Multiple Objectives of Lawful-Surveillance Protocols

Joan Feigenbaum
Yale

Bryan Ford
EPFL

Cambridge UK; March 20, 2017

JF at SPW 2014: "Surveillance Morass" Lament

- All-around, catastrophic failure of institutions and individuals
  - Moral, social, political, technological, intellectual, …
  - National governments (esp. [all 3 branches of] the US govt.), IT companies, telecommunications companies, the security-research community, news media, …
  - Citizens, users/consumers, …
- The security-research community has not stepped up.
  - Principled group statements opposing mass surveillance have been few in number, measured in tone, and not (yet?) influential.
- Recommendations:
  - Mass encryption
  - Jérémie Koenig: Decentralized cloud services (aka "the Renaissance Internet")
  - Activism!

JF at FOCI 2014: "Privacy-Preserving Surveillance"

- Law enforcement and intelligence agencies have legitimate roles to play.
  - LE and IC are justified in surveilling some people and collecting some data.
  - That does ***not*** mean that they should surveil everyone all the time.
  - Can they identify suspects and obtain actionable information without intruding upon innocent bystanders?
- The security-research community has ***not*** failed on this front.
  - Decades of work on SMC, PIR, and other privacy-pres. computational methods
- Recommendations:
  - ***Lawful***, privacy-preserving, accountable surveillance
  - Combine cryptographic protocols with public, black-letter law and appropriate administrative procedures.
  - Limit scope, distribute trust, build in oversight by regulators and ordinary citizens.

Case Study – High Country Bandits

2010 case – string of bank robberies in Arizona, Colorado

FBI intersection attack compared 3 cell-tower dumps totaling 150,000 users

- 1 number found in all 3 cell dumps – led to arrest
- 149,999 innocent users' information acquired

Segal, Ford, & F. Solution in FOCI 2014 (1)

- **Repositories** of *encrypted* cell-phone call records
- Multiple **agencies** that must authorize data collection
- **Targeted** vs. **untargeted** users
- **Known** vs. **unknown** targets

- Challenge:
  - As in the Bandits case, we need a "John-Doe warrant."
  - We seek a *superset* of the records needed to *identify* the target.
  - Can we collect the superset in encrypted form, whittle it down to the necessary subset, and *decrypt only that subset*?

Segal, Ford, & F. Solution in FOCI 2014 (2)

- **Privacy-preserving set intersection**
  - Implemented protocol is a variation of Vaidya and Clifton's "secure set-intersection cardinality" protocol [J. Computer Security, 2005].
  - One key technical ingredient is the *mutual commutativity* of the **ElGamal** and **Pohlig-Hellman** encryption schemes:

$$D_2(D_3(D_1(E_3(E_2(E_1(x)))))) = x$$

$$D_3(D_2(E_3(D_1(E_2(E_1(x)))))) = x$$

- **Efficient (offline) operation:** Completes 150,000-record instances in 10 minutes.

Satisfies Principles of Priv.-Pres. Surveillance

- Open process
  - **Must** follow rules and procedures of public law
  - **Need not** disclose targets and details of investigations
- Division of trust
  - No single agency can compromise privacy.
- Enforced scope limiting
  - Overly broad group of users' data are not captured.
- Sealing time and notification
  - Finite, reasonable time before users are notified.
- Accountability
  - Statistics on use of surveillance are presented regularly.

Related Work

- Kamara (2014) and Kroll, Felten, Boneh (2014)
  - Cryptographic protocols for privacy-preserving, accountable surveillance of **known** targets
- Kearns, Roth, Wu, Yaroslavtsev (2016)
  - Differentially private, graph-search algorithms for **distinguishing targeted users from untargeted users**
- Segal, Feigenbaum, Ford (2016)
  - Privacy-preserving, accountable **contact chaining through encrypted phone records to identify unknown targets** (same goal as "bandits," different algorithm)
- Ongoing and future work
  - Privacy-preserving, accountable surveillance of social-network data
  - Privacy-preserving, accountable video surveillance
- Support from funding agencies (since 2010 at least)
  - SPAR (IARPA – PIR); PROCEED and Brandeis (DARPA – PIR, SMC, HE, etc.)

Wide Range of Negative Reactions

- "Evil"; we (crypto researchers) should aim for "no surveillance"
- "Won't work"
  - LE and IC won't accept distributed trust, scope limits, etc.
  - FISA is not an "open" legal process, and FISC won't set meaningful limits or allow notification of targets or statistical reporting.
- "Exotic protocols" can't be used for these purposes
  - People who seek warrants won't know when these techniques are applicable, won't set appropriate parameters, and won't interpret results correctly.
  - Too hard to implement and deploy?
- "Function drag"
- "Slippery slope"
  - Justification for bulk collection of encrypted data might be morphed into a justification to backdoor all crypto protocols (because of malice or ignorance).

Discussion