

Network Forensics: Notions and Challenges

Ahmad Almulhem



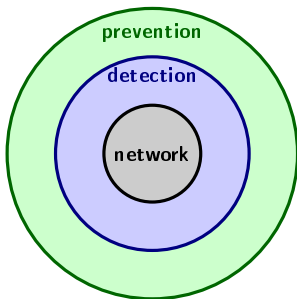
جامعة الملك فهد للبترول والمعادن
King Fahd University of Petroleum Et Minerals

ISSPIT'09 – Ajman, UAE

Outline

- 1 Network Security
- 2 Network Forensics
- 3 Related Technologies
- 4 Challenges
- 5 Conclusion

Network Security: The big picture



- Securing computer networks is challenging
- Mixture of Various technologies
- Lack of investigative features.
- Firewall logs and IDS alerts are not suitable for investigation.
- Network Forensics is proposed to support investigating incidents in computer network.

Technologies Used	2008
Anti-virus software	97%
Anti-spyware software	80%
Application-level firewalls	53%
Biometrics	23%
Data loss prevention / content monitoring	38%
Encryption of data in transit	71%
Encryption of data at rest (in storage)	53%
Endpoint security client software / NAC	34%
Firewalls	94%
Forensics tools	41%
Intrusion detection systems	69%
Intrusion prevention systems	54%
Log management software	51%
Public Key Infrastructure systems	36%
Server-based access control lists	50%
Smart cards and other one-time tokens	36%
Specialized wireless security systems	27%
Static account / login passwords	46%
Virtualization-specific tools	29%
Virtual Private Network (VPN)	85%
Vulnerability / patch management tools	65%
Web / URL filtering	61%
Other	3%

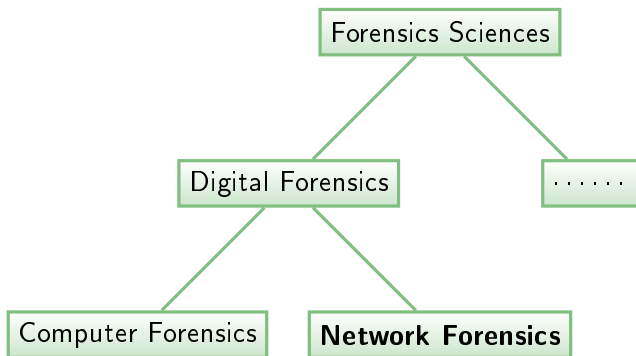
2008 CSI/FBI Computer Crime & Security Survey

Definition

The use of scientifically proved techniques to **collect** and **analyze** network packets and events for **investigative** purposes.

- It is not a **product**. It is a complex **process**.
 - technology (tools), human intelligence, law
- It is not to **replace** firewalls, IDS, etc.
- It **employs** IDS alerts, firewalls logs, packets, etc.

Where does it fit in the forensics family?

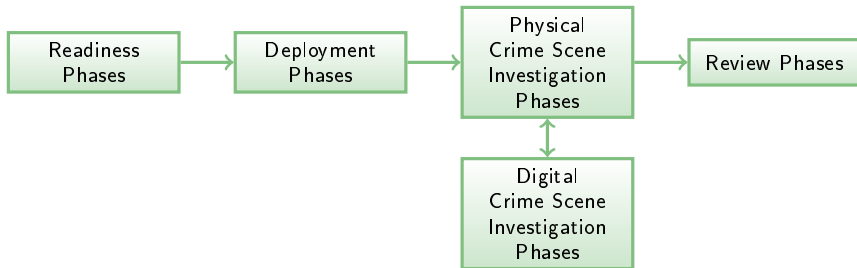


- New member of the family of **digital forensics**.
- Digital forensics in a **networked environment**.

Current Practice

- Generally means collecting and analyzing logs and captured packets in a networked environment to investigate a hacking incident.
- ad-hoc manual.
- Experienced system admins
- art/science.

Digital Forensics Modeling



- **Readiness phases:** The goal of these phases is to ensure that the personal and infrastructure are able to fully support an investigation when an incident occurs.
- **Deployment phases:** The goal of these phases is to provide a mechanism for an incident to be detected and confirmed.
- **Physical Crime Scene Investigation phases :** The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident.
- **Digital Crime Scene Investigation phases :** The goal of these phases is to analyze digital devices that were obtained from the physical investigation phases.
- **Review phases :** The goal of these phases is to review the whole investigation and identify areas of improvement.

Intrusion Detection Systems

A system designed to detect computer and network attacks

- 😊 A sensor to trigger the forensics process
- 😊 A source of data (Alerts)
- 😞 Detection Reliability
- 😞 Data details may not be adequate

Honeypots

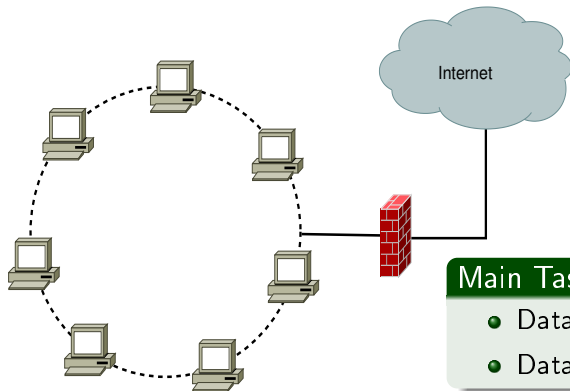
A system built to lure and contain intruders

- 😊 Study attackers and capture their tools (realtime)
- 😞 Legal issues (damage claim, entrapment)

Computer Forensics

Forensics analysis of standalone computers

- 😊 Investigate the computers as if they were not networked
- 😊 Distributed data sources issues: data correlation, attack propagation.
- 😊 Volatile data (network traffic)



Main Tasks

- Data Collection
- Data Analysis

Challenges

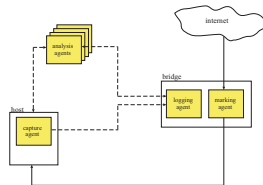
- Data Sources:
 - Which data sources? All or a subset?
- Data granularity
 - How much details? (e.g. complete packets or headers?)
- Data integrity
 - Ensure data integrity (deliberately or accidentally)
- Data as Legal Evidences
 - Court admissibility
- Privacy Issues
 - Handling sensitive information (authorization)
- Data Analysis
 - Automation, tools, data mining, visualization (art)

Concluding Remarks

- Network forensics is a dedicated investigation infrastructure for networks.
- It extends the network security model (prevention/detection).
- It is not a product; it is a complex process
- Challenges in term of collecting and analyzing data

Further Readings

- 1 G. Palmer, "A road map for digital forensic research," in *Digital Forensic Research Workshop*, Utica, New York, 2001.
- 2 A. Almulhem and I. Traore, "Experience with engineering a network forensics system," *Lecture Notes in Computer Science*, vol. 3391, pp. 62–71, Jan. 2005.



Questions?

<http://www.ccse.kfupm.edu.sa/~ahmadsm/>