信息安全技术

Personnel

- Instructors
  - 郑培嘉
  - Email: zhpj@mail.sysu.edu.cn

信息安全技术-2022年

群号：797714043

点击卡片更换背景

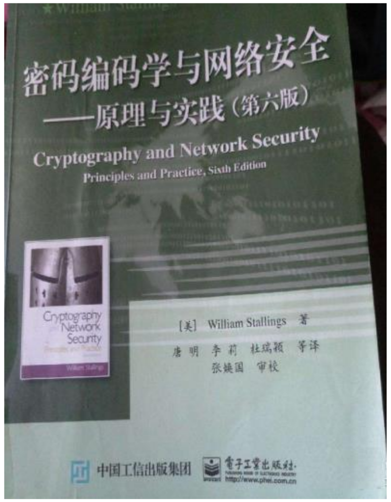
Objectives

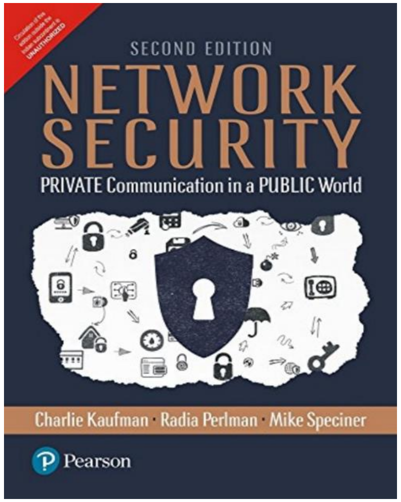
- Understand basic security concepts, principles, and algorithms
  - Cryptography
  - Authentication
  - Access control
  - Classic security protocols

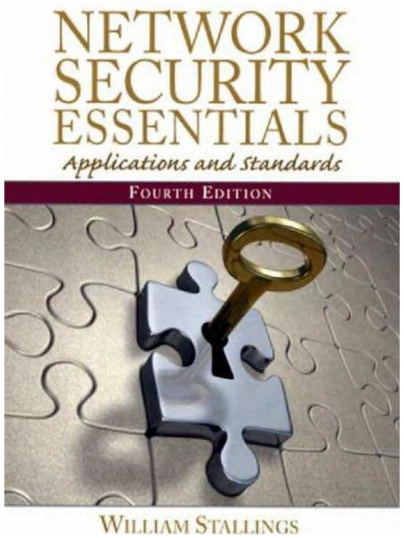
- Be able to choose appropriate security mechanisms to protect computers and networks

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




SECOND EDITION
NETWORK SECURITY
PRIVATE Communication in a PUBLIC World
Charlie Kaufman · Radia Perlman · Mike Speciner
Pearson



Grading

- Homework
- Mini-project
- 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

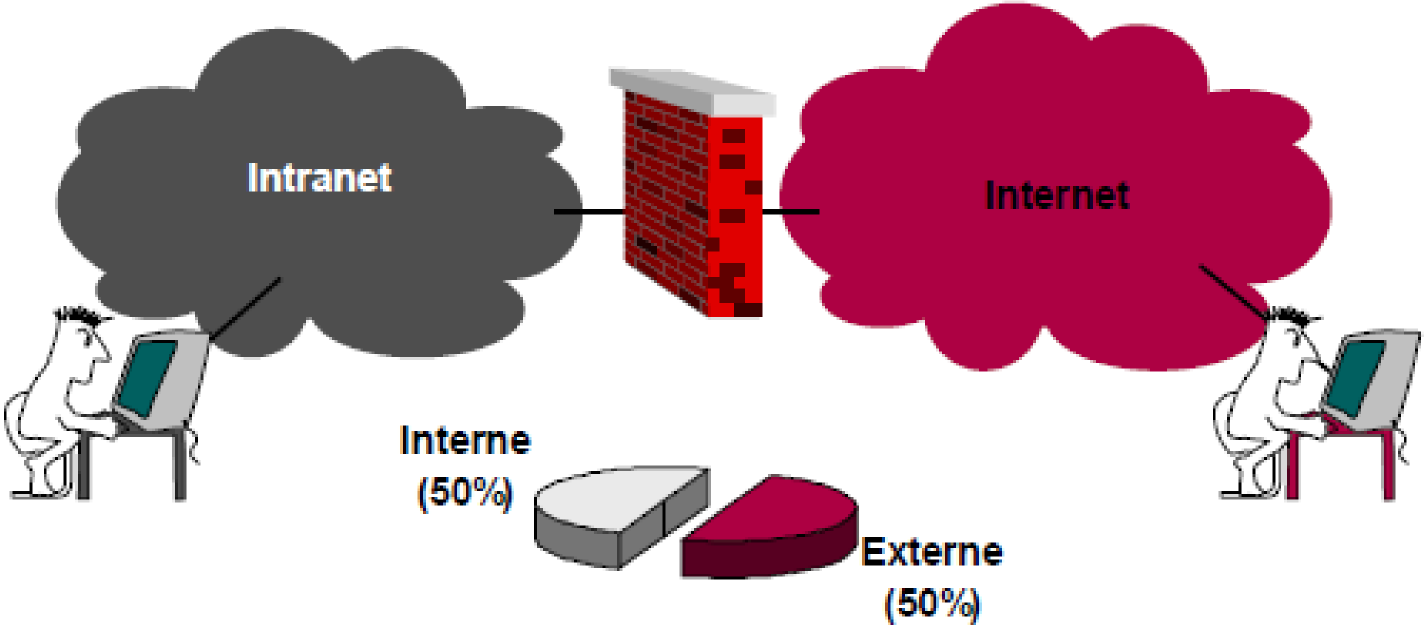
- A real problem
  - An unpatched PC survives less than 16 min
  - 61% of PCs in E.-U. infected by spy-ware
  - Annual loss: $100+ billion

Attacks

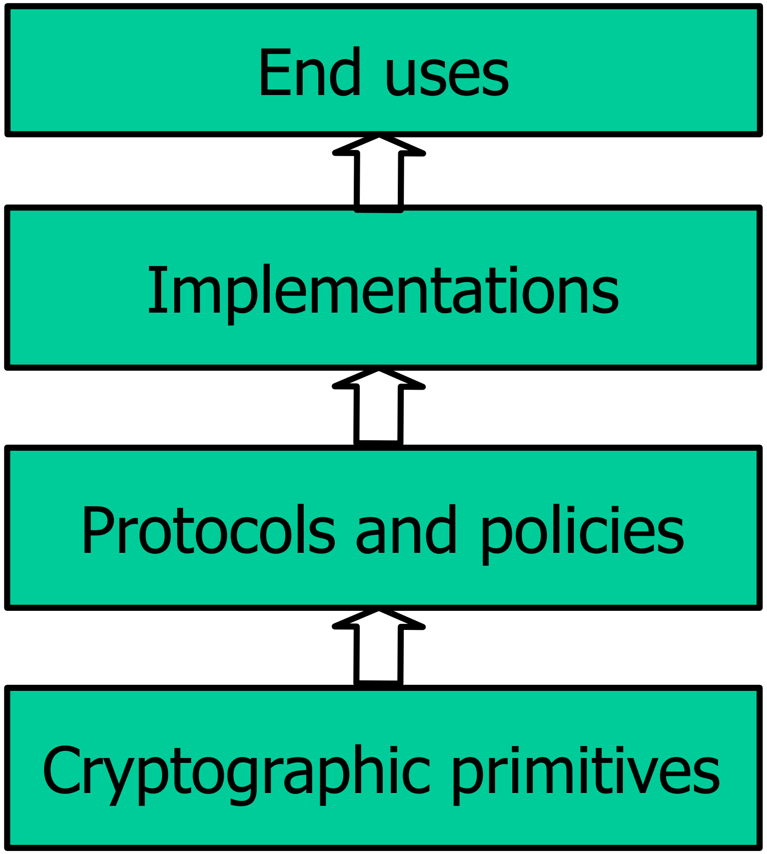
- Who are the attackers
  - Hackers, malicious insiders, spies, terrorists, press... Can be anyone!
  - White hat, gray hat, black hat, script kiddy
- Why do they attack
  - Financial motivation
  - Religious/political motivation
  - Industrial espionage
- Whom do they attack
  - Banks, governments,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

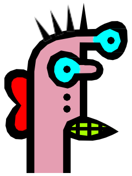
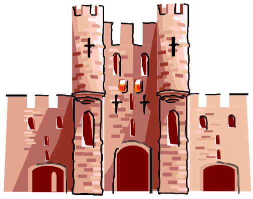
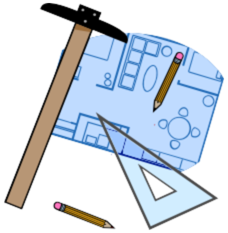
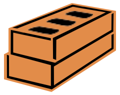
What is the source of a vulnerability?

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



System defenses



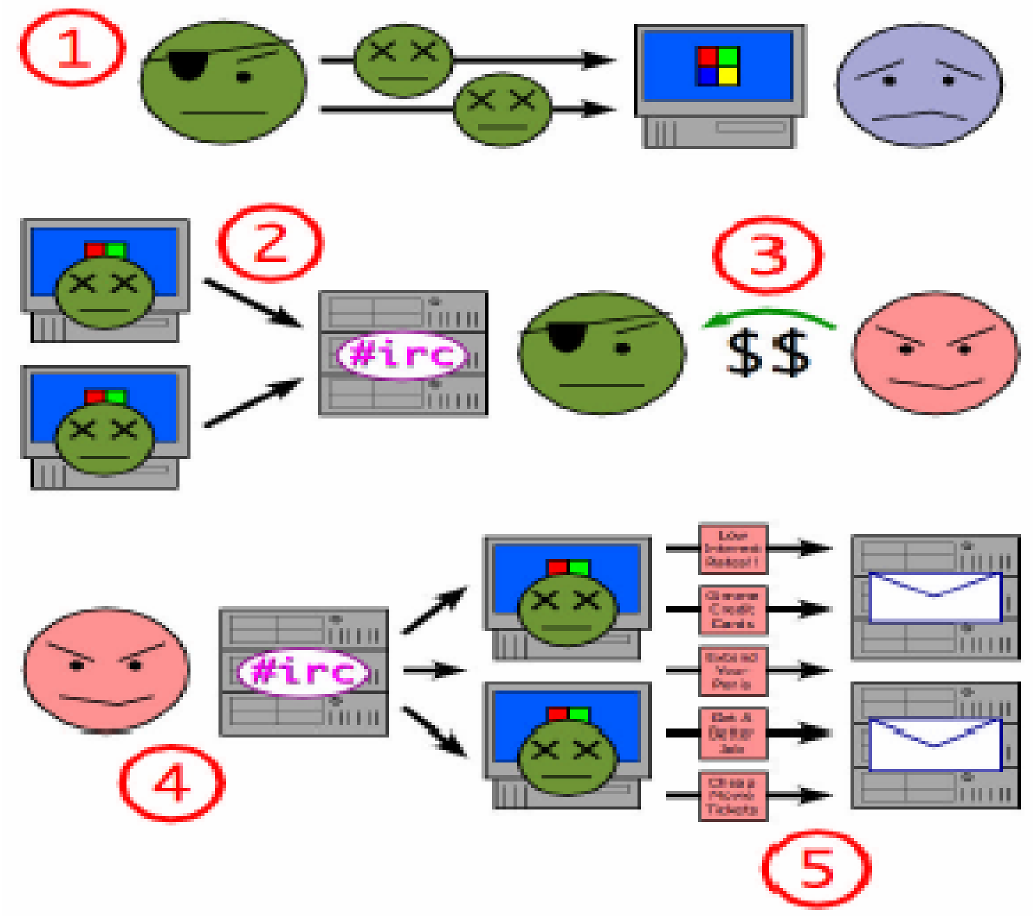
	People	End uses	*Password managers, company policies…*
	Systems	Implementations	*Firewalls, intrusion detection…*
	Blueprints	Protocols and policies	*TLS, IPsec, access control…*
	Building blocks	Cryptographic primitives	*RSA, DSS, SHA-1…*

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



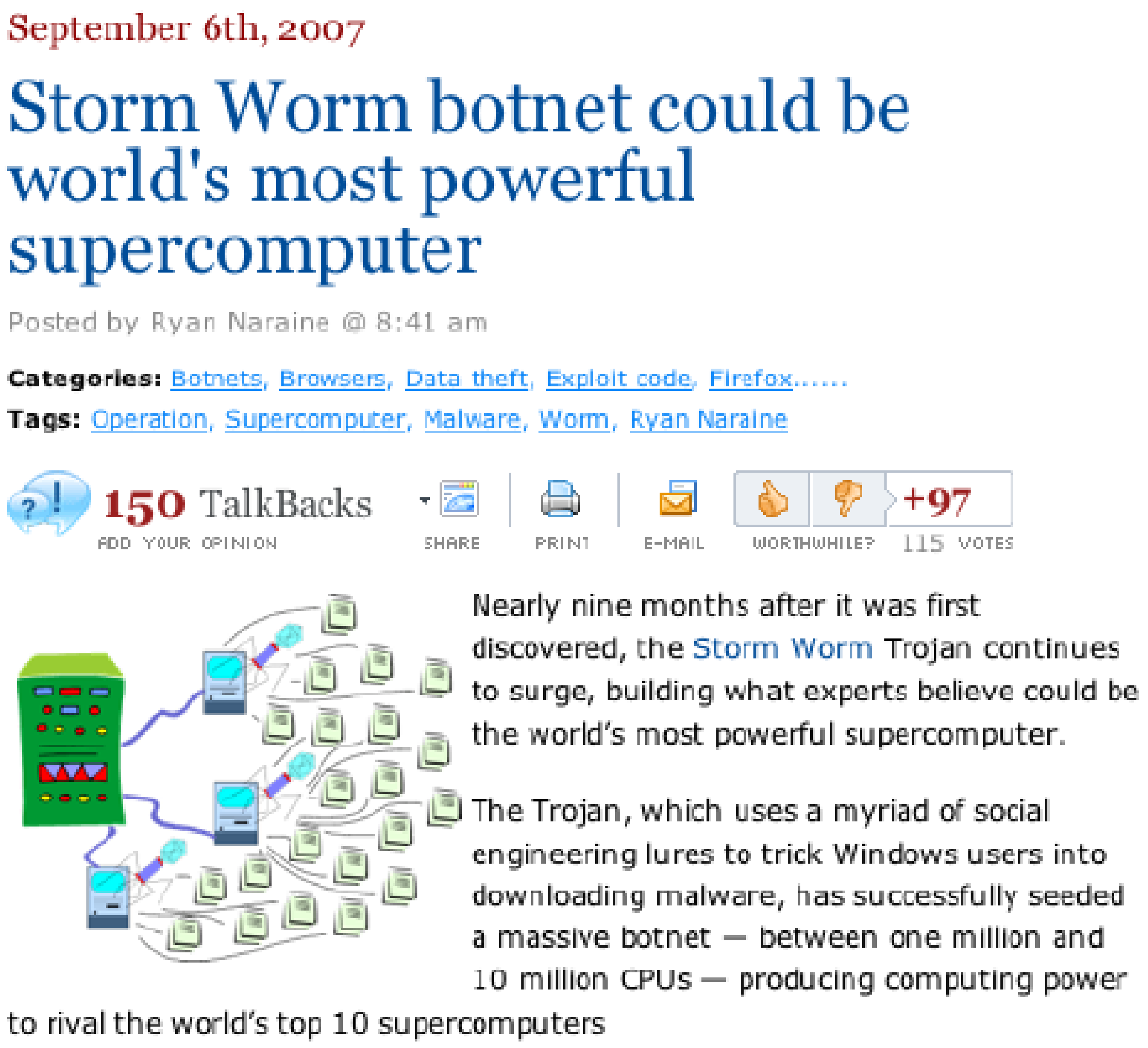
Botnet

- 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

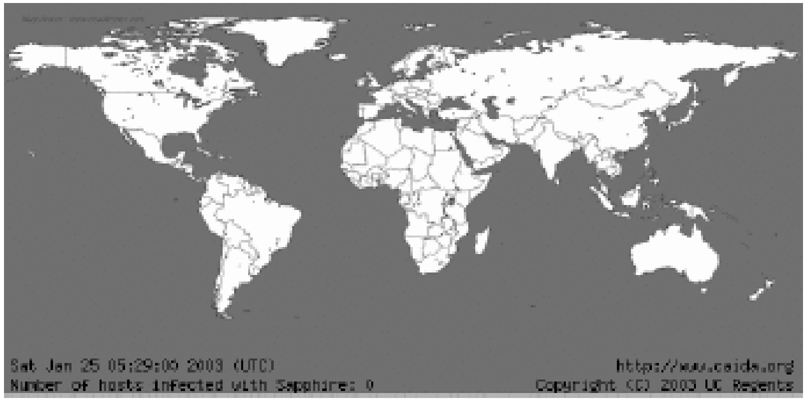
Nearly nine months after it was first discovered, the Storm Worm Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

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

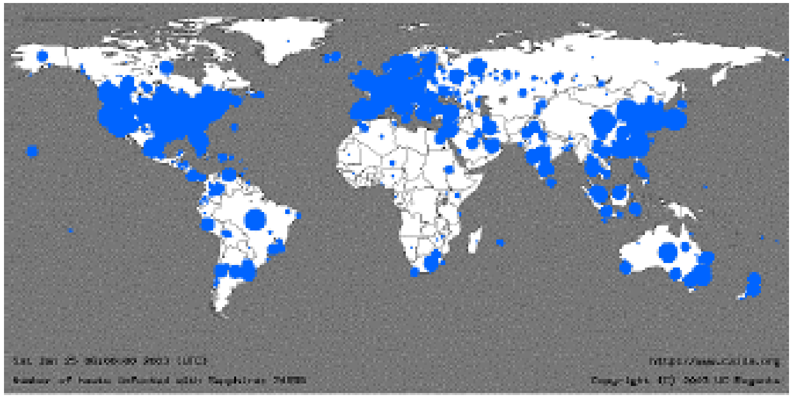
Worm

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

25 janvier 2003, 05:29 0 victime


Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
https://www.caida.org
Copyright (C) 2003 UC Regents

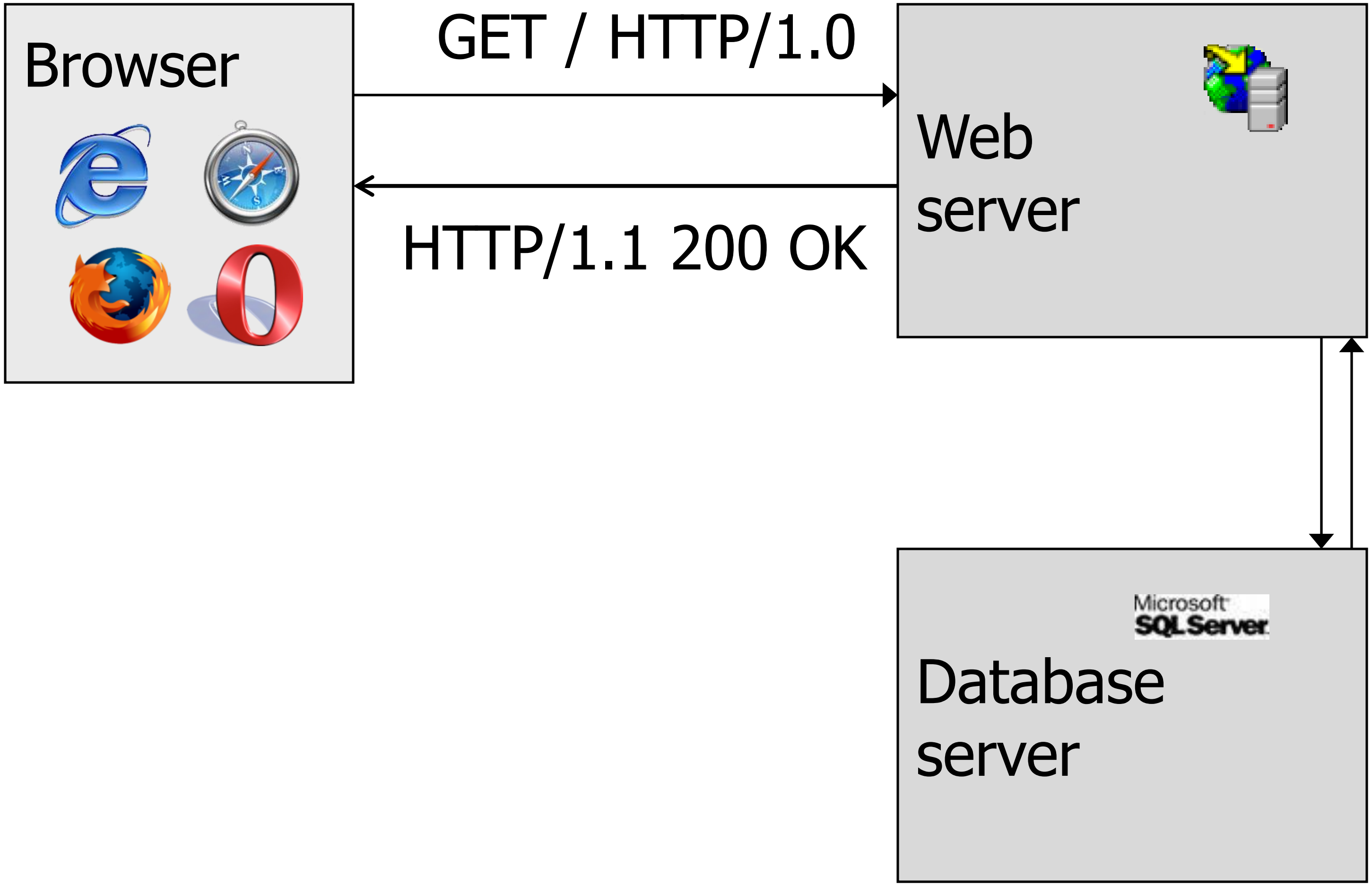
25 janvier 2003, 06:00 74 855 victimes


Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
https://www.caida.org
Copyright (C) 2003 UC Regents

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



Browser

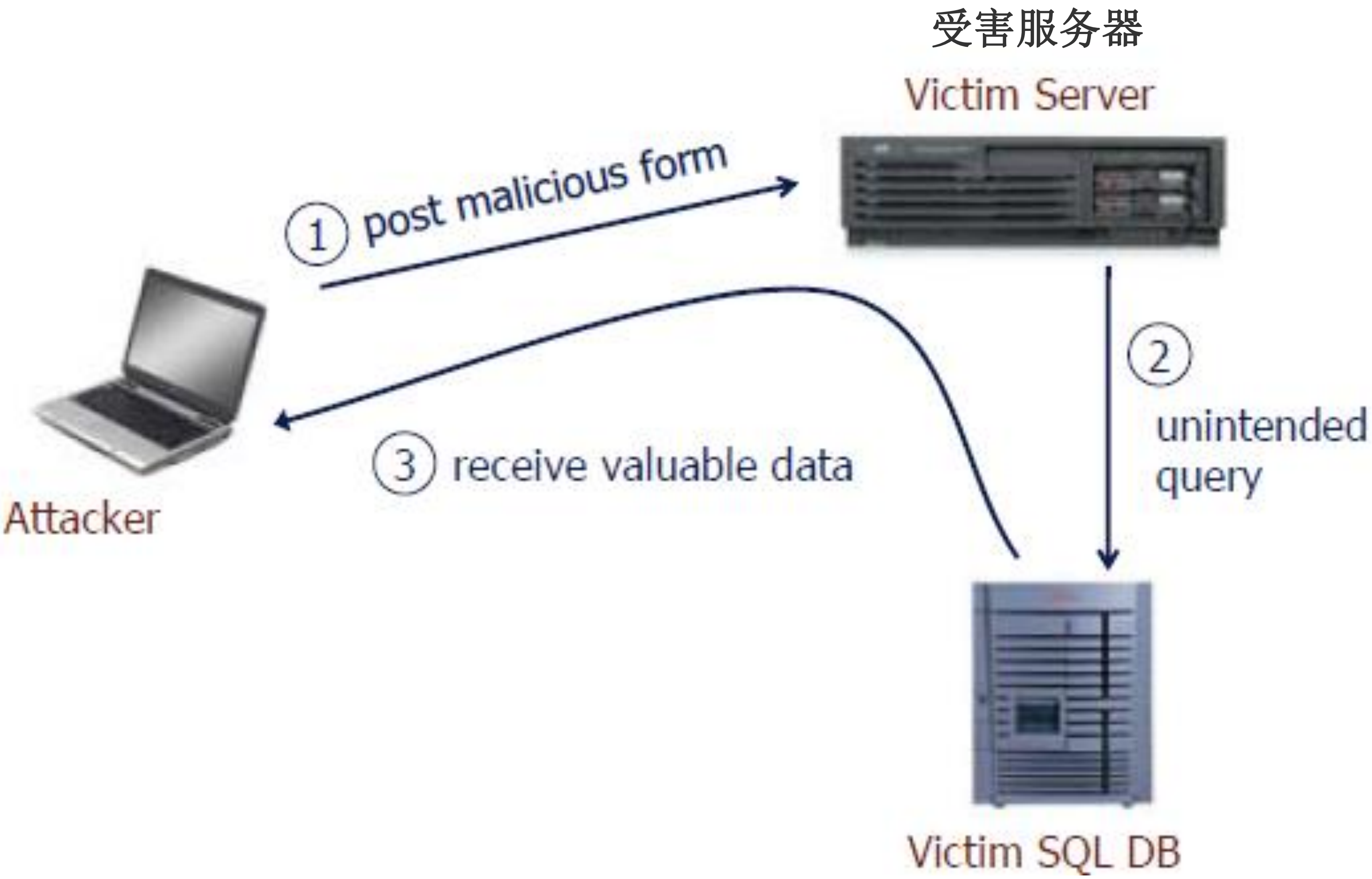
GET / HTTP/1.0

HTTP/1.1 200 OK

Web server

Database server

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.

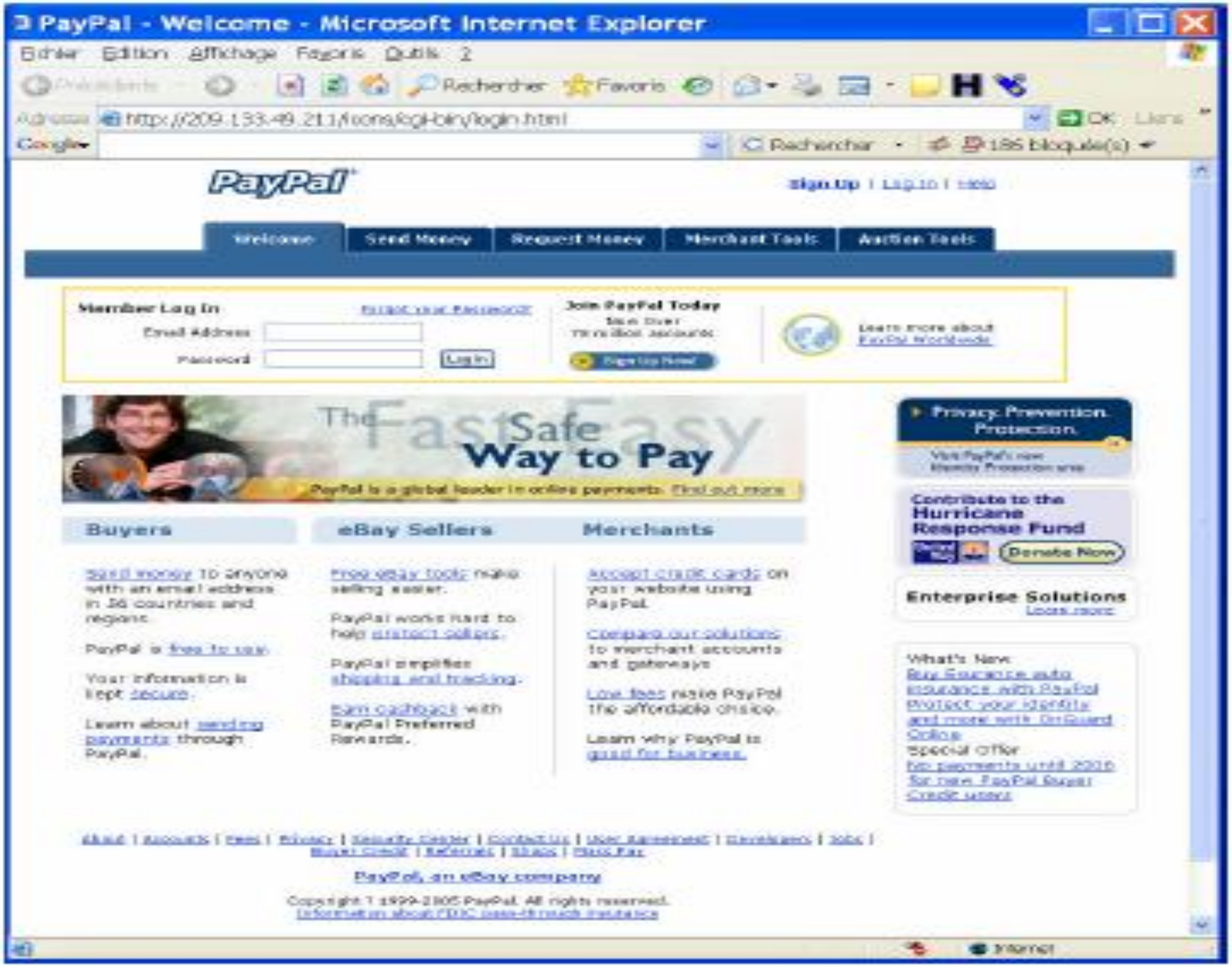
However, failure to update your records will result in account suspension. Please update your records on or before **Oct 04, 2015**.

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

Thank You.
PayPal® UPDATE TEAM

Phishing



http://209.133.49.211/icons/cgi-bin/login.html

Member Log In Forgot your Password?

Email Address

Password

Join PayPal Today
Now Over
[illegible] accounts

Learn more about PayPal Worldwide

The Fast Safe Easy Way to Pay

PayPal is a global leader in online payments. Find out more

Buyers

Send money to anyone with an email address in 36 countries and regions.

PayPal is free to use.

Your information is kept secure.

Learn about sending payments through PayPal.

eBay Sellers

Free eBay tools make selling easier.

PayPal works hard to help protect sellers.

PayPal simplifies shipping and tracking.

Earn cashback with PayPal Preferred Rewards.

Merchants

Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts and gateways.

Low fees make PayPal the affordable choice.

Learn why PayPal is good for business.

Privacy. Prevention. Protection.
Visit PayPal's new Identity Protection area

Contribute to the Hurricane Response Fund

Enterprise Solutions
Learn more

What's New
Buy Esurance auto insurance with PayPal
Protect your identity and more with [illegible] Online
Special Offer
No payments until 2006 for new PayPal Buyer Credit users

About | Accounts | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs |
Buyer Credit | Referrals | Shops | Mass Pay

PayPal, an eBay company

Copyright ? 1999-2005 PayPal. All rights reserved.
Information about FDIC pass-through insurance

What is security?

信息的概念

- ISO/IEC 的IT 安全管理指南（GMITS，即ISO/IEC TR 13335）对信息（Information）的解释是：信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。
- 一般意义上的信息概念是指事物运动的状态和方式，是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。通常情况下，可以把信息可以理解为消息、信号、数据、情报和知识。信息本身是无形的，借助于信息媒体以多种形式存在或传播，它可以存储在计算机、磁带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络等方式进行传播。

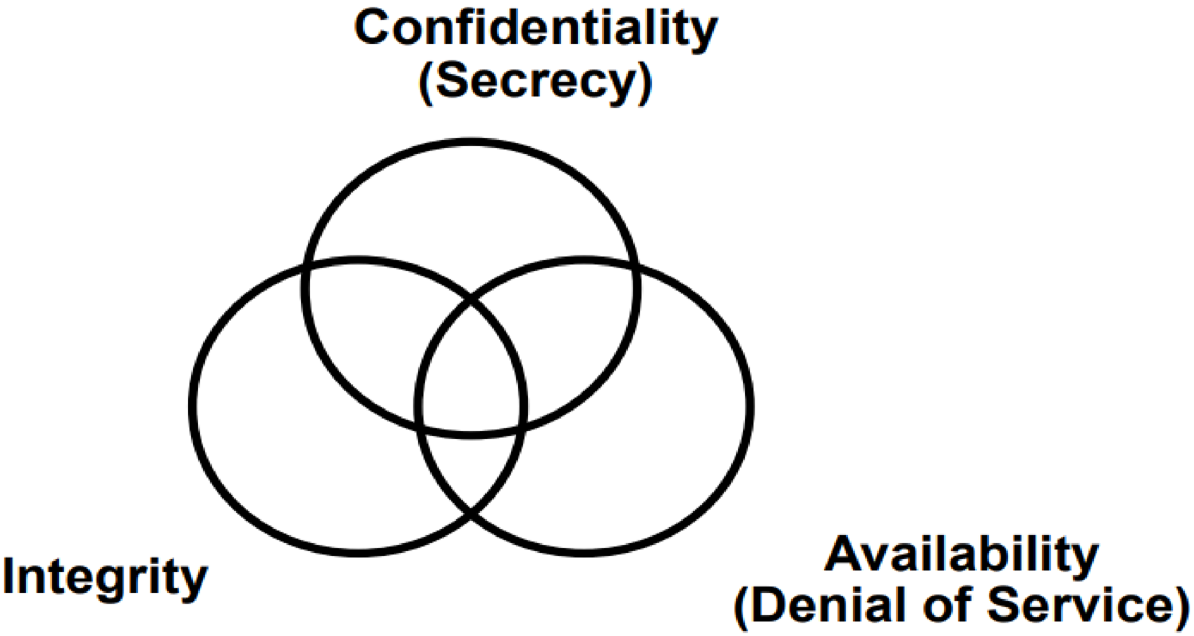
“安全”一词的基本含义

- “安全”一词的基本含义为：“远离危险的状态或特性”，或“主观上不存在威胁，主观上不存在恐惧”。在各个领域都存在着安全问题，安全问题是普遍存在的。随着计算机网络的迅速发展，人们对信息的存储、处理和传递过程中涉及的安全问题越来越关注，信息领域的安全问题变得非常突出。

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

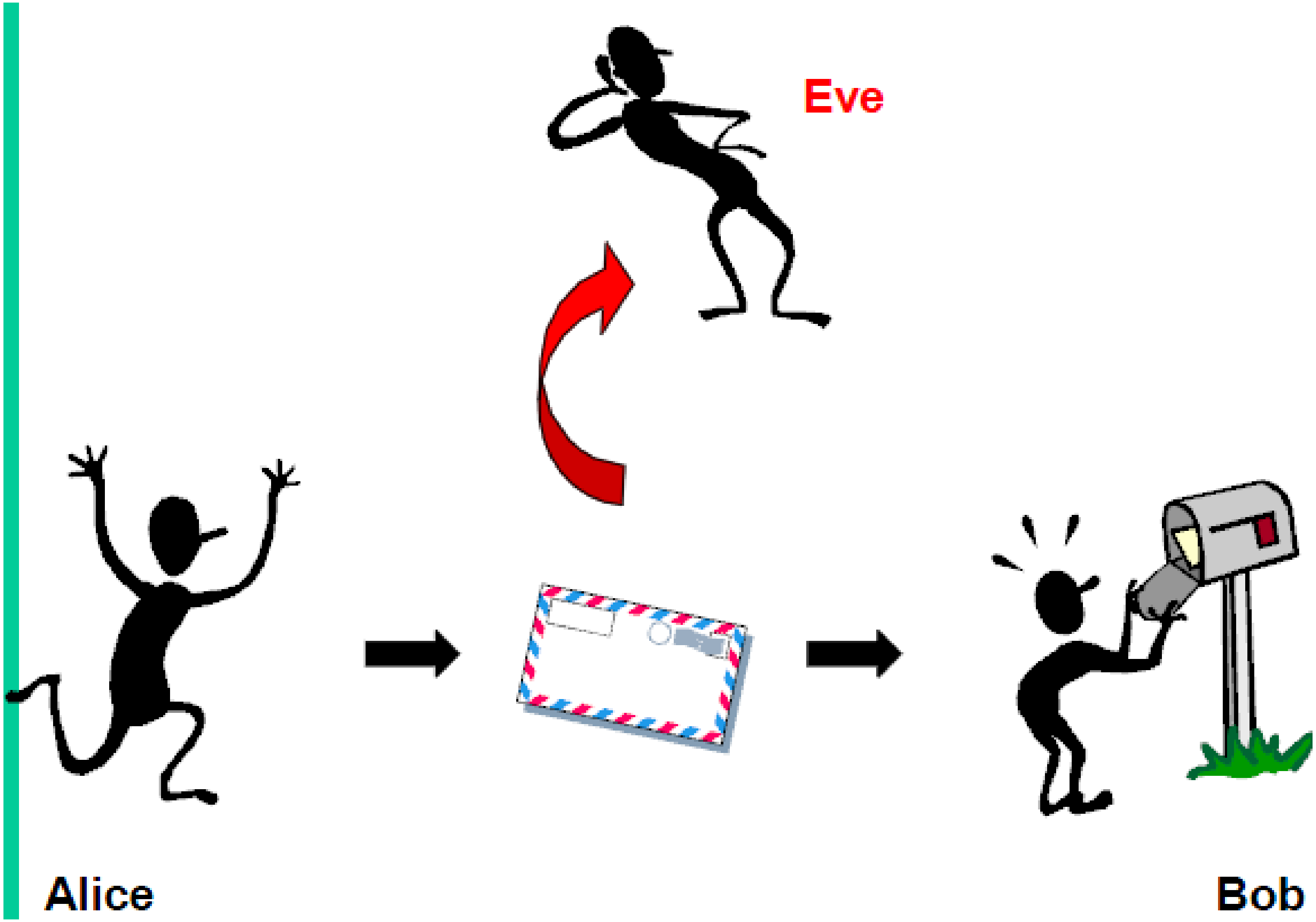
- In one phrase
  - Prevent/detect any improper action

Confidentiality

- Prevent/detect improper disclosure of information
- Information is accessible only by autorised entity
- Types of access: read, print, existance
- Exemples: confidentiality of text, an image, an information flow

- The most understood property

Confidentiality



Integrity

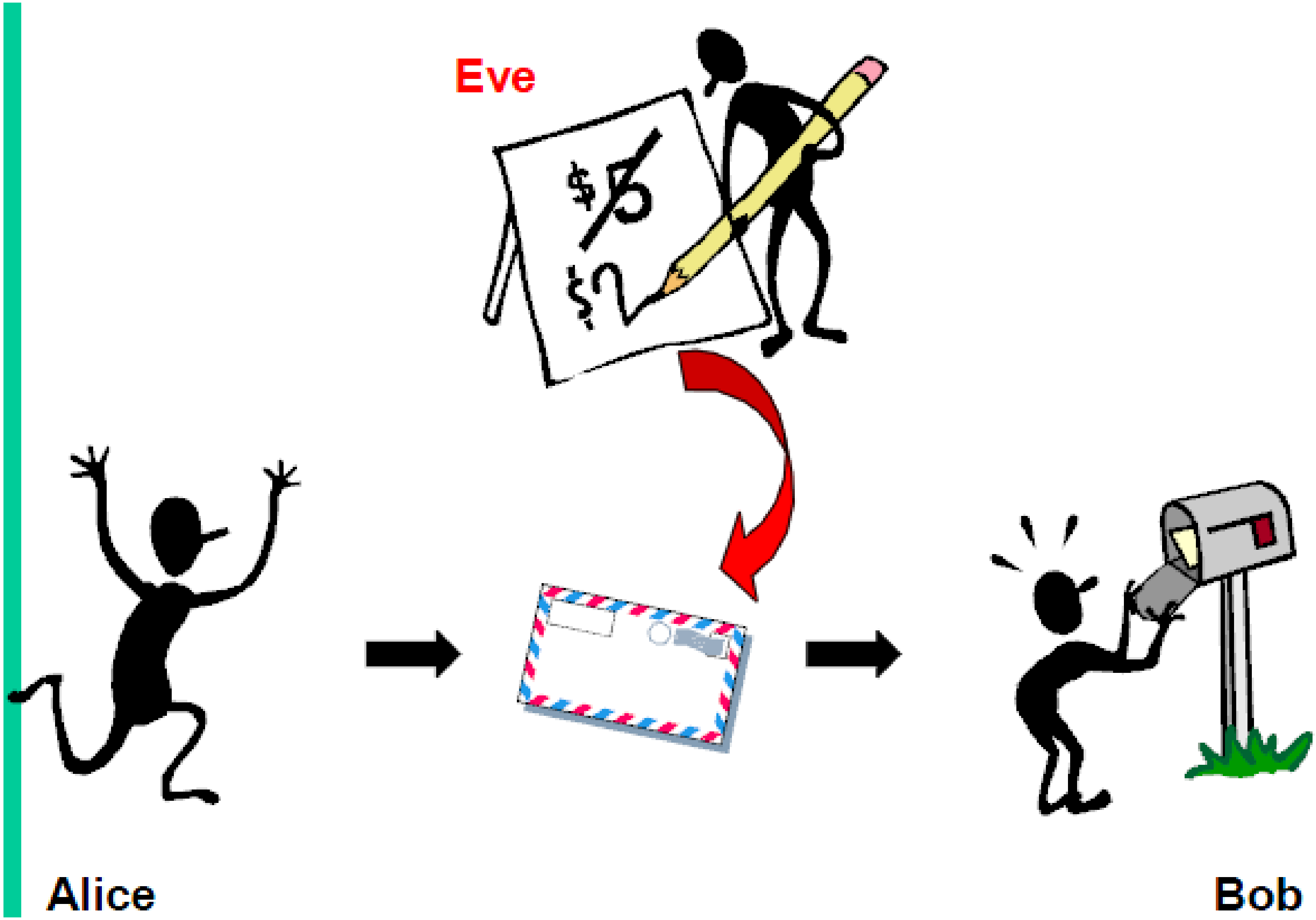
- Prevent/detect improper modification of information
  - Sometimes more important than confidentiality
- Information is modified only by autorised entity
- Types of access: write, create, delete, change status

- Data integrity
- System integrity

- Exemples: 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

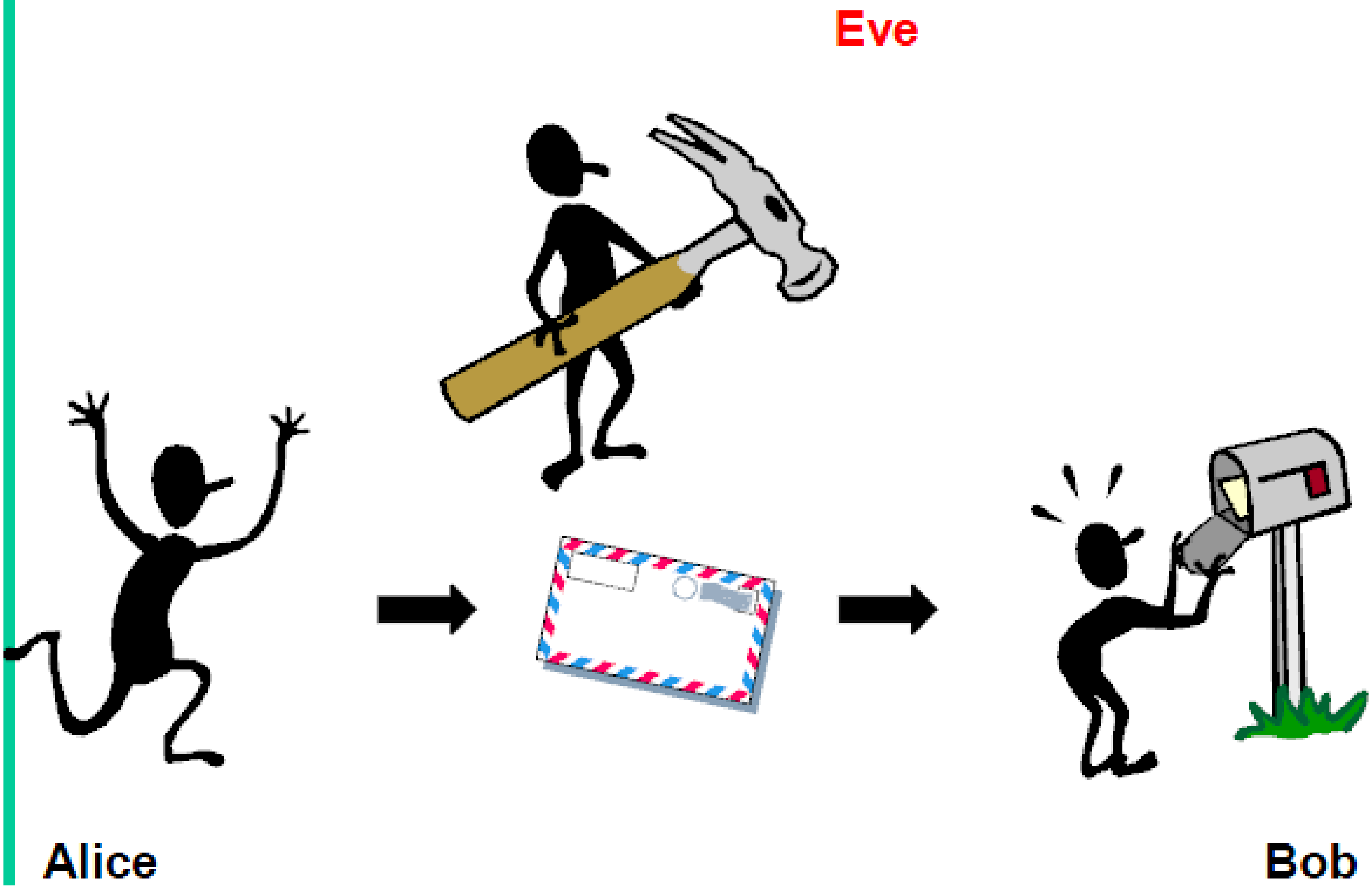
- Prevent/detect improper retention of information or resource
- Information/resource is accessible by autorised entity
- Exemples: availability of a server, a network
- Examples of attack: jamming, DoS, data retention

- 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



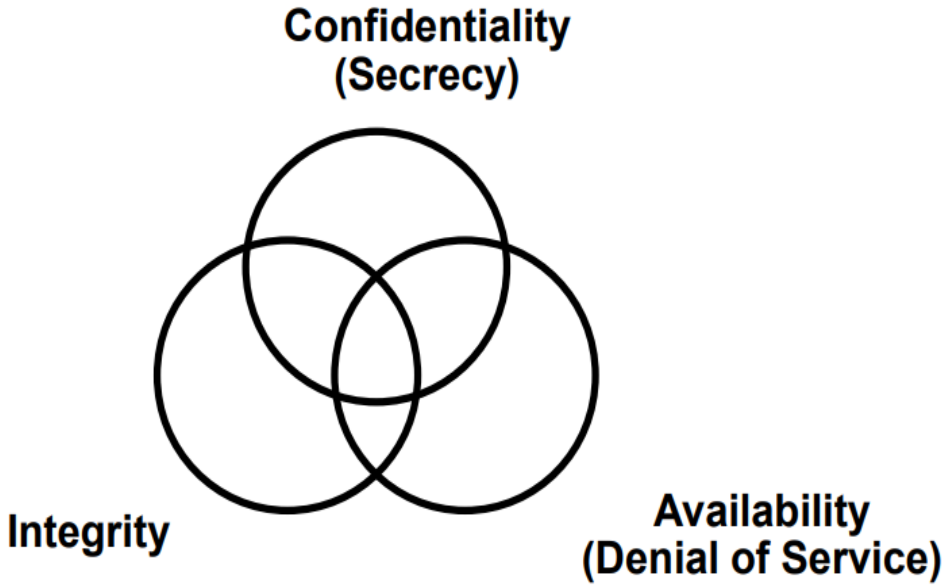
Commercial example

- 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

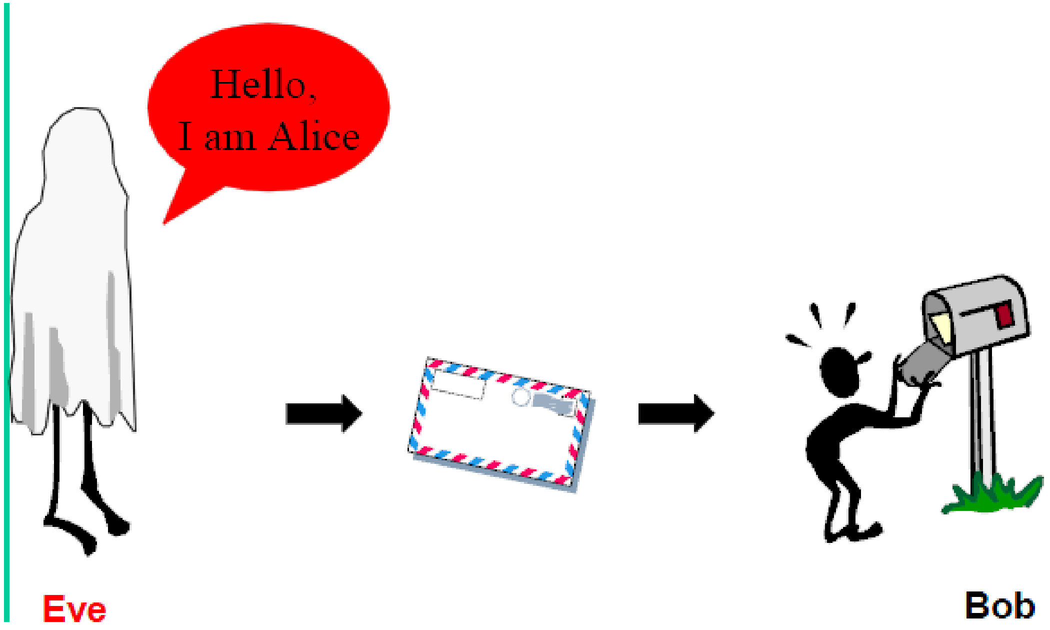
Interdependence of security properties



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

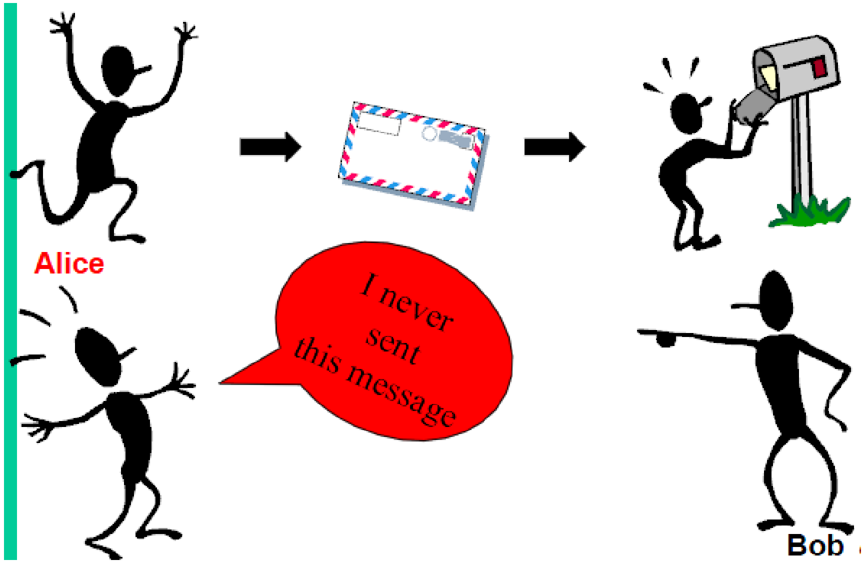
Authentication

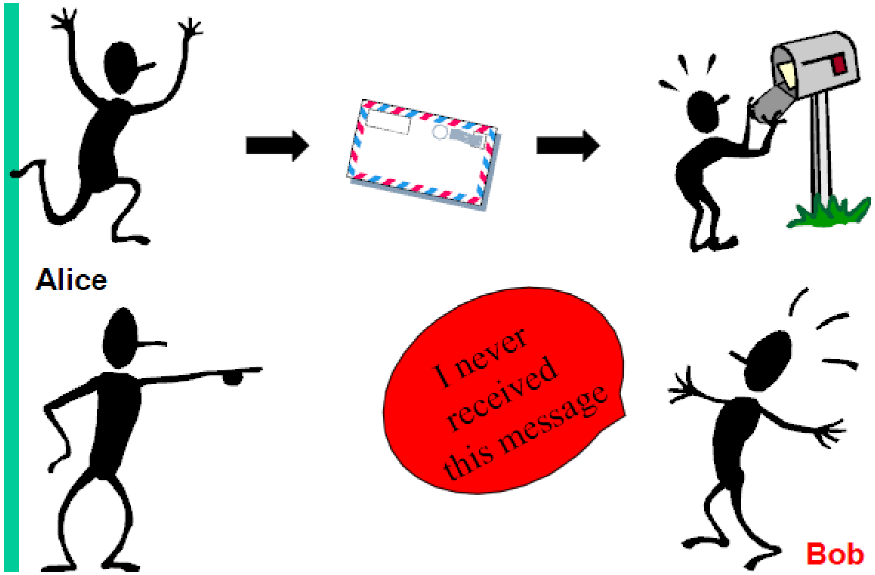
- Assuring that
  - Information is authentic: data authentication
  - Communication peer is authentic: entity authentication



Non-repudiation

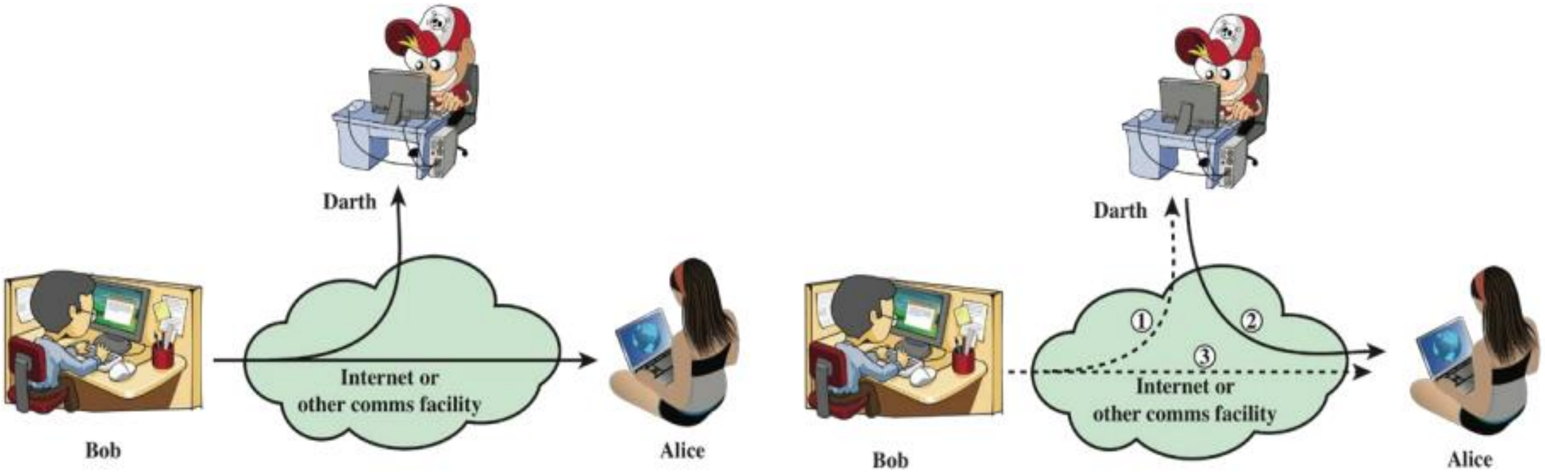
- Prevent/detect sender/receiver from denying a transmitted message





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



(a) Passive attacks

(b) Active attacks

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

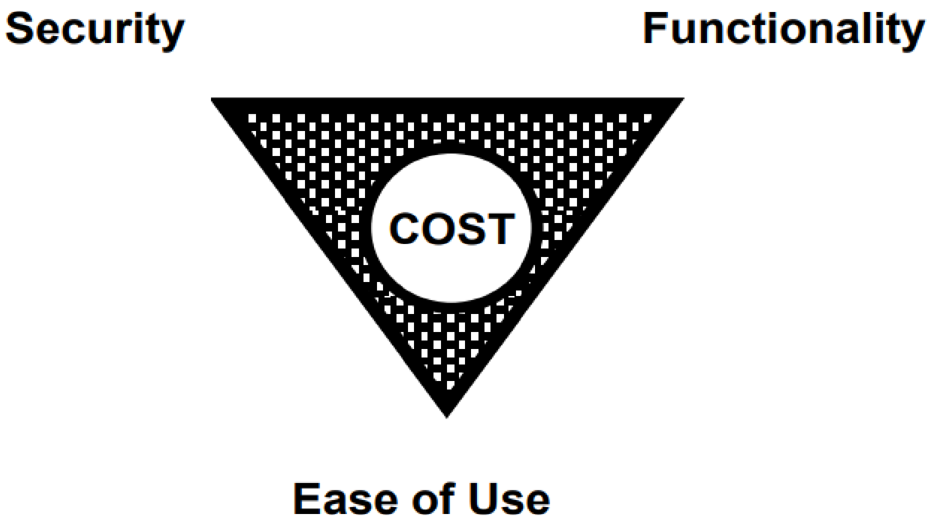
Security mechanisms

- 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