Are Scientific Experiments in Security Possible?

Vicraj Thomas
vthomas@bbn.com

18 November 2008
Experimentation is Difficult

• Difficult in any discipline
  – Time consuming, tedious
  – Expensive

• But…
  – It is a key piece of the scientific process
  – Journals in most scientific disciplines will not publish results not substantiated by analysis or by experimentation
    • Including social sciences!
Experimentation is Useful

• Many examples in CS of hypothesis validated / invalidated by experiments
• Locality of reference by programs
  – Experimentally confirmed
  – Principle used to optimize many techniques
• Independence of failure probability of multiple versions of a program
  – Experimentally disproven
  – Resulted in change in software development practices in aerospace industry
Yet Experimentation in CS is Lacking

- Lack of training in experimentation
- Unsubstantiated claims readily published
  - 40% of ACM papers in 1993 had no empirical or theoretical backing [Tichy et al., J. of Systems and Software, Jan 1995]
  - 40-50% of software engineering papers are unvalidated [Zelkovitz, IEEE Computer, May 1998]
- Demonstrations favored over experiments
- Situation is probably worse with security research
Lack of Experimentation Shows

• No good way to evaluate return on investment in security products
  – Large numbers of products of questionable value
• Fundamental mismatch between systems’ models of users and reality. Users blamed for poor security.
  – Unrealistic expectations for configuring security
    • 9 steps and six interfaces to configure permissions on a shared folder in Vista
  – Security “warnings” that are cryptic
    • Look just like other dialog boxes
    • No indication of level of risk
Experimentation in Security is Hard

• Large number of variables (factors)
  – Need to identify key factors
• Attacker modes are hard to specify
  – Unlike dependability community that has failure modes, failure rates, etc.
Needed: Canonical Attacker Models

• Models that reflect capabilities of the attacker
  – Access to compute resources, network resources; physical access
• Parallel: Attacker model used secure White House differs from attacker model used to secure our homes
• Example attacker model for a jamming-resistant wireless link:
  – Attacker’s max transmit energy, time to switch from listen to jamming mode, minimum distance from receiver, number of attackers
Needed: Testbeds and Data Sets

- Community accessible
- Configurable to repeat/extend experiments
- Realistic in number and type of resources
Testbeds: NSF GENI

• Infrastructure for long-running, realistic experiments in Network Science and Engineering
  – Experimentation in a controlled environment
  – Repeatability, archival
  – Community-based experimentation

• GENI needs you!
  – Solicitation 2 coming out shortly
Testbed: DARPA National Cyber Range

- For testing classified and unclassified software systems
- Ability to replicate large-scale military enclaves
- Repository for tools, recipes and architectures
- Forensic quality data collection, analysis and presentation
Future: Community Experimentation?

• Is community based experimentation the future?
  – Numbers of researchers and community members participating in experiments
    • Improve security of systems
    • Improve attacker models
Summary

- Science of Security is incomplete without experimentation
- Increased recognition of this fact
- Facilities being created to support experimentation
- Hope: We won’t have a panel discussion like this 3-5 years from now