Systematic and Practical Methods for Computer Attack Analysis and Forensics

Dr. Sean Peisert
UC Davis Computer Science Dept.

NSF I/UCRC Meeting ~ Davis, CA
June 17, 2008

When We Need Audit Logs

- Computer forensics in courts
- Recovering from an attack
- Compliance (HIPAA, SOx)
- Human resources cases
- Debugging or verifying correct results (e.g., electronic voting machines)
- Performance analysis
- Accounting

We’re terrible analyzing events on computers

Audit data is usually...

- overwhelming
- free-form
- useless
- misleading (easily altered)

We're collecting too much bad information...

...and using it in courts and elections.

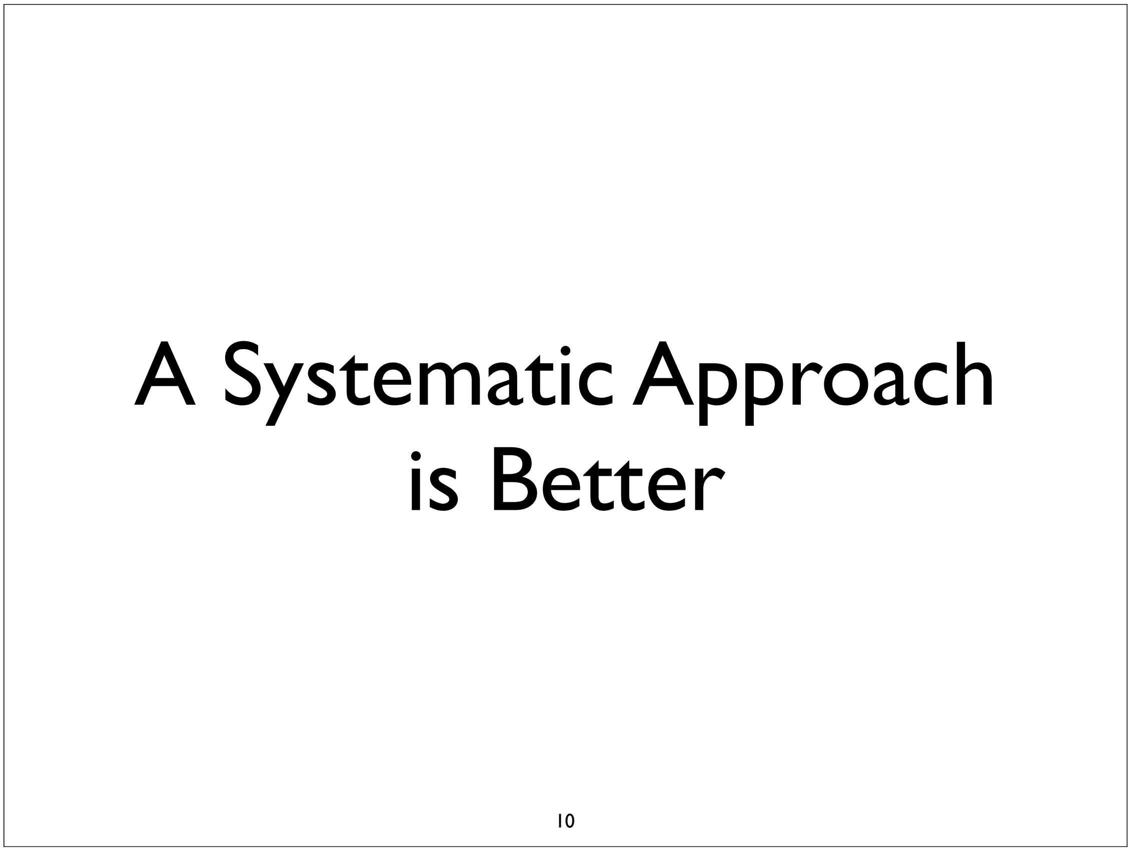
We need to...

- understand what the purpose of the analysis is
- understand what data can answer that purpose, with X% accuracy, and under a set of Y assumptions
- log the data
- give tools and techniques to an analyst to analyze that data

How is computer forensics done now?

- file & filesystem analysis (Coroner's Toolkit, Sleuth Kit, EnCase, FTK)
- syslog, tcpwrappers
- process accounting logs
- IDS logs
- packet sniffing

What do we need? What are we missing?



A Systematic Approach is Better

Forensic Art & Science

- But computer science can only answer part of it.
- Forensic analysis is an art, but there *are* scientific components. What are they?
  - Determining what to log
  - Determining relevance of logged data
    - what is relevant?
    - what is not relevant?
    - under what circumstances something might be relevant?
  - Using the results to constrain and correlate data.
  - *This can be measured, systematized and automated.*

Measurement Example: Empirical Study of Firewall Rules

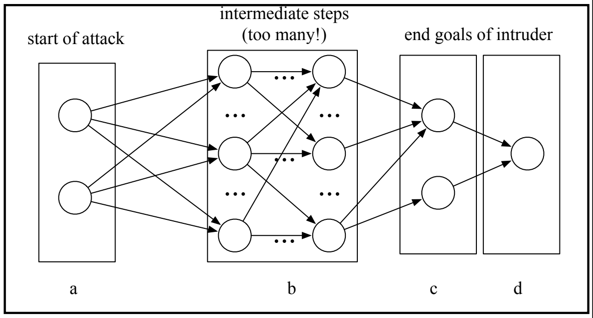
- How are firewalls configured?
- How should firewalls be configured?
  - What are the top, known vulnerabilities?
  - What are the top, known attacks?
- What are we missing? Is that OK?

Laocoön: A Model of Forensic Logging

- Attack graphs of goals.
- Goals can be attacker goals or defender goals (i.e.,“security policies”)
- Pre-conditions & post-conditions of those goals.
- Method of translating those conditions into logging requirements.
- Logs are in a standardized and parseable format.
- Logged data can be at arbitrary levels of granularity.

Attack Graphs

- Intruder goals can be enumerated.
- Vulnerabilities, attacks, and exploits cannot (or in many cases, we would patch them).
- Defender goals can also be enumerated. They are called security polices.



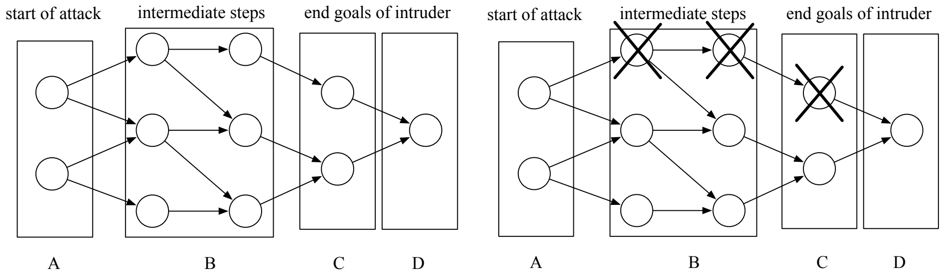
Security Policies

- Security policies can be reverse-engineered or enforced, automatically.
- Policies can be binary (block access) or flexible (log something).
- Policies can be static (always do this) or dynamic (uh oh—an intruder)

Applying Security Policies

- Applying Laocoön to security policies guides where to place instrumentation and what to log.
- The logged data needs to be correlated with a unique path identifier.
- Branches of a graph unrelated to the attack can be automatically pruned.
- Avoid recording data where events can be recreated because they are deterministic.

Pruning Paths



What are the assumptions for using current forensic tools?

- Often that there’s only one person who had access to the machine.
- Often that the owner of the machine was in complete control (as opposed to malware).
- Probably a lot of other assumptions that we have no clue about.

Summary: we can do better

- Forensics, attack analysis, logging, and auditing are broken.
- We seek to work on real-world problems with real-world data to construct and implement useful, usable, real-world software solutions.

Proposed Project

- Research practicality and tradeoffs in conditional access control (e.g., allow & log vs. block)
- Implement conditional access control with several countermeasures, including logging.
- For the logging portion, implement forensic logging of system & function calls, and analysis tools to correlate and prune data unrelated to the end goals that an analyst is concerned with.
- If there is time, attempt to do this via virtual machine introspection.

Selected Recent Publications

- S. Peisert, M. Bishop, and K, Marzullo, "Computer Forensics *In Forensis,*" *Proc. of the 3rd Intl. IEEE Wkshp. on Systematic Approaches to Digital Forensic Engineering*, May 2008.
- S. Peisert, M. Bishop, S. Karin, and K. Marzullo, "Analysis of Computer Intrusions Using Sequences of Function Calls," *IEEE Trans. on Dependable and Secure Computing (TDSC)*, 4(2), Apr.-June 2007.
- S. Peisert and M. Bishop, "How to Design Computer Security Experiments," *Proc. of the 5th World Conf. on Information Security Education*, June 2007.
- S. P. Peisert, "A Model of Forensic Analysis Using Goal-Oriented Logging," Ph.D. Dissertation, UC San Diego, Mar. 2007.
- S. Peisert, M. Bishop, S. Karin, and K. Marzullo, "Principles-Driven Forensic Analysis," *Proc. of the New Security Paradigms Workshop (NSPW)*, Sept. 2005.

Questions?

- Dr. Sean Peisert
  - Email: peisert@cs.ucdavis.edu
- More information and recent publications:
  - http://www.sdsc.edu/~peisert/