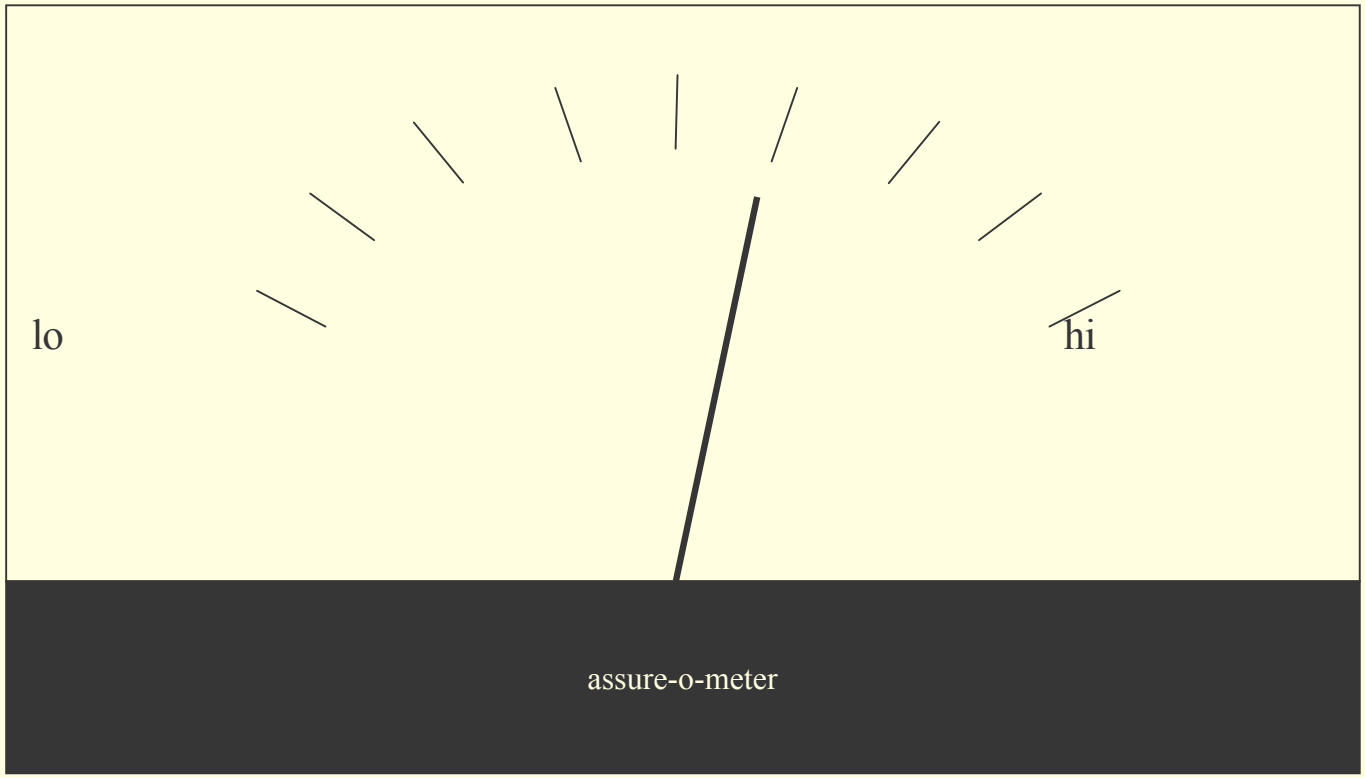
CS 591: Introduction to Computer Security

Lecture 13: Evaluation

James Hook

Evaluation



Evaluation

- Context:
  - DoD identifies computer security as important in ‘70s (Anderson 1972)
  - Recognizes trend toward networking: computing is communication
  - Economic forces dictate they purchase products built outside of the DoD
  - Need: Procurement guidelines for DoD to purchase security critical software

First Step

- James Anderson's "Computer Security Planning Study" provides a blueprint
- Needs analysis:
  - Multi-level operation
  - Systems connected to the world
  - On-line operation
  - Networks
- Vision
  - Security engineering
  - Secure components (hardware & software)
  - Handbook of Computer Security Techniques

Issues

- How to accelerate maturation of a discipline?
- Desire: codify best practices
- What if current practice is insufficient?
  - Legislate what we think best practices should be!
- Sullivan and R Anderson present two perspectives on the result
  - "Orange Book" over promised for formal methods
  - Organizations failed to deliver most trusted products
    - Good engineers thought they weren't solving the **real** problems
  - Common Criteria attempt to avoid some Orange Book faults
    - Still: some science, some science fiction (EAL 6 and 7)
  - Can post-hoc analysis ever work?

Bishop/Sullivan

- Chapter 18

Follow up

- NIST: National Institute of Standards
  - Founded to make fire fighting equipment interoperable across municipal boundaries
  - Now tasked with standards that support commerce
- NSA: National Security Agency
  - Signals Intelligence
  - Protect all sensitive information for DoD
  - Make the Internet safe for commerce (expanded interpretation of mission in last decade)

NIST and NSA

- Both agencies are involved in CC and Crypto certification
- NIST is the agency designated with to evaluated Engineering Assurance Levels 1 - 5 and FIPS crypto
- NSA is the agency designated to evaluate EAL 6 and 7 and DoD crypto

NSA's Crypto levels

- Type 1: Used for classified information. Tamper resistant. No tempest radiation. Uses NSA certified algorithms.
- Type 2: NSA endorsed for telecommunications. Not for classified data. Government proprietary algorithms.
- Type 3: NIST certified FIPS crypto
- Type 4: Registered with NIST but not certified

Aside:

- Data Mining, Security, and Privacy
- In the news last Winter and Spring:
  - NSA monitoring content outside of FISA (NY Times article)
  - NSA collecting massive amounts of call data (USA Today article last week)

References

- **Gary M. Weiss** (2005). Data Mining in . In O. Maimon and L. Rokach(eds.), *Data Mining and Knowledge Discovery Handbook: A Complete Guide for Practitioners and Researchers*, Kluwer Academic Publishers, 1189-1201.
- Corinna Cortes, Daryl Pregibon and Chris Volinsky, "Communities of Interest", The Fourth International Symposium of Intelligent Data Analysis (IDA 2001), 2001.
  - http://homepage.mac.com/corinnacortes/papers/portugal.ps

US Constitution
Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Credit Card Fraud detection

- Credit Card companies have done nearly real-time analysis of card usage
- Anomalies are flagged; card holder is contacted
- Customers have come to expect this service
  - It is considered a protection and an added value
- Discuss:
  - Abuse potential
  - Does government have a role? Why or why not?

Telephone

- Phone companies have collected "call detail data" for a long time
- Analyze data to build customer profiles
- One useful technique is the "Community of interest"
  - Top k callers in period of study (k is usually 9)
  - Can define a metric on communities
  - Tends to provide a good surrogate for identity ("Record Linkage Using COI-based matching")

Telephone fraud detection

- Historically, COI-based matching is used to detect a deadbeat customer who has assumed a new network identity
- Is this a legitimate business use?
- Is there a potential privacy issue?
- Discuss potential abuses

NY Times Story

- Revealed content of international phone calls between "persons of interest" were monitored outside of FISA
  - What not use FISA?
  - What if identity is a surrogate, not a name?

USA Today Story

- Several telephone companies providing call detail data to NSA
- "Largest database ever"
- Asserts no content being monitored
- Discussion/Conjecture:
  - What if they are calculating COI? Or COI-like data?
  - Could this serve as the source of the "surrogate identities" used for non-FISA wiretaps
  - If it is reasonable for business to use this technology for fraud detection is it reasonable for the government to exploit it as well?
  - What other personal information could be obtained from this data?