

# **Computer and Network Security**

**Lin CHEN**

**Fall 2020**

# Personnel

---

- Instructor

- CHEN Lin (陈林)
- Office hours: Tuesday and Friday 10-11h or by appointment
- Email: [chenlin69@mail.sysu.edu.cn](mailto:chenlin69@mail.sysu.edu.cn)

- TA

# Objectives

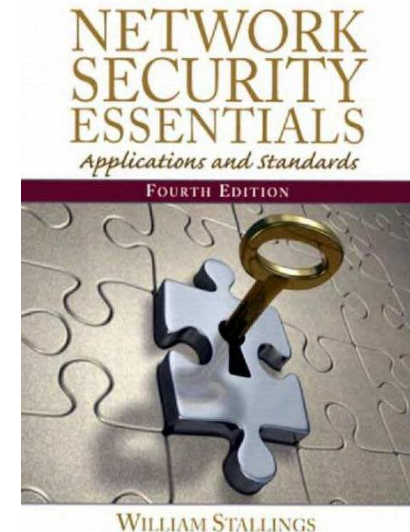
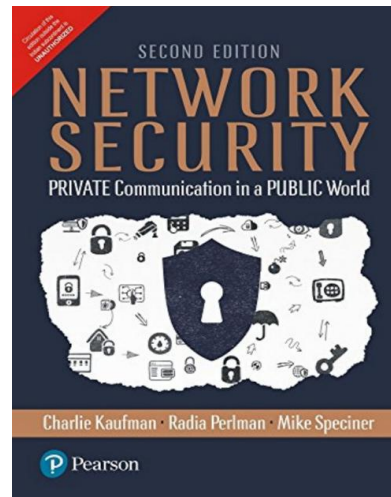
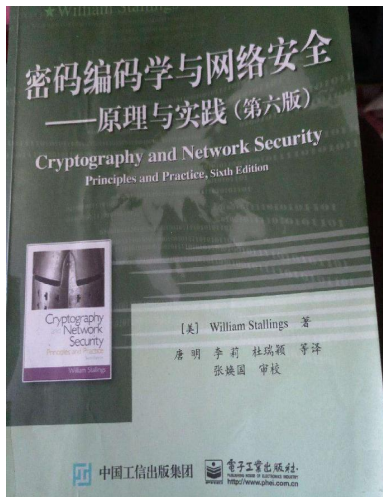
---

- Understand basic security concepts, principles, and algorithms
  - Cryptography
  - Authentication
  - Access control
  - Classic security protocols
- Be able to choose appropriate security mechanisms to protect computers and networks

# Textbook

---

- No official textbook
- Recommended classic books in security
  - Cryptography and Network Security Principles and Practice
    - by William Stallings
  - Network Security: Private Communication in a Public World
    - by Charlie Kaufman, Radia Perlman, and Mike Speciner
  - Network Security Essentials: applications and Standards
    - by William Stallings



# Grading

---

- Homework: 50%
- Mini-project: 50%
- Please respect deadlines

# Why security is an issue?

---

- Result CSI/FBI Computer crime and security survey
  - 90% users: security incidents
  - 80%: financial loss
  - 44%: can estimate loss
  - Most important loss: proprietary info., financial fraud
  
- A real problem
  - An unpatched PC survives less than 16 min
  - 61% of PCs in E.-U. infected by spy-ware
  - Annual loss: \$100+ billion

# Attacks

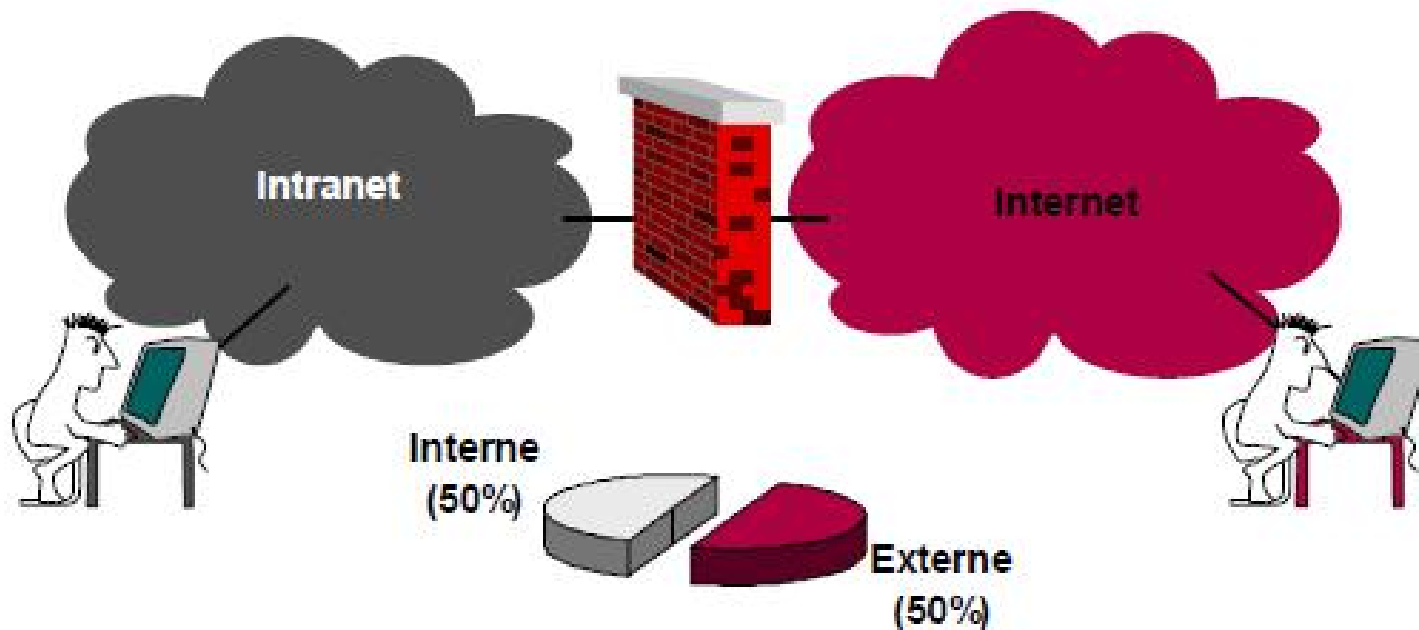
---

- Who are the attackers
  - Hackers, malicious insiders, spies, terrorists, press... Can be anyone!
  - White hat, gray hat, black hat, script kiddy
- Why do they attack
  - Financial motivation
  - Religious/political motivation
  - Industrial espionage
- Whom do they attack
  - Banks, governments, web sites, universities
- How do they attack
  - Network attacks
  - Exploit vulnerabilities in applications and security mechanisms
  - Physical access

# What is the source of a vulnerability?

---

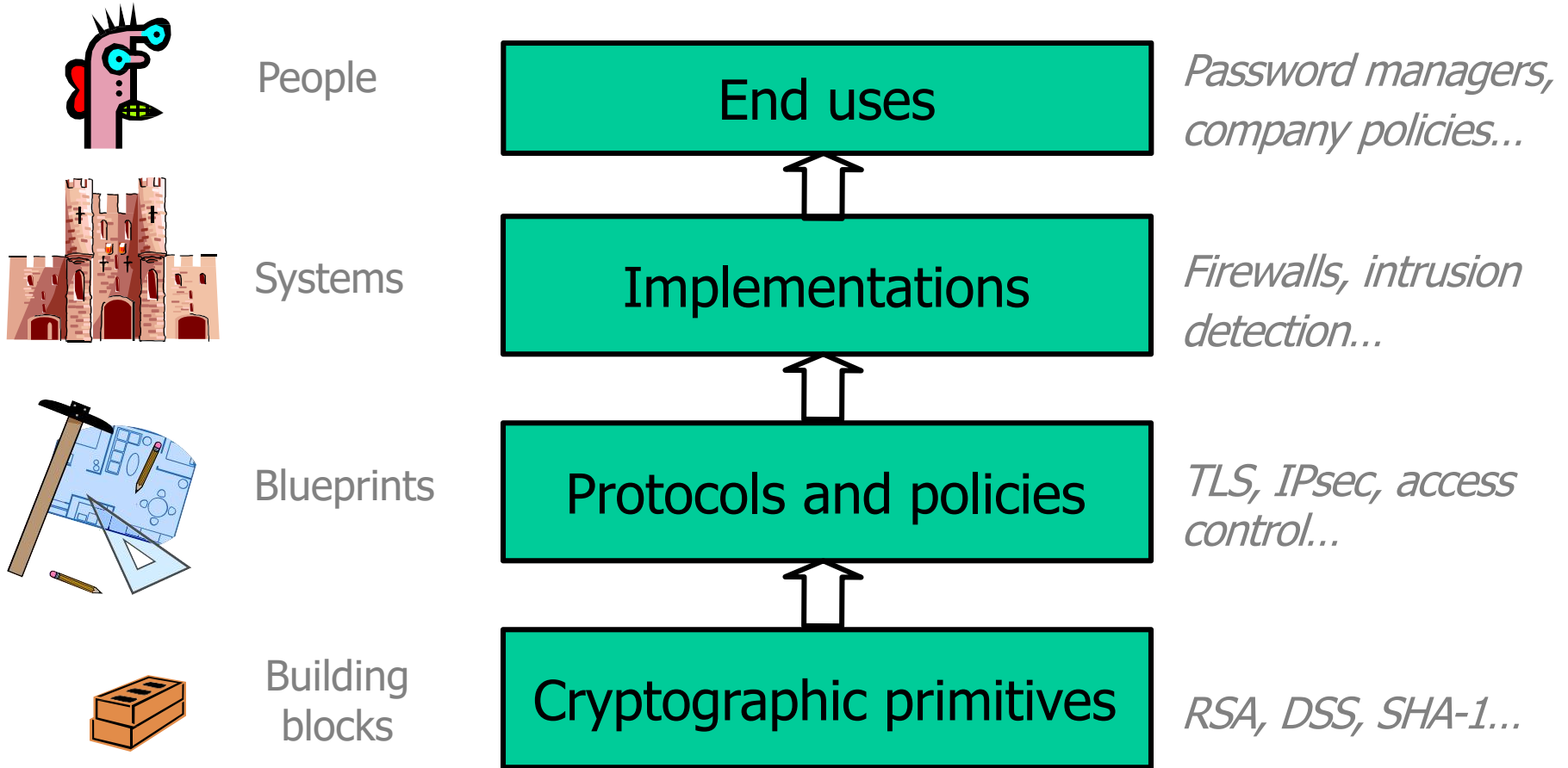
- Bad software/hardware
- Bad design
- Bad policy/configuration
- System misuse
- Unintended purpose or environment





# System defenses

---

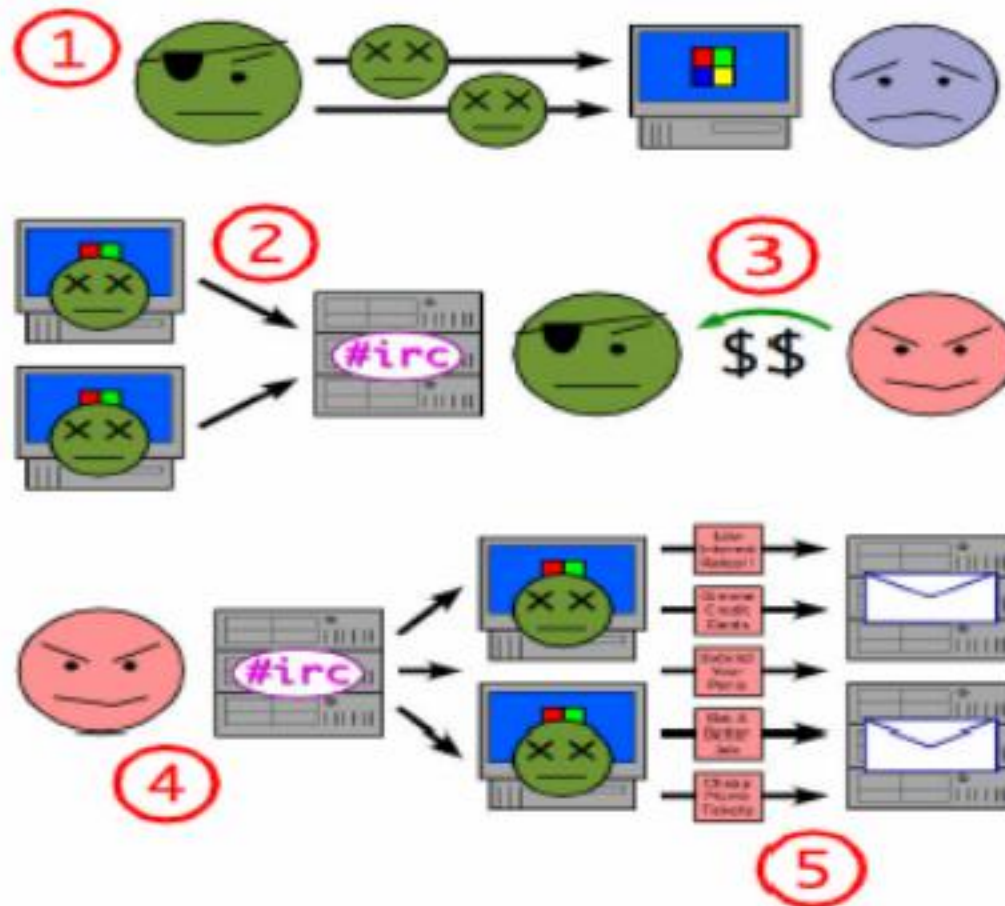


All defense mechanisms must work correctly and securely

Some examples of attacks

# Botnet

- Dated back to the first Internet relay chat system (~1990)
- Bot-net: a network of machines controlled by a botmaster



# Botnet

---

- 25% machines infected
  - >400 millions machines
  
- A botnet can be used to
  - Send spams
  - Steal information, e.g., via a keylogger
  - Install spy-wares
  - Paralyse a network by DoS attack
  - .....
  
- Jeanson James Ancheta, condemned 57 months in prison due to a botnet of ~400 000 machines in 2006

# An example of botnet

September 6th, 2007

## Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

**Categories:** [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code](#), [Firefox.....](#)

**Tags:** [Operation](#), [Supercomputer](#), [Malware](#), [Worm](#), [Ryan Naraine](#)



**150** TalkBacks

ADD YOUR OPINION



SHARE



PRINT



E-MAIL



**+97**

WORTHWHILE?

115 VOTES



Nearly nine months after it was first discovered, the [Storm Worm](#) Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

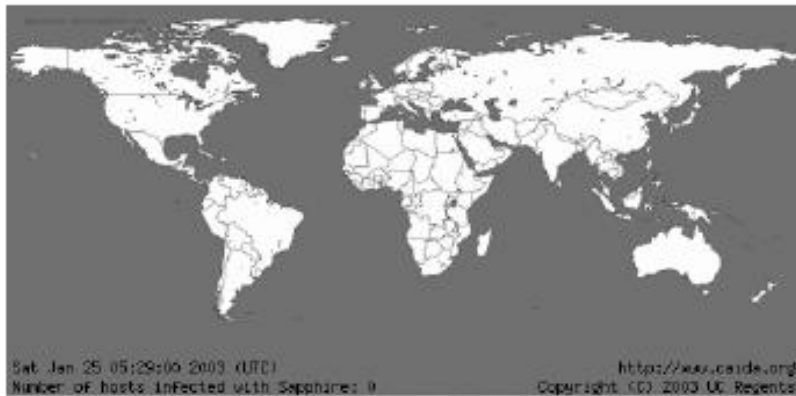
The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

to rival the world's top 10 supercomputers

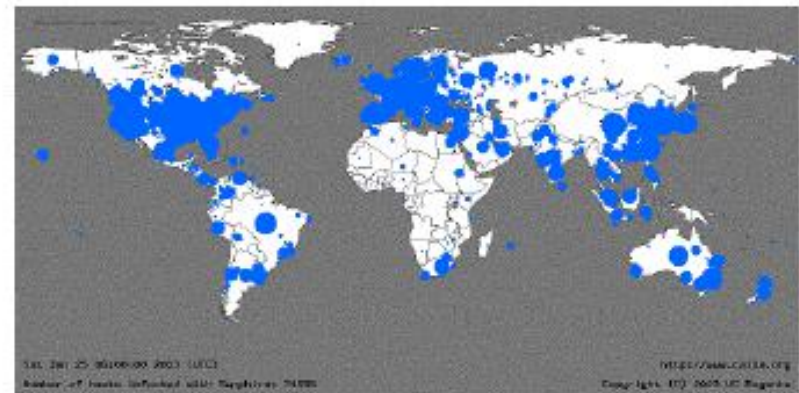
# Worm

- A program that can replicate itself to spread in the networks
  - E.g., via Outlook address book

25 janvier 2003, 05:29 0 victime



25 janvier 2003, 06:00 74 855 victimes



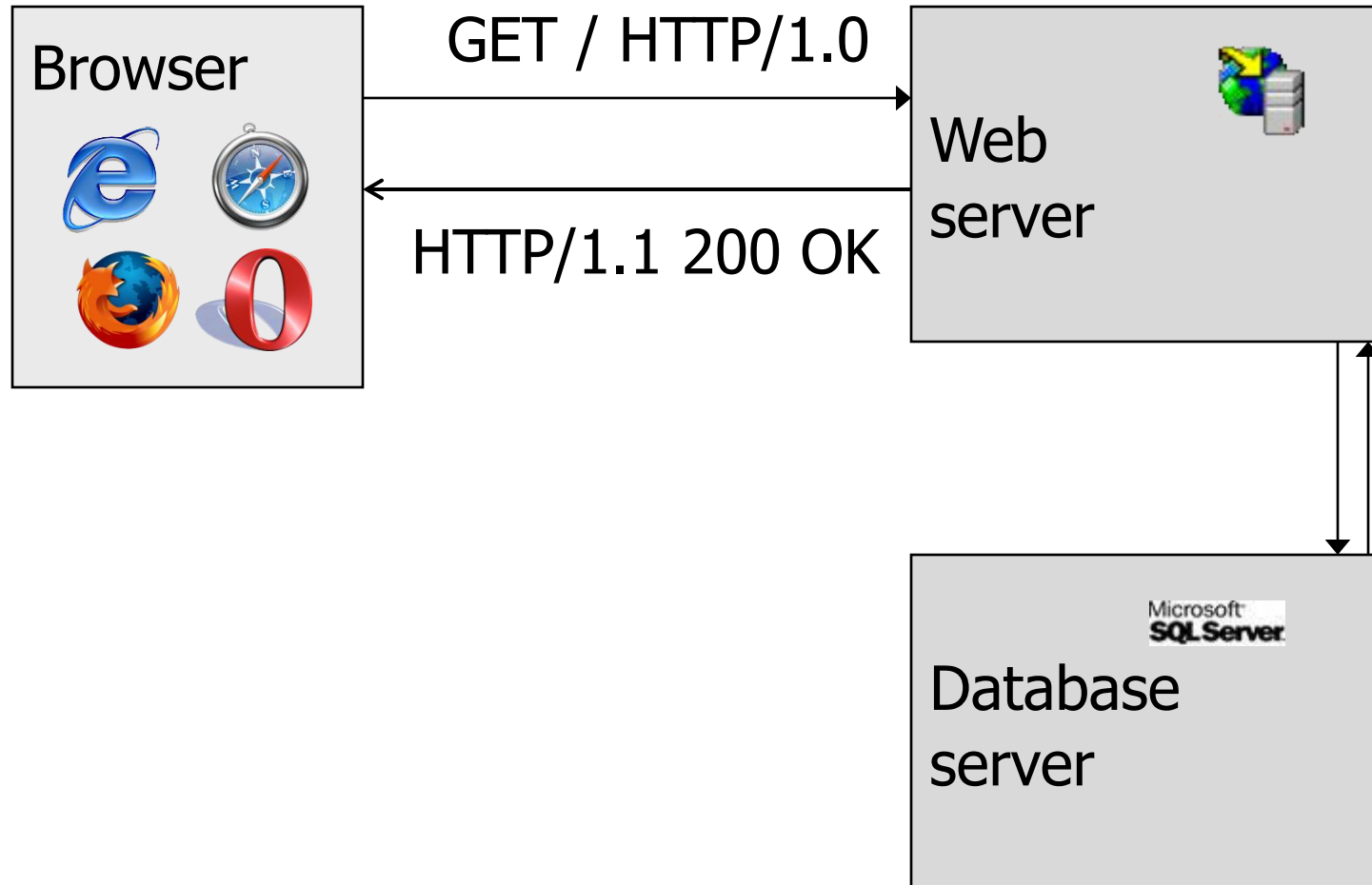
# Worm

---

- Out of service
  - 13000 bancomats of Bank of America
  - Microsoft XP activation servers
  - 300000 Internet users in Portugal (Netcabo)
  - Firemen IT system in Seattle
  - Air ticket booking and embarkment systems of the airport of Houston

# SQL injection

---





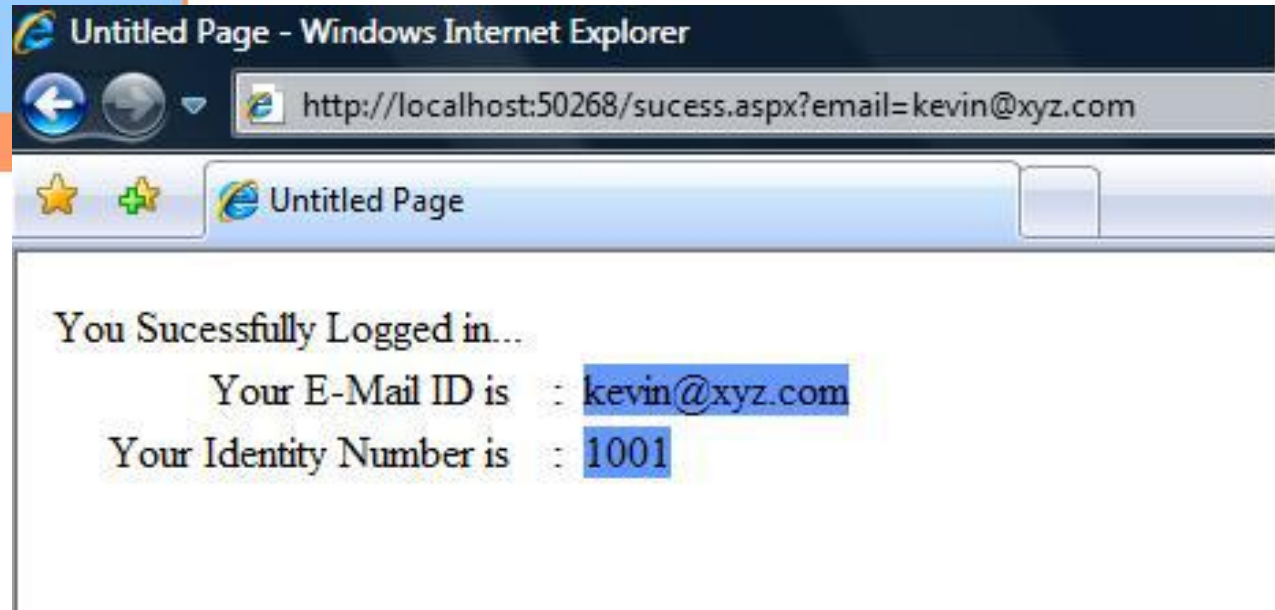
# SQL injection

---



# SQL injection

---



# Phishing

---

- PHreaking+fISHING
  - A social engineering attack to steal user data
- Attacker
  - masquerades as a trusted entity
  - dupes victim into opening emails, message, clicking addresses
- Addresses collected randomly but massively
  - The victim may receive an email from e.g., from his bank

# Phishing

---

**Dear valued PayPal® member:**

Due to concerns, for the safety and integrity of the Paypal account we have issued this warning message.

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before **Oct 04, 2015**.

**Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.**

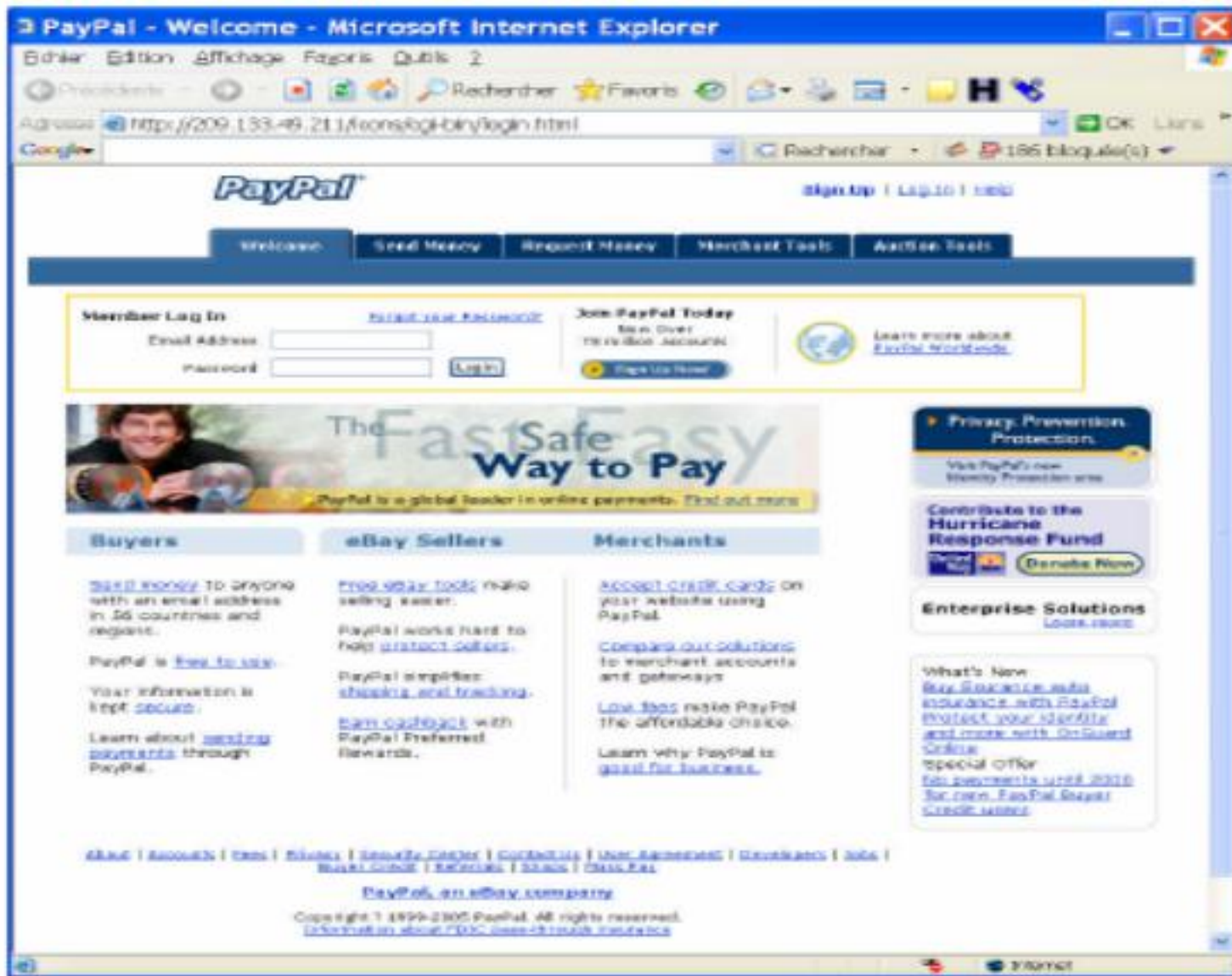
**To update your PayPal® records click on the following link:**

**[http://www.paypal.com/cgi-bin/webscr?cmd=\\_login-run](http://www.paypal.com/cgi-bin/webscr?cmd=_login-run)**

**Thank You.**

**PayPal® UPDATE TEAM**

# Phishing



# Cyberwar, cyberterrorism

## Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

ian Traynor in Brussels  
The Guardian, Thursday 17 May 2007  
Article history

August 11th, 2008

## Coordinated Russia vs Georgia cyber attack in progress

Posted by Dancho Danchev @ 4:23 pm

**Categories:** [Black Hat](#), [Botnets](#), [Denial of Service \(DoS\)](#), [Governments](#), [Hackers...](#)

**Tags:** [Security](#), [Cyber Warfare](#), [DDoS](#), [Georgia](#), [South Ossetia...](#)



Bronze Soldier, the Soviet war memorial removed from Tallinn  
Nisametdinov/AP

 **62 TalkBacks**
 **SHARE**
 **PRINT**
 **E-MAIL**
 **WORTHWHILE?**
 **24 VOTES**

In the wake of the [Russian-Georgian conflict](#), a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with [Georgia's Ministry of Foreign Affairs](#) undertaking a desperate step in order to disseminate real-time

Year	Model	Price	MPG (City)	MPG (Highway)	MPG (Combined)
1999	Alfa Romeo 156	18000	24	34	28
1999	Audi A8	45000	21	30	25
1999	BMW 5 Series	35000	21	30	25
1999	Mercedes-Benz S-Class	55000	21	30	25
1999	Volvo S80	30000	21	30	25
2000	Alfa Romeo 156	18000	24	34	28
2000	Audi A8	45000	21	30	25
2000	BMW 5 Series	35000	21	30	25
2000	Mercedes-Benz S-Class	55000	21	30	25
2000	Volvo S80	30000	21	30	25
2001	Alfa Romeo 156	18000	24	34	28
2001	Audi A8	45000	21	30	25
2001	BMW 5 Series	35000	21	30	25
2001	Mercedes-Benz S-Class	55000	21	30	25
2001	Volvo S80	30000	21	30	25
2002	Alfa Romeo 156	18000	24	34	28
2002	Audi A8	45000	21	30	25
2002	BMW 5 Series	35000	21	30	25
2002	Mercedes-Benz S-Class	55000	21	30	25
2002	Volvo S80	30000	21	30	25
2003	Alfa Romeo 156	18000	24	34	28
2003	Audi A8	45000	21	30	25
2003	BMW 5 Series	35000	21	30	25
2003	Mercedes-Benz S-Class	55000	21	30	25
2003	Volvo S80	30000	21	30	25
2004	Alfa Romeo 156	18000	24	34	28
2004	Audi A8	45000	21	30	25
2004	BMW 5 Series	35000	21	30	25
2004	Mercedes-Benz S-Class	55000	21	30	25
2004	Volvo S80	30000	21	30	25
2005	Alfa Romeo 156	18000	24	34	28
2005	Audi A8	45000	21	30	25
2005	BMW 5 Series	35000	21	30	25
2005	Mercedes-Benz S-Class	55000	21	30	25
2005	Volvo S80	30000	21	30	25
2006	Alfa Romeo 156	18000	24	34	28
2006	Audi A8	45000	21	30	25
2006	BMW 5 Series	35000	21	30	25
2006	Mercedes-Benz S-Class	55000	21	30	25
2006	Volvo S80	30000	21	30	25
2007	Alfa Romeo 156	18000	24	34	28
2007	Audi A8	45000	21	30	25
2007	BMW 5 Series	35000	21	30	25
2007	Mercedes-Benz S-Class	55000	21	30	25
2007	Volvo S80	30000	21	30	25
2008	Alfa Romeo 156	18000	24	34	28
2008	Audi A8	45000	21	30	25
2008	BMW 5 Series	35000	21	30	25
2008	Mercedes-Benz S-Class	55000	21	30	25
2008	Volvo S80	30000	21	30	25
2009	Alfa Romeo 156	18000	24	34	28
2009	Audi A8	45000	21	30	25
2009	BMW 5 Series	35000	21	30	25
2009	Mercedes-Benz S-Class	55000	21	30	25
2009	Volvo S80	30000	21	30	25
2010	Alfa Romeo 156	18000	24	34	28
2010	Audi A8	45000	21	30	25
2010	BMW 5 Series	35000	21	30	25
2010	Mercedes-Benz S-Class	55000	21	30	25
2010	Volvo S80	30000	21	30	25
2011	Alfa Romeo 156	18000	24	34	28
2011	Audi A8	45000	21	30	25
2011	BMW 5 Series	35000	21	30	25
2011	Mercedes-Benz S-Class	55000	21	30	25

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.



## U.S. cyber counterattack: Bomb 'em one way or the other

**National Cyber Response Coordination Group establishing proper response to cyberattacks**

*By [Ellen Messmer](#), Network World, 02/08/07*

San Francisco — If the United States found itself under a major cyberattack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source.

What is security?

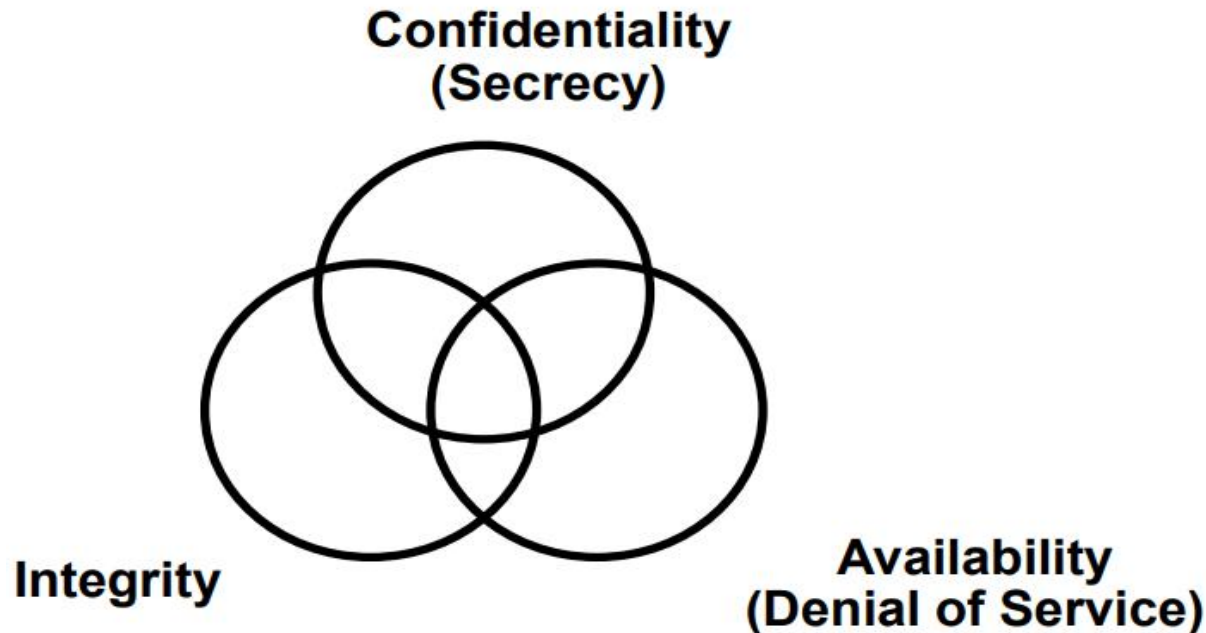


# What is security?

---

- Definition in NIST Computer Security Handbook :

*the protection afforded to an automated information system in order to attain the applicable objectives of **preserving the integrity, availability and confidentiality** of information system resources.*



# Security objectives (CIA)

---

- Confidentiality
  - Prevent/detect improper disclosure of information
- Integrity
  - Prevent/detect improper modification of information
- Availability
  - Prevent/detect improper denial of services
  
- In one phrase
  - Prevent/detect any improper action

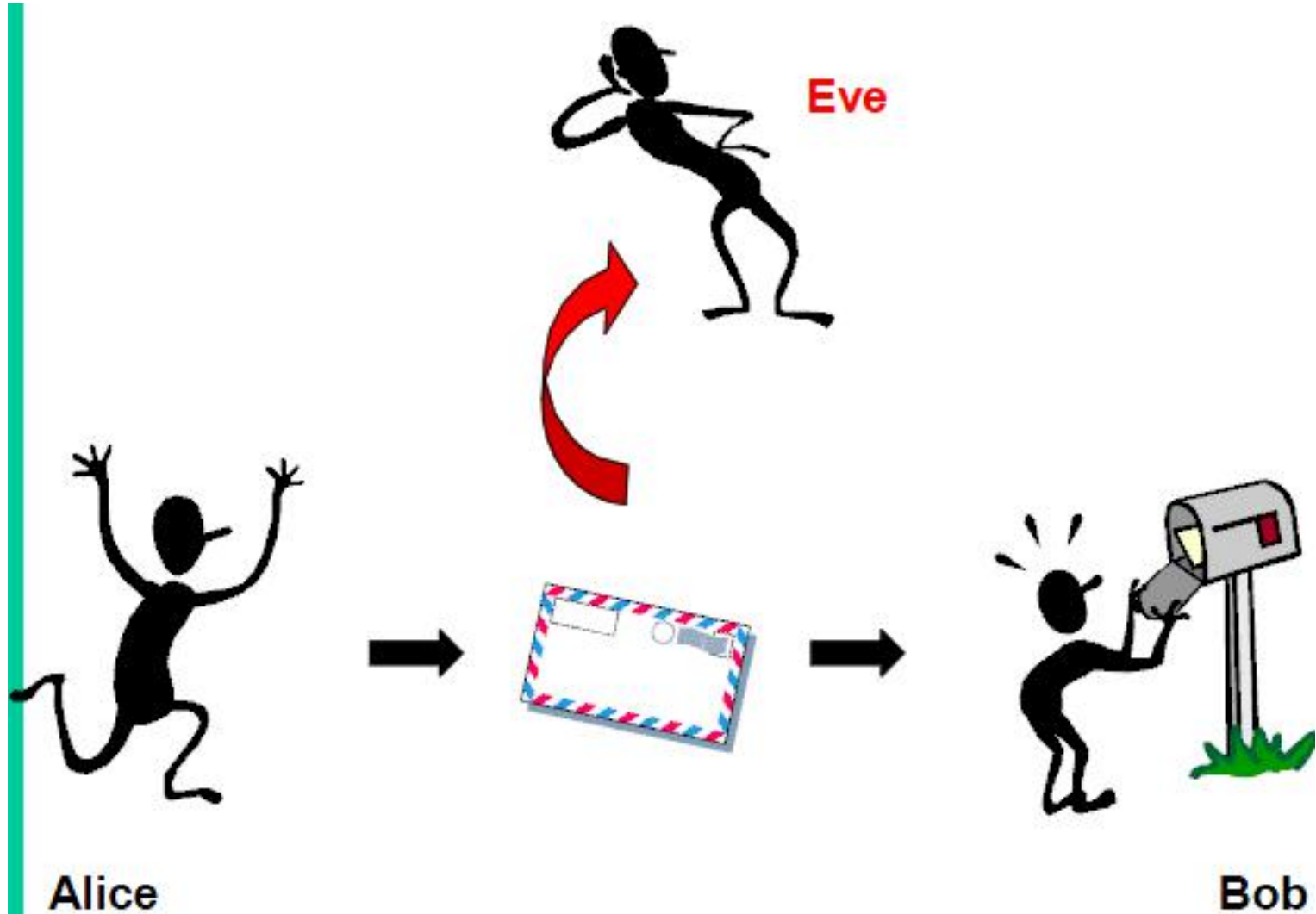
# Confidentiality

---

- Prevent/detect improper disclosure of information
- Information is accessible only by authorised entity
- Types of access: read, print, existence
- Examples: confidentiality of text, an image, an information flow
- The most understood property

# Confidentiality

---



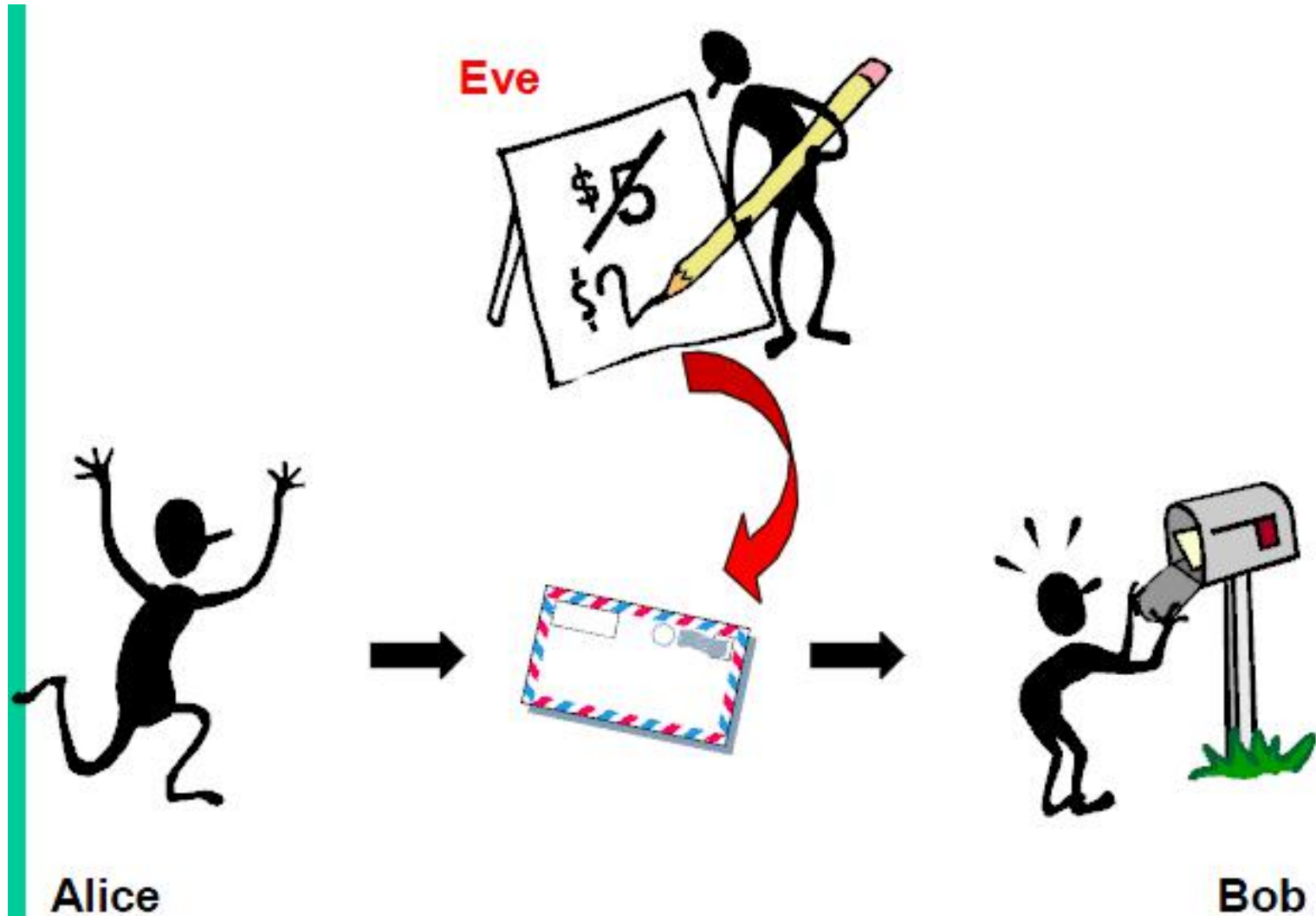
# Integrity

---

- Prevent/detect improper modification of information
  - Sometimes more important than confidentiality
- Information is modified only by authorised entity
- Types of access: write, create, delete, change status
  
- Data integrity
- System integrity
  
- Examples: integrity of a conversation, a program
  
- Attacks on integrity: falsification of a document, add a virus, manipulation of a video sequence, illicite write

# Integrity

---



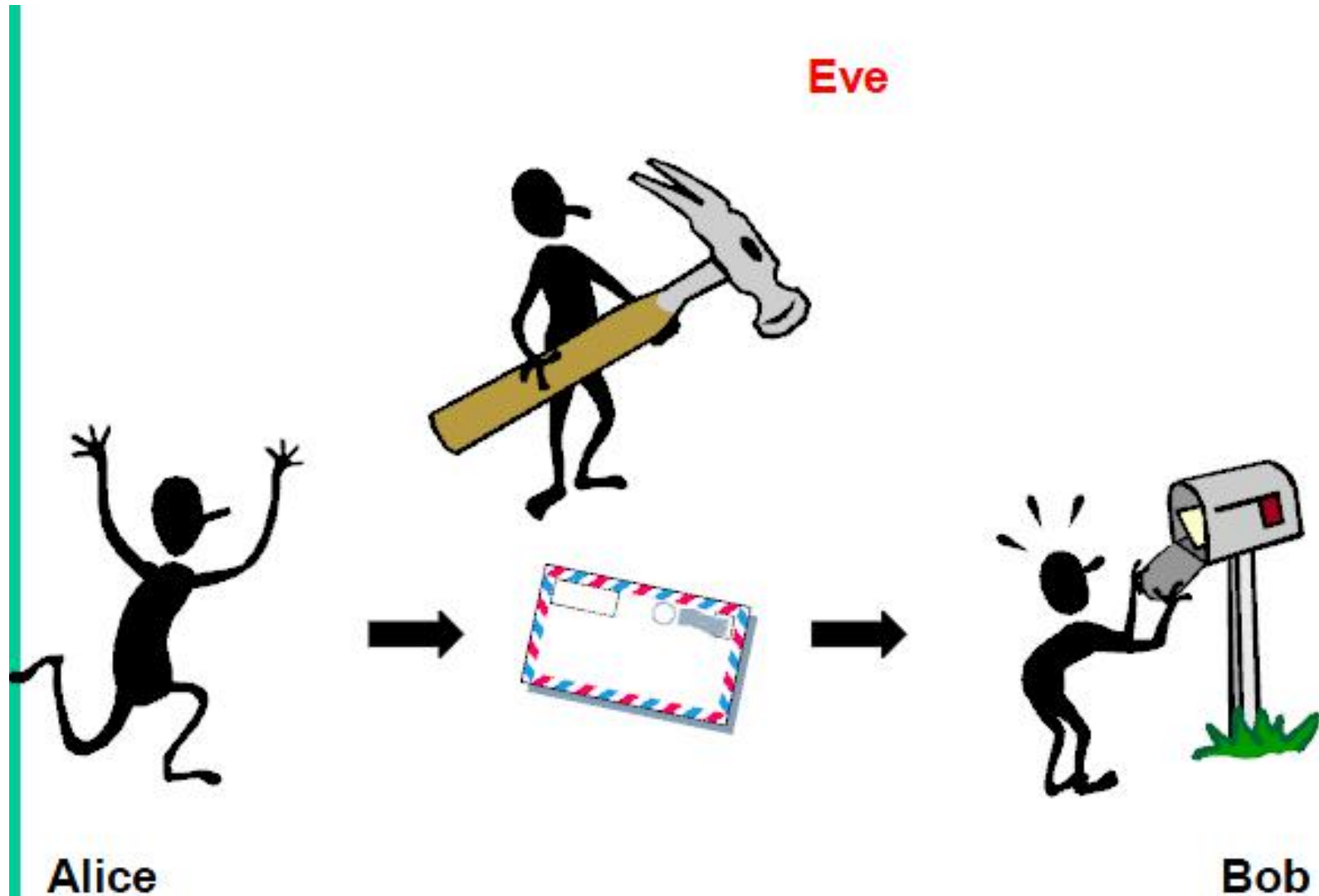
# Availability

---

- Prevent/detect improper retention of information or resource
- Information/resource is accessible by authorised entity
- Examples: availability of a server, a network
- Examples of attack: jamming, DoS, data retention
- Relatively complex concept: different aspects
  - Presence of available service
  - Capacity of providing a service
  - Progress: bounded waiting time
  - Fairness in resource allocation
- Availability = prevent/detect DoS attack
- Example: computer tuned off
  - confidentiality, integrity, but not availability

# Availability

---





# Commercial example

---

- Confidentiality
  - An employee should not know the salary of his manager
- Integrity
  - An employee should not be able to modify the employee's own salary
- Availability
  - Paychecks should be printed on time as stipulated by law

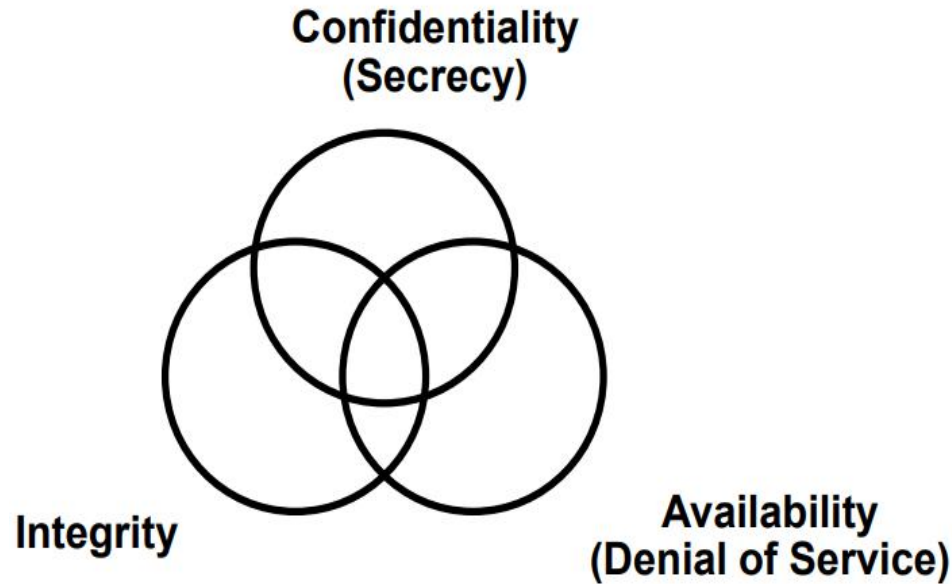
# Military Example

---

- Confidentiality
  - The target coordinates of a missile should not be improperly disclosed
- Integrity
  - The target coordinates of a missile should not be improperly modified
- Availability
  - When the proper command is issued the missile should fire

# Interdependence of security properties

---

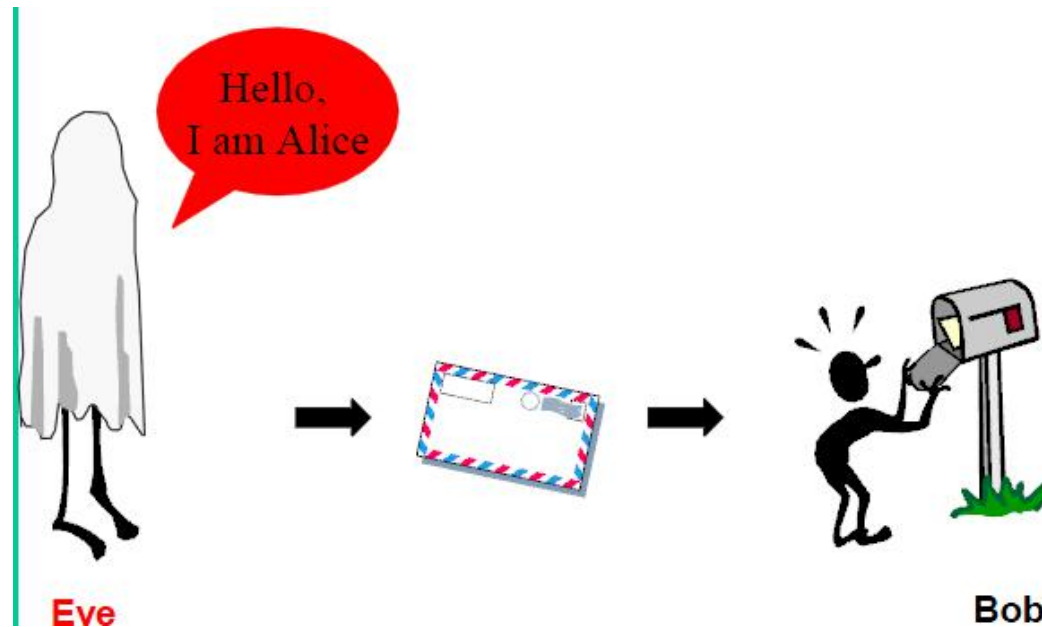


- Confidentiality, integrity, availability
  - Address different aspects of security
  - Possible mutual exclusion
  - Strong confidentiality protection may restrain availability

# Authentication

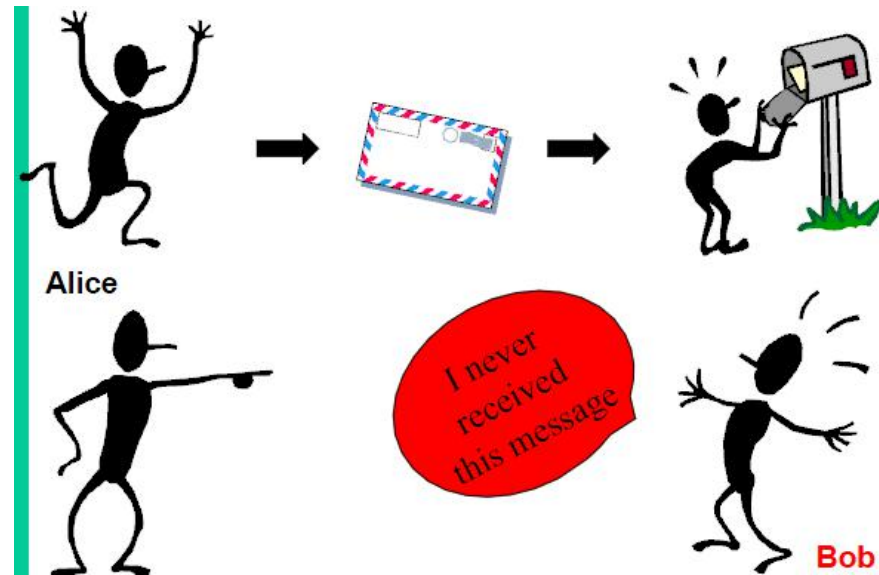
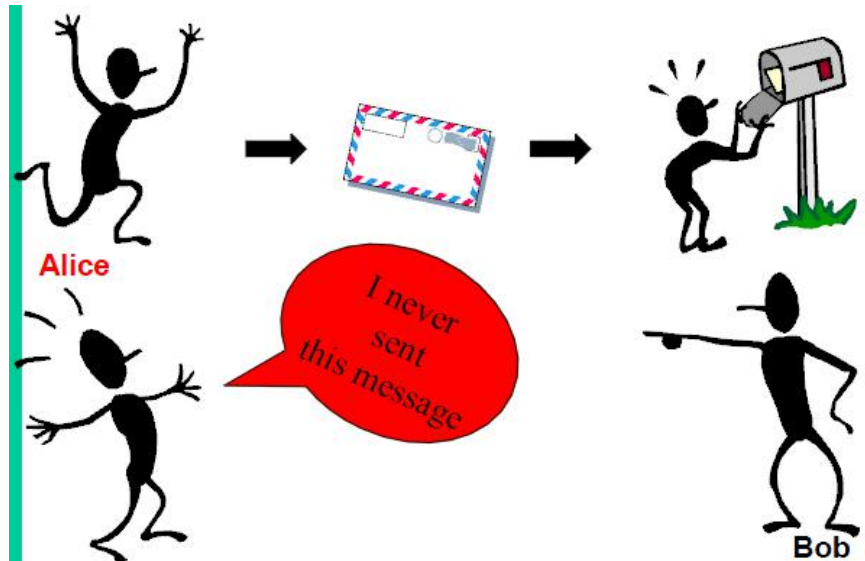
---

- Assuring that
  - Information is authentic: data authentication
  - Communication peer is authentic: entity authentication



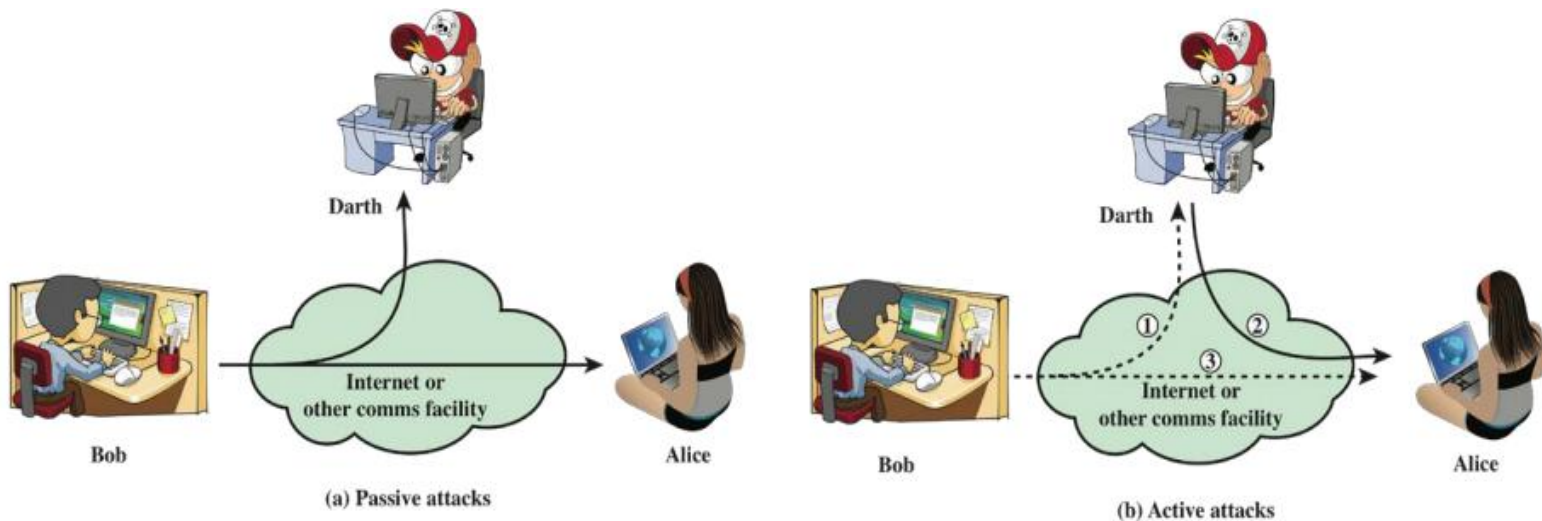
# Non-repudiation

- Prevent/detect sender/receiver from denying a transmitted message



# Security attacks

- Passive attack
  - Eavesdropping on, or monitoring of transmissions
  - Goal: obtain information transmitted
  - Two types of passive attacks
    - Release of message contents
    - Traffic analysis
- Active attack
  - Involve modification of data or creation of false data
  - Masquerade, replay, content modification, DoS



# Test

---

	Release of message contents	Traffic analysis	Masquerade	Replay	Deny of service
Confidentiality					
Integrity					
Availability					
Authentication					
Non-repudiation					

# Security management overview



# How to systematically manage security

---

- Security is not just encrypting
- It concerns the whole system
  - HW+SW+NW+people
- Security is challenging
  - Systems are complex
  - People make mistakes
- We need a systematic methodology
  - Security policy — What?
  - Security mechanism — How?
  - Security assurance — How well?

# Security policy

---

- Rules and procedures for all individuals to access information and resources
  - What is allowed or not
  - Formalism
- Bible of security for an enterprise

# Security mechanisms

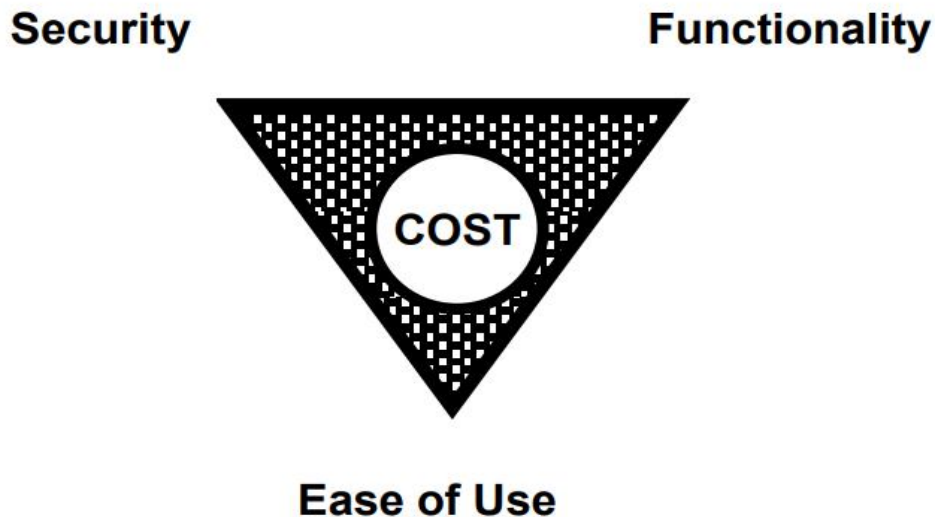
---

- Goal
  - Enforce security policy
- Prevention
  - Example: access control
- Detection
  - Example: intrusion detection
- Tolerance
  - Example: robust algorithm

# Security assurance

---

- How well security mechanisms guarantee security policy
  - Everyone wants high assurance
  - High assurance implies high cost
- May not be possible
  - Trade-off is needed
  - Security is sometimes engineering = making compromises
    - More cost-effective to prevent attack or recover *aposteriori*?



# Security by obscurity

---

- If we hide the inner workings of a system it will be secure
  - Example: military systems
- More and more applications open their standards
  - TCP/IP, 802.11
- Widespread computer knowledge and expertise

# Terminology

---

- Vulnerability
  - System weakness, e.g., bugs
- Attack
  - Action exploiting vulnerability
- Threat
  - Potential attack
  
- Attack vector
  - Means of attack
- Attack surface
  - Possible attacked places in systems
  - May or may not contain vulnerabilities