Information Security
CS 6324

Dr. Junia Valente
Outline

✧ **SECURITY GOALS**

✧ Usable Security
Security Goals: “Protect our data and systems from those who seek to misuse it”

Information security is defined as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction” ~U.S. law
Basic concepts:

To study different ways of protection, we use a framework that describes how systems may be harmed and how to counter or mitigate that harm.

**threat**: anything that has the potential to cause serious harm to a computer system.

**vulnerability**: a weakness in the system that might be exploited to cause loss or harm.

An **attack** happens when the vulnerability is exploited.

**Countermeasures**: A mechanism, action, process, or technique that removes or reduces a vulnerability.
Example: What can go wrong?

Consider smart toys that **intelligently** interact with a child.

Alice  speak  Dino  voice
reply

**Vulnerabilities** in the device threatens a child’s security (and safety & privacy)

Smart toys pose **threats** such as:
- Potential to leak information a child entrusts to their toy
- Potential to manipulate the device’s functionality
- Location tracking, etc.

**Countermeasures**: use of strong encryption, proper key management, authentication, integrity checks, etc.

Discovered vulnerabilities: **CVE-2017-8865/66/67**.
Security Goals:

- Confidentiality (prevents disclosure)
- Integrity (prevents deception / alteration)
- Availability (prevents denial of service)

Additional goals: authenticity, accountability, non-repudiation, reliability
Goal 1 – Confidentiality: Ability of a system to ensure that an asset is viewed only by authorized parties

- Concealment of information from all but those authorized
  - Privacy of customer info
  - Corporate information: payroll, strategic planning
  - Student records

- Failure of confidentiality leads to --> disclosure
  - Unauthorized party gets access to secret information
Privacy

- The ability of an individual to maintain control over the revelation of personal information, sensitive information to the individual
- Space for individual development that is safe from censure
  - Free to exercise thoughts and behaviors
  - Right to be left alone
- Note that confidentiality is similar but not the same as privacy
Goal 2 – Integrity: Ability to prevent data from being changed in an unauthorized or undesirable manner

- Guarding against improper information modification or destruction
  - Trustworthiness of data

- Failure of integrity leads to --> deception
  - Receives false information (and believes it to be true)
Authentication

- Integrity includes authenticity
- Authentication:
  - Verification of an identity
  - A set of methods we use to establish a claim of identity as being true
- Failure of authentication leads to --> impersonation
Goal 3 – Availability: Ability to access our data when we need it

- Ensuring timely and reliable access to and use of information

- Failure of availability leads to --> denial of service (DoS)
  - Prevention of authorized access to information
Computer security seeks to **prevent unauthorized viewing** (confidentiality) or **modification** (integrity) of data while **preserving access** (availability).
Outline

- Security Goals
- **Usable Security**
How can security fail?

(1) When it does not prevent the adversary from getting access into the system
   - E.g., social engineering can give the attacker access even in a hypothetical
     perfect technical security system

(2) When it gets in the way of getting things done
   - Security should minimize the intrusion to daily activities,
     but security should be as usable as possible
(1) Failing to keep the adversary out

Threat model gone wrong
How do we deal with deception?

Who looks more suspicious taking measurements at a highway?

Professor Bayen received a visit from the Police after multiple people called to report suspicious people in the highway

Best way to attack the highway? Wear an orange vest and a helmet!

(source: Alvaro Cardenas)
Trust

- Concerns related to trust:
  - How many of you opened the pdf syllabus I uploaded to course book?
  - How do you know you are going to the official webpage of a company?
  - Are Certificate Authorities trustworthy?
  - How can you be sure the website you are visiting is not serving up malware?
  - Facebook friend in need: Lost my wallet in Spain and need some cash.

- We trust a system when it performs as expected
Social Engineering:

- Recall: social engineering can give the attacker access even in a hypothetical perfect technical security system

- Why? Human factors!
  - Social engineering is a non-technical intrusion that relies on human interaction & often involves tricking people into breaking normal security procedures.

Social engineering attacks rely on people's willingness to be helpful. An attacker may pose as a co-worker or a friend in need of urgent help.
Social Engineering:
Attack Methods

- Phone: Pretexting
- Emails: “Please enter your information”
- Social Networks: Friend in need
- Dumpster Diving: Get info from trash (that could be used to carry out an attack)
- USB Drives: Install malware
Pretexting: practice of presenting oneself as someone else to obtain private information

- Someone calls pretending to be a court official
- Says you are selected for jury duty
  - Demands SSN and DOB
    - Applies for Credit Card in your name!
- If you deny this info
  - There are threats of arrest and imprisonment
Pretexting: practice of presenting oneself as someone else to obtain private information

- Example of pretexting to medical privacy: A typical private eye may pretend to be a doctor involved in the emergency care of a patient

- Training experiment at a healthcare organization:
  - Do not discuss medical records unless you initiated the call
  - Call to a number you obtain from a trusted site, not one you get from caller
  - After training staff, they detected 30 false-pretext calls a week!

- How was detected? The phone number the “attacker” gave did not match the phone number of the hospital he claimed to work.
Phishing:

- RSA Security LLC got hacked like this in 2011!

Attackers sent two different targeted phishing e-mails to four workers at its parent company EMC. The e-mails contained a malicious attachment that was identified in the subject line as “2011 Recruitment plan.xls.”
Phishing:

Amazon Refund Notification

Due to a system error you were double charged for your last order. A refund process was initiated but could not be completed due to errors in your billing information.

REF CODE: 2550CGE

You are required to provide us a valid billing address.

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days.

We hope to see you again soon.

Amazon.com
Email ID: [redacted]

IRST: You are eligible for refund

Hello [redacted],

After the last annual calculations of your fiscal activity we have determined that you are eligible for tax refund under section 501(c)(17) of the Internal Revenue Code.

Please submit the Tax Refund Request Form and allow us 3-9 days to process it.

Yours faithfully,
Internal Revenue Service
United States Department of the Treasury
Crying Wolf Phenomenon:

Microsoft was training people to click “OK” to get things done.
Operational Security:

It is not enough for rules to exist, you have to train staff who have access to confidential material and explain reasons behind rules.

Problem, how to scale to global population (e.g., phishing)?

We have to design usable security!
"We recognize the value of online banking—it’s quick, convenient, and available any time you need it.

Unfortunately, though, the threats posed by malware and identity theft are very real and all too common nowadays.

That’s why, when you’re finished with your online banking session, we recommend three simple steps to protect your personal information: (1) log out of your account, (2) close your web browser, and (3) then charter a seafaring vessel to take you 30 miles out into the open ocean and throw your computer overboard."

**CAPTCHAs:** People have tried to design protection mechanisms that use the brain's strengths rather than its weaknesses.

Appeared in 2003 with the goal to stop spammers from using scripts to automatically open thousands of accounts on free email services.

**Completely Automated Public Turing Test to Tell Computer and Humans Apart**

- Design Principles: Something believed to be hard for a computer to solve
- But “easy” for humans to solve
Problem: they get in the way!
Easy Way to Solve CAPTCHAs

- “Data processing workers”
- Earn over ten times more solving CAPTCHAs than through legitimate data processing jobs
Usability is one of the most important and yet hardest design problems in many secure systems.

It was long neglected as having less techie glamour than cryptographic algorithms; yet most real attacks nowadays target the user.