Science of Security
Security Experiments

John Mitchell
Stanford

What is security?

- **"Bad stuff does not happen"**
  - Contrast with functionality: good system input produces good output
- **Or,**
  - Given
    - System of interest
    - Set of desirable properties (specification, policy, ...)
    - Adversary model
      - Interface between the adversary and the system
      - Capabilities of the adversary for interaction through that interface
  - Good system properties are preserved, in face of adversary
- **Why is security hard?**
  - Subtle properties of system, adversary
  - Technically: quantification over adversaries

Example: The Web

- **Many desirable system properties**
  - E.g., Session integrity (ill-defined application-layer concept)
- **Many adversary models**
  - Network adversary: control of network
  - Web adversary
    - Controls arbitrary number of web sites, has certificates for them
    - Victim visits one or more attacker sites
  - Gadget adversary (terminology: mashups, gadgets, ...)
    - Web adversary
    - + installs one or more gadgets on mashup viewed by victim
- **Sample Question:**
  - What security guarantees do http-only cookies provide?

Security Experiments?

- **What properties can be evaluated by experiment?**
  - Usability?
    - By designers of system?
    - By additional users?
  - Performance?
    - Lab environment?
    - Under realistic conditions?
  - Security?
    - Resilience to known attacks?
    - Challenge community to explore new attacks?
    - Security against all attacks within given threat model?

Security Experiments

- **What properties can be evaluated by experiment?**
  - Usability?
    - By designers of system? **Yes**
    - By additional users? **Yes, if open user community**
  - Performance?
    - Lab environment? **Yes**
    - Under realistic conditions **Yes, if realistic user community**
  - Security?
    - Resilience to known attacks? **Yes**
    - Challenge community to explore new attacks? **Yes, if realistic user community**
    - Security against all attacks within threat model? **No, not an experimental property**
- **Position**
  - Experimental evaluation is important for security mechanisms, applications
  - Open experiments, allowing users other than designers, are essential

Policy/Specification Example

- **Spam**
  - Original specification of email system did not include "no spam"
  - Our understanding of what a system should and should not do evolves
    - Observed "bad behavior" leads to security requirements

Example: requirements for GENI facility

- ***Ability to determine performance effectively***
  - GENI facility must allow accurate measurement of a system under stress
- ***Resource allocation and accounting***
  - Example: resistance to DoS from an attacker with local but not global control of network.
  - Need to allocate specific resources to agents running in virtualized GENI environment
- ***Open access to experimental systems***
  - Usability studies informative only if the test user community is diverse and unlimited
- ***Isolation***
  - Experimental systems will subject to attack by designated and unknown attackers
  - GENI must provide isolation between independent slices allocated to diff experiments
- ***Privacy***
  - Experimental systems that offer privacy or anonymity to experimental users must not have these guarantees compromised arbitrarily by the GENI facility itself

Sample network security experiments

- **Spam-resistant email**
- **Electronic voting systems**
- **Distributed decentralized access control**
- **Worm propagation and mitigation**
- **Reputation systems**
- **Improved network infrastructure protocols**
- **Selective traceability and privacy**
- **SCADA simulation**
- **Botnet and overlay network security and detectability**
- **Economic incentives in network infrastructure and applications**
- **Anonymity in routing and applications**
- **Experimental combinations of security mechanisms for enterprise security**

Spam-resistant email

- **Motivation**
  - SPAM, is a pressing and widely recognized problem
  - S/MIME, SPF,… proposed; no effective widely adopted defense …
- **Experiment**
  - Develop experimental email infrastructure, compatible with existing clients
  - Operate in parallel with existing email systems, invite users
  - Provide reliable, authenticated email (e.g., program committee discussion)
  - Explore interoperability with existing email system
  - Must leave experimental system open to some form of attack
  - Are authentication, reputation useful concepts? What else might help?
- **References**
  - C Dwork, A Goldberg, M Naor, On Memory-Bound Functions for Fighting Spam …
  - L. Faith Cranor and B. H. LaMacchia, "Spam!," CACM, 1998.
  - M. Lentczner, M. Wong, "*Sender Policy Framework:* …
  - B. Ramsdell, RFC2633: S/MIME
  - Z Gyongyi, H Garcia-Molina, J Pedersen, Combating web spam with TrustRank, …

Main points

- **Security experiments are important**
  - Help refine design of system and set of properties it should have
  - Can provide insight into possible capabilities of adversary
  - Only way to test usability, performance, ...
  - Adoption by test user community is best indicator of usability
- **Security experiments do not provide security guarantees**
  - Security means: good properties are preserved against all attacks within some adversary model
  - Experimental systems must also be subjected to security analysis