
Computer forensics

Aiman Al-Refaei

Computer forensics

Definitions:

Forensics - The use of science and technology to investigate and establish facts in criminal or civil courts of law.

Computer Forensics - Commonly defined as the collection, preservation, analysis and court presentation of computer-related evidence.

Computer forensics

- ❑ Proper Acquisition and Preservation of Computer Evidence.
- ❑ Authentication of Collected Data for Court Presentation.
- ❑ Recovery of All Available Data, Including delete files.

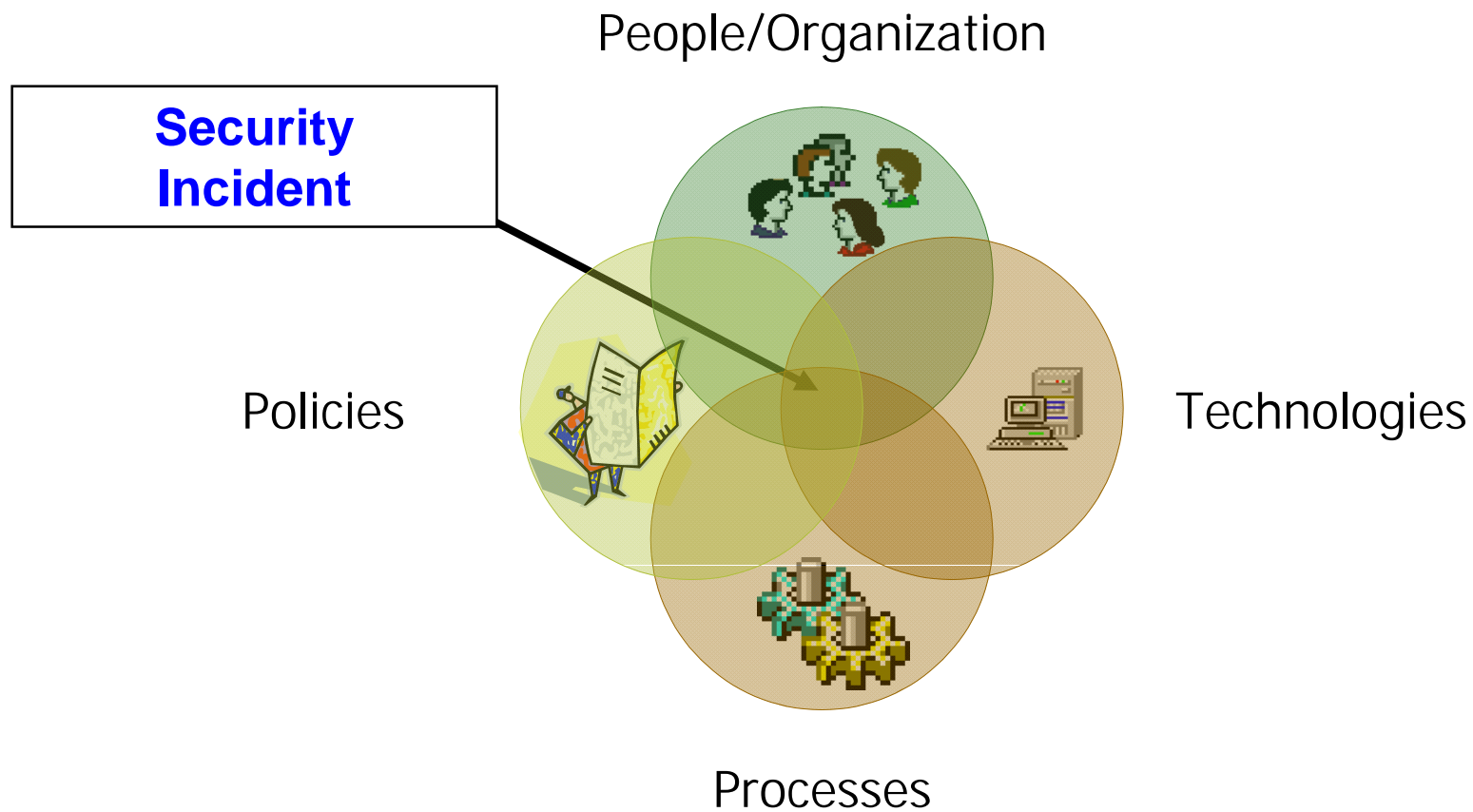
Computer Forensics scope and characteristics

- **Scope:** The collection and search of specific data that will serve as acceptable evidence in a court of law.
- Computer Forensics deals with:
 - storage media (e.g. hard disks),
 - the examination and analysis of network logs.

Incidents

- *Incident*: any security relevant *adverse event* that might threaten the security of a computer system or a network.
- An *event* must have observable and recordable characteristics:
 - The connection to a system via a network,
 - The file access,
 - System shutdown, etc.

Security Incident



Types of Incidents

- Most incidents point towards:
 - Confidentiality,
 - Integrity,
 - Availability.
- Different types of incidents:
 - Repudiation,
 - Harassment,
 - Pornography trafficking,
 - Organized crime activity,
 - Subversion.

Incident Response

- *Incident Response* is a new field with similar goals as IT Security.
- *Scope*: to negate or minimize the impact of an incident, reacting by taking certain actions.
- It can be used to restore confidentiality, integrity, and availability.
- A particular important part of the legal side of incident response is the area of *forensics*

Why is Evidence important?

- In the legal world, Evidence is *EVERYTHING*.
- Evidence is used to *establish facts*.
- The Forensic Examiner is not *biased*.
- Evidence must be:
 - Scientifically sound.
 - Legally accepted.

Types of Evidence

- **Inculpatory Evidence** – Supports a given theory
- **Exculpatory Evidence** – Contradicts a given theory
- **Evidence of Tampering** – Shows that the system was tampered with to avoid identification

Rules of Evidence

- Complete
- Authentic
- Admissible
- Reliable
- Believable

Who needs Computer Forensics?


- The Victim!
- Law Enforcement
- Insurance Carriers
- Legal System

Who are the Victims?

- Private Business
- Government
- Private Individuals




FOCUS ON THE ISSUES



e-business

{ www.FreeBorders.com is an IBM e-business. }

See why IBM was the perfect fit.



[Click Here](#)
[Click Here](#)

CNN.com

technology > **computing**

CNN.com EUROPE:

- [MAINPAGE](#)
- [EUROPE](#)
- [WORLD](#)
- [WEATHER](#)
- [BUSINESS](#)
- [SPORTS](#)
- TECHNOLOGY** <
- [ENTERTAINMENT](#)
- [IN-DEPTH](#)
- [NEWS BRIEF](#)

CNN.com:

Sections

[change default edition](#)

LOCAL LANGUAGES:

- [German](#)
- [Italian](#)
- [Swedish](#)
- [Norwegian](#)
- [Danish](#)
- [Spanish](#)
- [Portuguese](#)
- [Japanese](#)
- [Chinese Headlines](#)
- [Korean Headlines](#)

DISCUSSION:

- [message boards](#)
- [chat](#)
- [feedback](#)

Editions | [myCNN](#) | [Video](#) | [Audio](#) | [News Brief](#) | [Free E-mail](#) | [Feedback](#)

Hospital confirms copying of patient files by hacker

From...
COMPUTERWORLD
AN IDG.net SITE

December 15, 2000
Web posted at: 2:34 p.m. EST (1934 GMT)


by *Marc L. Songini*

(IDG) -- A major university hospital in Seattle Thursday confirmed that a hacker penetrated its computer network last summer and made off with files containing information about 5,000 patients.

Officials at the University of Washington Medical Center said the hacker -- who calls himself "Kane" -- stole user passwords and copied thousands of files while he had access to the hospital's systems. The hacker slipped into the network through a server in the hospital's pathology department, said medical center CIO Tom Martin.

Video on Demand

China could have space station by 2005



[Play video](#)
(QuickTime, Real or Windows Media)

Watch more [CNN VIDEO](#)

CNN.com NewsNet

CNN Sites

Search

CNN.com Europe

[Search tips](#)

TECHNOLOGY

TOP STORIES

- ['Ginger' inventor cools hype](#)
- [Hackers challenged on security](#)
- [Mobile phones: Hitting saturation point?](#)
- [Smooth sailing for Chinese spacecraft](#)

(MORE)

CNN.com. EUROPE

TOP STORIES

- [Fresh tremors shake El Salvador](#)

29.08.2006

Computer forensics

14

De viktigste nyhetene først.

CNN.no



[Click Here](#)

CNN.com technology > computing

CNN Sites

- [MAINPAGE](#)
- [WORLD](#)
- [U.S.](#)
- [WEATHER](#)
- [BUSINESS](#)
- [SPORTS](#)
- [TECHNOLOGY](#)
- [computing](#)
- [personal technology](#)
- [SPACE](#)
- [HEALTH](#)
- [ENTERTAINMENT](#)
- [POLITICS](#)
- [LAW](#)
- [CAREER](#)
- [TRAVEL](#)
- [FOOD](#)
- [ARTS & STYLE](#)
- [BOOKS](#)
- [NATURE](#)
- [IN-DEPTH](#)
- [ANALYSIS](#)
- [LOCAL](#)

EDITIONS:

- [CNN.com Europe](#)
- [change default edition](#)

[Editions](#) | [myCNN](#) | [Video](#) | [Audio](#) | [Headline News Brief](#) | [Free E-mail](#) | [Feedback](#)

Analysis: Home workers can imperil systems

From...
COMPUTERWORLD
AN IDG.net SITE

November 7, 2000
Web posted at: 9:09 a.m. EST (1409 GMT)

by Jaikumar Vijayan And Carol Sliwa

(IDG) -- The theory that hackers reached Microsoft Corp.'s product development servers via a home-based employee's computer demonstrates why it's critical for companies to ensure that their remote employees aren't stepping-stones into the corporate network, say security experts.

Attackers using a server in Russia penetrated Microsoft's corporate network in a high-profile security breach that was made public 10 days ago (see "Microsoft stung by hack attack," link below).

Meanwhile, on Friday, another hacker claimed to have penetrated the company's Web servers, and Microsoft confirmed that at least one server had been breached (see "Microsoft hit by another hacker," link below).



What are you looking for?

- Business gifts
- Travel Needs
- Home & Garden
- Electronics
- Sporting Goods
- Toys & Games
- Flowers
- Jewelry
- Cameras



CNN.com NewsNet

CNN Sites

Search

CNN.com

Find

TECHNOLOGY

TOP STORIES

['Ginger' inventor says speculation overblown](#)

[Computer security company to hackers: Bring it on](#)

[New Xbox games on the horizon](#)

[Smooth sailing for China's unmanned spacecraft](#)

[Electronic voting systems face obstacles to adoption](#)

[Group aims to make online ads more compelling](#)

(MORE)

Reasons for a Forensic Analysis

- ID the perpetrator.
- ID the method of the network that allowed the perpetrator to gain access into the system.
- Conduct a damage assessment of the victimized network.
- Preserve the Evidence for Judicial action.

Forensics Process

- Acquisition.
- Identification– Technical Analysis.
- Evaluation– What the Lawyers Do .
- Presentation.

Acquisition:

- Track or Observe a Live Intruder?
- Assess Extent of Live Intrusion?
- Preserve “Evidence” for Court?
- Close the Holes and Evict the Unwanted Guest?
- Support for Police Arrest?
- Support for Court Ordered Subpoena?

Identification:

- Physical Context: Exhibit A Seagate 4GB HD
- Logical Context: identified as /dev/hda1
mounted as / file:/etc/hosts.equiv
- Presentation/Use Context: /etc/hosts.equiv is used to control access to the system
- Opinion to support relevance of findings: a “+” was found appended to the end of this file
- Handling and labeling of objects submitted for forensic analysis is key.
- Following a documented procedure is key.

Evaluation:

- This is what lawyers (or those concerned with the case) do. Basically, determine relevance.
- Presentation of findings is key in this phase.
- Findings submitted for evaluation as evidence will not only be evaluated for validity but for “chain of custody” problems.

Presentation:

- Some findings will not be evaluated to be worthy of presentation as evidence.
- Few findings will need to withstand rigorous examination by another expert witness.
- The evaluator of evidence may be expected to defend their methods of handling the evidence being presented.
- The Chain of Custody may be challenged

Thank you