Session 3

Perspectives on Security as Empirical Science - Vern Paxson (UC-Berkley)

- Need Science = prediction + control via understanding/principles
  - Characterize/hypoth/predict/experiment/analyze/repeat
  - Disseminate/independently confirm → All with rigor
- Want a science
  - Like math (axiomatic)
  - Like physical science (truth can be discovered)
  - Like war/crime fighting (win versus adversary)
  - Like engineering: (functionality v. cost/time/effort)
  - Like a social science (contextual truths/behaviors)
- Comments:
  - Techno Science: observe properties of man-made systems
  - Need integration of previously separate scientific explanations
- Therefore ⇨ Empirical Basis for Socio-Economic Perspectives

Perspectives on Security as Empirical Science - Paxson

- Why Empirical Science?
  - Analogy: lessons learned from network communications
- USENET example
  - Plot was log linear through 1996
  - Two more data points didn’t fit invariant hypothesis
  - Analysis determined “ABUSE” started
    - Actually rich data set but first assess validity of data input
  - A second example: scan activity found major increase in traffic
    - 2002 when the WORM era began
    - 2004-06 Cyber crime takes off

Perspectives on Security as Empirical Science - Paxson

- Data – Where is it Obtained?
  - Hard to anonymize data
  - Major ground truth issues
- Hard to Validate Data
  - Issues in replicating data
- Invariants & Time Scales
  - Rate of change (e.g. PhD 5yr cycle)
  - Rareness of data events
- Why Harder than Hard Science
  - Secure systems ⇨ events probability near zero ⇨ hard to measure
  - Comment: FT (e.g. fly-by-wire systems) have dealt with this issue
- Why Softer than Hard Science?
  - Criminal laziness: motivates to sustain cash flow, not strategic

Perspectives on Security as Empirical Science - Paxson

- Why Softer than Hard Science?
    - Criminal laziness: motivates to sustain cash flow, not strategic
- Holistic Analysis
    - Phases of the value chain
        - Looked at different stages
        - Checked large set of spam to measure process & look at structured bottleneck
        - Found 3 “dirty” banks
    - Comments: discussion on is this computer science

Structure As an Aid to Good Science – Maxion

- “test of all knowledge is an experiment”
- Story Grammar
  - Characters/settings/begin/middle/end
- Discussion on method and grammars
  - Point is structure helps organize and communicate
- Apply approach to abstracts/papers/reviews/proposals
- Abstracts are informative/disruptive and should have elements:
  - Objectives/Methods/Results/Conclusions
  - Could facilitate automation
    - Enable scraping of websites and better correlation of interests to results
    - Be used by journals
  - Discussion on STRUCTURED v. WELL STRUCTURED

Structure As an Aid to Good Science – Maxion

- Structure in Papers
  - Poor structure
    - impedes comprehension ("no story")
    - Creates opportunities for errors in omission
- Hallmarks on Good Experiments
  - Valid/reliable/repeatable/reproducible/properly reported
- Parts of an Experimental paper
  - Comment: Should paper follow the structure of the abstract?
- Hierarchy/Levels of Evidence

Observations

- Opportunity to apply strategies and lessons learned from dependability initiatives
- Vulnerabilities exist whether they are intentional or accidental/natural
- A system perspective helps in structuring and understanding the problem.
  - First principle of dependability is fault avoidance, i.e. do not accept/encourage:
    - a poorly formulated problem
    - a poorly formulated architecture with many vulnerabilities

Observations

- Difficult to make progress in the science of security if standards used for certification are not influenced
- A customer will base acceptance and certification of a system on these standards
- System builders are motivated contractually to focus efforts in compliance
    - No extra credit for applying a new, and maybe even better, approach / process if the results/efficiencies are not part of the certification process
        - May even be considered a negative factor
        - Lack of knowledge/training of evaluators that would also require additional cost/time
        - Current program has a tight timeframe
            - Assigned staff/program management rotations
            - Budget/scheduling commitments that are restrictive