

INF3510 Information Security

University of Oslo

Spring 2010

Lecture 14

Privacy and Computer Forensics



Audun Jøsang

Outline

- Privacy
 - OECD principles
 - Legislation
 - Privacy challenges in Web 2.0
 - Privacy threats on the Internet
- Computer Forensics
 - Principles
 - Methods
 - Challenges

Origins of Privacy

- The right to be left alone
 - US Supreme Court, 1928
 - Assumed that the government was a possible threat
- Scandinavian countries introduced universal personal number, ca. 1970
- Combined with the emergence of electronic data processing
 - Possible to collect and analyze large quantities of information related to identifiable persons
 - In the interest of individuals to be protected from uncontrolled use of personal information, either by government or by private organisations

OECD Data Privacy Principles

- Sweden takes the case of privacy protection to the OECD in the 1970s.
- OECD created a set of guidelines in 1980
- Subsequent privacy legislation around the world are inspired by the OECD guidelines
 - Personregisterloven (Norway) 1978 , superseded by Personopplysningsloven, 2001
 - UK Data Protection Act, 1984
 - EU Directive, 1995 (“on the protection of individuals with regard to the processing of personal data and on the free movement of such data”)
- Only applies to living persons

1) Collection Limitation Principle

OECD 1980

- There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2) Data Quality Principle

OECD 1980

- Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3) Purpose Specification Principle

OECD 1980

- The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4) Use Limitation Principle

OECD 1980

- Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
 - a) with the consent of the data subject; or
 - b) by the authority of law.

5) Security Safeguards Principle

OECD 1980

- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6) Openness Principle

OECD 1980

- There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7) Individual Participation Principle

OECD 1980

- An individual should have the right:
 - a) to obtain confirmation of whether or not the data controller has data relating to him;
 - b) to have data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
 - c) to be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and
 - d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8) Accountability Principle

OECD 1980

- A data controller should be accountable for complying with measures which give effect to the principles stated above.

Inadequacy of the OECD Principles

- The "individual Participation Principle" assumes that personal information is stored in a structured form that is suitable for presentation to the individual.
 - This is rarely the case, and would require substantial effort by the organisation holding the data.
- Communicating personal information to the individual would require strong authentication
 - Strong authentication is costly to achieve in case there is no established business relationship between the organisation and the individual.

Changing business processes

International data transfers are now an integral part of the global economy

ca. 1980

- data transfers as discrete events, bulk transfers between identified parties, often by means of physical devices (punch-cards, tapes)
- Internet still in its infancy, with commercial uses prohibited

today

- information is the “raw material of the world economy”
- enabled globally distributed approach to tasks, 24/7, follow the sun model,
- human resources, financial services, education, e-commerce, health research, customer service
- Data moves across the corridor or around the world with the same operation and the same speed.

Privacy in Web 2.0

- Globalisation and new technologies are fundamentally changing the ways people communicate and companies handle customers.
- Web 2.0 and social online media are based on user-generated content that contain large amounts of personal information.
- The collection of data has become more ubiquitous; data mining, analytics, and behavioral targeting are becoming complex, powerful and common.
- Traditional privacy frameworks are inadequate in this environment.

Privacy in Web2.0

- Cynics/realists say privacy is a dead concept in the information age.
- The OECD and the EU have established working groups to revise the traditional privacy principles.
- In the mean time, be careful with what you communicate about yourself and others on the Internet

Attacks against privacy on the Internet



- Your computer could be watching every move you make, and report it to others without your knowledge
- Welcome to the post-privacy age!

Definitions

SPYWARE

A general term for a program that surreptitiously monitors your actions. While they are sometimes sinister, like a remote control program used by a hacker, software companies have been known to use Spyware to gather data about customers. The practice is generally frowned upon.

Definition from: BlackICE Internet Security Systems - <http://blackice.iss.net/glossary.php>

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data

Definition from: Texas State Library and Archives Commission - <http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.htm>

TROJAN HORSE

Effects of Spyware and Trojans

- Collection of data from your computer without consent
- Execution of code without consent
- Assignment of a unique code to identify you
- Collection of data pertaining to your habitual use
- Installation on your computer without your consent
- Inability to remove the software
- Performing other undesirable tasks without consent

Spyware advantages (to the user)

- Precision Marketing
 - Relevant pop-ups are better than all of them!
 - You may get some useful adverts!
- Useful Software
 - DivX Pro, IMesh, KaZaA, Winamp Pro
 - (Experienced) people understand what they are installing.
- Enhanced Website Interaction
 - Targeted banner adverts
 - Website customisation

Toolbars as spyware

The screenshot shows a Microsoft Internet Explorer browser window titled "Google Desktop: Advanced Features - Microsoft Internet Explorer". The address bar contains the URL "http://127.0.0.1:4664/setpersonalizedhome&s=vp9Nvxd5a3V4RCNLAbbWAGFxj8". The main content area displays the Google Desktop logo and a heading "Enable Advanced Features". Below this is a red warning: "Please read this carefully. It's not the usual yada yada." The text explains that using Advanced Features may send non-personal usage information to Google, such as news page visits for sidebar personalization and crash reports for performance improvement. A link to the "Privacy Policy" is provided. At the bottom, there are two buttons: "Enable Advanced Features" and "Disable Advanced Features". The status bar at the bottom shows "Done" and "Internet".

Google Desktop

Enable Advanced Features

Please read this carefully. It's not the usual yada yada.

When you use Advanced Features, you may be sending non-personal usage information and information about websites you visit to Google.

For example, Google Desktop sends Google information about the news pages you visit in order to personalize the news you see in Sidebar. We use other non-personal usage data, including crash reports, to help improve Desktop's performance. Please note that none of this data actually tells us who you are; we use it merely to improve Desktop's ability to give you the information that's most relevant to you.

To learn more about our privacy protections, read our [Privacy Policy](#).

Enable Advanced Features Disable Advanced Features

Done Internet

Disadvantages for the user

- Browsing profiles created for users without consent
 - Used for target marketing and statistical analysis
- Unable to remove Spyware programs or disable them
- Increased number of misleading / inappropriate pop-ups
- Invasion of user privacy (hidden from user)
- Often badly written programs corrupt user system
- Automatically provides unwanted “helpful” tools
- “20 million+ people have Spyware on their machines.”

Source - Dec '02 GartnerG2 Report

Spyware Defence

User Initiatives...

- **Issue Awareness**
- **Use Legitimate S/W Sources**
- **Improved Technical Ability**
- **Choice of Browser**
- **Choice of OS**
- **Legal action taken against breaches of privacy**
 - **DoubleClick**

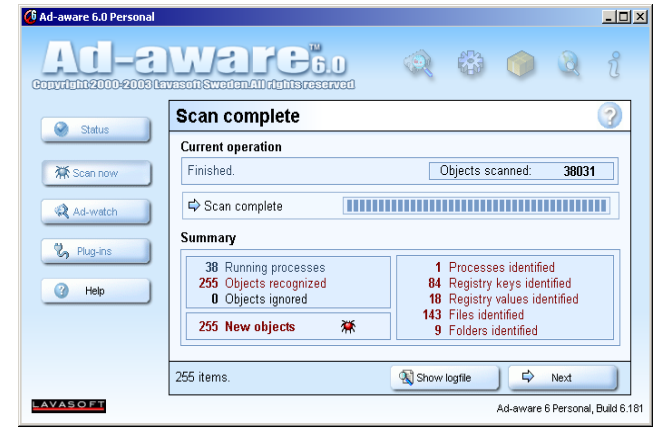
Technical Initiatives...

- **Spyware Removal Programs**
- **Pop-up Blockers**
- **Firewall Technology**
- **Disable ActiveX Controls**
 - **Not Sandboxed**
- **E-Mail Filters**
- **Download Patches**

Spyware Removers

Ad-aware (by Lavasoft)

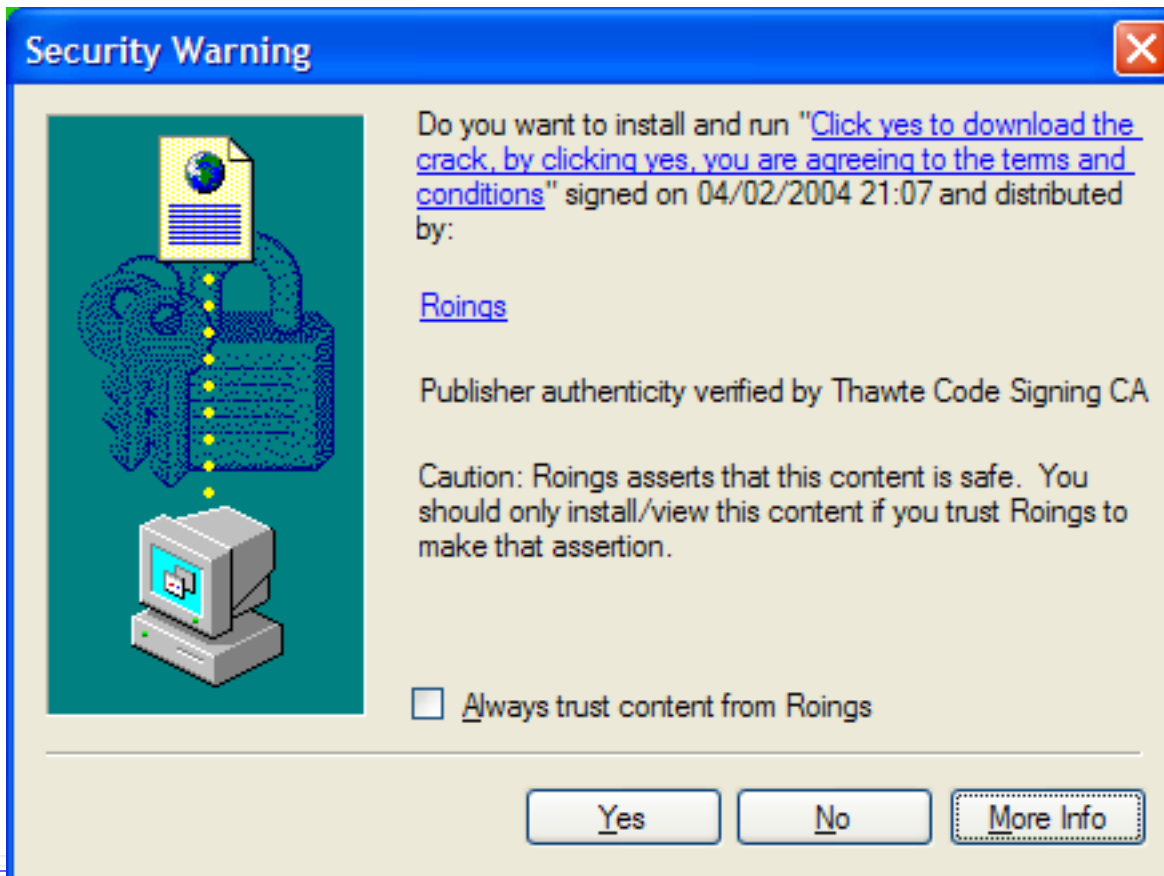
- Reverse Engineer Spyware
- Scans Memory, Registry and Hard Drive for...
 - **Data Mining components**
 - **Aggressive advertising components**
 - **Tracking components**
- Updates from Lavasoft
- Plug-ins available
 - **Extra file information**
 - **Disable Windows Messenger Service**



Trojan Infection

- Secretly installed when an infected executable is run
 - Much like a virus
 - Executables typically come from P2P networks or unscrupulous websites
- ActiveX controls on websites
 - ActiveX allows automatic installation of software from websites
 - User probably does not know what they are running
 - Misleading descriptions often given
 - Not sandboxed!
 - Digital signatures used, signing not necessary

Installation



- **Certificate Authority**
- **Misleading Certificate Description**
- **Who is trusted?**

Image Source – Screenshot of Microsoft Internet Explorer 6 security warning, prior to the installation of an ActiveX Control from "Roings".

Effects

- Allows remote access
 - To spy
 - To disrupt
 - To relay a malicious connection, so as to disguise the attacker's location (spam, hacking)
 - To access resources (i.e. bandwidth, files)
 - To launch a DDoS attack

Click-Stream

- Click-stream is the process of collecting, analyzing, and reporting data such as: order of web pages visited and mouse clicks visitors make.
- The information collected is identified by an ID number assigned to a cookie on the users computer.
- User information can remain anonymous, and not be linked to personal information unless the user agreed.
 - Breach of this principle during DoubleClicks attempt to merge with Abacus.

Case Study - DoubleClick

- Most regular web users will have a “doubleclick.net” cookie.
- Affiliated sites request the DoubleClick cookie on the users computer.
- The site then sends...
 - Who you are
 - All other information in your cookie file
- In return for...
 - All available marketing information on you - collected from other affiliated sites which the you have hit.

Case Study – DoubleClick

- Site targets banner adverts, e-mails and pop-ups to the user.
- If the user visits an affiliated site without a DoubleClick cookie, then one is sent to the user.
- The whole process is 'opaque' to the user and occurs without their consent.

DoubleClick's strategy to merge with Abacus (around 2000)

- DoubleClick's strategy was to integrate their Click-Stream database with Abacus's offline database. It could then better target internet users by knowing their buying and browser behavior.
- Websites would identify users by name.
- Click-stream information would be combined with personal information.
- Information would be collected by purchases, surveys and drawings.
- Users would have the opportunity to opt-out.
- Users could choose to receive targeted advertisements.
- No intention of selling information to 3rd parties.
- Would not ask information about medical, financial or, sexual browsing or transactions or children's browsing.
- Getting the right ad to the right person at the right time.
- Instead of target marketing the computer, they could now target the individual consumer. Since there can be many users per computer.

Abacus

- Abacus was the leader in collecting information from catalog purchases. It had a five year buying profile of 88 million households.
- Abacus collected Personal information such as:
 - Name
 - Address
 - Phone number
 - Credit card numbers
 - Income
 - Purchases history

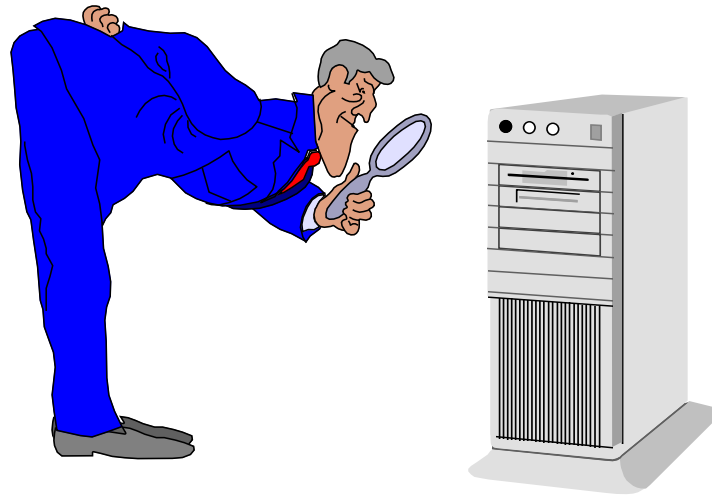
Controversy

- Because Abacus has a database with personal information, the idea of them joining with DoubleClick was a bad idea because, they specified in their contract they would not collect personal information unless the user consented.
- There was fear that DoubleClick would link the databases.
- DoubleClick canceled its plan to merge with Abacus's database. Now they had to come up with a strategy to gain public confidence back and remain in business.
- Google buys DoubleClick in 2008

Online Advertising

- The internet is free because of online advertising.
- TV, Radio and Newspapers were funded by advertising.
- We pay for free services with personal information
- Privacy Concerns
 - Because privacy policies can be changed at anytime, privacy activists became suspicious.
 - Companies can violate their policies without detection.
 - Click-stream data is invisible to users. Most people are not aware they are being tracked
 - Difficult to opt-out by disabling cookies, because it breaks functionality.
 - Consumers are tracked over and over without having a relationship with the click-stream or advertising company.

Computer Forensics



What is Computer Forensics?

- Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.
- Evidence might be required for a wide range of computer crimes and misuses
- Multiple methods of
 - Discovering data on computer system
 - Recovering deleted, encrypted, or damaged file information
 - Monitoring live activity
 - Detecting violations of corporate policy
- Information collected assists in arrests, prosecution, discovering attackers, and prevents future illegal activity

Digital Evidence

- What Constitutes Digital Evidence?
 - Any information being subject to human intervention or not, that can be extracted from a computer.
 - Must be in human-readable format or capable of being interpreted by a person with expertise in the subject.
- Computer Forensics Examples
 - Recovering thousands of deleted emails
 - Performing investigation post employment termination
 - Recovering evidence post formatting hard drive
 - Performing investigation after multiple users had taken over the system

Who Uses Computer Forensics?

- **Criminal Prosecutors**
 - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- **Civil Litigations**
 - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- **Insurance Companies**
 - Evidence discovered on computer can be used to modify costs (fraud, worker's compensation, arson, etc)
- **Private Corporations**
 - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases

Who Uses Computer Forensics? (cont)

- Law Enforcement Officials
 - Rely on computer forensics to backup search warrants and post-seizure handling
- Individual/Private Citizens
 - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment

Steps of Computer Forensics

- Computer Forensics is a four (4) step process
 - Acquisition
 - Physically or remotely obtaining possession of the computer, all network mappings from the system, and external storage devices
 - Identification
 - Identifying what data can be recovered, then electronically retrieving it by running various Computer Forensic tools and software suites
 - Evaluation
 - Evaluating the information/data recovered to determine if and how it could be used against the suspect for employment termination or prosecution in court.
 - Presentation
 - Presenting evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by United States and internal laws

Handling Evidence

- Admissibility of Evidence
 - Legal rules which determine whether potential evidence can be considered by a court
 - Must be obtained in a manner which ensures the authenticity and validity and that no tampering had taken place
- No possible evidence must have been damaged, destroyed, or otherwise compromised by the procedures used to search the computer
- Preventing viruses from being introduced to a computer during the analysis process
- Extracted / relevant evidence is properly handled and protected from later mechanical or electromagnetic damage

Handling Evidence (cont.)

- Establishing and maintaining a continuing chain of custody
- Limiting the amount of time business operations are affected
- Not divulging and respecting any ethically [and legally] client-attorney information that is inadvertently acquired during a forensic exploration

Initiating An Investigation

- DO NOT begin by exploring files on system randomly
- Establish evidence custodian - start a detailed journal with the date and time and date/information discovered
- If possible, designate equipment as “off-limits” to normal activity. This includes back-ups, remote or local house-keeping, and configuration changes
- Collect email, DNS, and other network service logs
- Capture external TCP and UDP port scans of the host
- When required, contact security personnel, national CERT, management, law enforcement, as well as affected sites or persons

Incidence Response

- Identify, designate, or become evidence custodian
- Review any existing journal of what has been done to system already and/or how intrusion was detected
- Begin new or maintain existing journal
- Install monitoring tools (sniffers, port detectors, etc.)
- Shutdown system only when appropriate
- Perform a copy of physical disk without rebooting or affecting running processes
- Capture network information, processes and files in use (e.g. dll, exe) and any config. information
- Receipt and signing of data

Handling Information

- Information and data being sought after and collected in the investigation must be properly handled
- Volatile Information
 - Network Information
 - Communication between system and the network
 - Active Processes
 - Programs and daemons currently active on the system
 - Logged-on Users
 - Users/employees currently using system
 - Open Files
 - Libraries in use; hidden files; Trojans (rootkit) loaded in system

Handling Information (cont)

- Non-Volatile Information
 - This includes information, configuration settings, system files and registry settings that are available after reboot
 - Accessed through drive mappings from system
 - This information should be investigated and reviewed from a backup copy

Computer Forensic Requirements

- Hardware
 - Familiarity with all internal and external devices/components of a computer
 - Thorough understanding of hard drives and settings
 - Understanding motherboards and the various chipsets used
 - Power connections
 - Memory
- BIOS
 - Understanding how the BIOS works
 - Familiarity with the various settings and limitations of the BIOS

Computer Forensic Requirements (cont)

- Operation Systems
 - Windows 3.1/95/98/ME/NT/2000/2003/XP/Vista/7
 - DOS
 - MacOS
 - UNIX/Linux
 - VAX/VMS
- Software
 - Familiarity with most popular software packages such as Office, Open Office, Acrobat etc.
- Forensic Tools
 - Familiarity with computer forensic techniques and the software packages that could be used

Anti-Forensics

- Software that limits and/or corrupts evidence that could be collected by an investigator
- Performs data hiding and distortion
- Exploits limitations of known and used forensic tools
- Works both on Windows and LINUX based systems
- In place prior to or post system acquisition

Evidence Processing Guidelines

- New Technologies Inc. recommends following 16 steps (<http://www.forensics-intl.com/index.html>)
 - Step 1: Shut down the computer
 - Considerations must be given to volatile information
 - Prevents remote access to machine and destruction of evidence
 - Step 2: Document the hardware configuration of the system
 - Note everything about the computer configuration prior to relocating
 - Step 3: Transport the computer system to a secure location
 - Always store equipment in locked room, never leave unattended
 - Step 4: Make bit stream backups of hard disks and other storage media
 - Step 5: Mathematically authenticate data on all storage devices
 - Must be able to prove that you did not alter any of the evidence after the computer came into your possession

Evidence Processing Guidelines (cont)

- Step 6: Document the system date and time
- Step 7: Make a list of key search words
- Step 8: Evaluate the windows swap file
- Step 9: Evaluate file slack
 - File slack is a data storage area of which most computer users are unaware; a source of significant security leakage.
- Step 10: Evaluate unallocated space (erased files)
- Step 11: Search files, file slack and unallocated space for key words
- Step 12: Document file names, dates and times
- Step 13: Identify file, program and storage anomalies
- Step 14: Evaluate program functionality
- Step 15: Document your findings
- Step 16: Retain copies of software used

Methods of Hiding Data

- To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These are media exploited using new controversial logical encodings: steganography and marking.
- **Steganography:** The art of storing information in such a way that the existence of the information is hidden.

Methods of Hiding Data (cont)

- **Steganography:** Hiding data within data
 - Information can be hidden in almost any file format.
 - File formats with more room for compression are best
 - Image files (JPEG, GIF)
 - Sound files (MP3, WAV)
 - Video files (MPG, AVI)
 - The hidden information *may* be encrypted, but not necessarily
 - Numerous software applications will do this for you:
Many are freely available online

Methods of Detecting/Recovering Data

- Steganalysis - the art of detecting and decoding hidden data
 - Hiding information within electronic media requires alterations of the media properties that may introduce some form of degradation or unusual characteristics
 - The pattern of degradation or the unusual characteristic of a specific type of steganography method is called a signature
 - Steganalysis software can be trained to look for a signature

Methods of Hiding Data (cont)

- Encryption: The problem with this is that existence of data is not hidden, instead it draws attention to itself.
 - With strong enough encryption, it doesn't matter if its existence is known
- Changing Clock
 - By setting the time different from real time, events will be recorded with wrong time stamps. Can be used falsify dating of contracts, agreements etc.

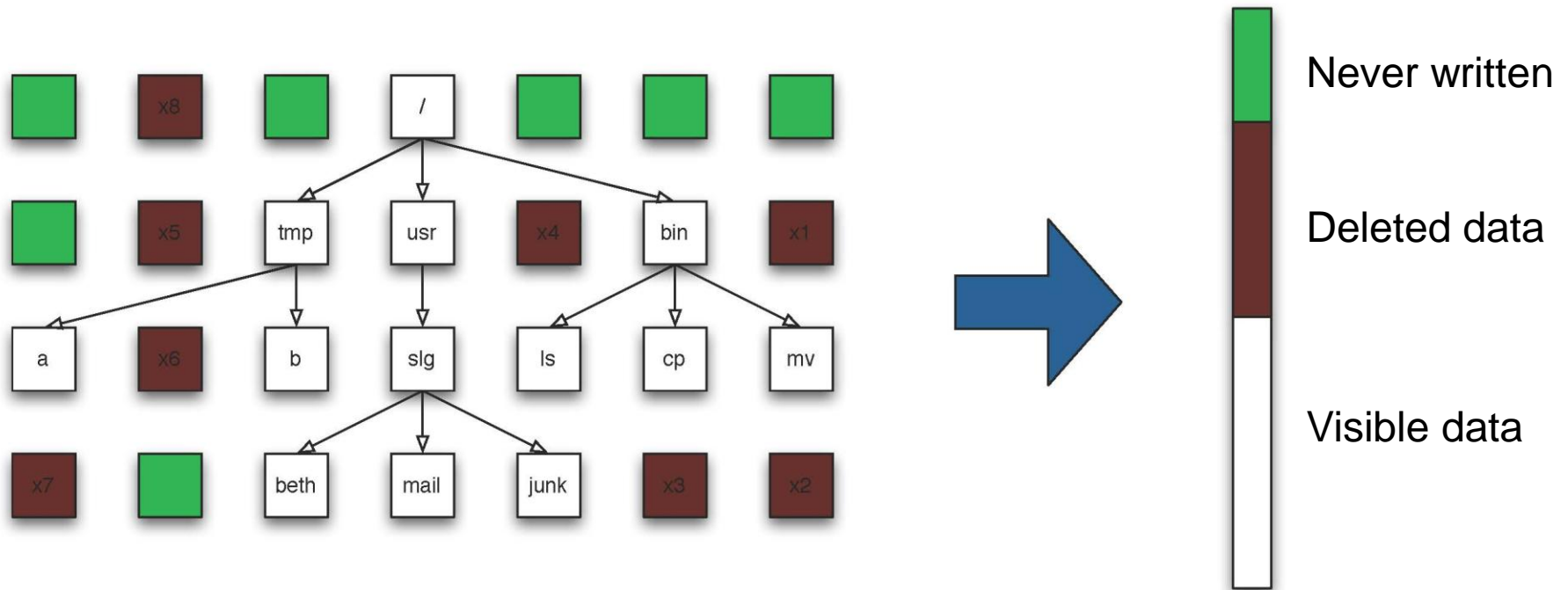
Methods of Hiding Data (cont)

- Hard Drive/File System manipulation
 - Slack Space is the space between the logical end and the physical end of file and is called the file slack
 - Slack space can be accessed directly using a hex editor.
 - This does not add any “used space” information to the drive
 - Partition waste space is the rest of the unused track which the boot sector is stored on – usually 10s, possibly 100s of sectors skipped
 - After the boot sector, the rest of the track is left empty
 - Bad sectors occur when the OS attempts to read info from a sector unsuccessfully. After a (specified) # of unsuccessful tries, it copies (if possible) the information to another sector and marks (flags) the sector as bad so it is not read from/written to again
 - users can control the flagging of bad sectors
 - Flagged sectors can be accessed directly using a hex editor

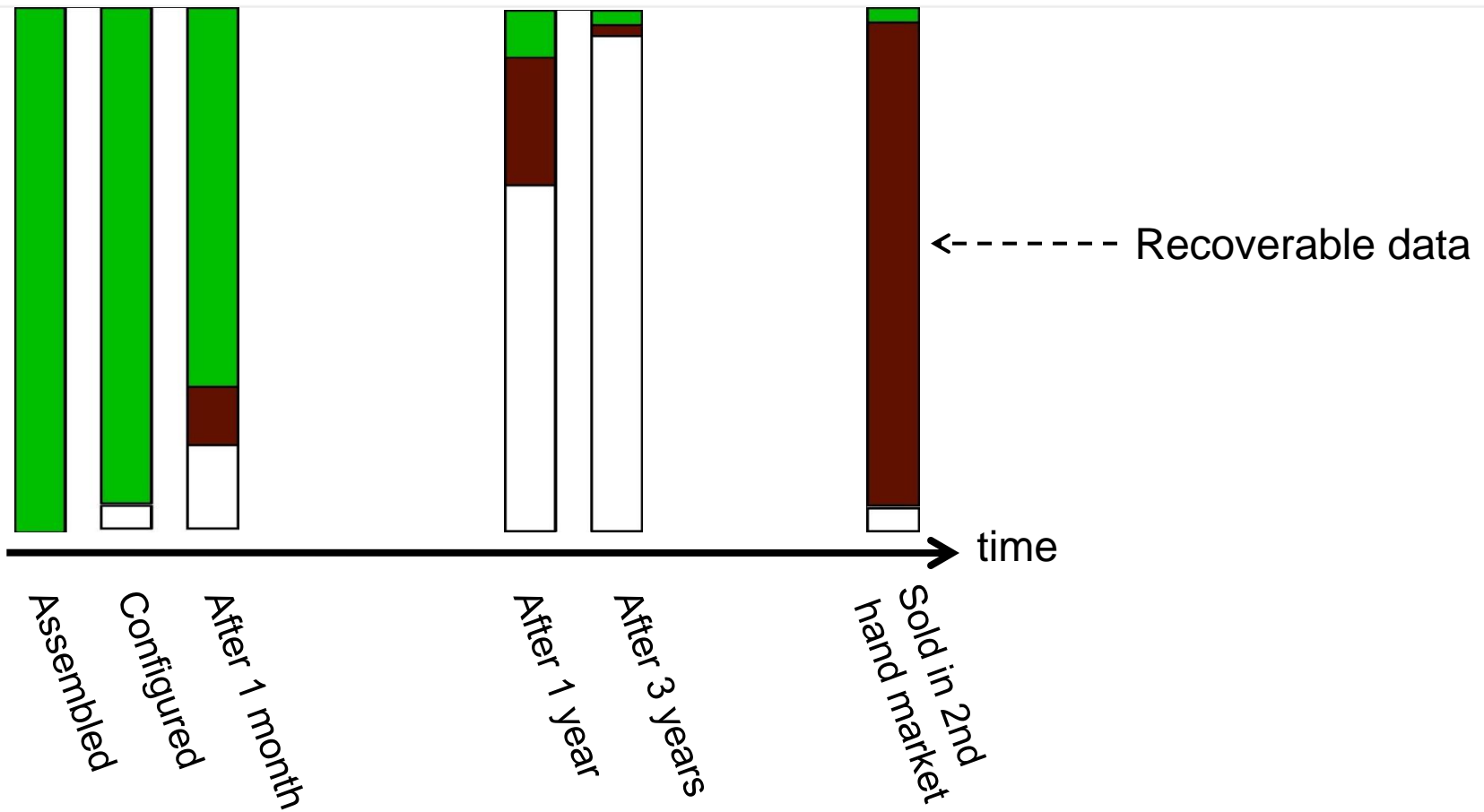
The importance of deleting data

- Data often remains on storage device when deleted
- Proper deletion requires one of the following
 - Overwriting
 - Destruction of medium
 - Destroying encryption key

The anatomy of a file system



The life of a file system











Challenges in Computer Forensics

- Forensic evidence to be accepted as legal evidence
 - must prove that there is no tampering
 - all evidence must be fully accounted for
 - computer forensic specialists must have complete knowledge of legal requirements, evidence handling and storage and documentation procedures
- Costs
 - producing electronic records & preserving them is extremely costly
- Presents the potential for exposing privileged documents
- Legal practitioners must have computer knowledge

Challenges in Computer Forensics

- Changing technology
 - Mobile phones
 - New operating systems
 - Cloud computing
 - Increasing storage capacity (how to inspect 2TB ?)
- Platforms actively managed remotely
 - File update, patching
 - Diffused accountability
- Education and training
 - Lack of skilled professionals

Questions to ask Computer Forensic Consultants

-  What are their daily, weekend, after-hours rates?
-  Do they charge for machine time?
-  Ask how many forensic cases they have worked on
-  Ask how long they have been in the forensic business
-  How many cases have they done similar to yours?
-  Ask to see their training and certifications
-  Ask them if they ever testified as an expert witness
-  Ask them for references from previous clients

End of lecture
