Secure Protocol for Accountable Warrant Execution

Dan Boneh, Ed Felten, Joshua Kroll, Valeria Nikolaenko, David Wu, Joe Zimmerman

Stanford University, Law School, 2 Nov 2016
Currently investigator can access data directly

A ⇔ C
11/01/2016, other data
Currently investigator can access data directly

A ⇆ C
11/01/2016, other data

B ⇆ C
11/01/2016, other data
Currently investigator can access data directly

A ⇔ C
11/01/2016, other data

B ⇔ C
11/01/2016, other data

D ⇔ A
11/02/2016, other data
Currently investigator can access data directly

Need A’s metadata for Nov 2016

data

A ⇔ C
11/01/2016, other data

B ⇔ C
11/01/2016, other data

D ⇔ A
11/02/2016, other data
Meta-data retention required by law: 1.5 years

47 CFR 42.6 - Retention of telephone toll records.

§ 42.6 Retention of telephone toll records.
Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier.

2015: personal data of 21 million Federal employees got stolen (*)

(*) Information About OPM Cybersecurity Incidents, OPM.GOV, https://www.opm.gov/cybersecurity/
Problem #1:

data is stored in the clear!
Warrants: National Security Letters starting 1986

- NSL may be issued to
  - Credit reporting agency
  - Telecommunication provider
  - Financial institution
  - Travel agency

- Requires no prior approval by a judge
- May still be challenged in court \(^1\)
  - Out of 300,000 NSLs issued (2003-2013)
  - Only 7 were challenged in court
- In 2013 nearly 60 NSLs per day \(^2\)

---

\(^1\) [https://www.eff.org/issues/national-security-letters/faq](https://www.eff.org/issues/national-security-letters/faq)

\(^2\) [https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf](https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf)
Problem #2: 

no court’s approval
No way to learn if you were investigated

Attention: Canary Watch is no longer being maintained, and the links listed have not been updated past the last checked date. Please read our blog post for more info.

Till May 2016
Problem #3:

no audit records
High level goals:

Clear, just and correct workflow of warrant execution

- **Encryption**: no secret keys or data held at carriers
- **Authorized access**: ensure court approves every access to data
- **Transparency**: audit records of all data access events (to allow after the fact verification)
Enforcing court’s approval

A, Nov 2016: $\text{Enc}_{pk}(\text{meta-data})$

Need A’s metadata for Nov 2016

Yes: meta-data
Adding audit capabilities

- Every decryption request is logged
- Log learns nothing
- After the fact audit

A, Nov 2016

\[ \text{ct} = \text{Enc}_{pk}(\text{meta-data}) \]

\[ \sigma = \text{sign}(\text{ct}) \]

pk

sk

court

auditor

pk

sk

- No secrets on carriers
- Court’s approval
- Audit records
Need A’s metadata for Nov 2016

ct = Enc_{pk}(meta-data)

ct

A, Nov 2016

Yes: meta-data

σ = sign(ct)

court

sk

sk_1

sk_2

sk_3

auditor
Guarantees and assumptions

We assume that

- the parties are honest, but can be curious
- at most one party is malicious

We guarantee that

- records are secret from everyone, except
  - the data-carrier, initially
  - the investigator after court’s authorization
- investigator can justify any records it holds
- if there is a malicious party, the logs will show who this is
Performance

Encrypting meta-data for **500,000,000 calls** (~ 1 day for one carrier)

<table>
<thead>
<tr>
<th>Record size</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 KiB</td>
<td>3.31 hours</td>
</tr>
<tr>
<td>4 KiB</td>
<td>3.54 hours</td>
</tr>
<tr>
<td>16 KiB</td>
<td>5.44 hours</td>
</tr>
</tbody>
</table>

Needed hardware at carriers: 52 machines (550 cores)

Court’s response to a data query: 4 trustees: 1.7 sec
Conclusions

- **Design** a system for secure execution of warrants
- **We assume** that all parties (except possibly one) is honest but curious
- **We show** that it guarantees:
  - record secrecy
  - accountability
  - robustness to partial compromise
  - audit reveals the requests
- **We demonstrate** good performance
Need A’s metadata for Nov 2016

$\text{ct} = \text{Enc}_{\text{pk}}(\text{meta-data})$

A, Nov 2016

Yes: meta-data

$\sigma = \text{sign}(\text{ct})$

auditor

investigator

court

sk
Meta-data retention in mobile carries: 1-10 years

Companies’ data retention policies vary by state and by data type.

Examples (as of May 2015):

- Verizon Wireless: 1 year retention.
- AT&T: 5 years (according to spokesman Michael Balmoris).
- T-Mobile: 10 years (spokesman Viet Nguyen says).
- MetroPCS: 2 years
- Sprint: 1.5 years (spokeswoman Stephanie Vinge Walsh says)
- U.S. Cellular 1 year (spokeswoman Katie Frey)