Digital Forensics

Module 11
CS 996
Outline of Module #11

- Return of old lab homework: Kulesh
- Presentation on ??: Yuliya
- Presentation on security best practices
- Discussion on cyberlaw issues
- Forensics challenge
- Reminder for final exam: May 11, 6-8pm.
Expert Forensic Testimony

- “My Cousin Vinny”: forensic testimony
- Background facts for case
- Two opposing experts on tire tracks
- FBI prosecution expert
  - “Constructive” cross-examination
  - Didn’t look for all possible theories
- Vinny’s expert
  - Voir dire: prosecutor’s mistake
  - General automotive knowledge
  - Deflects trick questions successfully
Implementing IT Security: 3 Steps

- Prevention
- Detection
  - Proactive monitoring
- Response
  - Incident response forensics
Audits Drive Security Requirements

- Financial audit
  - GAAP
  - IS auditors
  - IT Control Objectives and Controls

- Attestation services
  - SAS 70 (www.sas70.com)
  - WebTrust
  - Customer selects tests!!!
www.postini.com

- Leading message outsourcer for law firms
- WebTrust seal for security, availability, privacy
- KPMG certifies that
  - Postini provides reasonable assurance of security, privacy and availability
  - Report is dated June, 2004 only; future projections may be invalid
  - Error or fraud may occur and not be detected
Security “Best Practices”

- Control objectives
  - Physical Access Control-Make sure that controls are in place to limit access to computers, media and documentation to authorized people

- Control practice or activity
  - Regular review of firewall and router log files

- Policies: technology agnostic

- Standards: technology specific system specifications or procedures
Best Practices: Examples

- COBIT: Control Objectives for Information and Related Technology (www.isaca.org)
- ITIL: IT Infrastructure Library (www.itil.org)
- SANS: IT Policies (www.sans.org)
- BS7799: www.iso.org (ISO 17799)
- CIS: Center for Internet Security (www.cisecurity.com)
Industry Specific Best Practices

  - US government

Legal Issues in Cyber Investigations

- What are the three legal regimes?
- Limits on search and seizure by government?
- Reasonable expectation of privacy (REP)?
- Entrapment; honeypots?
Forensics Challenge: Cheating in Chicago Public Schools

- Grades on standardized tests seem too high
  - 400,000 students in school system
  - No Child Left Behind
- How to go about looking for cheating?
- We are looking for cheating by the teachers
- Forensics challenge: classrooms A and B
Review 1

- Definition of “Digital Forensics”
- Standards of Evidence
- Basic procedures
- 18 USC 1030 Computer Fraud and Abuse Act
- Cybersurveillance
  - Pen register, trap and trace
  - Wiretap
- Hard drive storage layout
US v. Rajib K. Mitra (April, 2005)

- Grad student interfered with emergency radio communications systems in Madison, WI
  - 19 signal channels for police, fire, etc.
  - 1 signalling channel
- He was tried and convicted under CFAA, 18 USC § 1030
- He appealed in 7th Circuit (Chicago, IL)
  - CFAA applies only to interstate commerce
  - CFAA doesn’t apply to mobile radios, only computers
- What do you think?
AA v. FareChase (2003)

- FareChase markets software to help browse travel web sites, including www.aa.com
- FareChase aggregates fare information
- AA sued to block access to its site
- Texas Penal Code § 33.02
  - “a person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner”. 
FareChase Proxy Architecture

INTERNET

FARECHASE SERVER

TRAVEL AGENT

WWW.AA.COM
WWW.DELTA.COM
WWW.UNITED.COM
Analysis of Damage to Site

WEB SITE RESPONSE TIME

RESPONSE TIME (SEC.)

NUMBER OF DAILY USERS
Review 2

- Google hacking
- Hard drive layout: MBR, partitioning, etc.
- File system types, FAT, NTFS
- Investigating email spam, phishing, etc.
- Email message transfer
- Analyzing message headers
- CAN Spam Do’s and Don’ts
Review 3

- Document metadata
- Eliminating metadata
- Information search methods
  - Key word
  - Concept
  - Boolean
- Concept search
  - Thesaurus
  - Training: “budget” > amortization, EBITA, etc.
- Electronic discovery in litigation - 3 types
Review 4

- Using EnCase
- Acquisition
- Analysis
  - String search
  - Signature matches
  - Compound file analysis
  - Bookmarks
- EnCase image file
- EnCase scripts
- FileViewers
Bank of America Case

- Lopez v. B of A filed 2/7/05
  - $90,000 stolen from his account and transferred to Latvia
  - Found a keystroke logger on his PC
- Lopez claims bank was negligent in not advising him about risks of Trojans
- First lawsuit where plaintiff alleges inadequate security practices!
- FDIC coverage?
Phantom Withdrawals

- Credit card liability: $50, by law
- Debit card liability
  - Up to $500 if <48 hours notification
  - Everything in account +overdraft if >60 days notification
- FDIC coverage ($100,000 for physical robberies)
  - Personal account ??
  - Business account ??
Review 5

- EnCase features, continued
  - Gallery
  - Timeline
  - Reporting
  - Disk

- Unix forensics
  - mount, dd, fdisk, stat, grep, loop device, md5sum, ls
  - Drive naming
  - File properties: types and permissions
  - MAC times
Review 6

- Open Source forensic tools
  - Sleuthkit
  - Autopsy
  - Helix

- Windows system investigation
  - Application log files, temp files, recycle, history, registry, hidden files (ADS)
  - Windows logfiles
Review 7

- Linux forensics: where?
  - history file, user accounts, logfiles, program size, root kits, /etc config files, mac times, /sbin displaced inodes, files with ‘.’ or spaces

- Using Helix for windows systems
  - File recovery
  - GRAB: file acquisition
Review 8

- Forensic sources: networks
- SIM tools
  - Event correlation methods
- Log files
- ADS files
Log File Formats

- **CheckPoint**
  - Proprietary binary format, not human readable
    - Time | Action | Firewall | Interface | Product | Source | Source Port | Dest. | Service | Protocol | Translation (NAT)

- **Cisco PIX**
  - Syslog format
    - Date | Time | IP/Hostname | Message Code | Message

- **NetScreen**
  - Syslog format
    - Date | Time | Module | Severity | Type | Message Text
  - **Syslog: time stamp | hostname | message**
Review 9-10

- Incident response strategies
- Internet search: Google + Copernic
- Courtroom presentations
References

- Stepping Through the IS Audit, Bayuk, 2004.
- Freakonomics, Steven Levitt, 2005.
- www.headfry.com (IT security issues)
- www.loganalysis.org