Bachelor of Information System

IS2109 - Information System Security

Additional Lecture - 1

Kasun de Zoysa
kasun@ucsc.cmb.ac.lk

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

What do we mean by “secure”?

- At one time Bank robbery was common. Now its very rare. What has changed or been implemented to provide this security?
  - Sophisticated alarms
  - Criminal investigation techniques (DNA testing)
  - Change in “assets” (cash was/is inherently insecure)
  - Improvements in communication and transportation
- Risk becomes so high that it is no longer beneficial.

Security is all about protecting valuables

- In our case the “valuables” are computer related assets instead of money
  - Though these days money is so electronic that one can argue that the protection of money is a subset of computer asset security
- Information seems to be the currency of the 21st century.

Trends in Usage of Information Systems

Business (international) transactions

Storage of business documents

Financial flows

Industrial cooperation

Functionality and Dependability

Money vs. Information

- Size and portability
  - Banks are large and unportable.
  - Storage of information can be very small and extremely portable. (So small that an entire corporations intellectual property can be stored on something the size of a postage stamp.) Ability to avoid physical contact
  - Banks: physical interaction with the bank and the loot is unavoidable or impossible to circumvent
  - Computers: require no physical contact to either gain access to, copy or remove data.
- Value of assets:
  - Bank: generally very high (or why would somebody bother to put it in a bank?)
  - Computers: Variable, from very low (useless) to very high.

Required Properties of Information Systems

Availability

Reliability (accountability)

New functionalities

Resistance to attacks

Information System Security

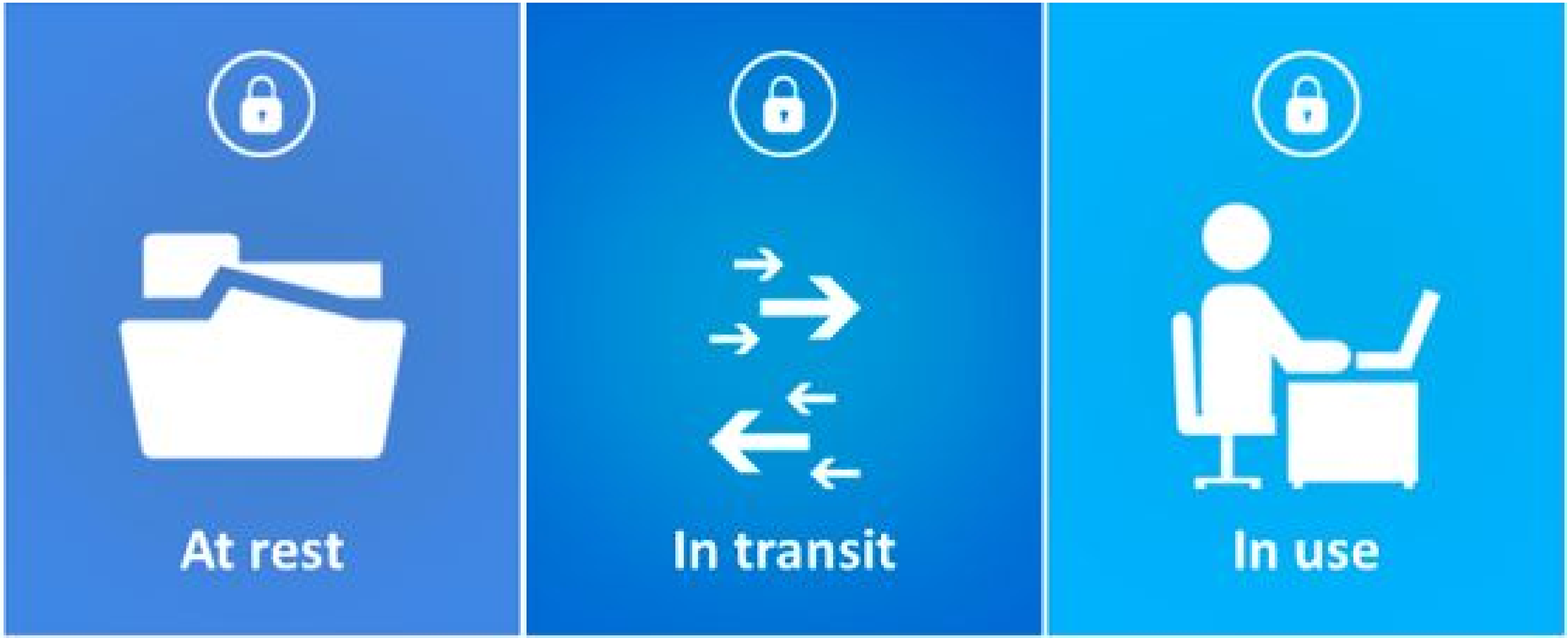
Security!!

- **Information Security** focuses on data in all forms.
- **Information System Security** focuses on the systems managing data.
- **Cybersecurity** focuses on defending against threats in the cyberspace (The internet and connected systems).

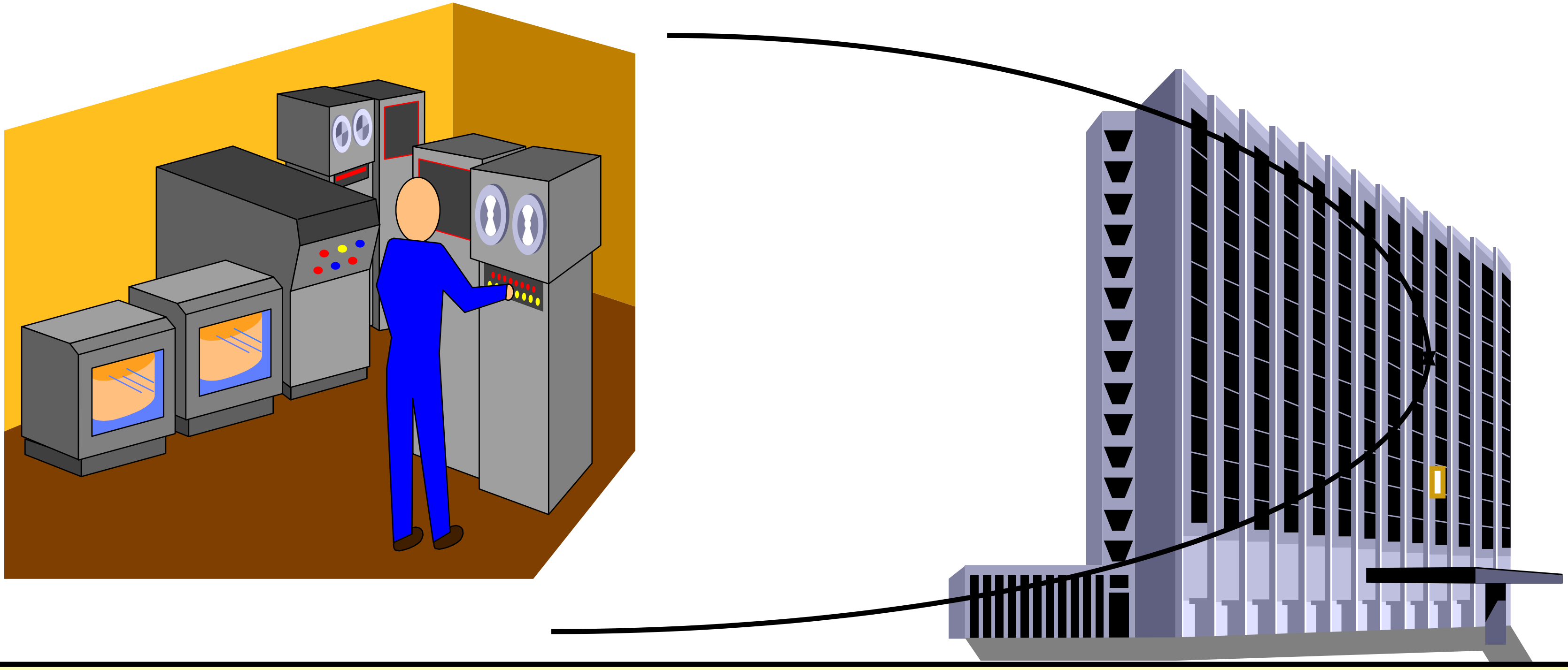
Cybersecurity

- The definition of cybersecurity is often confused with the definition of information security.
- Information security, often referred to as 'IT security', looks to protect all information assets, whether as a hard copy or in digital form.
- **Cyber security is a subset of information security.** It specifically focuses on protecting computer systems and their components from Cyberattacks.

Life Cycle of the Information

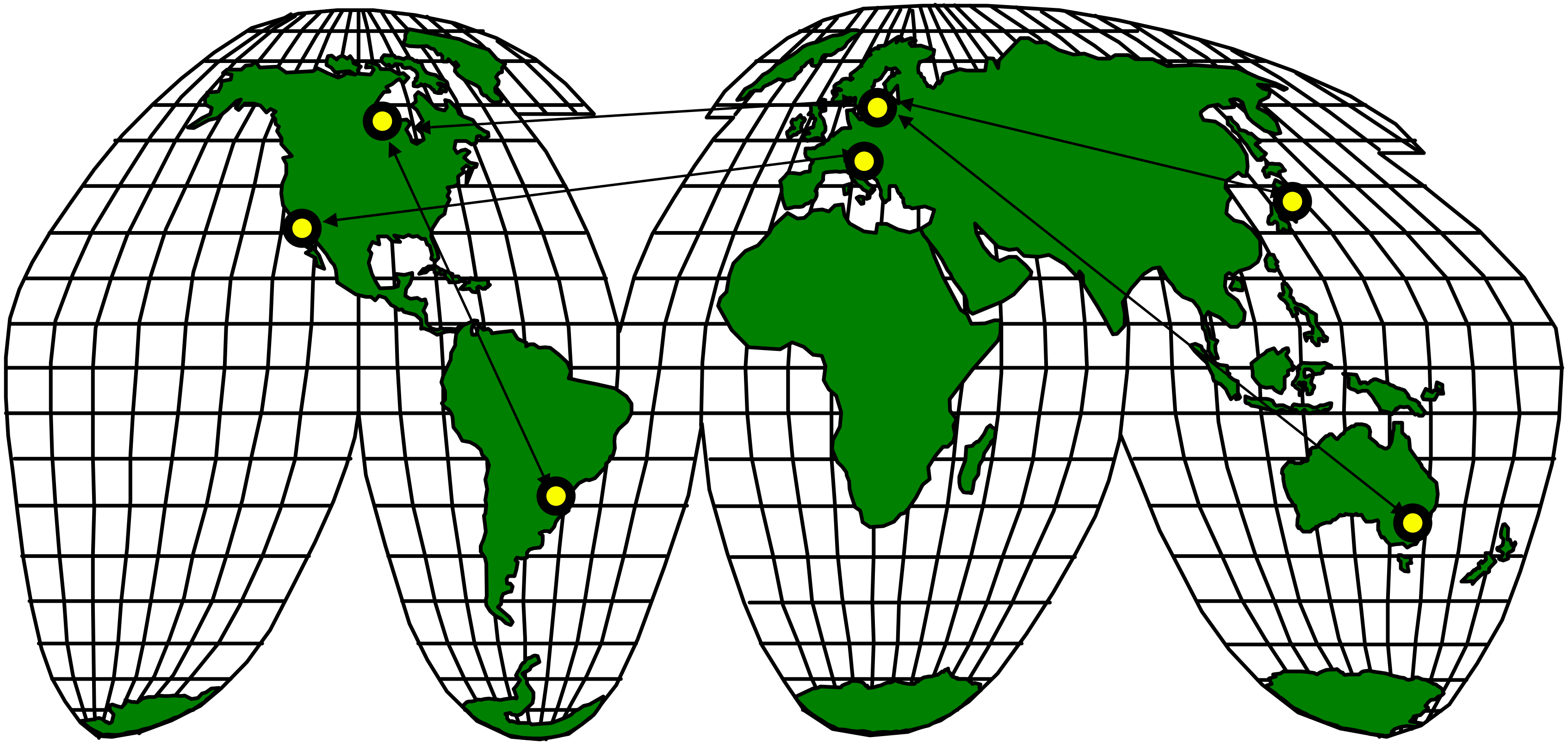


Past Situation (Single Systems)



Physical security and control of access to computers

Current Situation (Int’l networks and open systems)



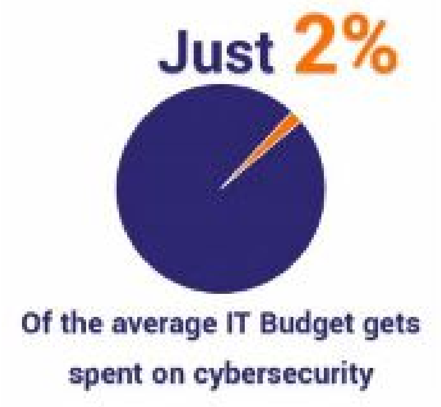
Authentication, message protection, authorization

Method, Opportunity and Motive

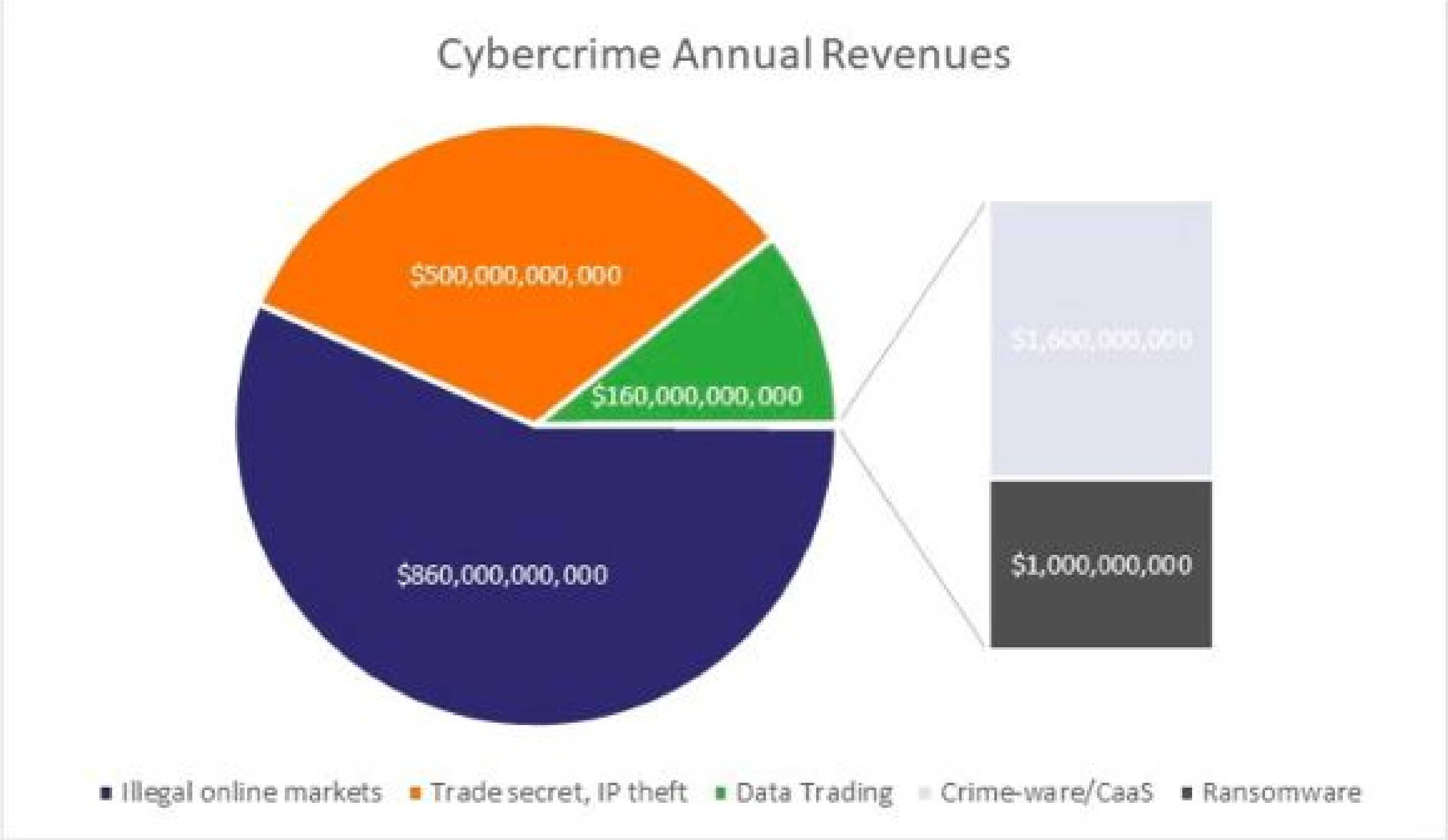
- **Method**: The skills knowledge and tools that enable the attack
- **Opportunity**: The time, access and circumstances that allow for the attack
- **Motive**: The reason why the perpetrator wants to commit the attack

Eye-Opening Information Security Statistics

- 70% of employees don't understand information security.
- 30% of the world's top websites unsecure
- Outdated and unpatched software constitutes 22% of security issues
- 60% of organizations use cloud technology for sensitive or confidential data



Cybercrime will create over $1.5 trillion in profits in 2018



The People Involved

Amateurs . . .

Crackers

Criminals

Regular users

Accidental access to unauthorized resources and execution of unauthorized operations (no harm to regular users)

The People Involved

- Amateurs
- **Crackers . . .**
- Criminals
- Regular users

Active attempts to access sensitive resources and to discover system vulnerabilities
(minor inconveniences
to regular users)

The People Involved

- Amateurs
- Crackers
- Criminals . . .
- Regular users

Active attempts to utilize weaknesses in protection system in order to steal or destroy resources (serious problems to regular users)

The People Involved

Amateurs

Crackers

Criminals

Regular users . . .

Special requirements: authentication in open networks, authorization, message integrity, non-repudiation, special transactions

Vulnerability, Attack, Threats, Problems, Risks and Control

- Vulnerability: A weakness in the security system.
- Attack: A human exploitation of a vulnerability.
- Threat: a set of circumstances that has the potential to cause loss or harm.
- Problems : Consequences of unintentional accidental errors
- Risks : Probabilities that some threat or problem will occur due to system vulnerabilities
- Control: A protective measure. An action, device or measure taken that removes, reduces or neutralizes a vulnerability.

Types of Concerns

Attacks on hardware or software (Active threats)

Problems with data and software transfer and manipulation (Accidental errors)

Requirements for reliable, trusted and authorized transactions

Categories of Attacks

Attacks on hardware : destruction

Attacks on software :

- Software deletion
- Software modification
- Software theft

Attacks on data :

- Data secrecy
- Data integrity

Categories of Threats

Interruption : A resource is lost,unavailable or unusable

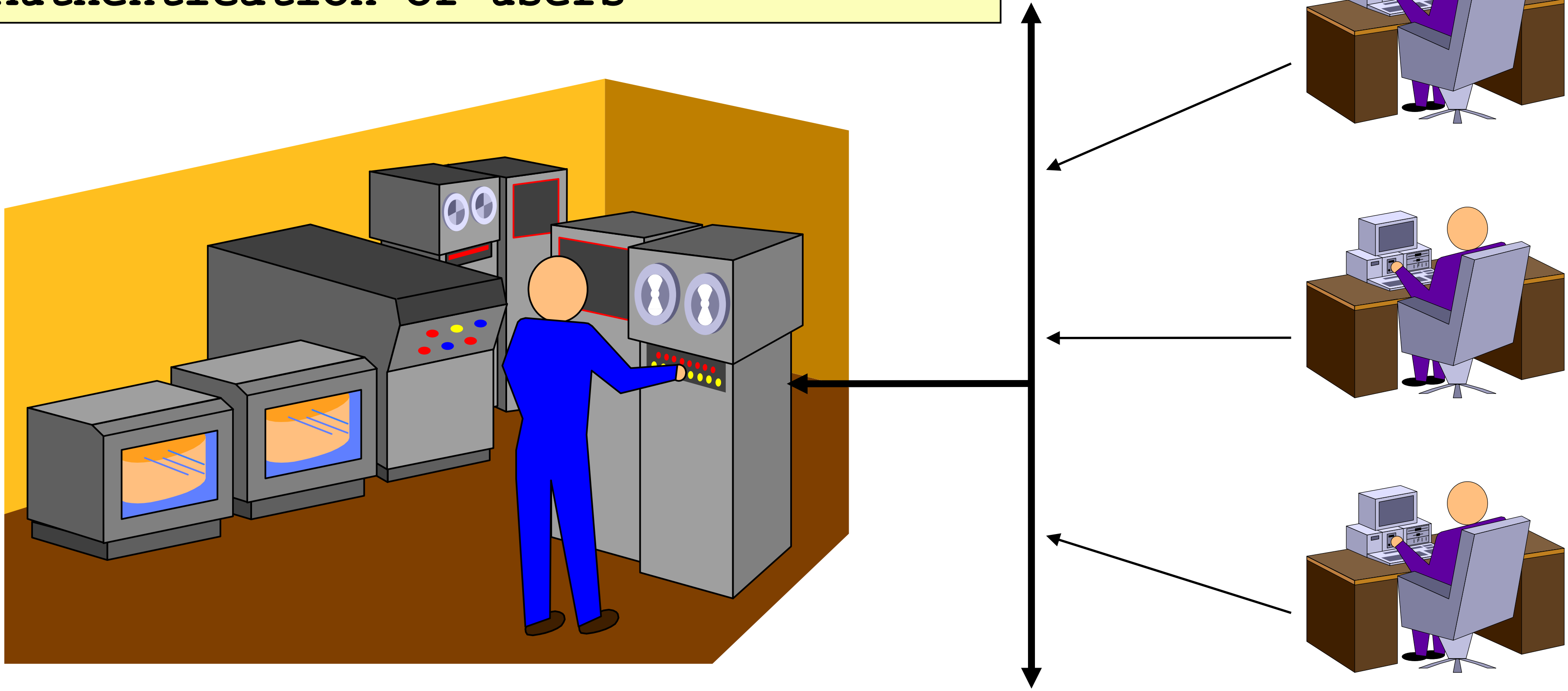
Interception : Unauthorized access to some computer resource

Modification : Illegal or accidental change (tampering) with a resource

Fabrication : Creation of illegal or incorrect resources

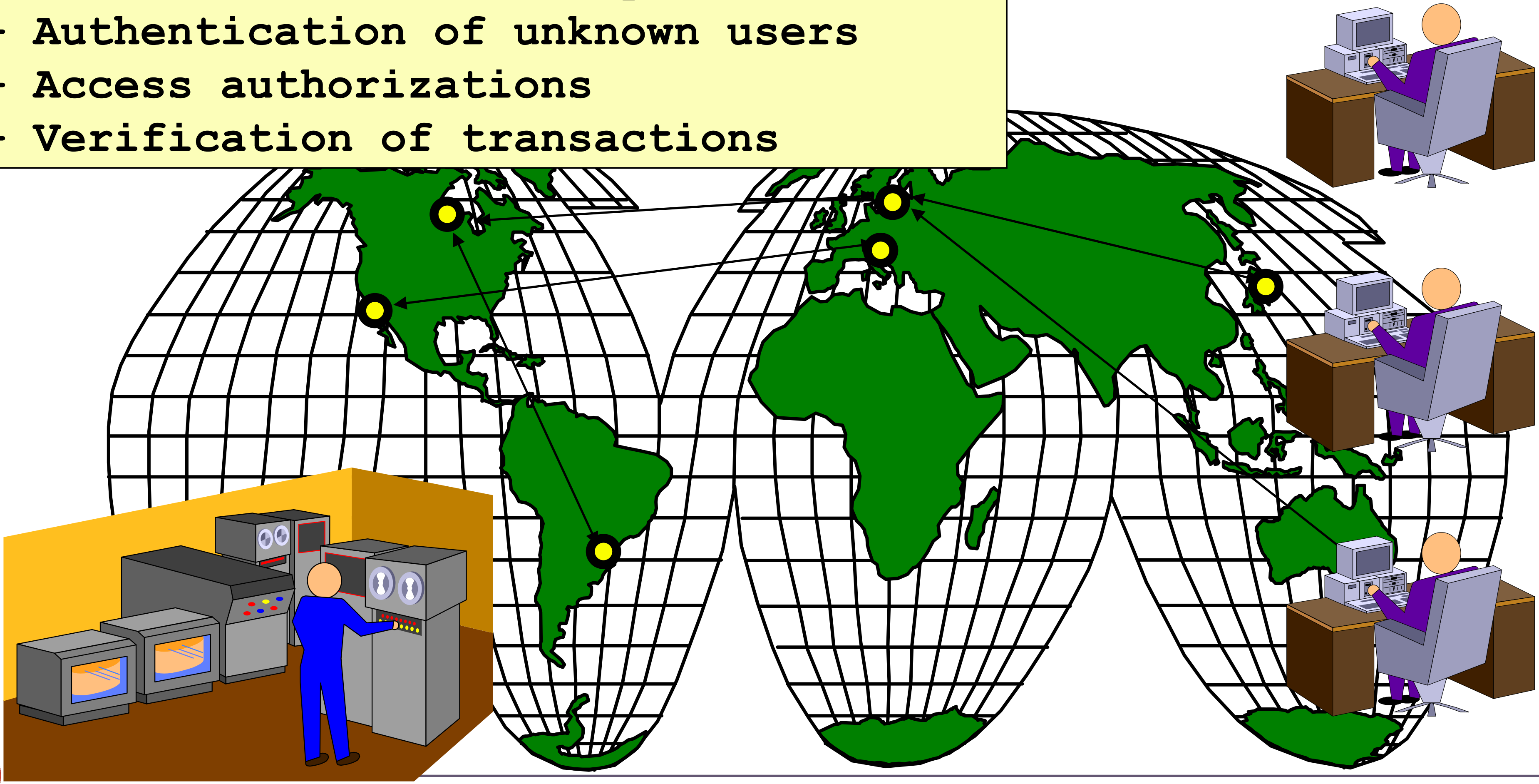
Threats with a single system

- Illegal access to a system
- Authentication of users



Threats with international networks

- Communications security
- Authentication of unknown users
- Access authorizations
- Verification of transactions



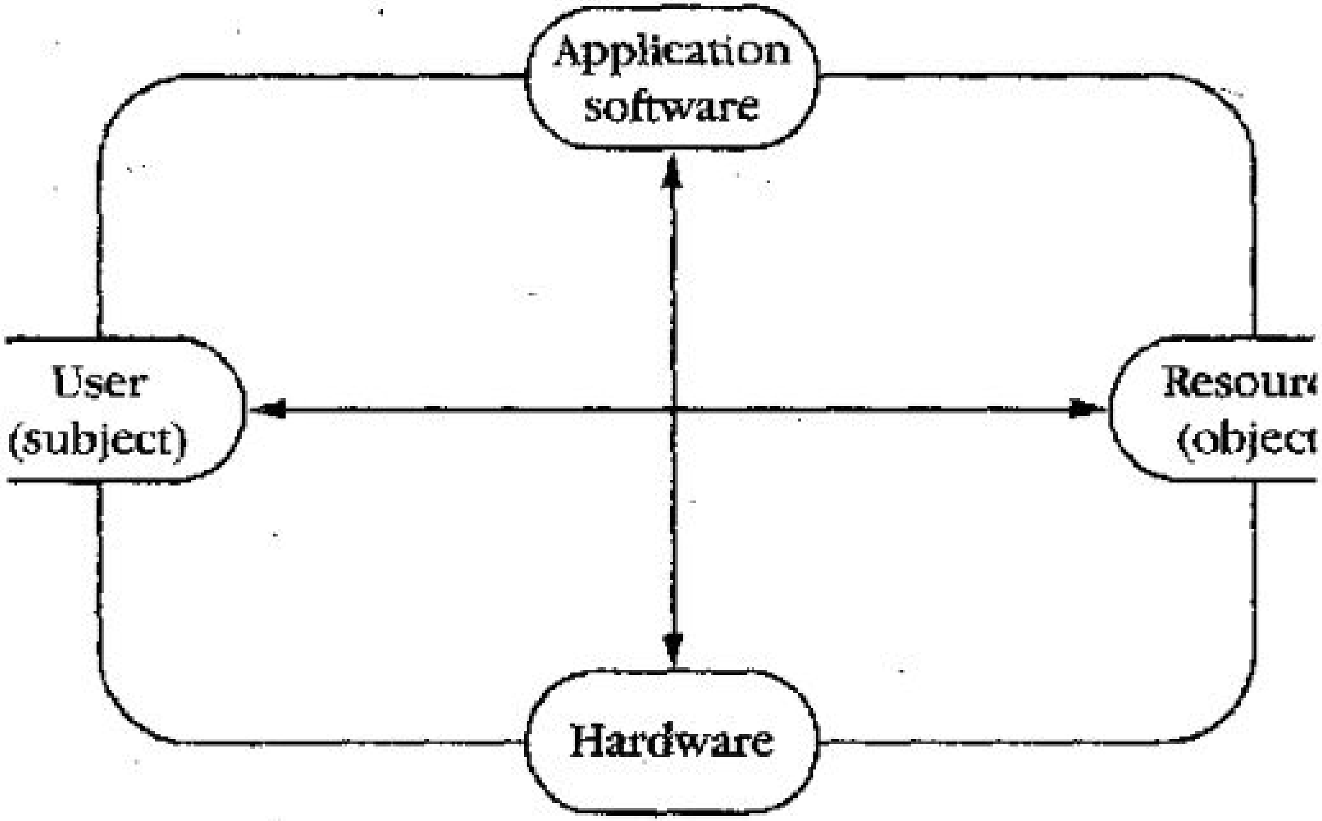
Security is not always about locks, firewalls, virus scanner and hardware

- Public Image often gets in the way of defeats security.
  - Would you deposit your money in a bank that just revealed that it lost fifteen million dollars due to a computer security oversight?
  - Things like this probably happen a lot more often than we care to have nightmares about.

So what does information security concern itself with?

- The entire system:
  - Hardware
  - Software
  - Storage media
  - Data
  - Memory
  - People
  - Organizations
  - Communications

The Dimensions of Information Security

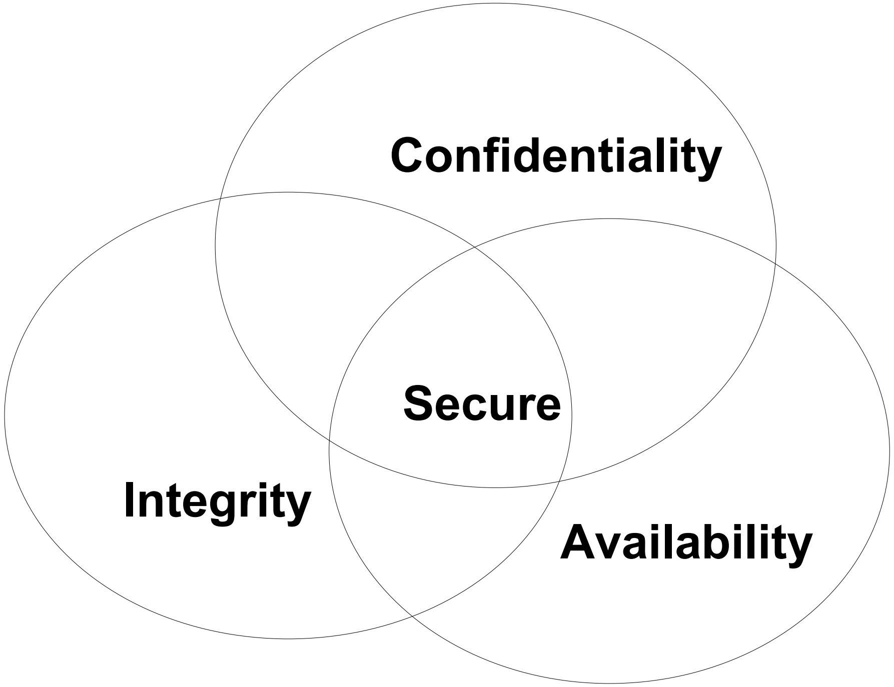


Security Goals (Requirements)

- What makes a “secure” system?
  - Financial “Security” requirements
  - Home “security”
  - Country “security”
  - Physical “security”
  - Computer “security”
- All these concepts of security have different requirements. We are, of course, interested mostly on information security; which requires three items.

Presence of all three

- The presence of all three things yields a secure system:



Thing one:

- Confidentiality:

  Computer related assets are only available to authorized parties. Only those that should have access to something will actually get that access.

  - "Access" isn't limited to reading. But also to viewing, printing or...
  - Simply even knowing that the particular asset exists (steganography)

  – Straight forward concept but very hard to implement.

Thing two:

- Integrity

  Can mean many things: Something has integrity if it is:

  - Precise
  - Accurate
  - Unmodified
  - Consistent
  - Meaningful and usable

Integrity

- Three important aspects towards providing computer related integrity:
  - Authorized actions
  - Separation and protection of resources
  - Error detection and correction.
- Again, rather hard to implement; usually done so through rigorous control of who or what can have access to data and in what ways.

Thing three:

- Availability
  - There is a timely response to our requests
  - There is a fair allocation of resources (no starvation)
  - Reliability (software and hardware failures lead to graceful cessation of services and not an abrupt crash)
  - Service can be used easily and in the manner it was intended to be used.
  - Controlled concurrency, support for simultaneous access with proper deadlock and access management.

Principles of Information Security

Confidentiality . . .

Integrity

Availability

Functionality

Threats to Data and Programs: illegal read, illegal access, data (files) deletion, illegal users, criminal acts, sabotage, etc.

Principles of Information Security

Confidentiality

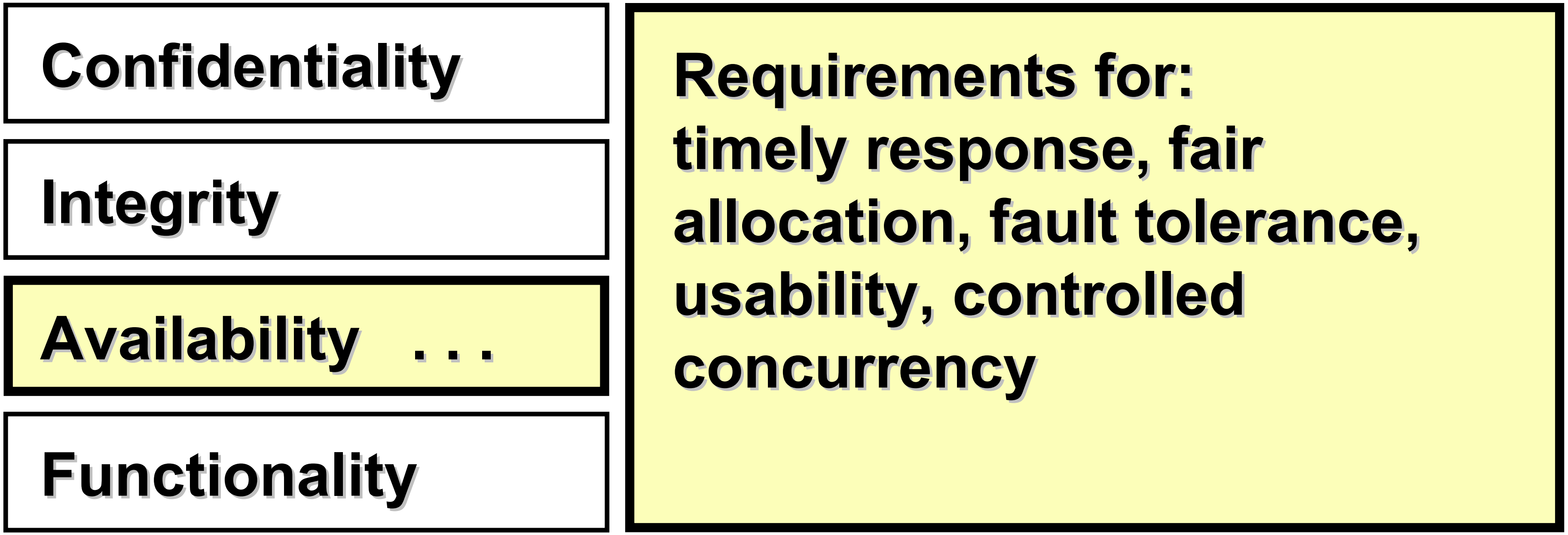
Integrity . . .

Availability

Functionality

Threats to software and data: technical errors, software errors, processing errors, transmission correctness, etc.

Principles of Information Security



Confidentiality

Integrity

Availability . . .

Functionality

Requirements for:
timely response, fair allocation, fault tolerance, usability, controlled concurrency

Principles of Information Security

Confidentiality

Integrity

Availability

Functionality . . .

New functions needed for electronic data transactions: authentication, digital signature, confidentiality, and others

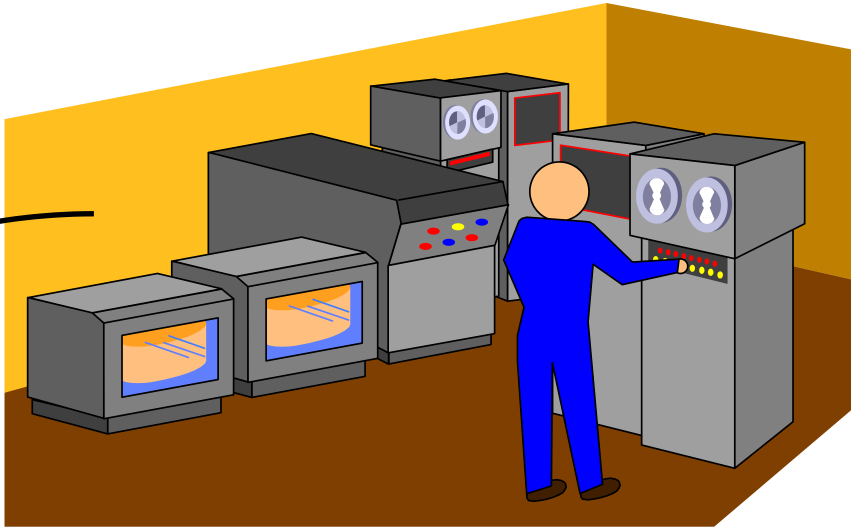
. . . in Single Systems

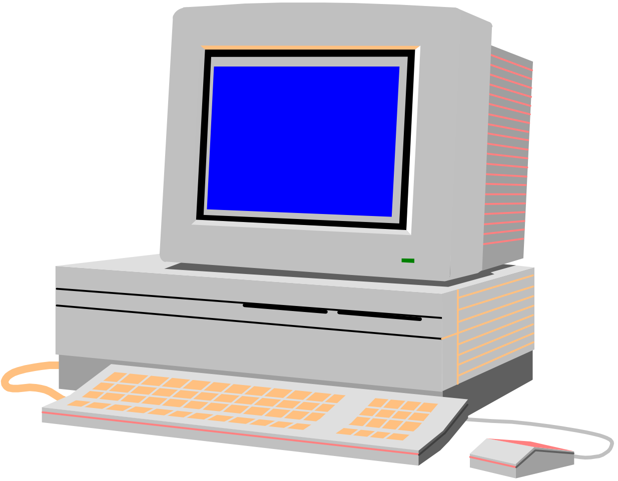
Confidentiality

Integrity

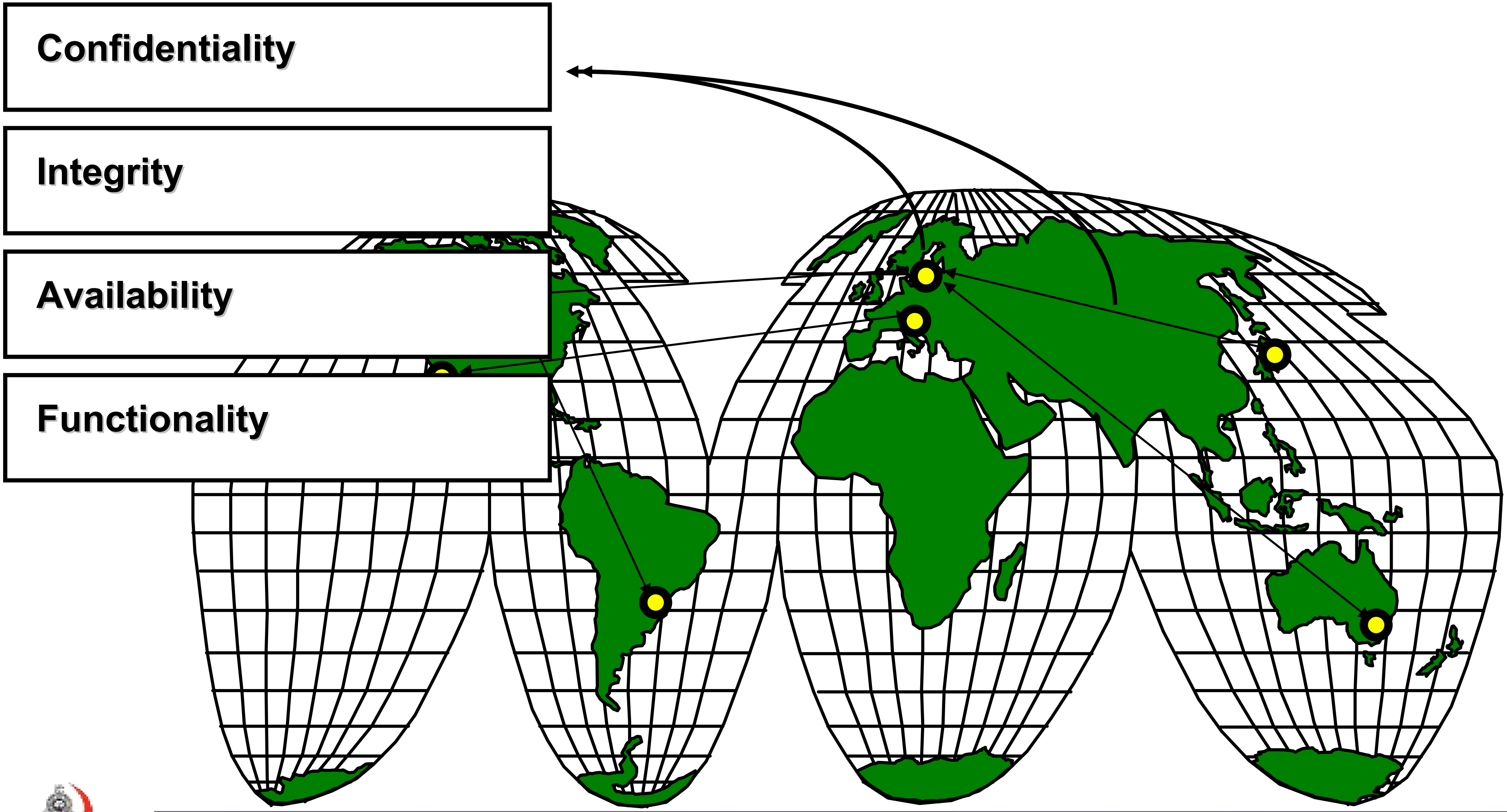
Availability

Functionality





. . . in Global Networks



Confidentiality

Integrity

Availability

Functionality

“Definition” of Information System Security

Information System security
are methods and technologies
for protection, integrity, availability,
authenticity and extended functionality
of software and data

Goals and Principles

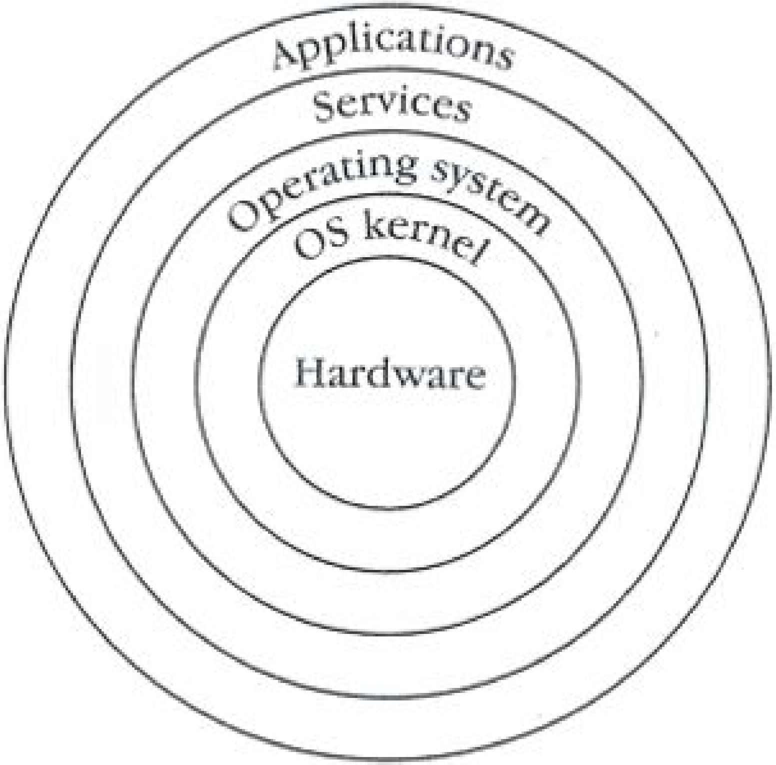
Simplicity . . . to understand, develop and use

Consistency . . . policies and existing schemes

Scalability . . . in a single WS, LAN, WAN, Internet

Independence . . . of technologies

Hierarchy Model of Protection Mechanisms



Protection Methods

Encryption

SW & HW Controls

Policies

Physical controls

Protection Methods

Encryption . . .

SW & HW Controls

Policies

Physical controls

Effective for:
confidentiality,
users and messages
authentication, access
control

Protection Methods

Encryption

SW & HW Controls

Policies

Physical controls

Available methods: software and hardware controls (internal SW, OS controls, development controls, special HW devices)

Protection Methods

Encryption

SW & HW Controls

Policies . . .

Physical controls

Precise specifications: special procedures, security methods, security parameters, organizational issues

Protection Methods

Encryption

SW & HW Controls

Policies

Physical controls

Measures for:
isolation of equipment,
access to equipment,
authorization for personnel,
backup and archiving

“Definition” of Information Security

Information security
are methods and technologies
for protection, integrity, availability,
authenticity and extended functionality
of computer programs and data

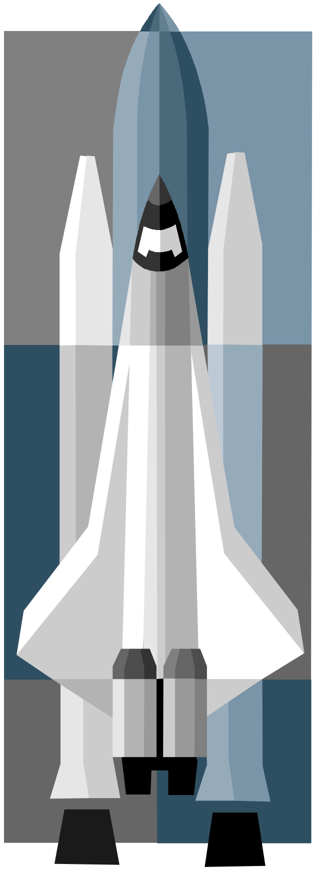
Sec_rity is not Complete without U

You, as a Device User, have to make your contribution to Information Security: **You are responsible for the security and protection** of your computers, the operating systems you run, the application you install, the software you program, the data you own - and the services and systems you manage.

Brute Force Search

- Always possible to simply try every key
- Most basic attack, proportional to key size
- Assume either know/recognize plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/µs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

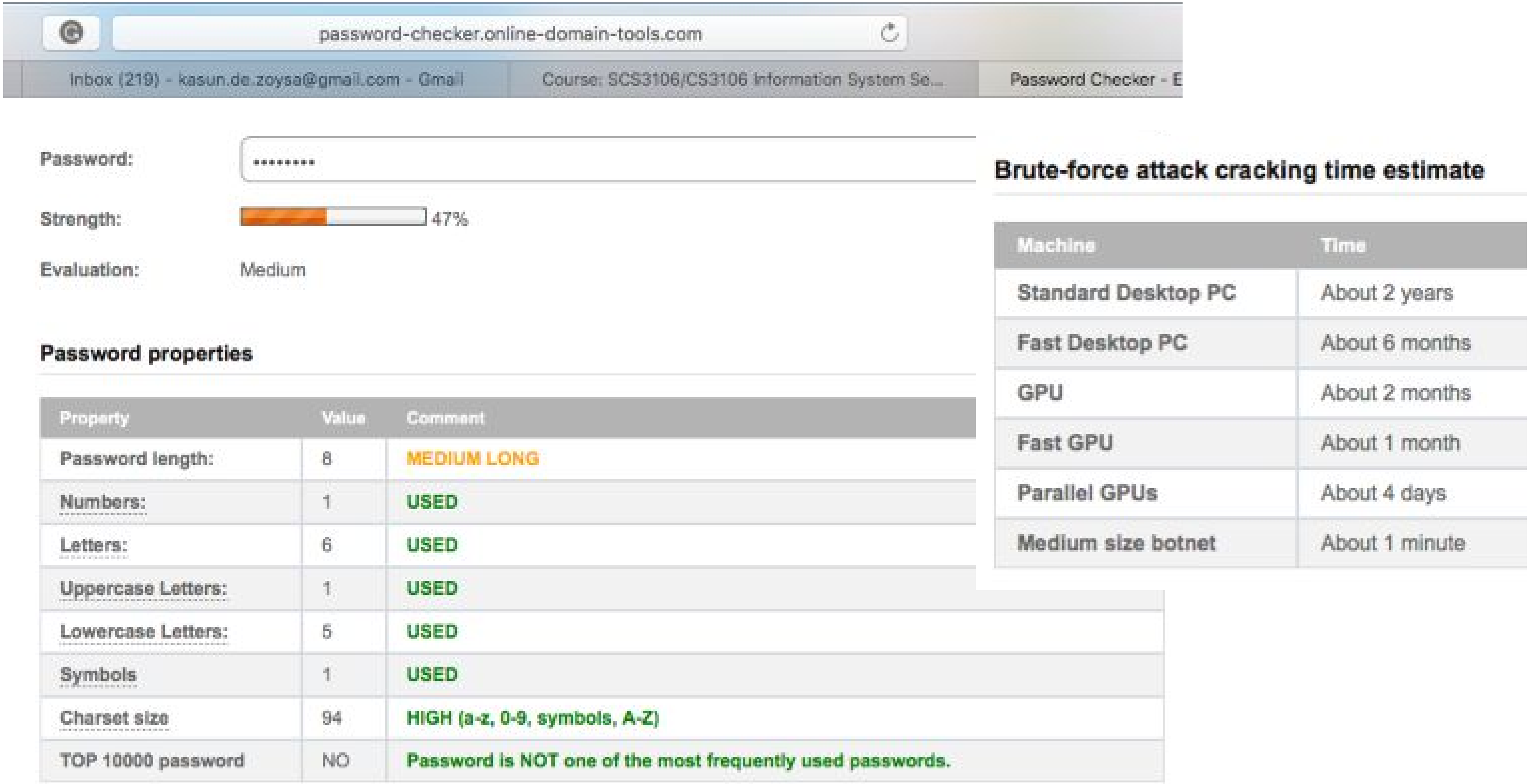


Unconditional/Computational Security

Unconditional security
no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

Computational security
given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken

http://password-checker.online-domain-tools.com



password-checker.online-domain-tools.com
Inbox (219) - kasun.de.zoysa@gmail.com - Gmail
Course: SCS3106/CS3106 Information System Se...
Password Checker - E

Password: •••••••••

Strength: 47%

Evaluation: Medium

Password properties

Property	Value	Comment
Password length:	8	MEDIUM LONG
Numbers:	1	USED
Letters:	6	USED
Uppercase Letters:	1	USED
Lowercase Letters:	5	USED
Symbols	1	USED
Charset size	94	HIGH (a-z, 0-9, symbols, A-Z)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 2 years
Fast Desktop PC	About 6 months
GPU	About 2 months
Fast GPU	About 1 month
Parallel GPUs	About 4 days
Medium size botnet	About 1 minute

Discussion