COMP 2555 Principles of Computer Forensics

Lecture 16

Ramki Thurimella, PhD

Overview

- Project 3 discussion
- Chapter 8 (Vacca) Computer Image Verification & Authentication
- Your Botnet is My Botnet

Best Evidence

- Two copies
  - One sealed in front of the owner (master copy) and placed in secure storage
  - If the computer has been seized, it will constitute the *best evidence*
- Assumption: while in secure storage, it has not been tampered
- Growing problem: Expensive, both time & money, to make copies when the size of the drives is large

Evidential Authentication Requirements

- Data should not have been altered since the copy was taken
- The copy is the one taken at the time and on the computer in question
- Authenticode
  - Origins of programs
  - Shareware is not signed many times
  - Code signing certificate can be obtained for ~$200 from places like VeriSign

Authenticode

- Used for
  - .cab files
  - .exe files
  - Active X controls
- Certification Authorities
- X.509 Standard
- Certificates expire

Practical Considerations

- Data collection should be complete and non-software specific, thus avoiding software traps and hidden partitioning
- Quick and simple
- Ease of use of data collection system (a technician should be able to do it)
- Necessary costs to be kept to a minimum
- Security is like insurance—you don't know when you need it

Security Considerations

- Allow employees to do everything they need to do to be efficient from a business standpoint without opening the door to an attack
- CIOs should do risk management
- Difficult measure ROI