Computer Forensics *In Forensis*

Sean Peisert, UC Davis
Matt Bishop, UC Davis
Keith Marzullo, UC San Diego

SADFE ~ May 22, 2008
Oakland, CA

What happened??

Tradeoffs & Forensics

- Security vs. Usability
- Forensic Logging vs. Privacy
- Any Forensic Data vs. Accurate Forensic Data

Physical Forensics

- DNA evidence
- Physical mechanics
- Chemical analysis

Claims in court

- “50% of the FBI’s cases involve a computer” (FBI, 2002)
- Computer objects
- Virtual world
- Computer events

State of Connecticut v. Julie Amero

- Classroom computer displayed pornographic pop-ups.
- Investigators found child pornography on her (spyware-infected) computer and in logs.
- Convicted of "contributing to the delinquency of minors"
- QED.

State of Connecticut v. Julie Amero

- What if the email was part of browser popups or email spam?
- What if someone else used the computer?
- What if malware hijacked the computer?

Firewall Vulnerabilities

- Symantec Raptor / Enterprise Firewall FTP Bounce Vulnerability (2002, Bugtraq 4522)
- Symantec Enterprise Firewall SMTP Proxy Information Leak Vulnerability (2002, Bugtraq 4141)
- Multiple Firewall Vendor FTP Server Vulnerability (2000, Bugtraq 979)
- Microsoft Windows Internet Connection Firewall Filter Bypass Vulnerability (2004, Bugtraq 10930)
- SCO OpenServer reject Buffer Overflow Vulnerability (2001, Bugtraq 2592)

Virus Scanner Vulnerabilities

- Symantec AntiVirus Remote Stack Buffer Overflow Vulnerability (CVE-2006-2630)
- F-PROT Antivirus CHM File Heap Buffer Overflow Vulnerability (CVE-2006-6294, CVE-2006-6293

NIST's Role

- National Institute of Standards and Technology (NIST):
  - "Computer Forensic Tool Testing Program"
- How well tools conform to specific requirements
- E.g., NIST Deleted File Recovery spec.

The Players

- Forensic practitioners
- Judges
- Lawyers (prosecution & defense)
- Computer scientists

Open Questions

- Language
- Goals/needs
- Tools

Definitions

- *forensis* ~ “in public”
- *forum* ~ “a public square or marketplace used for judicial and other business”
- forensics
- computer/digital forensics

Forensic Language and Terminology

- "The tools and techniques to recover, preserve, and examine data stored or transmitted in binary form."
- "Valid tools and techniques applied against computer networks, systems, peripherals, software, data, and/or users—to identify actors, actions, and/or states of interest."
- software forensics: "tracing code to its authors"

Uses of Forensic Techniques

- Inside the courtroom:
  - 80% of "computer crime" cases involve child pornography
- Outside of the courtroom:
  - Compliance (HIPAA, SOx)
  - Debugging
  - Performance
  - Accounting/Billing

E-Voting Example

- Electronic voting machines were used in Goshen, New York
- After 999 votes, the counter reset and all votes were lost

Forensic Questions

- Who attacked this computer system?
- What actions did they take?
- What damage did they do?
- With what degree of certainty can we assert the result?
- Will those assertions be acceptable in court?

Forensic Systems

- Two parts of forensics:
  - Logging
  - Analysis
- Two types of logging:
  - State-based
  - Transition-based
- Two more types of data collection:
  - logging (syslog, BSM, IDS, firewall)
  - *post mortem* examination (Coroner's Toolkit, EnCase, FTK)

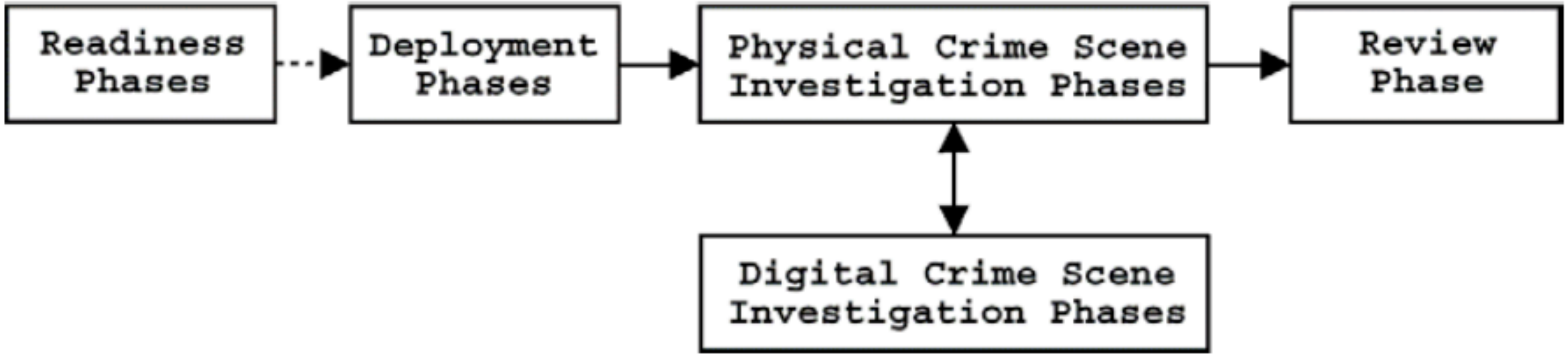
Scientific Method

1. Define question
2. Form hypothesis
3. Perform experiment and collect data
4. Analyze data
5. Interpret data and draw conclusions
6. Publish results, return to #3 and iterate

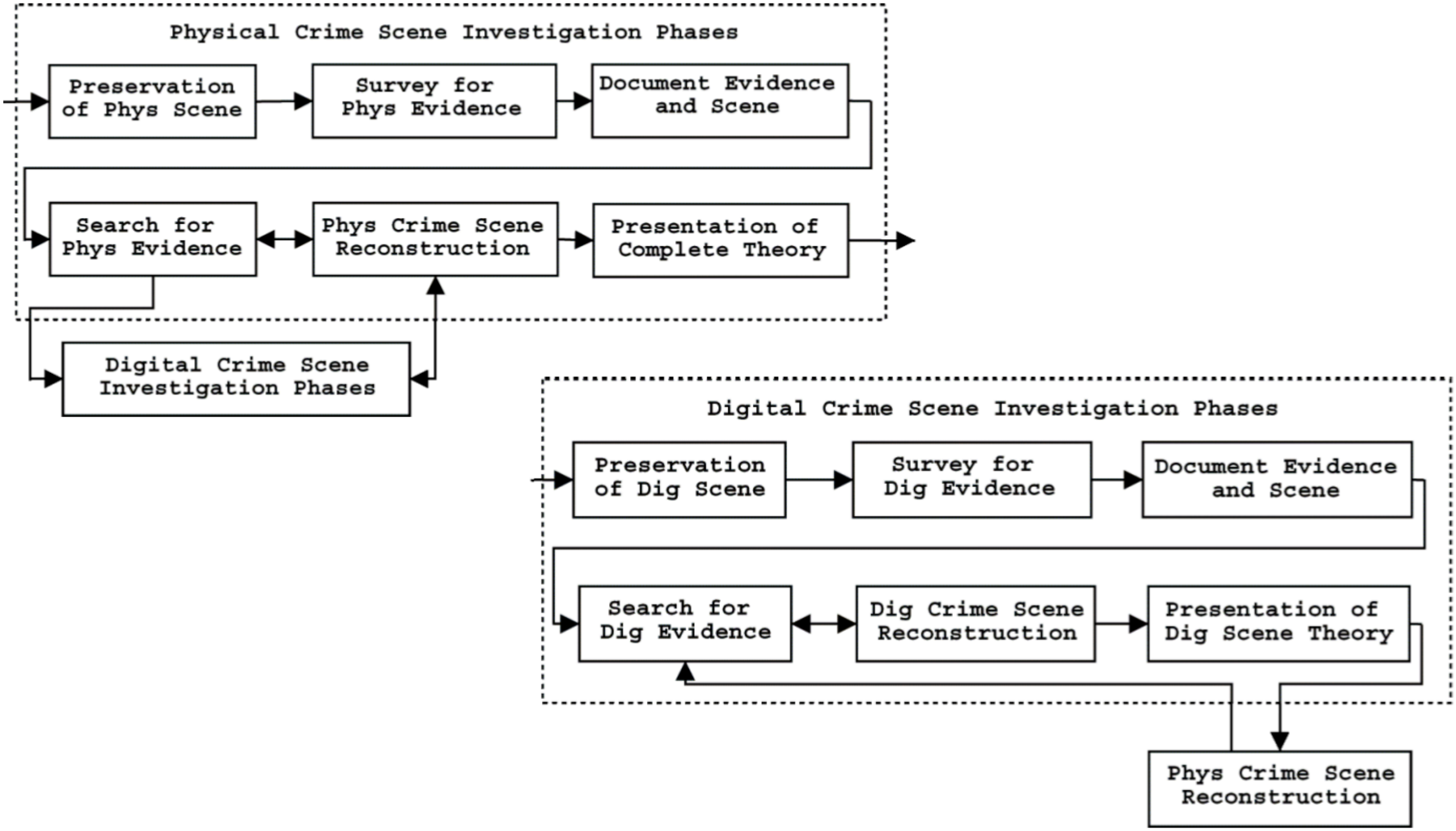
Forensic Models

- Practitioners
  - A series of steps for examining evidence.
- Computer scientists
  - An abstraction useful as a predictive formula.

Carrier's Model


Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Brian Carrier's Model



Physical Crime Scene Investigation Phases

Preservation of Phys Scene

Survey for Phys Evidence

Document Evidence and Scene

Search for Phys Evidence

Phys Crime Scene Reconstruction

Presentation of Complete Theory

Digital Crime Scene Investigation Phases

Digital Crime Scene Investigation Phases

Preservation of Dig Scene

Survey for Dig Evidence

Document Evidence and Scene

Search for Dig Evidence

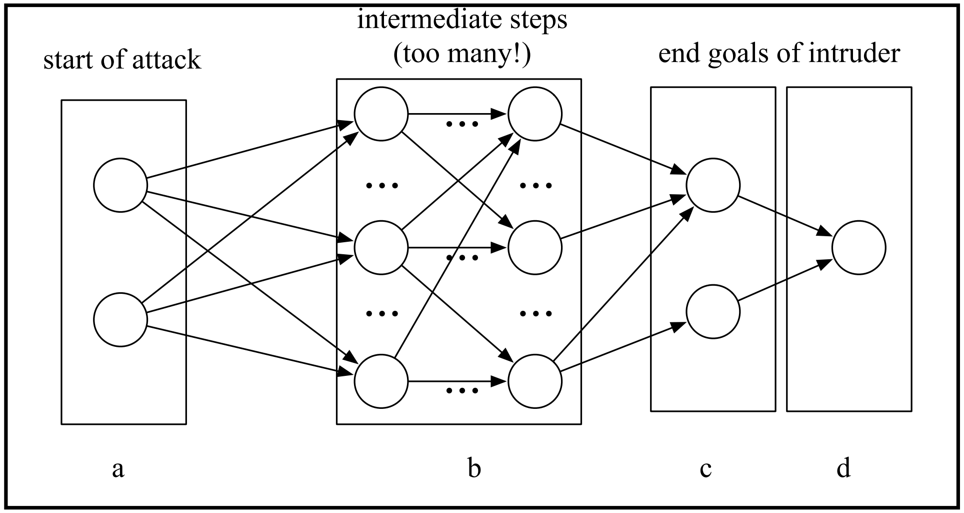
Dig Crime Scene Reconstruction

Presentation of Dig Scene Theory

Phys Crime Scene Reconstruction

Our Forensic Model (Laocoön)

- Attack graphs of intruder goals.
- Pre-conditions & post-conditions of those goals.
- Method of translating those conditions into logging requirements.



Unified Forensic Model

One that answers...

- how accurate is the method used to produce the data?
- how accurate is the method used to analyze the data?
- what claims can be made about the data?
- what assumptions must be made to make those claims?
- what can we do to reduce the amount of assumptions without reducing utility of the data?

Case Study #1: *Gates v. Bando*

- Facts
  - Former employee accused of stealing a proprietary computer program.
  - Gates subpoenaed the hard drive.
  - Gates alleged that evidence on the drive had been destroyed.
- *Norton Unerase was run by the prosecution's expert witness* ***from the target drive.***

Case Study #2: Electronic Voting

- Florida CD13 showed an anomaly: an order of magnitude more undervotes than expected.
- Only occurred in one race.
- No VVPATs
- State audit concluded that the software did not contribute to the problem.
- A VVPAT would not have helped.

Evaluating Forensic Systems Example: *Sleuth Kit*

- What does it do?
- What doesn't it do?
- How accurate is it?
- What can we say with the data?
- What assumptions must me made?
- What can we do to reduce the assumptions?

Open Research Questions

- What does a unified model look like?
- How do we characterize the limits and assumptions of forensic tools?
- How can we compare the model of the process to the evaluations of the tools to find the gaps and overlaps?

Forensics = Science

"The principle of science, the definition, almost, is the following: *The test of all knowledge is experiment.* Experiment is the *sole judge* of scientific "truth."

—Nobel Laureate Richard P. Feynman,
California Institute of Technology,
September 26, 1961

Final Thoughts

- Data accuracy
- Claims
- Assumptions

Questions?

Sean Peisert
peisert@cs.ucdavis.edu
http://www.sdsc.edu/~peisert/