Foundation of Computer Security

Asst. Prof. Mihai Bucicoiu

SYSTEMS LABORATORY

Computer Science
& Engineering
Department

Honor Code

"My job is to talk to you, and your job is to listen. If you finish first, please let me know."

Harry Hershfield

Lecture structure

- 10 lectures on selected topics:
  - OS Security Design
  - Hardware Security
  - Application Security
  - Forensics
  - Usable Security
  - Access Control
  - Cryptography
  - Network Security
  - Web Security
- 3 homework by Intel Romania
  - Thanks! ☺
  - Internships with Intel Romania

Last lecture: Jeopardy

Lecture information

- http://ocw.cs.pub.ro/courses/isc

What this lecture is **not** about

- Reverse engineering (go to http://ocw.cs.pub.ro/courses/cns)
- Detailed information on selected topic
- Hacking
- Security Certifications (Comptia Security+, CEH, CISSP, CISCO Security, etc.)

What this lecture is about

- An overview of what is out in the wild and how to protect against it
- A selection of tools interesting enough to be mentioned
- A focus on the academic component
- Security vocabulary

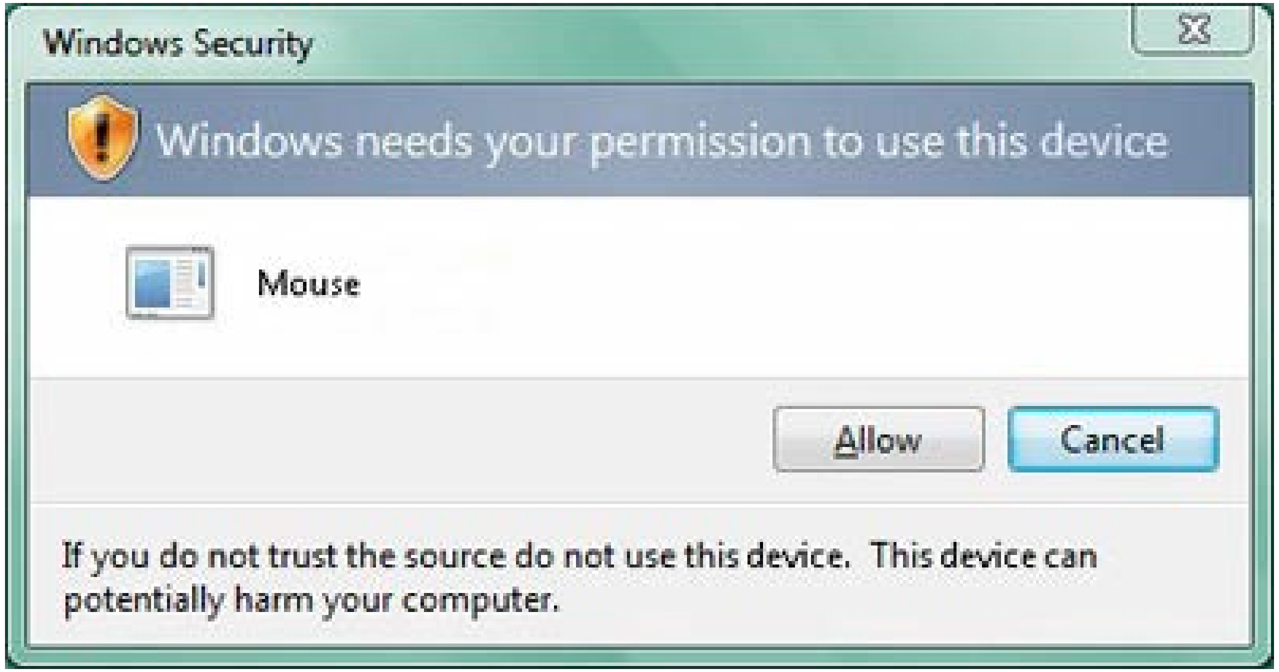
Logistics Questions?

What is security?

- Computer Security is, given an attacker’s model, the technique to control who may use or modify the computer or the information contained in it.

Security Theatre

- Bruce Schneier — measures designed to produce a feeling of security rather than the reality



Windows needs your permission to use this device

Mouse

If you do not trust the source do not use this device. This device can potentially harm your computer.

Security vs. Reality

- Don’t protect $1B with encryption that can be broken for $1M.
- Don’t spend $10M to protect $1M.
- Interesting map
  - https://cybermap.kaspersky.com/

Example - OS Security Design

- CVE-2015-7001 : Razvan Deaconescu and Mihai Bucicoiu of University POLITEHNICA of Bucharest; Luke Deshotels and William Enck of North Carolina State University; Lucas Vincenzo Davi and Ahmad-Reza Sadeghi of TU Darmstadt
- Description: An issue existed in the sandbox's handling of hard links. This issue was addressed through improved hardening of the app sandbox.

Example - Application Security

- CVE-2014-0160 (Heartbleed): (Riku, Antti and Matti) at Codenomicon and Neel Mehta of Google Security
- Description: Bug is in the OpenSSL's implementation of the TLS/DTLS (transport layer security protocols) heartbeat extension (RFC6520). When it is exploited it leads to the leak of memory contents from the server to the client and from the client to the server.

Example - Hardware Security

- Chip and Skim: cloning EMV cards with the pre-play attack *Mike Bond,* ***Omar Choudary,*** *Steven J. Murdoch, Sergei Skorobogatov, and Ross Anderson*
- Description: “We have discovered that some EMV implementers have merely used counters, timestamps or home-grown algorithms to supply this number.[…] Card cloning is the very type of fraud that EMV was supposed to prevent.”

Example - Access Control

- Description: “In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification.”

Example - Network Security

- DDOS of 300 Gbps Cyberbunker vs Spamhaus
- Description: “DNS amplification attacks “

Example - Web Security

- https://www.owasp.org/index.php/Main_Page

Example - Cryptography

Example - Cryptography

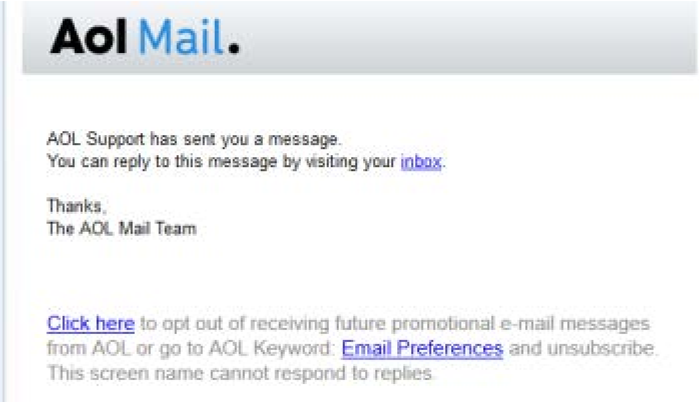
- MD5 – Developed in 1992
- Description (2004): “How to Break MD5 and Other Hash Functions” Xiaoyun Wang and Hongbo Yu
- Usage (2008): http://www.win.tue.nl/hashclash/rogue-ca/

Example - Usable Security

- Description “Usability is one of the most important and yet hardest design problems in many secure systems.” *by Ross Anderson*

- Technology writer David Pogue calculated we spend 17 man-years every day on CAPTCHAs (Scientific American, March 2012)

- Phishing
  - 1996



AOL Support has sent you a message.
You can reply to this message by visiting your inbox.

Thanks,
The AOL Mail Team

Click here to opt out of receiving future promotional e-mail messages from AOL or go to AOL Keyword: Email Preferences and unsubscribe.
This screen name cannot respond to replies.

- “Given a choice between dancing pigs and security, users will pick dancing pigs every time.” *by Edward Felten and Gary McGraw*

Dancing pigs!

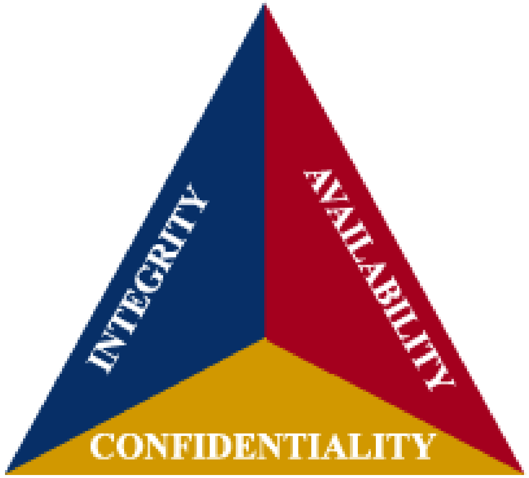
Romanian Legislation (not translated)

- Introducerea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatics […] se pedepseşte cu închisoarea de la 2 la 7 ani.
- (1) Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.
- (2) Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani.
- (3) Dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care […] accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.

Security Theatre

Security Basics

- Confidentiality
  - Prevent the disclosure of sensitive information from unauthorized people, resources, and processes
- Integrity
  - The protection of system information or processes from intentional or accidental modification
- Availability
  - The assurance that systems and data are accessible by authorized users when needed



Confidentiality

- Data protection/personal data privacy
  - fair collection and use of personal data, in Europe a set of legal requirements
- Anonymity/untraceability
  - ability to use a resource without disclosing identity/location
- Unlinkability
  - ability to use a resource multiple times without others being able to link these uses together
  - Bad examples: HTTP “cookies”
- Pseudonymity
  - anonymity with accountability for actions.
- Unobservability
  - ability to use a resource without revealing this activity to third parties
- Copy protection, information flow control
  - ability to control the use and flow of information

Integrity and Availability

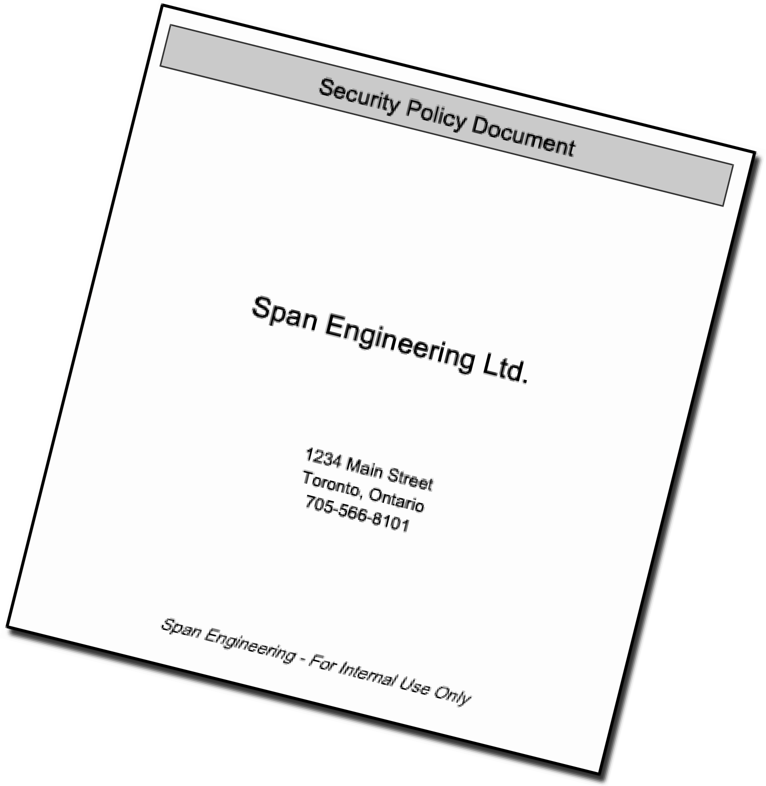
- Rollback
  - ability to return to a well-defined valid earlier state (backup, revision control, undo)
- Authenticity – verification of the claimed identity of a communication partner
- Non-repudiation – origin and/or reception of message cannot be denied in front of third party
- Audit – monitoring and recording of user-initiated events to detect and deter security violations
- Intrusion detection – automatically notifying unusual events

What is there to secure?

- Stored data
  - Personal information (employees, customers, users, etc)
  - Copyrighted software
  - Securing data must also ensure persistence
    - Data must not be lost due to attacks or lack of skill
- Transactions
  - Protect information from being tampered with
  - Make sure that the sender is who he/she claims to be
  - Make sure the receiver is the one intended
  - Data is often sent across public (insecure) networks – it can easily be intercepted
- Secure access
  - Access to computers / networks / certain privileges

Security Administration

- Policies
- Standards
- Guidelines
- Procedures
- Baselines



Security Policy Document

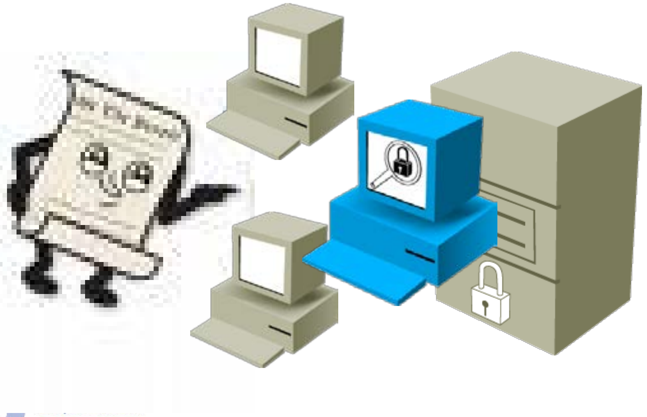
Span Engineering Ltd.

1234 Main Street
Toronto, Ontario
705-566-8101

Span Engineering - For Internal Use Only

What Is a Security Policy?

- A document that states how an organization plans to protect its tangible and intangible information assets
  - Management instructions indicating a course of action, a guiding principle, or appropriate procedure
  - High-level statements that provide guidance to workers who must make present and future decisions
  - Generalized requirements that must be written down and communicated to others



Documents Supporting Policies

- Standards – dictate specific minimum requirements in our policies
- Guidelines – suggest the best way to accomplish certain tasks
- Procedures – provide a method by which a policy is accomplished (the instructions)

Security and complexity

- Downside: Complexity brings vulnerability
    - How secure is a 1000-computer network with >1000 users and 200 different applications?
    - How secure is a simple button?
- Still, we DO need complexity to accomplish our tasks

Least privilege

- Complex systems are more difficult to secure.
- The more application deployed, the more possible vulnerabilities.

Security and humans

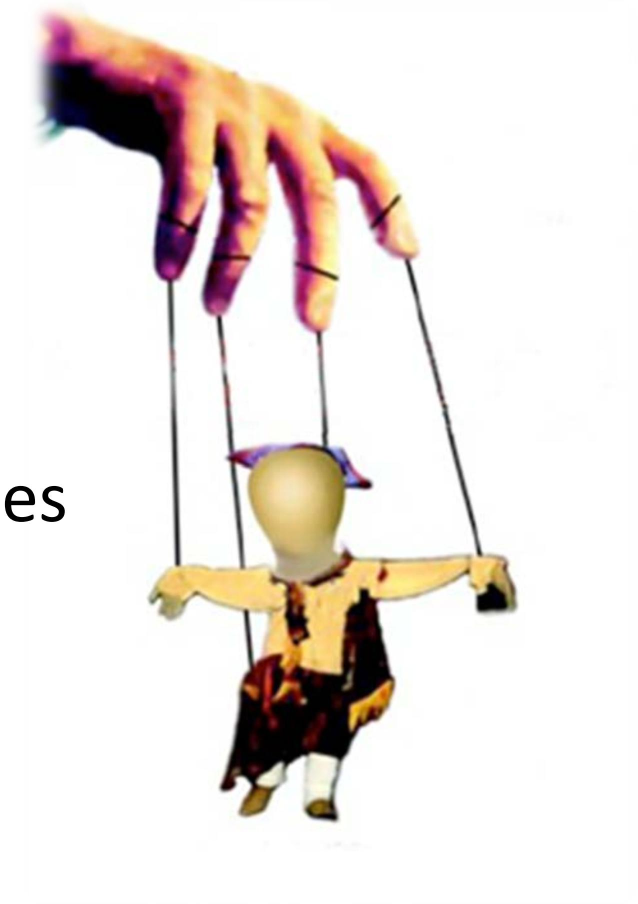
- Security policies must be in place

  …and must be followed.

- Regardless of how strong (and expensive) your secure deployment is:
  - Humans can still write their passwords on post-it notes
  - Humans can still give their passwords to anyone they trust
  - Humans can still open tempting attachments…

Social engineering

- Non-technical intrusion
- Involves tricking people to break security policies
  - Manipulation
- Relies on false confidence
  - Everyone trusts someone
  - Authority is usually trusted by default
  - Non-technical people don’t want to admit their lack of expertise
    - They ask fewer questions.
  - Most people are eager to help.
    - When the attacker poses as a fellow employee in need.



Social engineering

- People are not aware of the value of the information they posess.
- Vanity, authority, eavesdropping – they all work.
- When successful, social engineering bypasses ANY kind of security.

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

References

1. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
2. http://www.phishing.org/history-of-phishing/
3. https://www.owasp.org/images/2/25/OWASP_angela_sasse_appsec_eu_aug2013.pdf
4. http://www.criminalitate.info/2014/02/noul-cod-penal-2014-infractiuni-informatice-criminalitate-informatica.html
5. http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

References

6. http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/
7. https://www.us-cert.gov/ncas/alerts/TA13-088A