Security in Computing & Information Technology

Lecture 1

Introduction

Course Aims

- To introduce the concept of security
  - System management aspects
  - User aspects
- What we will study
  - Basic technical concepts
  - Basic application security
- What we will NOT study
  - Use of specific security tools
  - Hacking

Course Structure

- Lectures
  - Present security topics
  - Focus on concepts
  - Illustrations for specific platforms
- Tutorials
  - Relate to lectures
  - Discuss practical examples
- Labs
  - Provide hands-on experience with different methods
  - Use different products & tools

Assessment

- Weblearn tests
  - To (help you) monitor your progress with the material during the semester
- Assignments
  - Practical applications of concepts learned
- Final exam
  - Understanding of concepts

Path to Success

- Understand the material
  - Read your lecture notes regularly
  - Prepare for your tutorial classes
  - Do the lab exercises
  - Discuss with your friends, search on google/bing/etc whatever you need to know
- Apply your knowledge to practical tasks in the assignment
  - Assignments relate to what you may need to do in your job

Lecture Schedule

Foundations

1. Introduction
2. Vulnerabilities, Threats, Attacks

Basic mechanisms

3. Security mechanisms, Elementary cryptography
4. Authentication
5. Access control

Major computing security areas

6. Operating systems
7. Databases
8. Networks
9. Web
10. Mobile computing

Applications

11. Privacy
12. Internet banking

Lecture Topics

- Concept of security
- Adversaries
- Security services

Security

- What is it?
  - Freedom from danger or anxiety
  - Unlikely to have risks
- Protection of assets
  - Stages
    - Deterrence

      "Don't dare to mess with my system"
    - Prevention

      "You can't mess with my system"
    - Detection

      "I caught you"
    - Reaction

      "I get rid of you"

Cybersecurity and Physical Security
The Unchanging World

- Cyberspace is inhabited by people (just like the physical world)
- People interact with others, form communities, have business and social relationships
- The threats in the digital world mirror the threats in the physical world

  For example

  - Invasion of privacy (telephoto or spyware)
  - Bank robbery (armed attack or credit card fraud)

    Where there is money, there are criminals. (Organised crime prefers large-scale actions for large profit)

Cybersecurity and Physical Security
The Changing World (1)

The goals may be similar to those in the physical world, but the techniques are different

- Automation
  - Computers excel at dull, repetitive tasks
    - E.g. Salami attack: stealing fractions of cents from interest-bearing accounts
    - In the physical world the yield would be too low
  - Data can be easily collected about large segments of the population
    - Data mining: identifying people with specific attributes

Cybersecurity and Physical Security
The Changing World (2)

- Action at a distance
  - The Internet has no borders
    - Computers are accessible from almost anywhere
  - Attackers don't have to be near their prey
  - Difficult to trace down perpetrators
  - Prosecution in another jurisdiction is difficult
- Technique propagation
  - Successful techniques can easily propagate
    - E.g. worms and viruses

Security

- Security through obscurity

  Hide internal working, sensitive components, details …

  - May work in some cases
  - Computing attracts crackers
- Security through legislation

  Laws prescribe allowable user activities

  - Efficacy is limited (offender may be in another jurisdiction)
  - Good only as an additional method

    E.g. violators are prosecuted or handed over to police

Data and Information

- Data

  Represents certain aspects of our world
- Information

  Meaning (interpretation) of data
- Often there is a close relationship between them
- Sometimes they are different
  - Covert channel: data has a subliminal meaning

    E.g. the existence or absence of data carries the information, the actual value is irrelevant
  - Inference: aggregation of different data can reveal additional information

    E.g. combination of different database queries can lead to identifying a person

Information Flow

Communication channels

- Overt channels
  - Openly publicised, documented channel for authorised transfer of data
- Covert channels
  - Channel not intended for transfer of information
  - May transfer the information bit by bit – very slow
  - Often created by misusing overt channels
  - Examples
    - Timing channel

      Process modulates its own use of system resources

      E.g. Malware causing the hard drive LED to blink (experiment has shown to work up to 4 kbits/sec)
    - Storage channel

      Communicate by modifying a stored object

      E.g. File lock (open/close) channel
    - Data hiding in the OSI model

      E.g. in ICMP error packets

Information Security

- What is it?
  - Reliability
  - Trustworthiness
  - Dependability
- Goals & needs
  - Security is a need
  - Goals may override it (e.g. finish it quickly/cheaply)
- It is easier to notice the absence of security, than prove its presence
  - E.g. system failure

Data Security

- Basic aspects
  - Confidentiality

    Unauthorised users cannot <u>read</u> information
  - Integrity

    Unauthorised users cannot <u>alter</u> information
  - Availability

    Authorised users can <u>access</u> information
- The interpretation of these aspects depends on the context
- They are dictated by the needs of individuals, customs and laws of an organisation

Availability

- Reliability
  - Ability to function under normal circumstances
    - How often the system fails
    - System uptime between failures
- Resilience
  - Ability to perform in the presence of faults or other abnormal circumstances
    - How resistant is the system to failures
    - How quickly the system recovers from failures
- Performance
  - Ratio of (useful work completed) to (time and resources used)
    - Ability to cope with excessive load
    - Resistance to Denial-of-service attacks

Threats to Security

- Interference with normal operation
  - Malware
    - Viruses: attached to a host program
    - Worms: self-propagating
    - Trojans (from the city of Troy): performs hidden operations
    - Spyware: collects data in an unauthorised manner
    - Rootkit: hides the presence of malware
  - Denial of service (DoS): Blocking access to a service
    - Distributed DoS (DDoS) attacks
- Pursuing acceptable aims in an unacceptable manner
  - Nuisance
    - Spam

Types of Threats

- Different aspects of security can be targeted
  - Confidentiality

    E.g. Disclosure of medical/financial/other information
  - Integrity

    E.g. illegal transfer of funds from bank accounts
  - Availability

    E.g. Denial of Service attack
- Threats and attacks can take various forms

  Insertion (deletion) of messages (objects), exclusion of valid users, …

Adversaries (1)

- Hackers
  - Who are they: Well educated users with above average computer skills
    - White hat hacker: computer expert specialised in security testing
    - Black hat hacker (cracker): computer expert who uses his expertise for criminal activities
    - Hacktivist: utilises technology to announce a (usually ideological or political) message
  - Aim: to make a point, meet a challenge

Adversaries (2)

- Amateurs (lamers)
  - Who are they: Regular, sometimes uneducated users trying to exploit some vulnerabilities (e.g. script kiddies)
  - Aim: thrill
- Career criminals
  - Who are they: Criminals, may lack computer skills and employ corrupt hackers
  - Aim: financial gain, (industrial) espionage
  - Becoming the predominant type of computer criminals

Adversaries (3)

- Malicious insiders
- Industrial espionage
- Press
- Terrorists
- Infowarriors
- …

Computer Crime

Using the computer for criminal activities

Cybercrime: using the Internet for crime

- Theft
  - Information
  - Intellectual property
  - Identity
- Criminal conduct
  - Fraud e.g. bank fraud, extortion
  - Abuse e.g. harassment, intimidation, defamation …
  - Misuse e.g. obscene or offensive content

Achieving Security (1)

	Your home	Your computer
Have a plan	Protect doors, windows from illegal entry	Protect access (physical and electronic)
Have proper mechanisms	Locks, iron bars, etc	Protected room, access control (login, resource management)
Be in control	Lock the door/windows, mind your key	Log out / log in, don't publicize your password

Achieving Security (2)

- Policies

  Describe the aims of protection

  E.g. resources should be available to authorised users only

- Mechanisms

  Implement the policies

  E.g. users need to log in in order to use the resources

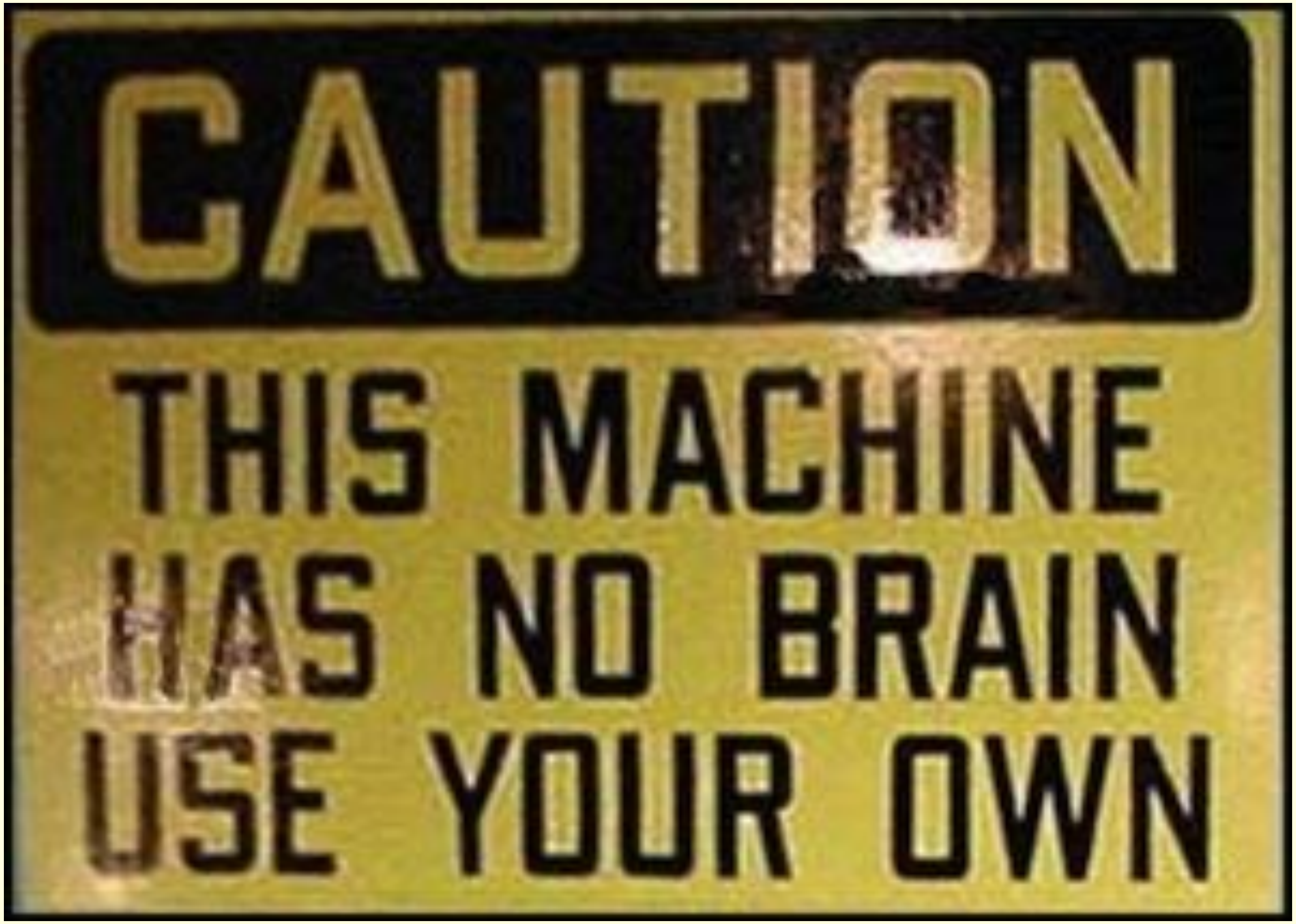
- Evaluation/assurance

  Tells the quality of protection

  E.g. Is it possible to bypass the login authentication?

Software Development

- Security should be an integral part of software development
  - Security objectives are just as important as other business objectives
  - Early consideration of security reduces remediating tasks by up to 50% (2016 State of DevOps Report)
- Steps
  - Conduct security reviews together with other reviews
  - Integrate security into the entire software lifecycle
  - Automated testing of security requirements
  - Ensure the availability of pre-approved libraries, packages, tools and processes for developers


CAUTION
THIS MACHINE
HAS NO BRAIN
USE YOUR OWN

Security Policies

- Implementation-independent statements about protecting the system
  - Restrict/prohibit certain types of activities
- Goals for security related work
- Describe the objectives
  - What needs to be protected
    - You cannot protect everything (too expensive)
  - Against what things need to be protected
    - Specific threats
    - What operations are allowed/denied
- Do not refer to actual implementation details

Security Services

- Confidentiality

  Restricts read access

- Integrity

  Restricts write access

- Privacy

  Restricts the use of legally obtained data

- Authenticity

  Verifiable source of origin

Confidentiality

- The secrecy of information is a basic concept in security
- Meaning: only authorised entities (humans or computer programs) can acquire knowledge of some data content
- It is associated with the information itself, not with the storage medium or the computer
- Example

  Medical records, student results should not be disclosed improperly

Integrity

- In many cases more important than confidentiality
- Meaning: only authorised entities (humans or computer programs) can modify some data content
- Implicit meaning: the data is correct and comes from a trustworthy source
- Example

  Bank statement should show correct transaction details

Privacy

> "It seems to me … that the advance of civilization is nothing but an exercise in the limiting of privacy" Asimov: Foundation's Edge

- Often confused with confidentiality
- Meaning: only authorised entities (humans or computer programs) can disclose legally obtained data to secondary users
- Part of it is being in control of information about oneself
- Related to
  - Accountability
    - Responsibility of one's action
    - Traceability (log of actions)
  - Non-repudiation
    - Non-deniability
- Example

  A company cannot sell your personal data without your approval

  Case in point: Tomtom sold motorists' GPS data (collected via their navigation systems) to Dutch police, who then used it for planting speed cameras

Authenticity

- The quality of being genuine, trustworthy
  - Truthfulness of origin, attributes
- Meaning: the source of a document, identity of a person, is as claimed
- Computers check authenticity in a number of ways
  - Main categories
    - Origin authentication
    - User authentication

Human Aspects

- Individual rights
  - Privacy
  - Free speech vs censorship
- Identity protection
  - Identity theft is the fastest growing crime
- Intellectual property
  - Copyright and its violation
- Personal agenda
  - Hate crime, e.g. racist attacks
  - Disgruntled (former) employee's insider attack

Summary

- Cybersecurity and everyday security both involve humans, just the tools of trade are different
- Security has different meanings in different contexts
- Security aims in a particular environment are defined in policies and implemented by mechanisms