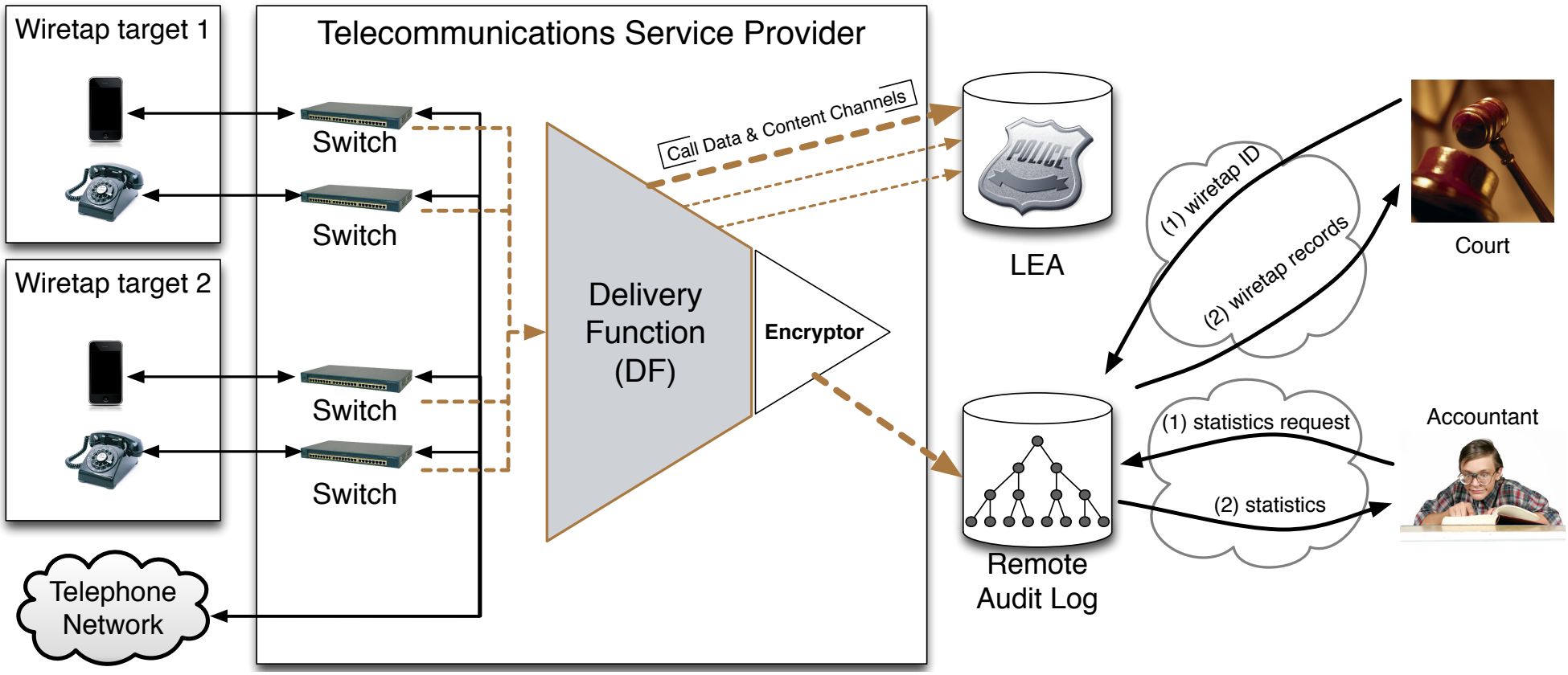
Design: Overview



Design: Overview



Design: Overview



Design: Threat Model

UNIVERSITY OF OREGON

- 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

UNIVERSITY OF OREGON

Encryptor-to-Log Message (Signed)		Encryption
(1)	Wiretap Event	Record Key
(2)	Event Count (per wiretap)	Record Key
(3)	Hash of (1), (2)	Record Key
(4)	Aggregate Block	Accountant Public Key
(5)	Event Timestamp	Cleartext

Protocol: Court Audits

UNIVERSITY OF OREGON

Wishing to receive the records associated with wiretap order ω from time T_s to T_e, the court issues request:

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

Message	M_i	M_{i+1}	M_{i+2}	M_{i+3}	M_{i+4}
Time	t_s	t_{s+1}	t_{s+2}	t_{s+3}	t_e
Key	r_ω	r_ν	r_ν	r_ω	r_ω

Protocol: Court Audits

UNIVERSITY OF OREGON

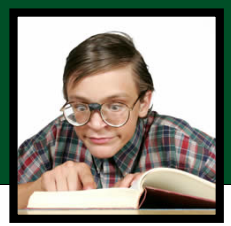
Wishing to receive the records associated with wiretap order ω from time T_s to T_e, the court issues request:

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

	✓	✗	✗	✓	✓
	M_i	M_{i+1}	M_{i+2}	M_{i+3}	M_{i+4}

Message					
Time	t_s	t_{s+1}	t_{s+2}	t_{s+3}	t_e
Key	r_ω	r_ν	r_ν	r_ω	r_ω

Protocol: Accounting Audits

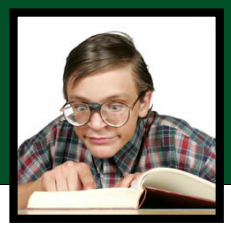


UNIVERSITY OF OREGON

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 , $\mathcal{D}_{G^-}(\mathcal{E}_{G^+}(Q_1) \cdot \mathcal{E}_{G^+}(Q_2)) = Q_1 + Q_2$.

Block	B_i	B_{i+1}	B_{i+2}	B_{i+3}	B_{i+4}
Bit Set?	$\mathcal{E}_{G^+}(1)$	$\mathcal{E}_{G^+}(0)$	$\mathcal{E}_{G^+}(0)$	$\mathcal{E}_{G^+}(1)$	$\mathcal{E}_{G^+}(1)$

Protocol: Accounting Audits



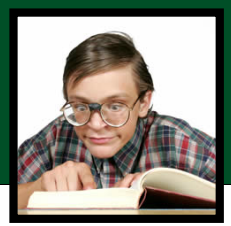
UNIVERSITY OF OREGON

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 , $\mathcal{D}_{G^-}(\mathcal{E}_{G^+}(Q_1) \cdot \mathcal{E}_{G^+}(Q_2)) = Q_1 + Q_2$.

$$B_i \oplus B_{i+1} \oplus B_{i+2} \oplus B_{i+3} \oplus B_{i+4} = \mathcal{E}_{G^+}(3)$$

Block					
Bit Set?	$\mathcal{E}_{G^+}(1)$	$\mathcal{E}_{G^+}(0)$	$\mathcal{E}_{G^+}(0)$	$\mathcal{E}_{G^+}(1)$	$\mathcal{E}_{G^+}(1)$

Protocol: Accounting Audits



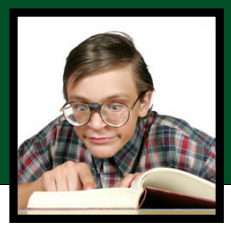
UNIVERSITY OF OREGON

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 , $\mathcal{D}_{G^-}(\mathcal{E}_{G^+}(Q_1) \cdot \mathcal{E}_{G^+}(Q_2)) = Q_1 + Q_2$.

Aggregation Block Message Structure

Random seqno	Previous seqno	Pen Register, New	Audio Intercept, New	Pen Register, Expiring	Audio Intercept, Expiring

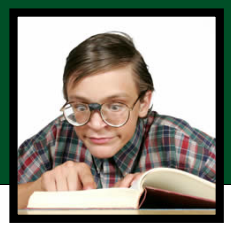
Protocol: Accounting Audits



UNIVERSITY OF OREGON

The accountant can use aggregate block sequence numbers to confirm that no records were omitted.

Protocol: Accounting Audits



UNIVERSITY OF OREGON

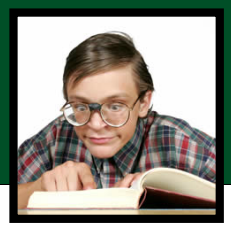
The accountant can use aggregate block sequence numbers to confirm that no records were omitted.

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

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

Random seqno	Previous seqno
s_1	s_0
s_2	s_1
s_3	s_2
s_4	s_3

Protocol: Accounting Audits



UNIVERSITY OF OREGON

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 $s_4 - s_0$.

Random seqno	Previous seqno
	s_0
s_4	

Protocol: Message Type Summary

UNIVERSITY OF OREGON

	Type	Description
(1)	Wiretap Event	Transmits legitimate wiretap data
(2)	Wiretap Start, Stop	Sets counters in aggregate block
(3)	Heartbeat Message	Bounds Log record omission
(4)	Noise	Thwarts timing analysis of channel

Security Analysis

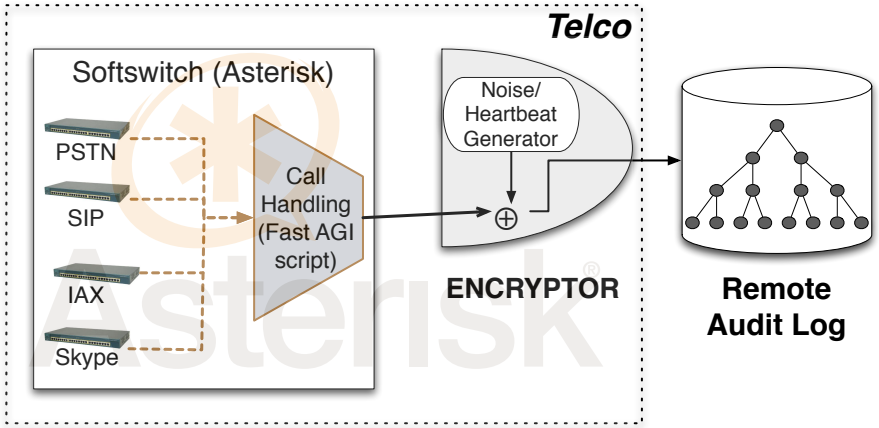
UNIVERSITY OF OREGON

- 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

UNIVERSITY OF OREGON

- 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.

Operation	1024-bit Block	2048-bit Block
Encrypt Data	< 1%	< 1%
Hash Data	< 1%	< 1%
Encrypt Block	96%	99%
Sign Record	3%	< 1%
Transmission	< 1%	< 1%
Events per second:	30.53	4.98

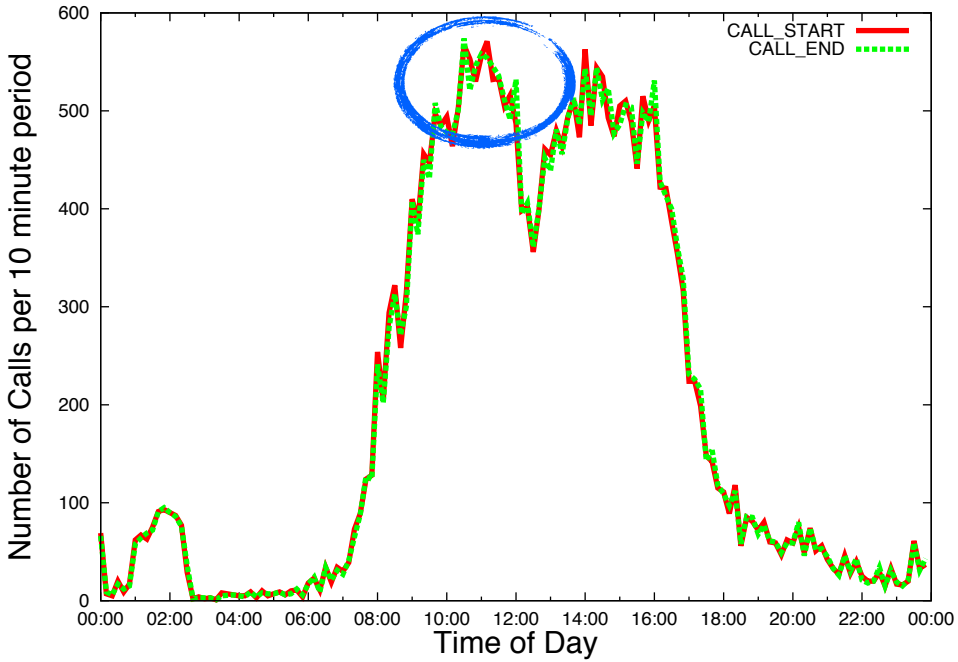
Evaluation: University Traffic Test

UNIVERSITY OF OREGON

- 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!

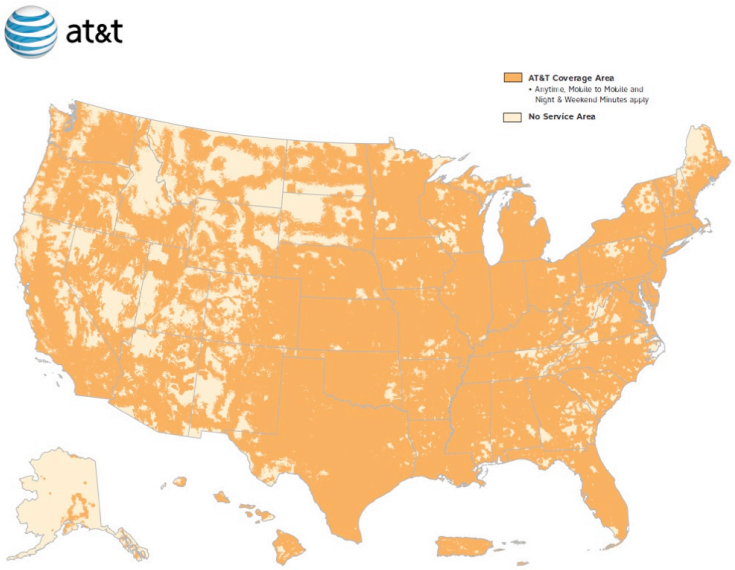


Evaluation: Additional Calculations

UNIVERSITY OF OREGON

- 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.



Conclusion

UNIVERSITY OF OREGON

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?

UNIVERSITY OF OREGON

Adam Bates

amb@cs.uoregon.edu

When wiretaps go bad...

UNIVERSITY OF OREGON

When wiretaps go bad...

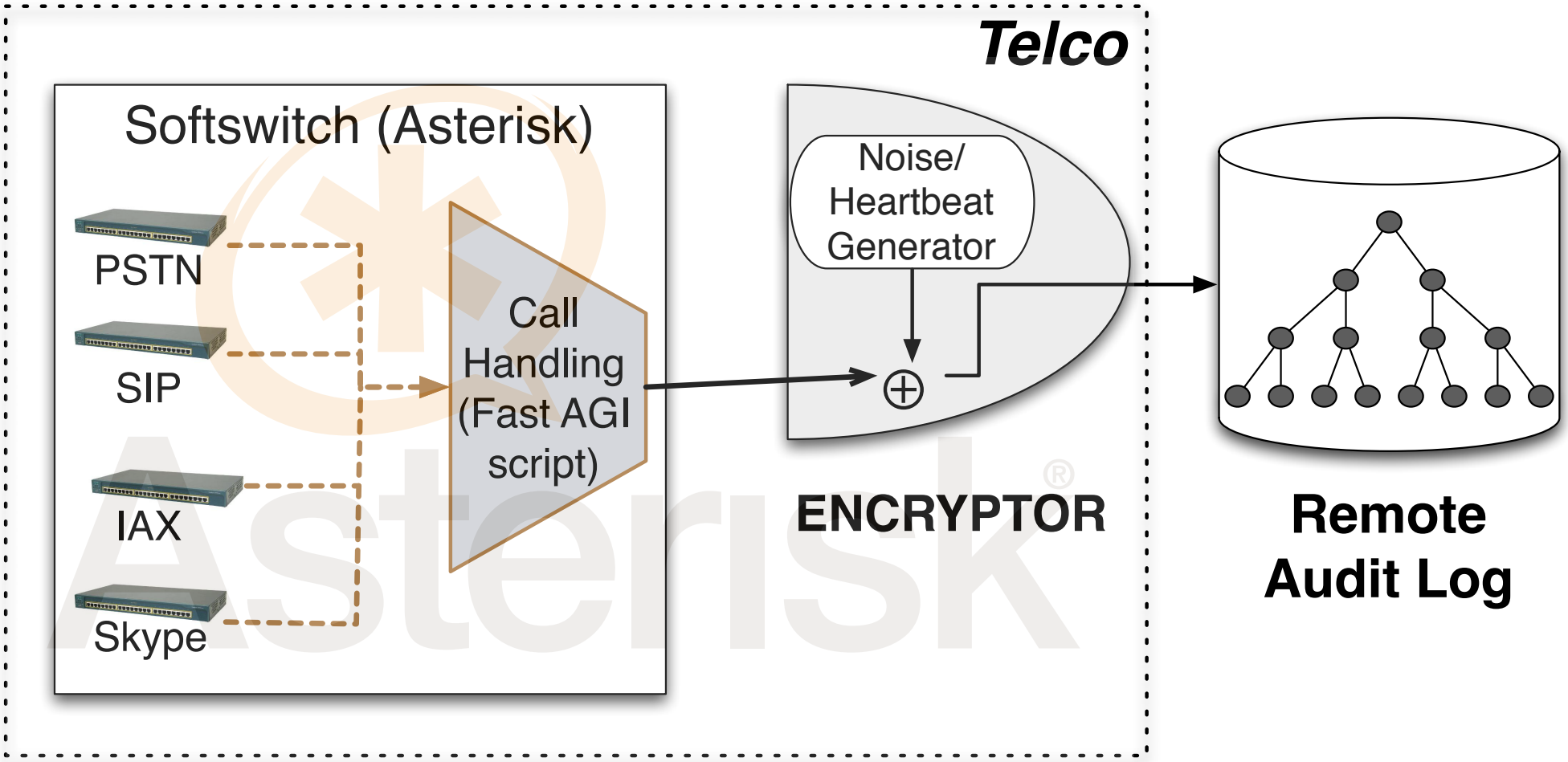
UNIVERSITY OF OREGON

When wiretaps go bad...

UNIVERSITY OF OREGON

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.

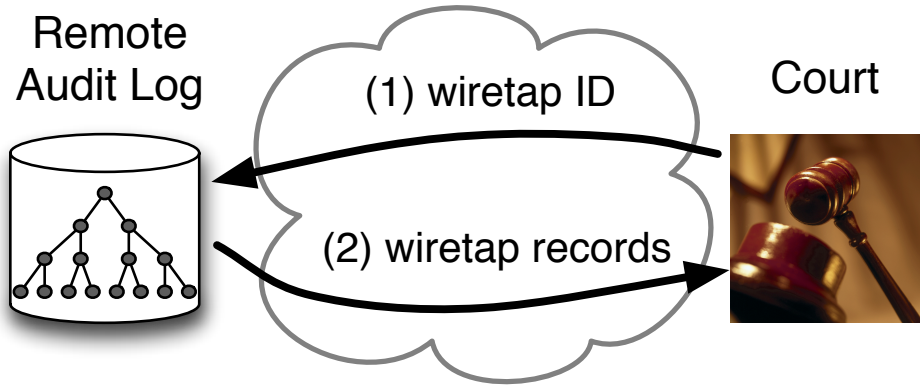
Evaluation: Implementation



Design: Log Access Control

UNIVERSITY OF OREGON

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



- <u>Accounting Audit</u>: an accountants may issue statistic requests to **Log** to discover the total number of wiretaps in a date range.

Centralized, Untrusted Storage...

UNIVERSITY OF OREGON

"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..."

VERINT
POWERING ACTIONABLE INTELLIGENCE®