Introduction to Cybersecurity

Kasun De Zoysa

Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka

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.

Cyberspace

- The notional environment in which communication over computer networks occurs.
- The physical world is static, well-defined, and incremental with fixed contours.
- On the other hand, the cyberspace is dynamic, undefined, and exponential.

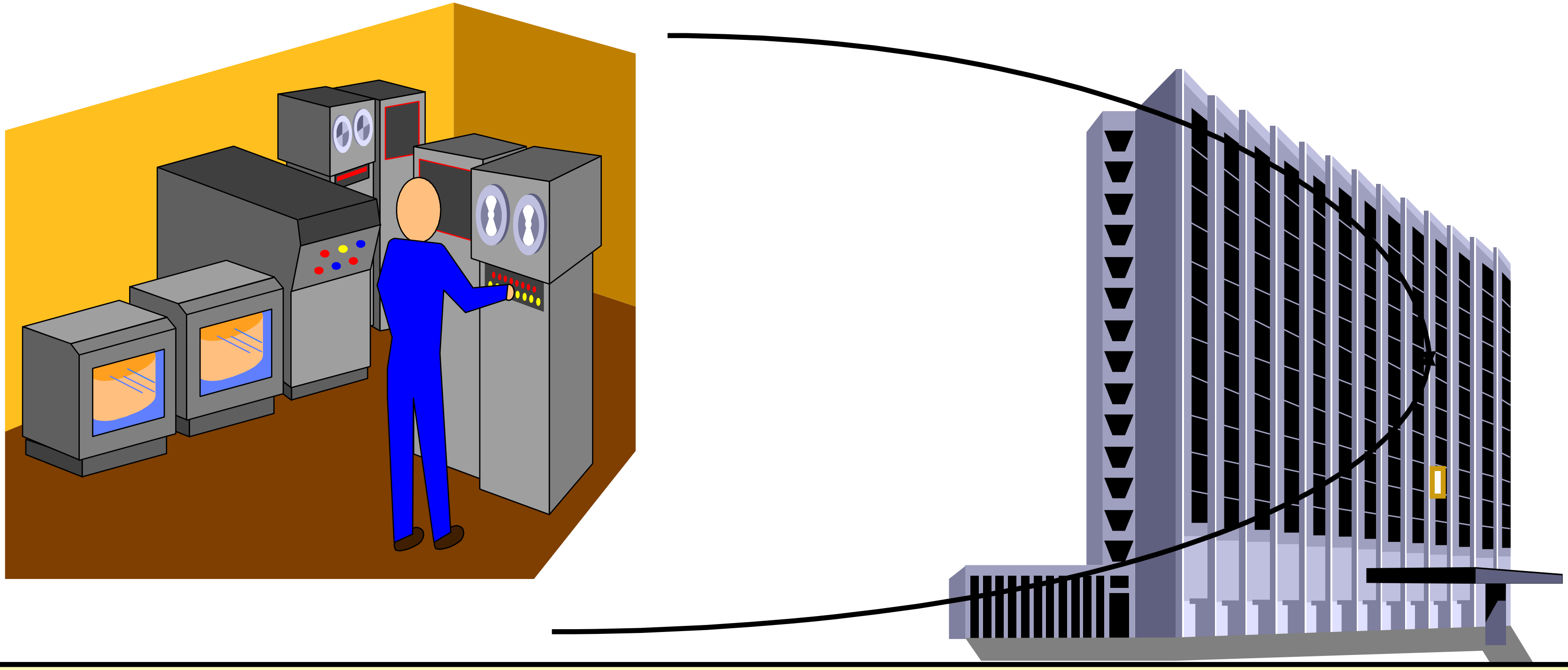
Cybersecurity

- 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.

Cyberattack

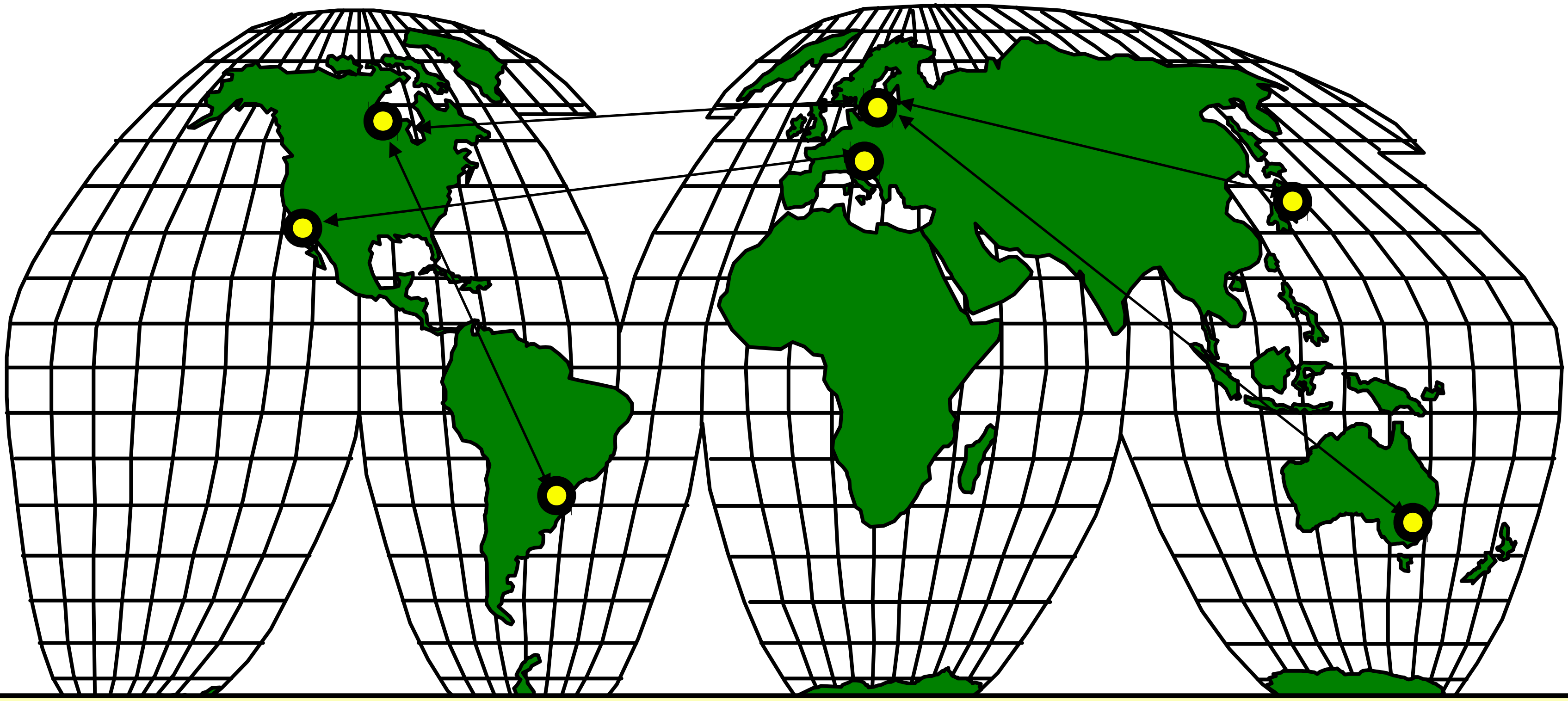
- A cyberattack is any type of offensive maneuver that targets information systems, infrastructures, computer networks, or personal computer devices.
- An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.
- Depending on context, cyberattacks can be part of cyberwarfare or cyberterrorism.

Past Situation (Single Systems)



Physical security and control of access to computers

Current Situation (Int’l networks and open systems)



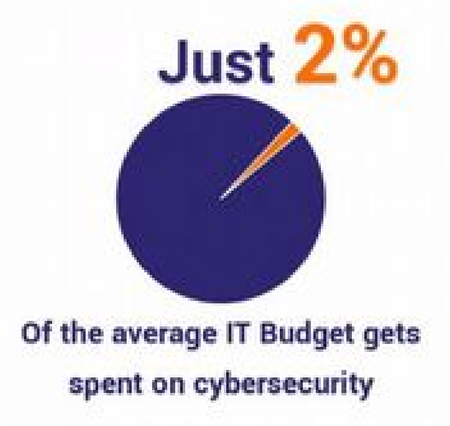
Authentication, message protection, authorization

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

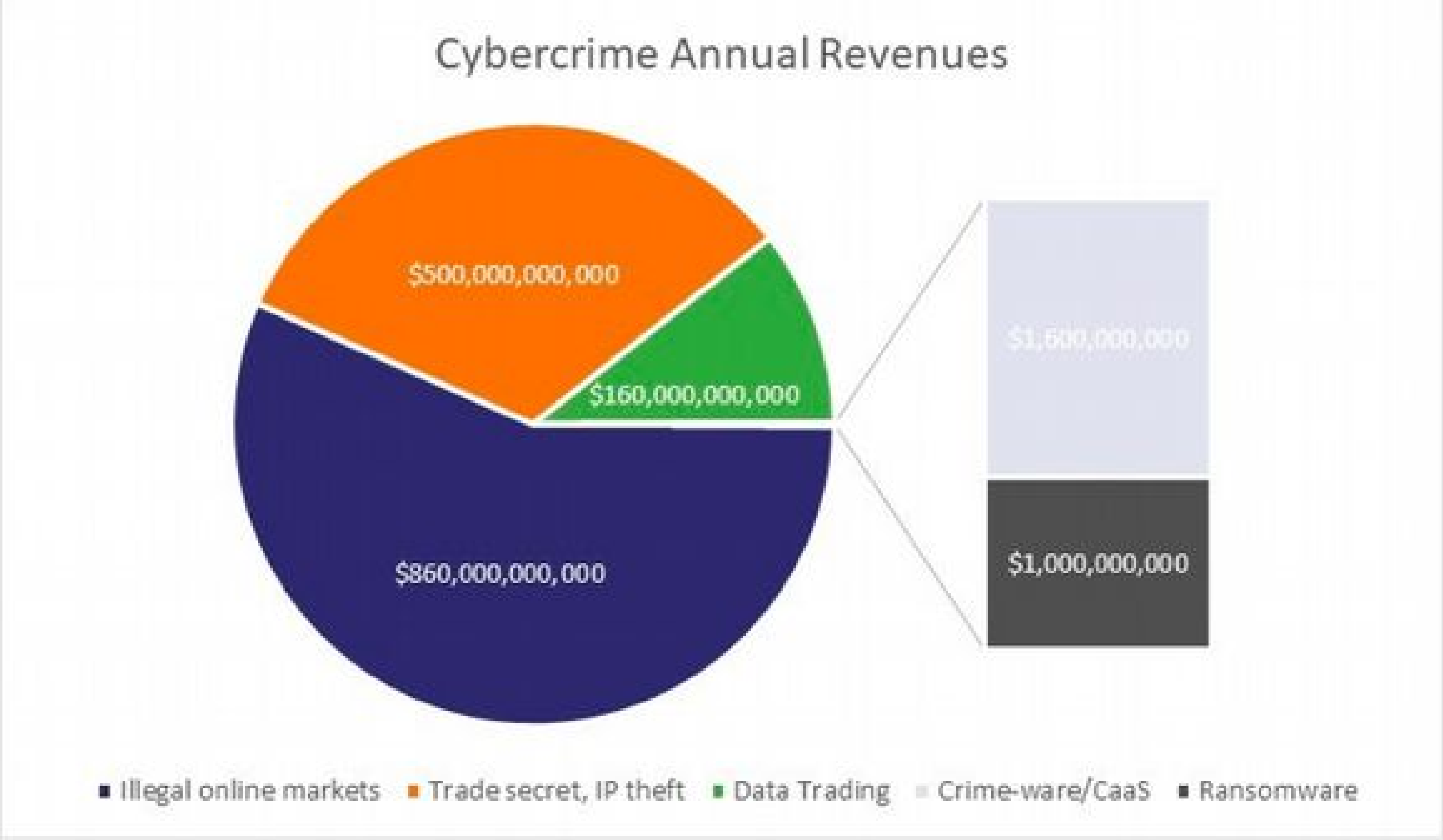
Eye-Opening Cyber Security Statistics for 2019

- 70% of employees don’t understand cybersecurity.
- 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



https://www.thesslstore.com/blog/2018-cybercrime-statistics/

Cybercrime will create over $1.5 trillion in profits in 2018



https://www.thesslstore.com/blog/2018-cybercrime-statistics/

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 . . .

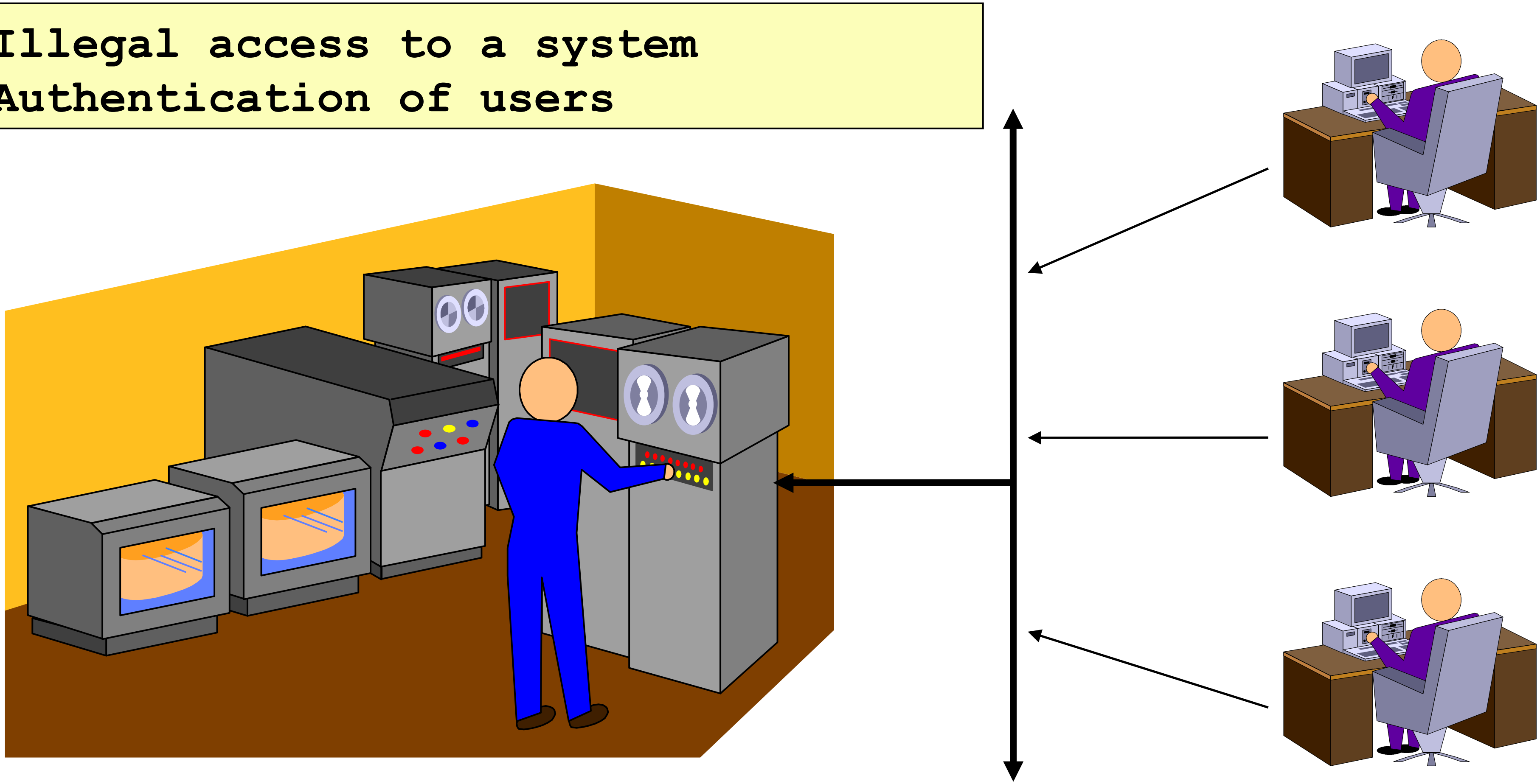
Special requirements: authentication in open networks, authorization, message integrity, non-repudiation, special transactions

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.

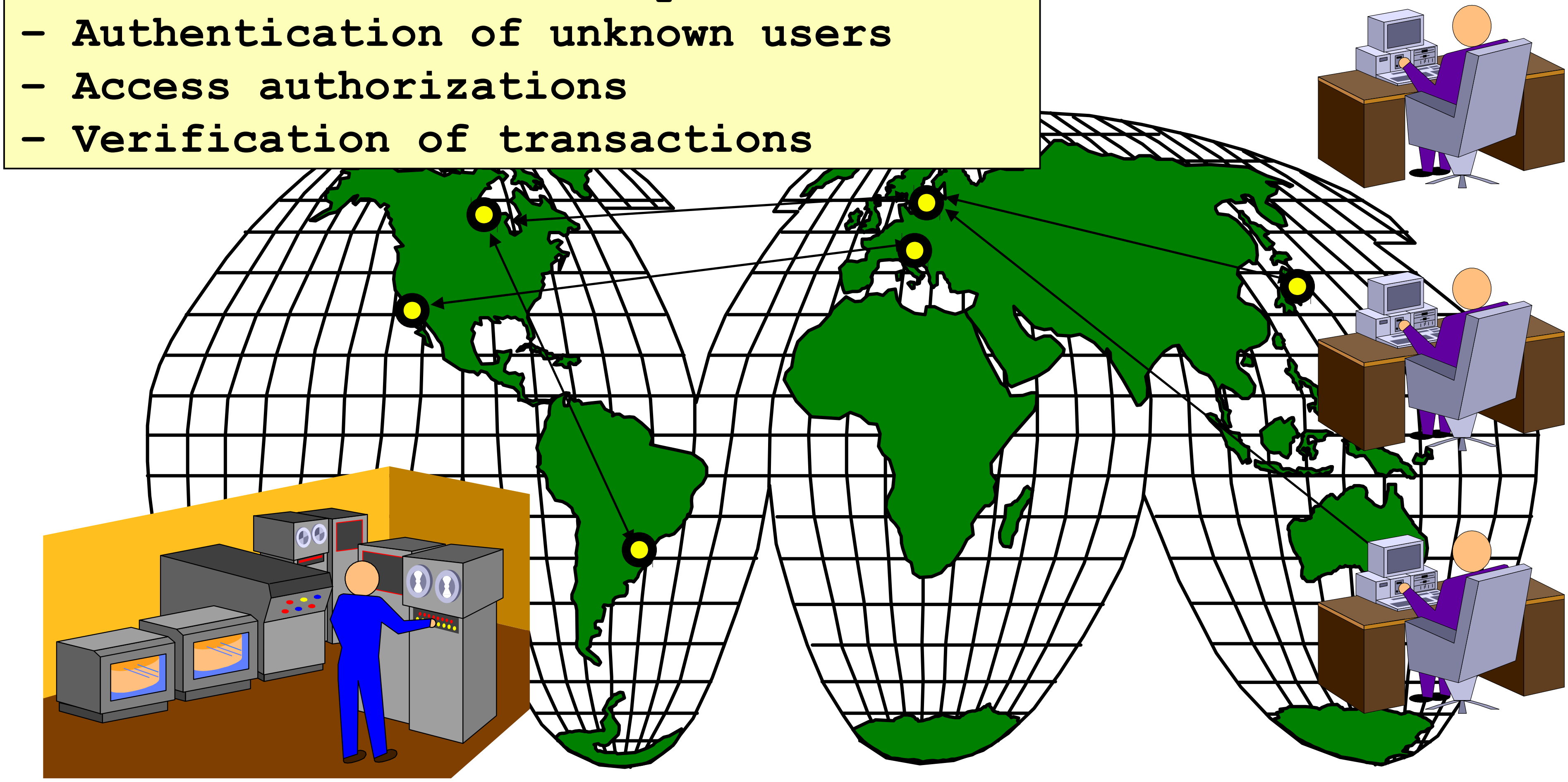
Threats with a single system

- Illegal access to a system
- Authentication of users



Threats with international networks

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



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

So what does Cybersecurity concern itself with?

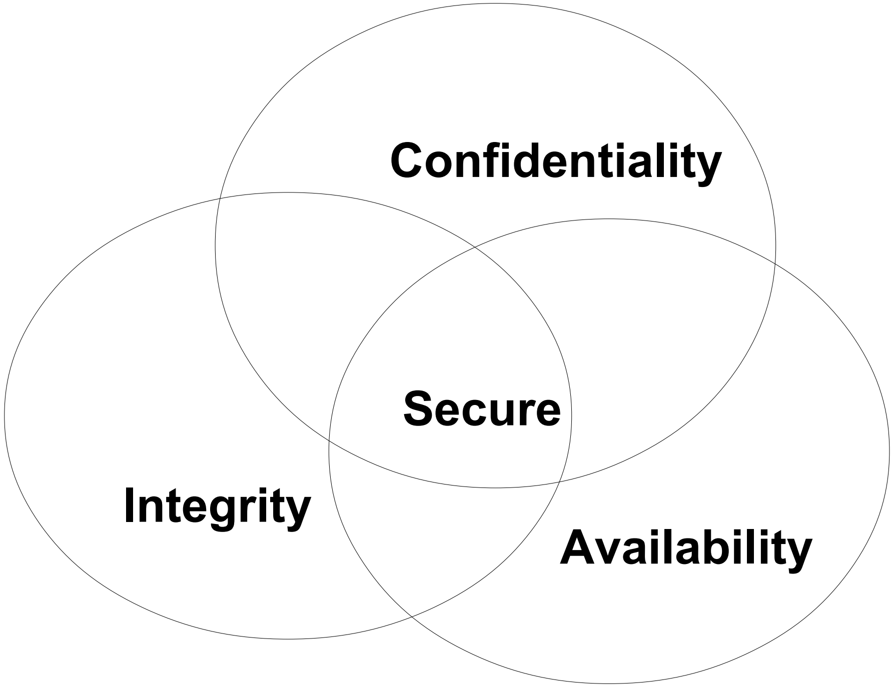
- The entire system:
  - Hardware
  - Software
  - Storage media
  - Data
  - Memory
  - People
  - Organizations
  - Communications

Cybersecurity 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 computer 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

Thing three:

- Availability
  - There is a timely response to our requests
  - There is a fair allocation of resources
  - Reliability (software and hardware failures lead to graceful cessation of services)
  - 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 Cybersecurity

Confidentiality . . .

Integrity

Availability

Functionality

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

Principles of Cybersecurity

Confidentiality

Integrity . . .

Availability

Functionality

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

Principles of Cybersecurity

Confidentiality

Integrity

Availability . . .

Functionality

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

Principles of Cybersecurity

Confidentiality

Integrity

Availability

Functionality . . .

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

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

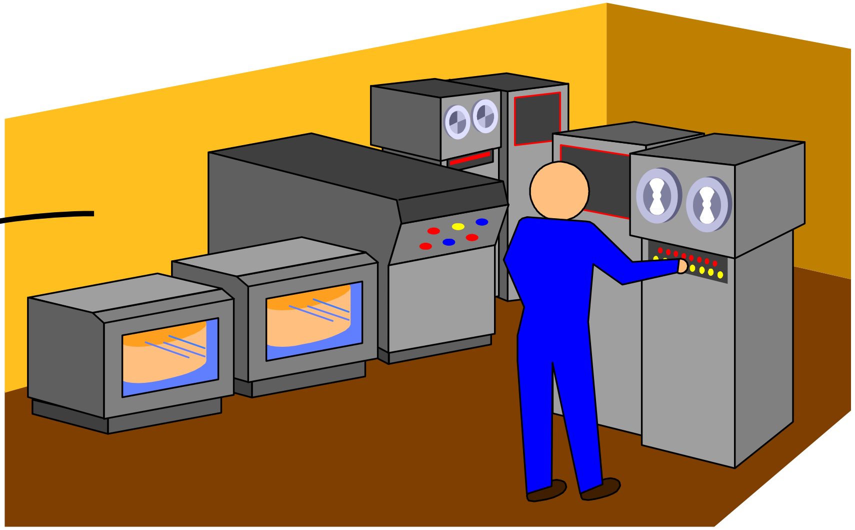
. . . in Single Systems

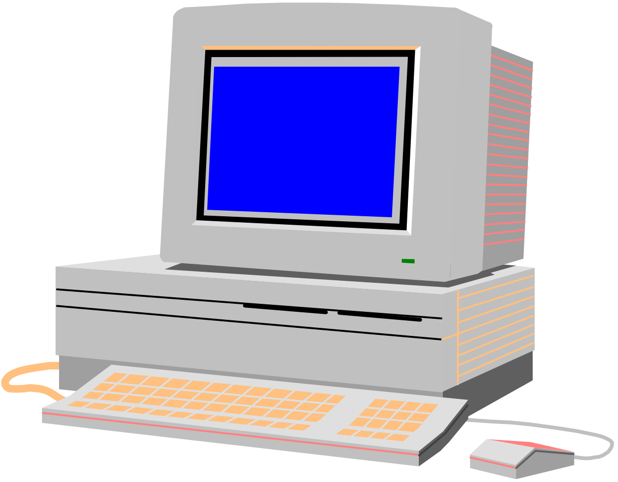
Confidentiality

Integrity

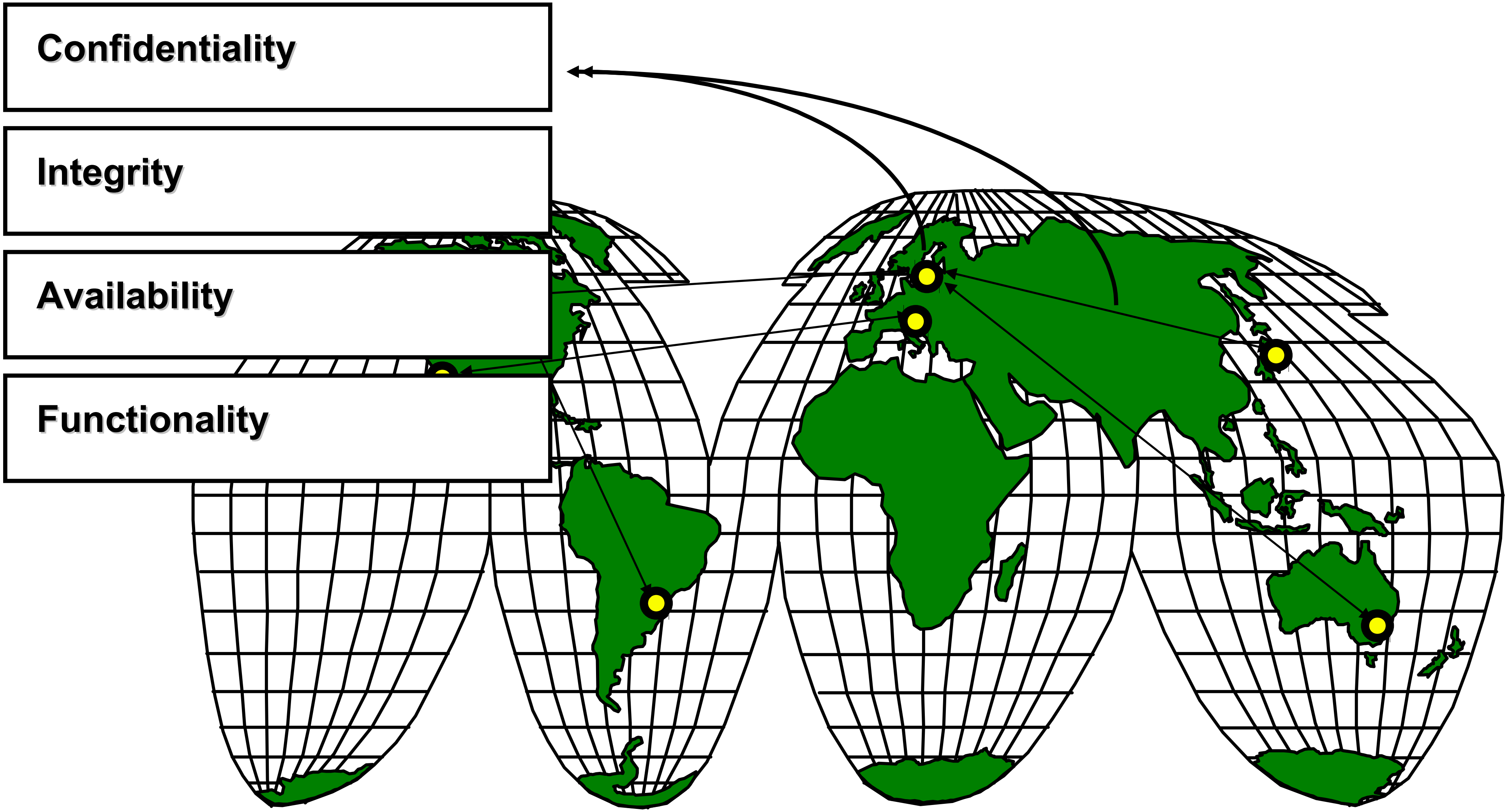
Availability

Functionality





. . . in Global Networks



Confidentiality

Integrity

Availability

Functionality

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

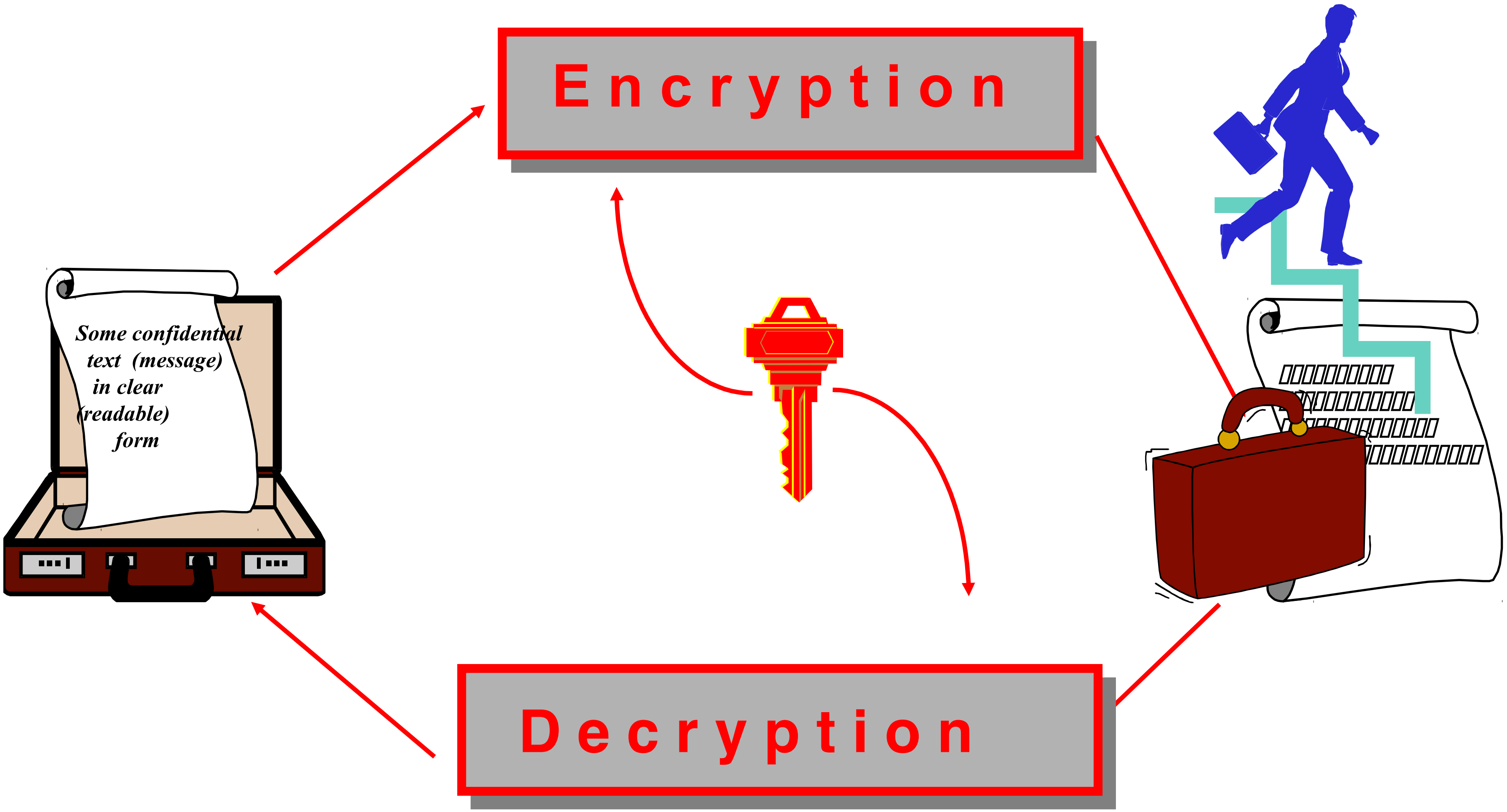
Physical controls

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

Cryptography

- **Encryption(Encipher)**
  - act of scrambling
- **Decryption(Decipher)**
  - descrambling with secret key
- **Key**
  - secret sequence governing en/deciphering

Symmetric key Cryptograms

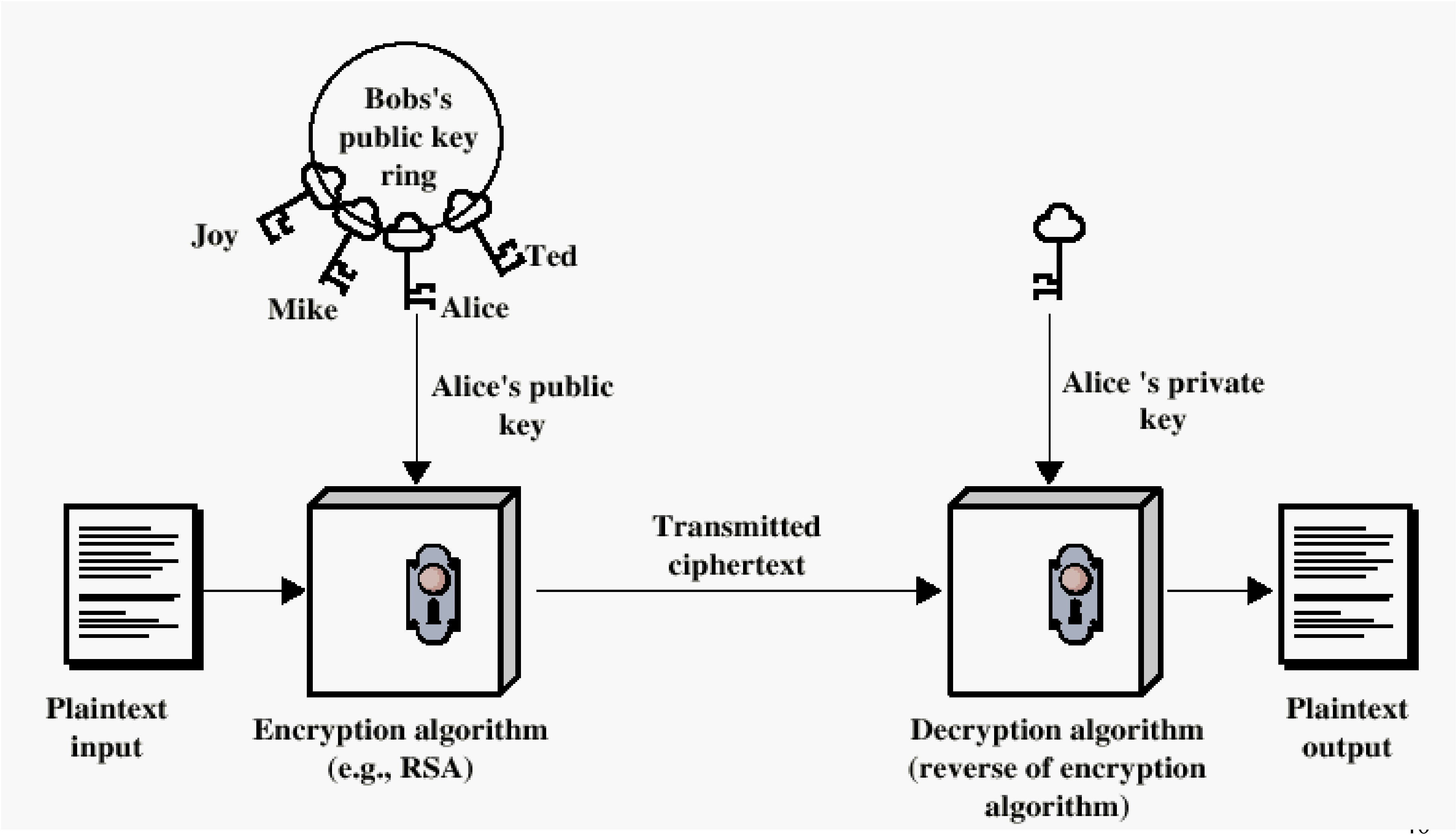


Encryption

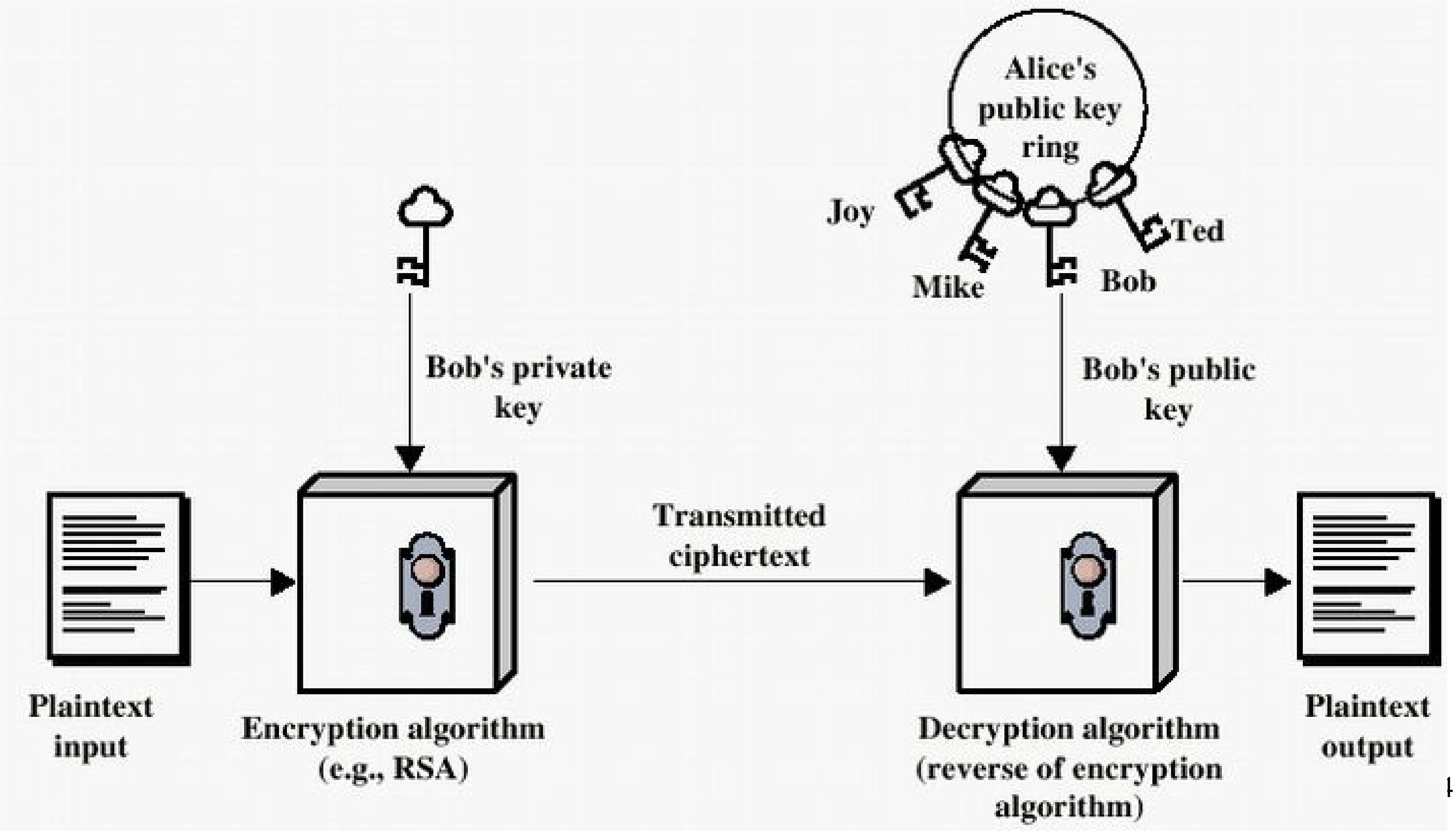
Decryption

Some confidential text (message) in clear (readable) form

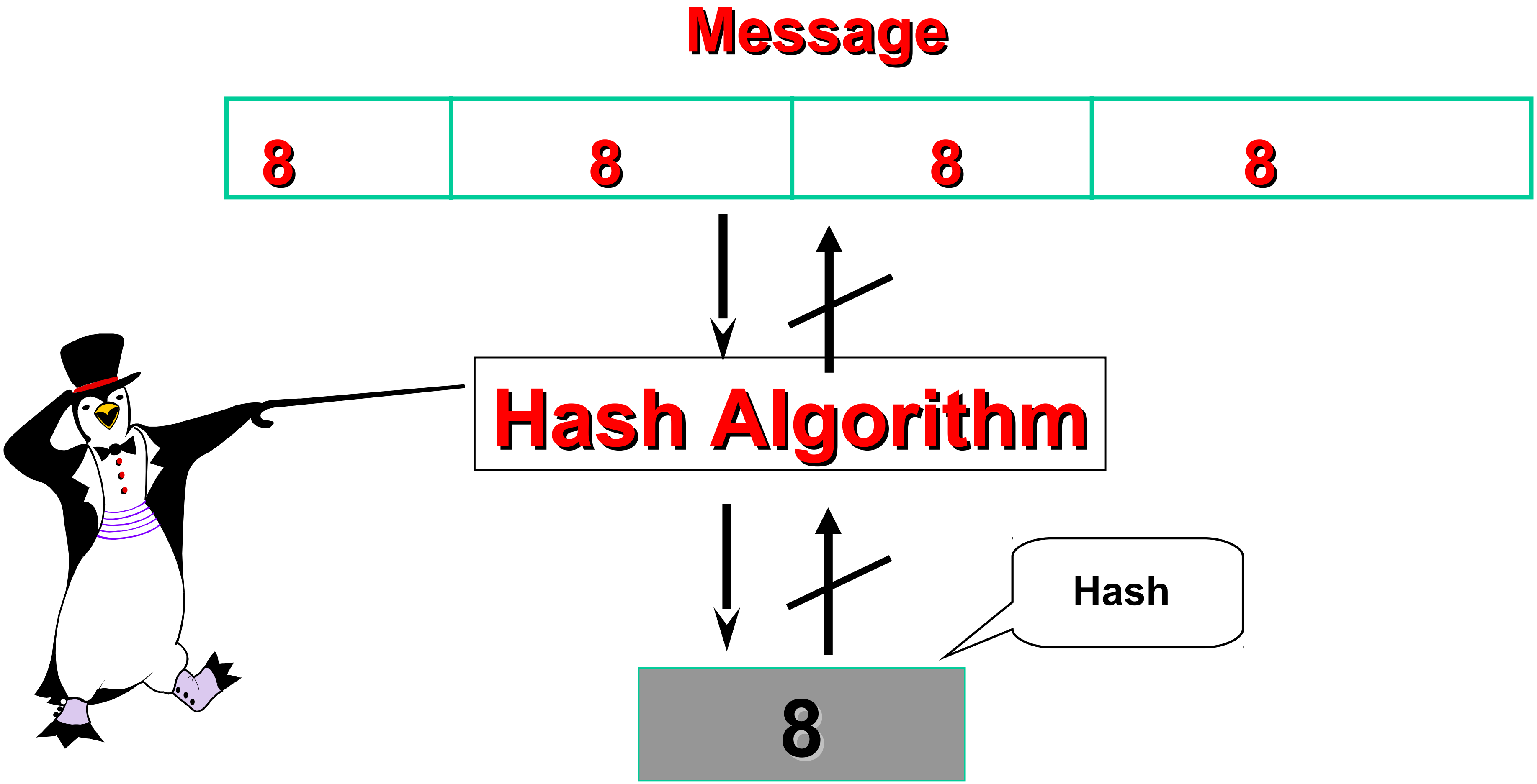
Encryption using Public-Key system



Authentication using Public-Key System



Hash Functions



Message

8 8 8 8

Hash Algorithm

Hash

8

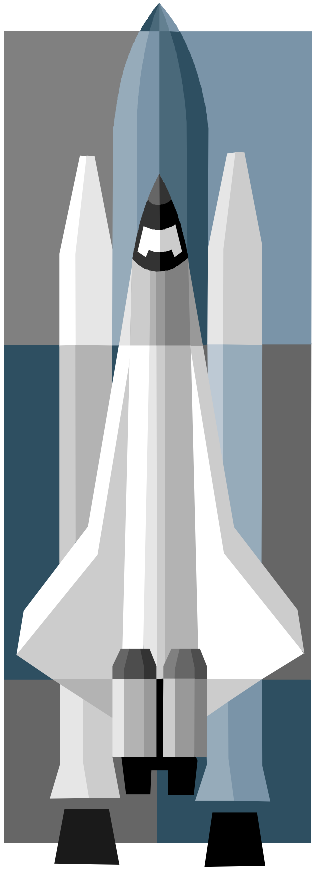
Cryptosystem

- **Confidentiality** To ensure that unauthorized parties cannot access the data, message or information
- **Authenticity** To ensure that the source / sender of the data, message or information is identifiable
- **Integrity** To ensure that the data. Message or Information was not modified during transmission
- **Nonrepudiation** To ensure that either party cannot deny sending or receiving the data, message or information

Brute Force Search

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

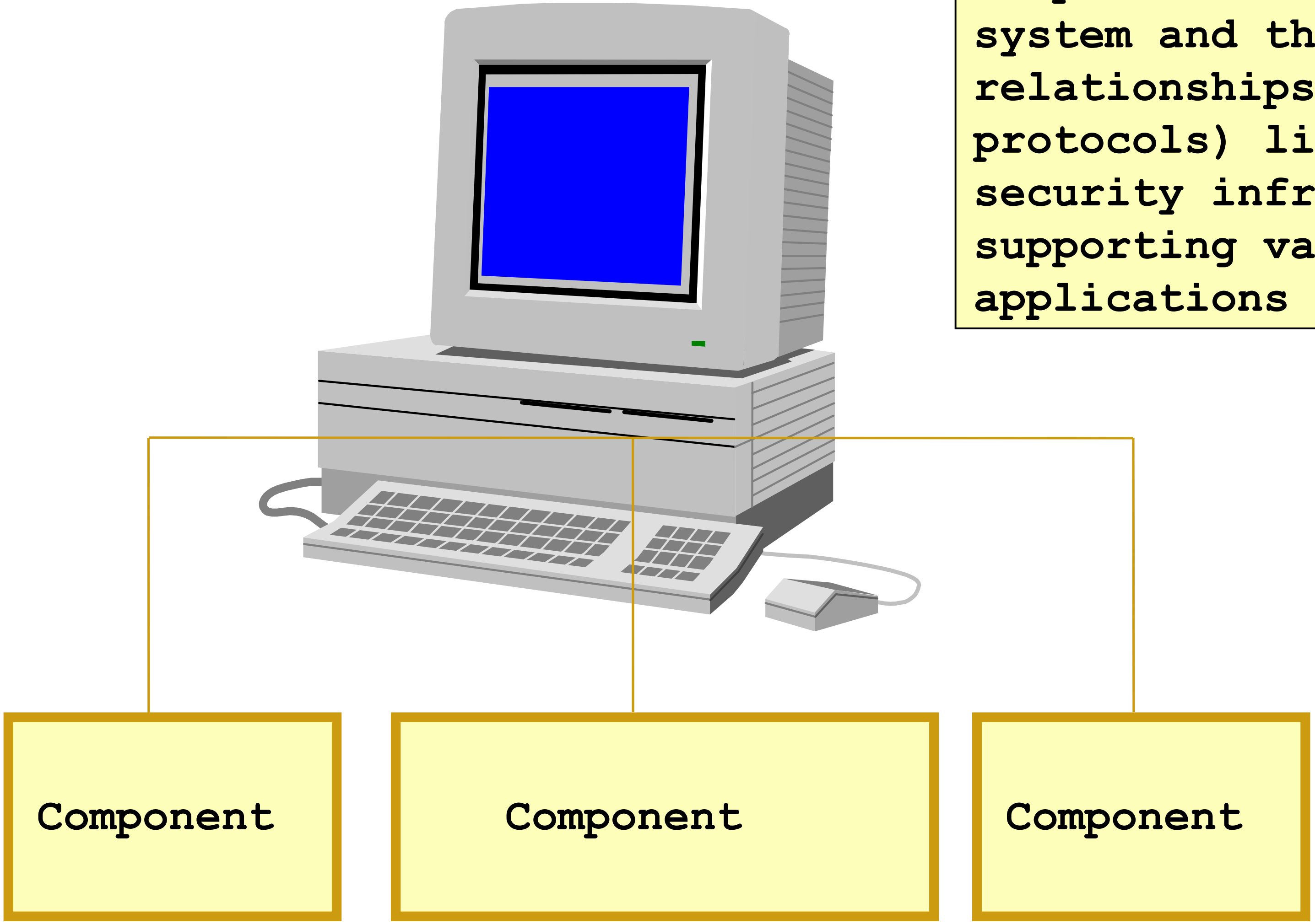
Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/µs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years



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

Security Reference Model

Security reference model are components of a security system and their relationships (security protocols) linked into security infrastructure, supporting various secure applications

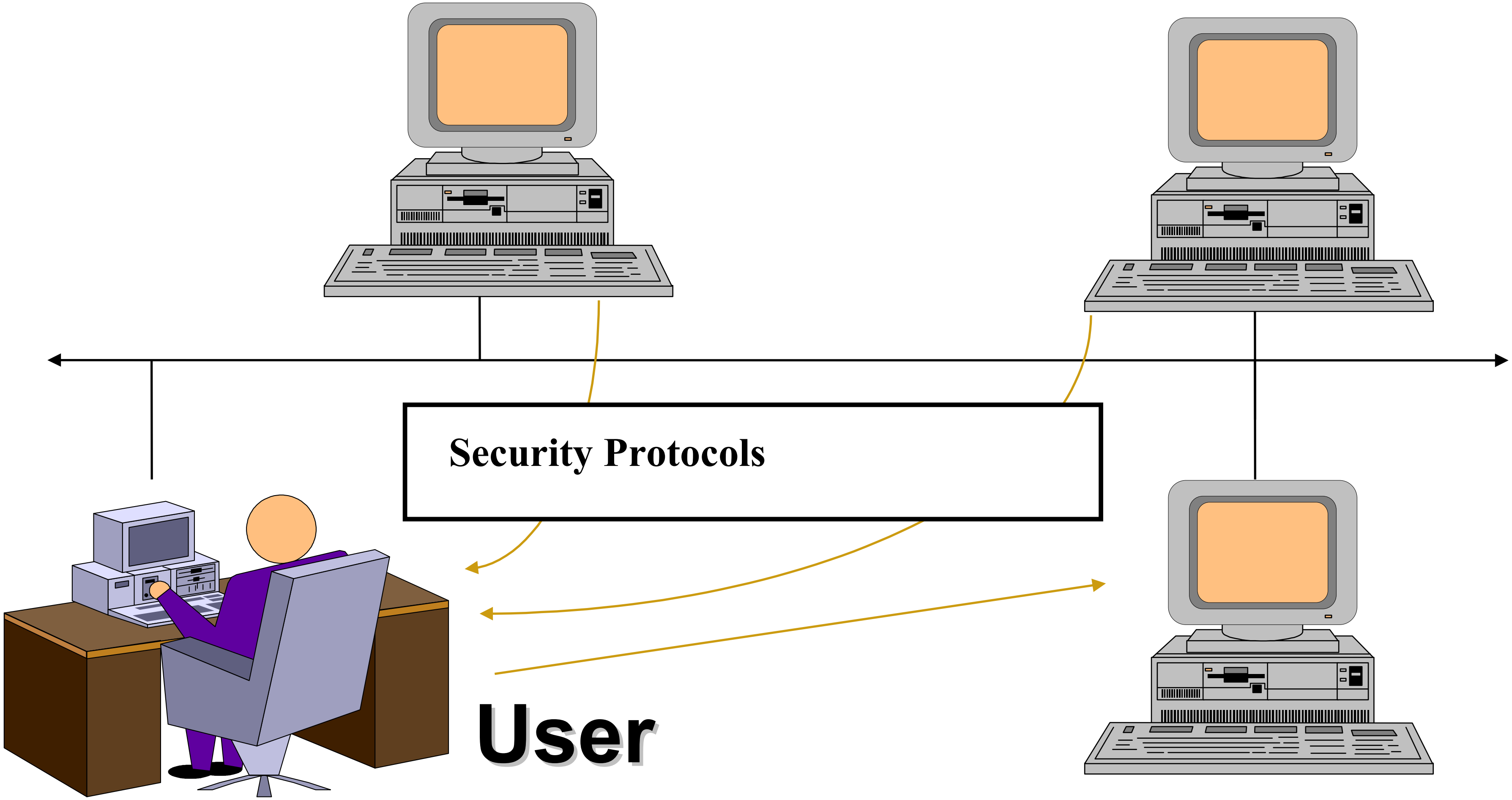


Component

Component

Component

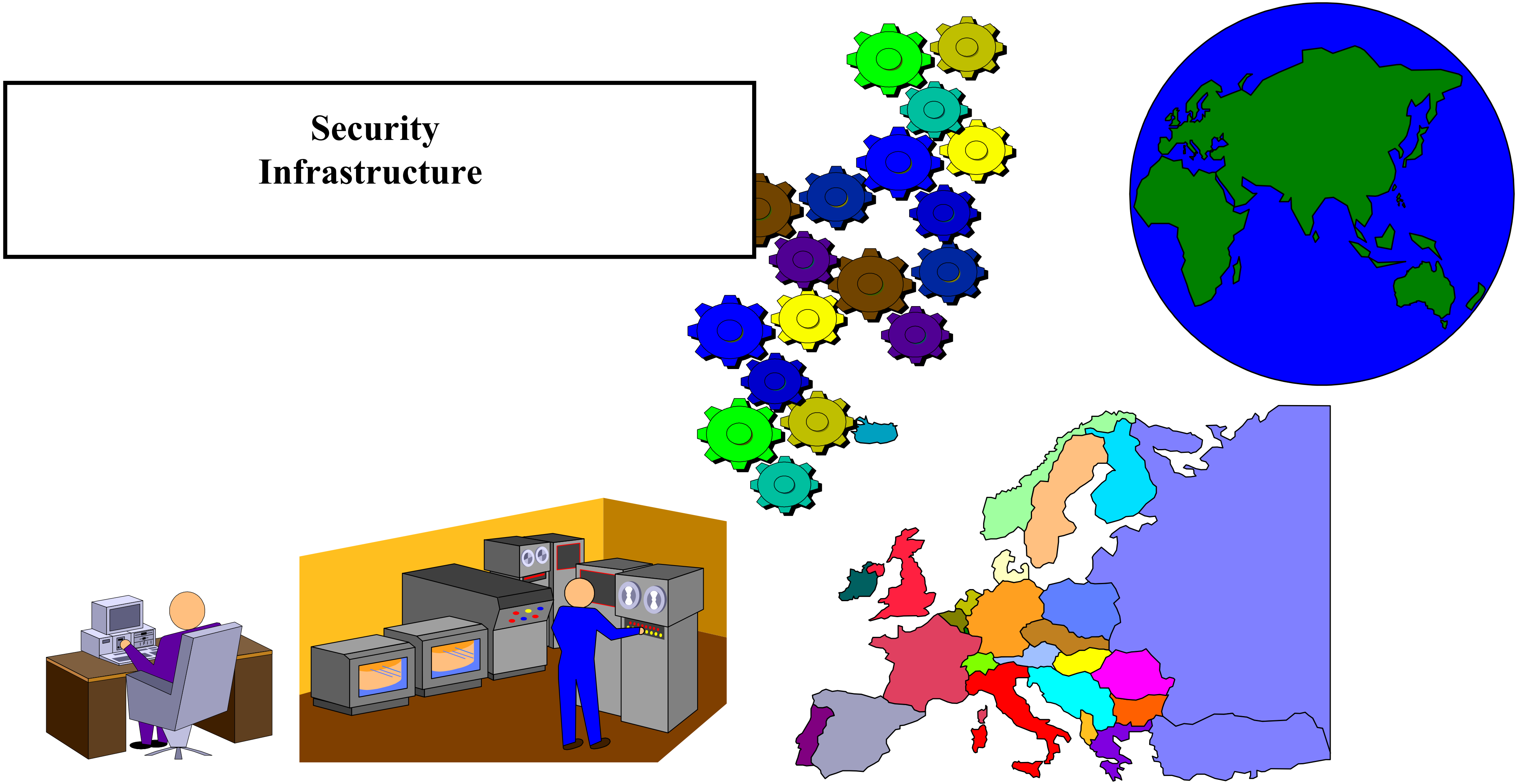
Security Reference Model



Security Protocols

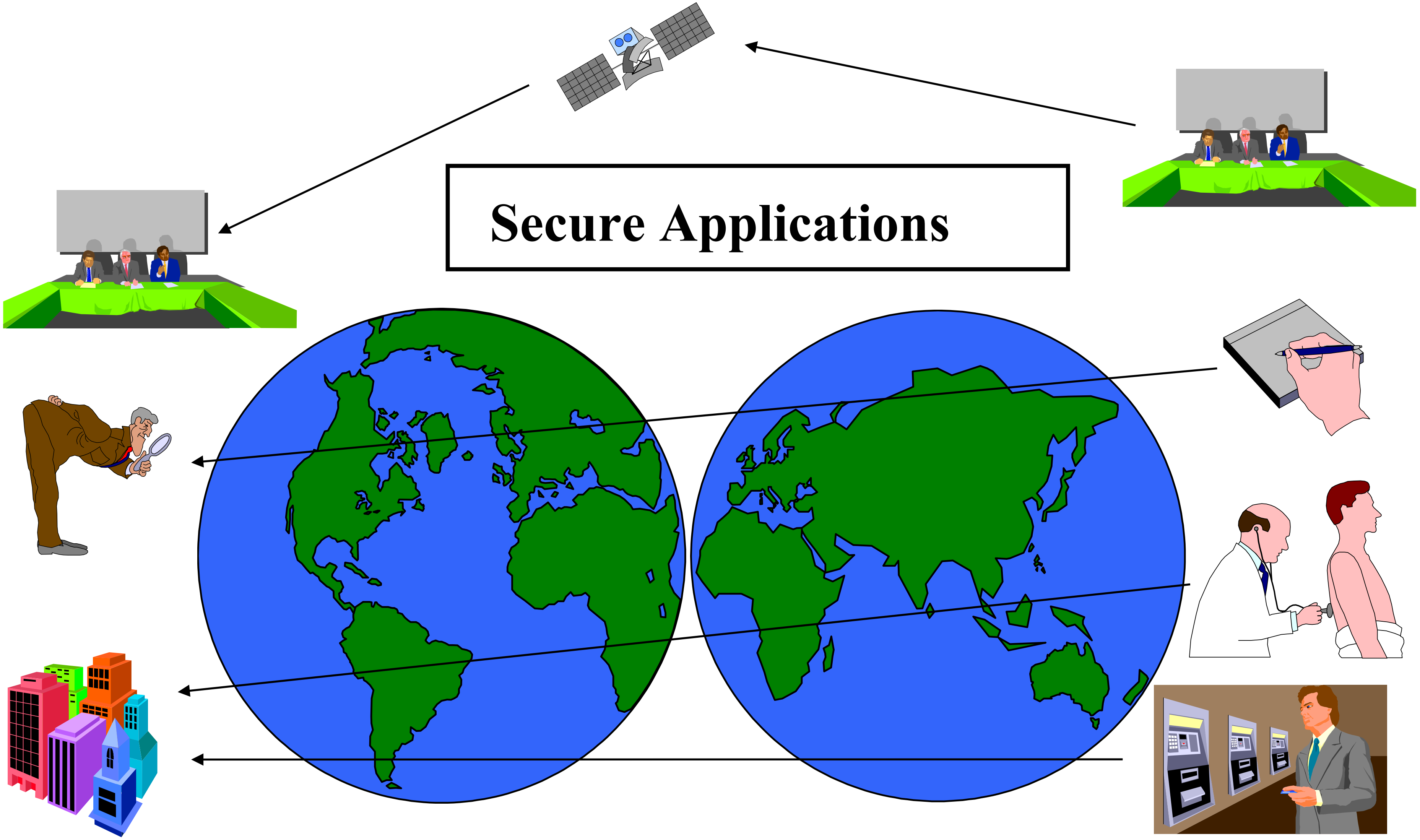
User

Security Reference Model



Security
Infrastructure

Security Reference Model



Secure Applications

Sec_rity is not Complete without U

You, as a Computer User, have to make your contribution to Cybersecurity: **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.

Dr. Kasun De Zoysa
e-mail: kasun@ucsc.cmb.ac.lk