COMP 2555 Principles of Computer Forensics

Lecture 4

Ramki Thurimella, PhD

Overview

- Review of Lecture 3
- Exercises from Chapter 2 of Vacca
- Key Points of Chapter 2 of CERT Book
- Material from Chapter 3 of Vacca
  - Types of Computer Forensic Systems
- Demos: Recovery of data from floppy
- Useful open source tools & other links
- Conclusion

Types of Forensic Systems

- Internet Security
- IDS
- Firewalls
- Storage area networks
- Network disaster recovery
- PKI
- Wireless security
- Satellite encryption
- IM security
- Net Privacy
- Identity management
- Biometric
- Homeland security

Internet Security Systems

- Draft high-level policy
  - Measures to safeguard systems, networks, transactions, and data
  - List of assets
  - Internet security & limiting physical security (secure access to routers etc.)
  - Roles & privileges
  - Password security (if too restrictive, people bypass)
- Examine and enumerate risks
  - Grades
  - Employee salary information
  - Customer credit card information
  - FUSER
- Implementation Strategy (at DU)
  - VPNs
  - Remote connectivity
  - Web email

Authentication Mechanisms

- What you know (password, favorite color)
- What you have (smart card, RFID, USB token)
- Who you are (biometrics: fingerprints, voices, faces, iris and DNA)
- Where you are (GPS)

PKI

- Review of background material from Network Security Chapter
- Public key, private key
- Diffie-Hellman key exchange

IDS (yet another idea that doesn't work)

- From Dirk Ourston, Sara Matzner, William Stump, and Bryan Hopkins. Coordinated internet attacks: Responding to attack complexity. *Journal of Computer Security*, 12(2):165–190, 2004.

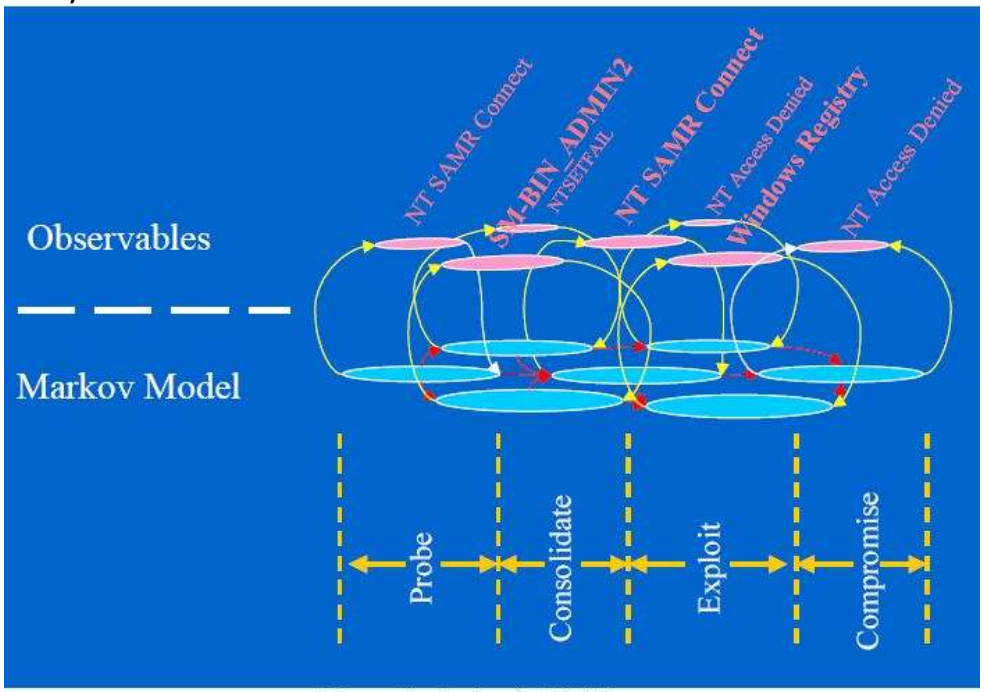

Figure 1. A simple HMM

Weakness

"A single record of the real-time data consists of the type of alert being reported by the network sensor, as well as various types of context information including bytes transferred, source host address, target host address, and so on."

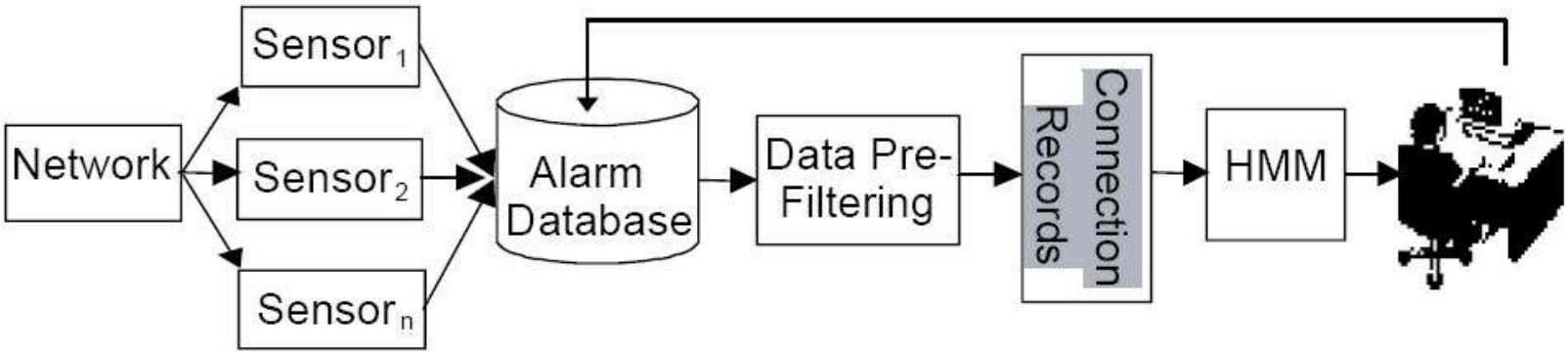

Figure 2. System architecture

Additional reading

- Schneier on privacy & Amendment 4
  - http://www.wired.com/print/politics/security/commentary/securitymatters/2009/03/securitymatters_0326
- Judge orders defendant to decrypt
  - http://www.techworld.com/news/index.cfm?newsID=111731&printerfriendly=1

Useful links

- http://www.opensourceforensics.org/tools/index.html
- http://www.dfrws.org
- Debugger: http://www.ollydbg.de/
- http://foremost.sourceforge.net/