Privacy Principles for Sharing Cyber Security Data

Gina Fisk, Calvin Ardi, Neale Pickett,
John Heidemann, Mike Fisk,
Christos Papadopoulos

Los Alamos NATIONAL LABORATORY EST. 1943

USC Viterbi Information Sciences Institute

Colorado State University

Cyber Security Data Privacy and Sharing

- We need to have visibility into inherently distributed (and expensive!) cyber attacks.
  - Sony (2011): $170M
  - Target (2013): $148M + banks $200M
- Conflicting legislation and requirements.
  - HIPAA: Medical data must stay private.
  - Human Subjects: PII must stay private.
  - CISPA: Share actionable, situational cyber data.
  - Open Data: Data management plans for reproducibility.
- Sharing cyber data brings both privacy risks and organizational risks.
  - Complicated by privacy preservation vs. utility.

Retro-Future

- A system that allows controlled information sharing across and within organizations.
  - Includes tools to capture and rewind network events (traffic, routing, naming).
  - Balances privacy, risk, and the ability to recover from cyber attacks.
- Our work is guided by three privacy principles and associated corollaries.
  - Principle of Least Disclosure.
  - Principle of Qualitative Evaluation.
  - Principle of Forward Progress.

Principle of Least Disclosure

- Disclose the minimum amount of information that is sufficient to achieve the objective.
  - Internal Disclosure: Collecting data, even if it has not been released, is a source of potential disclosure.
  - Privacy Balance: You must balance the privacy of the inquirer and the responder.
  - Inquiry-Specific Release: Access to the data must be moderated and limited.

Engineering Approaches for Least Disclosure

- Minimal Requisite Fidelity
  - Fisk et al. introduced in the field of steganography in 2002.
  - In communications: The minimum degree of signal fidelity that is acceptable to end users but destructive to covert communications.
  - Extended to privacy: The MRF of a transaction would be the minimum amount of trust, data exchange, and disclosure between data owner and requester to minimize information leakage.
    - Example Query: "Have you seen the string 'EmH0t=.q' in TCP connections on port 927 on May 1, 2015?
    - Traditional Response: Send back all matching packets
    - MRF Response: "Yes, I did."

Engineering Approaches for Least Disclosure

- Data Confinement
  - Data owners keep their data and answer questions about it instead of making copies of it and losing control over its dissemination.
- Query Management
  - Moderated Queries
    - Provide a structure for requesters to ask questions, which the owner decides if/when to answer.
  - Poker Queries
    - Queries that minimize what information you disclose when making a query.

Principle of Qualitative Evaluation

- One must balance (subjectively) costs and benefits for privacy and progress.
  - Legal Constraints: Organizations must live within legal and ethical constraints.
    - Institutional Review Boards – formal committee designated to review, approve, and monitor behavioral research involving humans.
  - Technical Limitations: Technical methods alone are not a viable approach to privacy.
    - You must separate mechanism from policy.
      - Have a policy on data sharing to prevent ad hoc sharing by individuals.
      - There is no single “fix” for privacy.

Principle of Forward Progress

- Organizations must not become paralyzed by Least Disclosure and Qualitative Evaluation.
  - Sharing must be allowed, but in a controlled manner with consideration of benefits.
- Engineering Approaches
  - Controlled Disclosure – rate limiting responses.
  - Data Aging – after a certain time window, data should be reduced to a new format.
    - New format reduces space and reduces sensitive information.
    - Example: DNS
      - Stored as raw packets for 30 days.
      - Reduced to a daily summary of lookup counts for each host.
        - Removes who did the lookups and the timing.

Conclusion

- Balancing privacy, organizational risk, and the ability to improve response to security events is a challenging problem that requires careful engineering.
- The Retro-Future system is guided by the Principles of Least Disclosure, Qualitative Evaluation, and Forward Progress to allow simultaneous privacy protection and effective data sharing.