## **Science of Security Security Experiments**

John Mitchell Stanford

Science of Security, Oakland CA

November 18, 2008

#### 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 November 18, 2008 Science of Security, Oakland CA

Science of Security, Oakland CA

4

**Example: The Web Security Experiments?** What properties can be evaluated by experiment? Many desirable system properties Usability? E.g., Session integrity (ill-defined application-layer concept) By designers of system? Many adversary models By additional users? Network adversary: control of network Performance? Web adversary Lab environment? Controls arbitrary number of web sites, has certificates for them Under realistic conditions? Victim visits one or more attacker sites Security? Gadget adversary (terminology: mashups, gadgets, ...) Resilience to known attacks? Web adversary Challenge community to explore new attacks? + installs one or more gadgets on mashup viewed by victim Security against all attacks within given threat model? Sample Question: What security guarantees do http-only cookies provide? Science of Security, Oakland CA November 18, 2008 November 18, 2008

Copyright © 2004 by Michael Reiter All rights reserved.





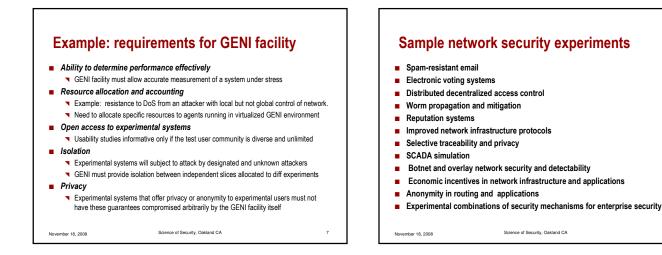
#### Spam

- 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

ember 18, 2008

Science of Security, Oakland CA

8



Copyright © 2004 by Michael Reiter All rights reserved.

### 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, ... Science of Security, Oakland CA

November 18, 2008

#### 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

November 18, 2008 Science of Security, Oakland CA 10