Computer Forensics

Dr. Marc Rogers PhD. CISSP
Director, Information Security Services

MANAGEXW INFORMATION SYSTEMS SECURITY TEAM
LOOKING OUT FOR YOUR SECURITY
Agenda

- Types of Computer Crime
- The Cost
- Computer Forensics
- Evidence Management
- Tools
- Summary
- References
Hong Kong Reuters Office Hacked: Traders at 5 banks lose price data for 36 hours

PA Teenager Charged With 5 Counts of Hacking: Southwestern Bell, BellCore, Sprint, and SRI hit. Costs to Southwestern Bell alone exceed $500,000.

Citibank Hit in $10 Million Hack: Russian hacker had inside help. Several $100K not yet recovered.

Computer Attacks Cost $36 Million Total in 2000

Technology terrorism: 10 products that will.

De Beers security hole reveals customer information

By Stefanie Olsen
Staff Writer, CNET News.com
April 4, 2000, 4:45 p.m. PT

About 35,000 customer email and home addresses were exposed on Adiamonddisforever.com, an informational site about diamonds, De Beers, CNET News.com has learned.

10. Back Orifice

Facts

- Thick: Allows someone to control your PC remotely--without authorization.
- Treat: Your archenemy deletes your files just for the heck of it.
The Net

AOL outage brief but dangerous
By Janet Kornblum
Staff Writer, CNET NEWS.COM
February 24, 1998, 1:00 p.m. PT

news analysis The last time America Online (AOL) suffered a total blackout, members were knocked offline for 19 hours. Last night's outage, by comparison, lasted a relatively painless 2-1/2 hours.

Pentagon says computers invaded by hackers
By Jaret Kornblum

Student finds AOL bug
By Jaret Kornblum

9.9% Fixed (not an introductory rate!)
No Annual Fee

Computer Glitch Halts NYSE Trading for One Hour - Netscape
By Ianthe Jeanne Dugan and Mark Leibovich
Washington Post Staff Writers
Tuesday, October 27, 1998, Page C01

Dr. Marc Rogers Ph.D., CISSP
Computer Crime

- What is a computer crime?
- 3 generic categories
  - Computer Assisted
  - Computer Specific
  - Computer Incidental
Computer Crime

- **Computer Assisted Crime:**
  Criminals activities that are not unique to computers, but merely use computers as tools to assist the criminal endeavor (e.g., fraud, child pornography).

- **Computer Specific or Targeted Crime:**
  Crimes directed at computers, networks and the information store on these systems (e.g., denial of service, sniffers, attacking passwords).

- **Incidental:**
  The computer is incidental to the criminal activity (e.g., customer lists for traffickers).
The Problem

- How big is the problem?
  - USD $400 Million?
  - USD $10 Billion?
- Canadian Stats?
- Under-reported
- F.U.D.
Privacy/Security issues could potentially put an $18 billion dent in the projected $40 billion 2002 e-Commerce revenue (Jupiter Communications, 2000).
Terms

- **Computer Forensics**: The study of computer technology as it relates to the law.
- **Forensic Analysis**: Examination of material and/or data to determine its essential features and their relationship in an effort to discover evidence in a manner that is admissible in a court of law; post-mortem examination.
- **Electronic Evidence**: Evidence relating to the issue that consists of computer files, or data, in their electronic state.
- **Electronic Media Discovery**: The discoverability of electronic data or files.
- **Chain of Custody**: A means of accountability, that shows who obtained the evidence, where and when the evidence was obtained, who secured the evidence, who had control or possession of the evidence.
- **Rules of Evidence**: Evidence must be competent, relevant, and material to the issue.
Computer Forensics

- **History**
  - **1984** FBI Computer Analysis and Response Team (CART)
  - **1991** International Law Enforcement meeting to discuss computer forensics & the need for standardized approach
  - **1997** Scientific Working Group on Digital Evidence (SWGDE) established to develop standards
  - **2002** Still no standards developed or common body of knowledge (CBK)
Computer Forensics

- Computer Forensics involves:
  - *Preservation, identification, extraction, documentation*, and *interpretation* of computer data.
  - It is both an *art* as well as a *science*!
Computer Forensics

- **3 Basic Principles**
  - **Acquire** the evidence (data) without altering or damaging the original data or scene
  - **Authenticate** that your recovered evidence is the same as the original data
  - **Analyze** the data without modifying it

- **Sometimes easier said than done!**
Investigative Chronology

- Time attributes (Modified, Accessed, Changed).
- Allow an investigator to develop a time line or Chronology of the incident.
- The time line is vital when examining logs, & event files.
- Improperly accessing or searching a system can alter the time lines, destroying evidence or erasing trails.
MAC Times

- **Mtime** (modified time), **atime** (accessed time), **ctime** (changed time)
- Reading a file or running a program changes the **atime**
- **Mtimes** are changed by modifying a file’s content
MAC Times

- **Ctime** keeps track of when the meta-information about the file was changed (e.g., owner, group, file permission)

- Some systems have **dtimes** (deleted time). **Ctime** can be used as an approximation of when a file was deleted
Digital Evidence

- Digital evidence is *fragile*
- Can be *contaminated* very easily
- Only really *one* chance to do things correctly
- Admissibility in court depends on *establishing the authenticity and integrity of the evidence*
Digital Evidence

- **Authenticity** - does the material come from where it purports?
- **Reliability** - can the substance of the story the material tells be believed and is it consistent? In the case of computer-derived material are there reasons for doubting the correct working of the computer?
- **Completeness** - is the story that the material purports to tell complete? Are there other stories which the material also tells which might have a bearing on the legal dispute or hearing?
- Acceptable levels of freedom from interference and contamination as a result of forensic investigation and other post-event handling
Chain of Custody

- Protects integrity of the evidence
- Effective process of documenting the complete journey of the evidence during the life of the case
- Allows you to answer the following questions:
  - Who collected it?
  - How & where?
  - Who took possession of it?
  - How was it stored & protected in storage?
  - Who took it out of storage & why?
Drive Imaging

- Forensic Copies
  - **Bit for Bit** copying captures all the data on the copied media including hidden and residual data (e.g., slack space, shadow space, swap, residue, unused space, deleted files etc.)
  - Normal imaging *only* copies the data the file system recognizes
- Often the "smoking gun" is found in the deleted & residual data.
- Image Integrity (mathematical fingerprint)
  - **MD5**, **CRC**
Drive Imaging Tools

- SafeBack ([www.forensics-intl.com](http://www.forensics-intl.com))
- Ghost ([www.symantec.com](http://www.symantec.com))
  - Newest version of Ghost has a forensic “switch”
- DD (standard unix/linux utility)
  - `#dd if=device of=device bs=blocksize`
- Encase ([www.encase.com](http://www.encase.com))
Drive Examination Tools

- Encase
- Forensix
- Coroner’s tool kit
- Autopsy browser
- @Stake TASK
- iLook
- Hex editors
Issues

- Private Sector vs. Law Enforcement
- Civil vs. Criminal remedies
- Proprietary tools
- Changing definitions of best evidence
- No National or International Computer Forensics Standards
Issues

- No International Definitions of Computer Crime
- No International agreements on extraditions
- Multitude of OS platforms
- Incredibly large storage capacity
  - 100 Gig +
  - Terabytes
  - SANs
- Networked environments
- RAID systems
Summary

- Computer Forensics is a **growth** industry
- Very easy to do **wrong**!
- Computer Forensics is **not** a piece of software
- Computer Forensics **is** a **methodology**
- **Technical skills** need to be **combined** with **investigative skills**
- Need for a **CBK** and **International Standards**
- Unless properly trained in forensics **turn** the suspect system **over** to someone who **is** trained!
Questions/ Comments
Contact Information

Dr. Marc Rogers Ph.D., CISSP
Ph: 989-8750

E-mail: mkr@manageworx.com
Web: www.manageworx.com
Book References

Web References

- www.cybercrime.gov
- www.encase.com
- www.sans.org
- www.ijde.org
- www.nist.gov