Computer Security Research: Science, Art, or Voodoo? Observations from a Prodigal Son

Steve J. Chapin
Center for Systems Assurance
Syracuse University

Overview

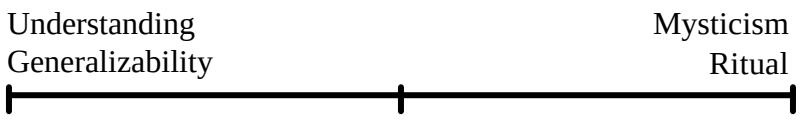
- Definitions of Terms
- The State of the World
- Examples of good and bad
- Summary & Congrats

Defining Terms

- Science: A branch of knowledge or study dealing with a body of facts or truths systematically arranged and showing the operation of general laws.
- Art: The principles or methods governing any craft or branch of learning; skill in conducting any human activity; trickery, cunning.

Definitions II

- Voodoo: A group of magical rites; black magic, sorcery; characterized by deceptively simple, almost magical solutions or ideas



Examples of Progression

- Medicine
  - bleeding -> medicine -> genetics
- Woodworking
  - lashing -> joinery -> compression/load
- Civil Engineering
  - huts on Survivor -> over- and under-engineered buildings (earthquakes) -> structural analysis

That Was Then (1992)

- I was but a lowly grad student, and Spaf spake unto me, and he said…
- Cyptography well understood, on a sound basis (science)
- Intrusion detection was rudimentary (art)
- System configuration and application development was dreck (voodoo)

...This Is Now

- I was but a simple professor, and everyone spake unto me, and said…
- Cyptography still a science
- Intrusion detection is a better understood art (too much reliance on pattern matching)
- System configuration and application development ranges from voodoo to art

Why So Little Progress?

- Technical solutions to social problems
- Too much science, not enough engineering (lab vs. reality; plane in Seattle)
- Wide deployment among an ignorant public:
  - Everyone's a sysadmin
  - We are not held accountable (P. T. Barnum and Henry Gondorff would be proud)
- Ease of use trumps security

Poor Solutions

- Virus scanners: no generality (but currently necessary)
  - Monty Python and the Holy Grail
- Head-on defense
  - assumes the bad guys follow your rules
  - easily sidestepped
- Misapplied good defenses
  - “A man’s got to know his limitations.”
    -- Dirty Harry

Poor Solutions II

- Microsoft “release first, secure second” (just when you thought it was safe…)
  - April 12: Steve Lipner, head of MS Security Response team, speaks at RSA conference and publicly attacks open source systems for being inherently less secure than closed source.
  - April 17: Internet Security and Acceleration Server shown to have simple DoS bug w/long URL
  - April 19: SMBRelay attack (CotDC) is yet another MitM attack on NetBIOS, still active in WinNT/2k.

Good Solutions

- Crytographic systems
- Wrapper technology
  - user-level
  - kernel-level
    - NAI wrappers
    - Argus Pitbull (remember the castles?)
    - Security-enhanced Linux (NSA)
- Some non-signature based IDS (based on invariants)

An Example: Trusted Time

- What time is it?
  - How do you know?
  - How do we agree?
  - Not important for many applications, but critically important for others
    - forensics/evidence gathering
    - temporal guarantees
    - transactions
    - legal documents

Trusted Time II

- We have authoritative time servers…but they won't serve the general public.
- Let's provide a service to sign a document, including a timestamp
  - not a new idea
  - but having the timestamp be provably traceable to a legally-accepted, authoritative source is

Trusted Time III

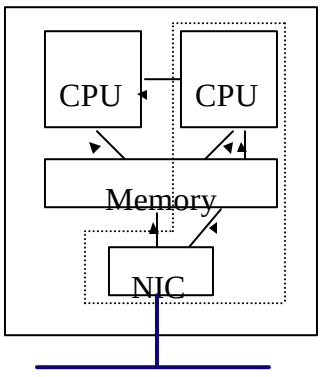
- The IBM 4758 is a great base
  - FIPS level 4 certified
  - tamper proof, full crypto support on card
- But that's only a tool
- Formal models of protocols and time drift to make provable guarantees
- Synergy of theory and practice

Another Example: Interface-Based Intrusion Detection

- Put more smarts in the NIC
- Can ease load on both routers and hosts
  - routers don't have to do as much processing on each packet
  - fewer network issues for hosts
- Completely local defense model

Abstract Approach

- Use dual-processor Pentium boxes running Linux
- One processor acts as normal
- Second processor handles all network I/O, acts as smart extension to NIC
- Rule-based filters (not just signatures)



Summary

- The state-of-the-art is a losing game
- Move from ad-hoc to general
  - invariants, abstractions, models
  - bring science into the real world
- Holistic approach to security/assurance
  - throughout the process
  - multidisciplinary
- Practice devious thinking: play more (board) games!

Congratulations!

- CheewBeng Ang
- S. R. Avasarala
- Brian Carrier
- Jared Crane
- Mei-Ching Lien
- Kevin Du
- Jim Early
- Rajeev Gopalakrishna
- Jung-Ho Chung
- Karthik Jaganathan
- Daniel Leaird
- Long Li
- Salvador Mandujano
- Craigh McDonough
- Dina Mohamed
- Sanket Naik
- Dmitri Nizovstev
- Venkatesh Prabhakar
- Chris Telfer
- Jamie Van Randwyk
- Saurabh Sandhir
- Jaideep Vaiya
- Diego Zamboni

SU/CSA is Hiring

- Major institutional commitment to IA
- $2.1M from State of NY for next two years, Rome AFRL funding, DARPA, ...
- Faculty
- Staff
- Sabbatical Fellows (academia, government, and industry)