An overview of IT Security Forensics

Manu Malek, Ph.D.
Stevens Institute of Technology
mmalek@ieee.org
www.cs.stevens.edu/~mmalek
April 2008

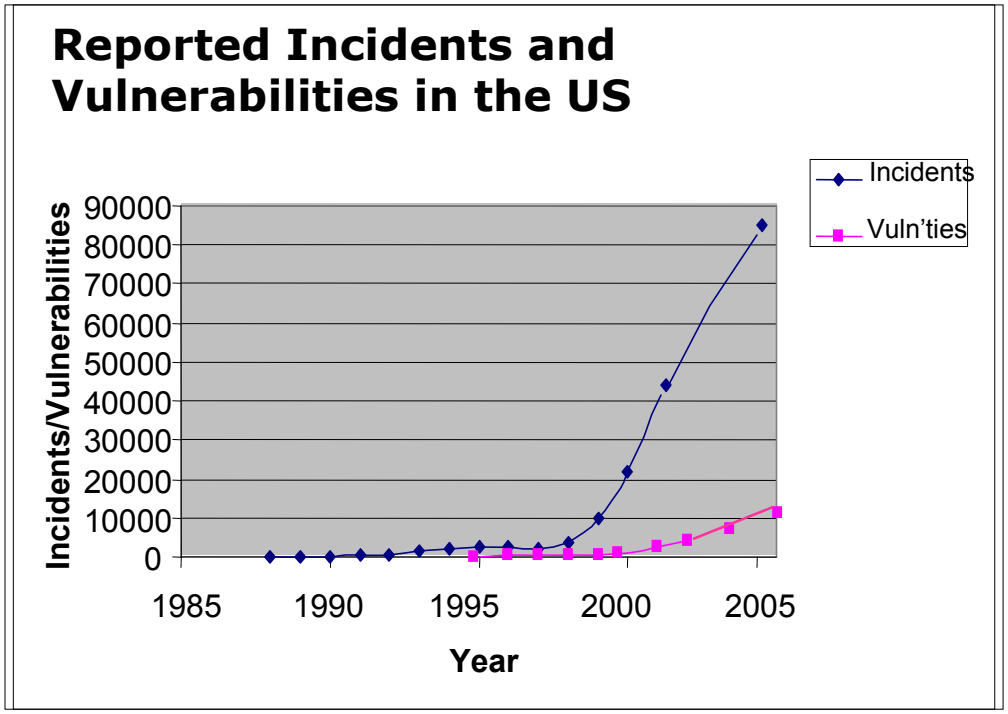
Outline

- Growing Threats/Attacks
- Need for Security Forensics
- Basic Methodology
- Forensic Tools
- A Sample Tool

Growing Threats/Attacks

- Cyber attacks are on the rise
  - An increase of over 30 times during the past 5 years
  - An increase of 10 times during the past 3 years
- *Cyberterrorism*:

  The potential exists for attackers to break into computer networks controlling sensitive processes.



Adopted from *www.cert.org*

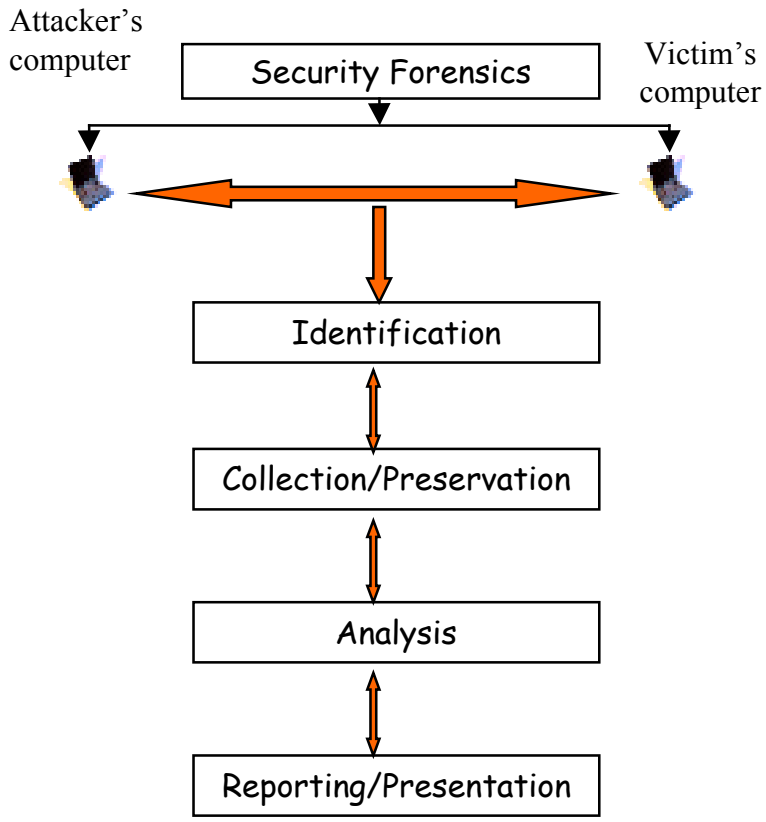
Trends Affecting Safe Internet Usage

- Faster discovery of vulnerabilities
- Automation and rising speed of attack tools
  - Scanning for vulnerable systems
  - Coordinated attack tools
- Increasing sophistication of attack tools
  - Dynamic behavior
  - Anti-forensics
- Increasing permeability of firewalls

What is Security Forensics?

- Forensic: *Belonging to, or used in, public debate or court of law*
- Security Forensics: Application of science and engineering to dealing with evidence stored on computers and network devices
- It is the process of
  - Identifying,
  - Collecting and preserving,
  - Analyzing, and
  - Reporting and presenting

  digital evidence in a manner that is legally acceptable.

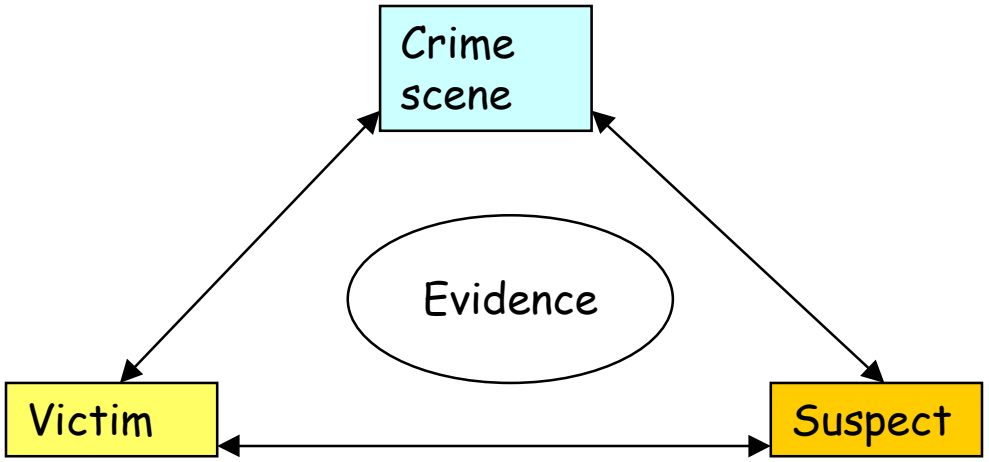


Need for Security Forensics

- Forensic methods are used to
  - Determine root cause of events
  - Support litigation
- Examples:
  - Today's corporate environment requires preparation for possibilities of future litigation, e.g., for
    - Wrongful termination claims
    - Intellectual property claims
    - Antitrust cases
  - Law enforcement agencies use computer forensics in civil and criminal suits

Locard's Principle and Continuity of Offense

- Locard's Exchange Principle: When any two objects come into contact, there is transference of material from one object to another.
- Continuity of offense: Attribute the crime to its perpetrator by providing compelling links between the suspect offender, victim, and crime scene.



IT Requirements for Forensics

- The following capabilities are needed to support Computer Forensics:
  - Being able to collect relevant information from systems
  - Being able to positively identify users who log on to systems
  - Being able to handle challenges to data ownership or audit trails found on a system
- Examples of activities to meet these requirements:
  - Logging user actions
  - Logging system and network events
  - Maintaining time servers and standard time settings
  - Giving each new employee a computer with a forensically clean disk and a standard set of applications
  - Duplicating all the data on an employee's computer before he/she is informed of job termination

Forensic Data Collection in Client Computers

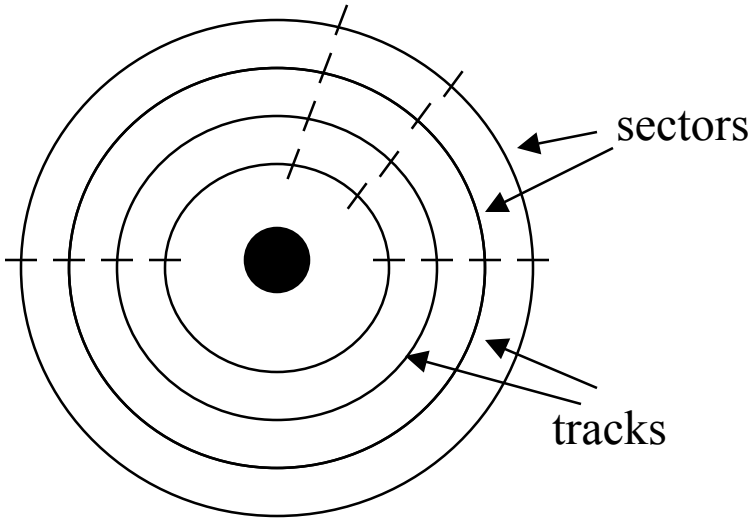
- Most operating systems provide significant logging capabilities.
  - Windows systems (2000/NT/XP) store log files in the directory %systemroot%\system32\config\
  - In UNIX, information about running processes is usually stored in *var/log/syslog*
- Device logs; for example, one can find out if
  - A USB device has been used
  - A CD burner has been used
  - A file has been printed
- Protecting logs
  - Attackers could delete or modify logs
  - Logs should be protected

Demo: Windows event log and viewing

Hidden Evidence

- Evidentiary data is not often readily observable.
- Evidence could be in
  - Deleted files
  - Encrypted files
  - Files hidden in other files
  - Files in parts of the hard drive that are not readily exposed:
    - File slack
    - ATA "Protected Area"

A Disk Platter



A sector

Demo: File Scavenger

Network-based Evidence

- Network monitoring can be performed to collect evidence:
  - Event monitoring: collecting network events, such as IDS alerts, network health monitoring alerts
  - Trap-and-trace monitoring: transaction data such as protocol flags
  - Full-content monitoring: collecting raw packets
- Network-based evidence can be found at endpoints and intermediate systems, such as
    - Authentication servers
    - Router logs
    - Firewall logs
    - Event logs from IDSs
    - Caller ID systems

Demo: Ethereal

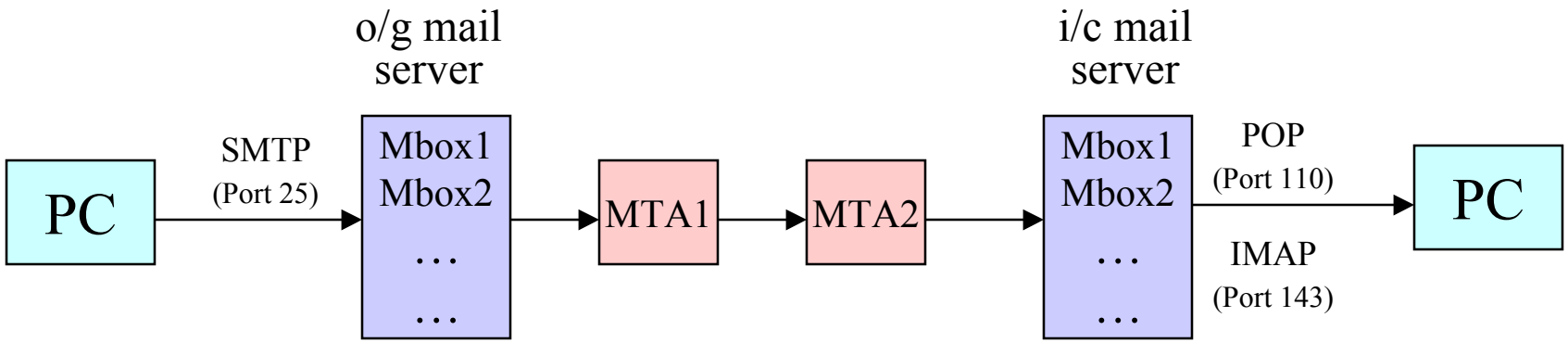
Forensic Tools

- Many forensic tools and applications exist, e.g., for
  - Hard disk duplication
  - Text and file searching
  - Internet history analysis
  - Analysis of email files
  - Analysis of data stores
  - Network forensics
- Some popular tools:
  - *EnCase* for drive forensics
  - *E-Trust* for industrial espionage cases
  - *Forensic Toolkit* (FTK)
  - *ProDiscover*
- Hardware and software-based key loggers can collect key strokes for specified periods of time.

Example - Email Forensics

- Email is one of the important security forensic areas.
- Tracking email may become necessary to try to identify, e.g.,
  - The sender of a threatening message
  - The sender of malicious software
  - Unauthorized disclosure of corporate information
  - Spammers

Simplified email architecture



MTA: Mail Transfer Agent

SMTP Extended Header

- To investigate a case involving email, the SMTP Extended Header must be analyzed.
- SMTP Extended Header includes information like shown below:

Return-path: <mmalek@ieee.org>

Received: from box.stevens.edu (box.stevens.edu [155.246.154.13]) by nexus.stevens.edu
(iPlanet Messaging Server 5.2 HotFix 2.04 (built Feb 8 2007))
with ESMTP id <0ILM00LKAW6TJT@nexus.stevens.edu> for mmalek@stevens.edu; Mon, 22 Aug 2007 13:20:53 -0400 (EDT)

Received: from mta1.srv.hcvlny.cv.net (mta1.srv.hcvlny.cv.net [167.206.4.196])
by box.stevens.edu (8.12.11/8.12.11) with ESMTP id j7MHKqDa009401 for
<mmalek@stevens.edu>; Mon, 22 Aug 2007 13:20:52 -0400 (envelope-from mmalek@ieee.org)

→ **Received: from** mypc (ool-44c4a45b.dyn.optonline.net [**68.196.164.91**])
by mta1.srv.hcvlny.cv.net (Sun Java System Messaging Server 6.2-2.06 (built May 11 2007))
with SMTP id <0ILM00JVNW6RUH6O@mta1.srv.hcvlny.cv.net> for mmalek@stevens.edu; Mon, 22 Aug 2007 13:20:52 -0400 (EDT)

Date: Mon, 22 Aug 2007 13:22:44 -0400

From: Manu Malek <mmalek@ieee.org>

Subject: Test email

To: Manu Malek <mmalek@stevens.edu>

Message-id: <055701c5a73e$1ba84270$5ba4c444@yourd137mzmhow>

MIME-version: 1.0

X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

X-Mailer: Microsoft Outlook Express

Content-type: text/plain; reply-type=original; charset=iso-8859-1; …

Finding the Perpetrator

- When the sender's IP address is found, the user with that assigned IP address must be determined.
  - For an email initiated within an enterprise, check the authentication and DHCP server logs.
  - In the case of an external user, review the ISP *AAA* server logs.
- If the user used a dial-up connection to the ISP, the RADIUS session log includes the IP address assigned to a specific login during a session.
  - The ISP can then use caller ID to find the telephone number used to originate the session, and determine which login name was using that IP address.
- Once the user has been identified, the user's workstation needs to be seized and analyzed.