Challenges of Securing Information

- **Security figures prominently in 21st century world**
  - Personal security
  - Information security (focused on protecting the electronic information of organizations and users)
- Securing information
  - No simple solution
  - Many different types of attacks
  - Defending against attacks often difficult

Information security continues to rank as the number one concern of IT managers and tens of billions of dollars are spent annually on information security, the number of successful attacks continues to increase.

Today's Security Attacks

- Examples of recent attacks
  - Fake anti-virus
  - Taking control of wireless cameras
  - ATM machine attacks (Malware called Ploutus)
  - Taking over Twitter accounts
  - Attackers using online sites such as Craigslist and eBay to lure victims to download malware

What is Information?

- Something meaningful
- Conveyed by a sequence of symbols.
- Symbols can be alphabetics, characters, numbers, punctuations etc.
- Physical or logical. So, a book or something on a computer.
- Contextualised , relevant, purposeful, that is specific and can be organized.

What Is Security?

- The state of being free from danger or threats.
- Can be applied to both physical and logical scenarios.
- Cambridge English Dictionary “Security is the protection of a building, a person, an organization or a country against threats such as crime”.
- Security can be provided through
  - **Physical** artifacts such as walls and locks.
  - **Logical** people and processes, inspections, surveillance, authorizations such as we find in airports.

What Is Information Security?

Combining information and security, we see useful definitions.

- Information security is defined as the practice of defending information from un-authorized access, use, disclosure, disruption, modification, inspection, recording or destruction.
- A computing-based discipline involving technology, people, information, and processes to enable secured operations of an organization.
- It involves the creation, the operations, analysis and testing of secure computer systems.
- It is an interdisciplinary course of study, which includes aspects of law, policy, human factors, ethics, and risk management in the context of adversaries.

COMPUTER SECURITY

The NIST *Computer Security Handbook* defines the term computer security as:

"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."

(includes hardware, software, firmware, information/data, and telecommunications)

Understanding Security

- Security is:
  - The goal to be free from danger
  - The process that achieves that freedom
- Harm/danger may come from one of two sources:
  - From a direct action that is intended to inflict (impose) damage
  - From an indirect and unintentional action
- As security is increased, convenience is often decreased
  - The more secure something is, the less convenient it may become to use

Understanding Security

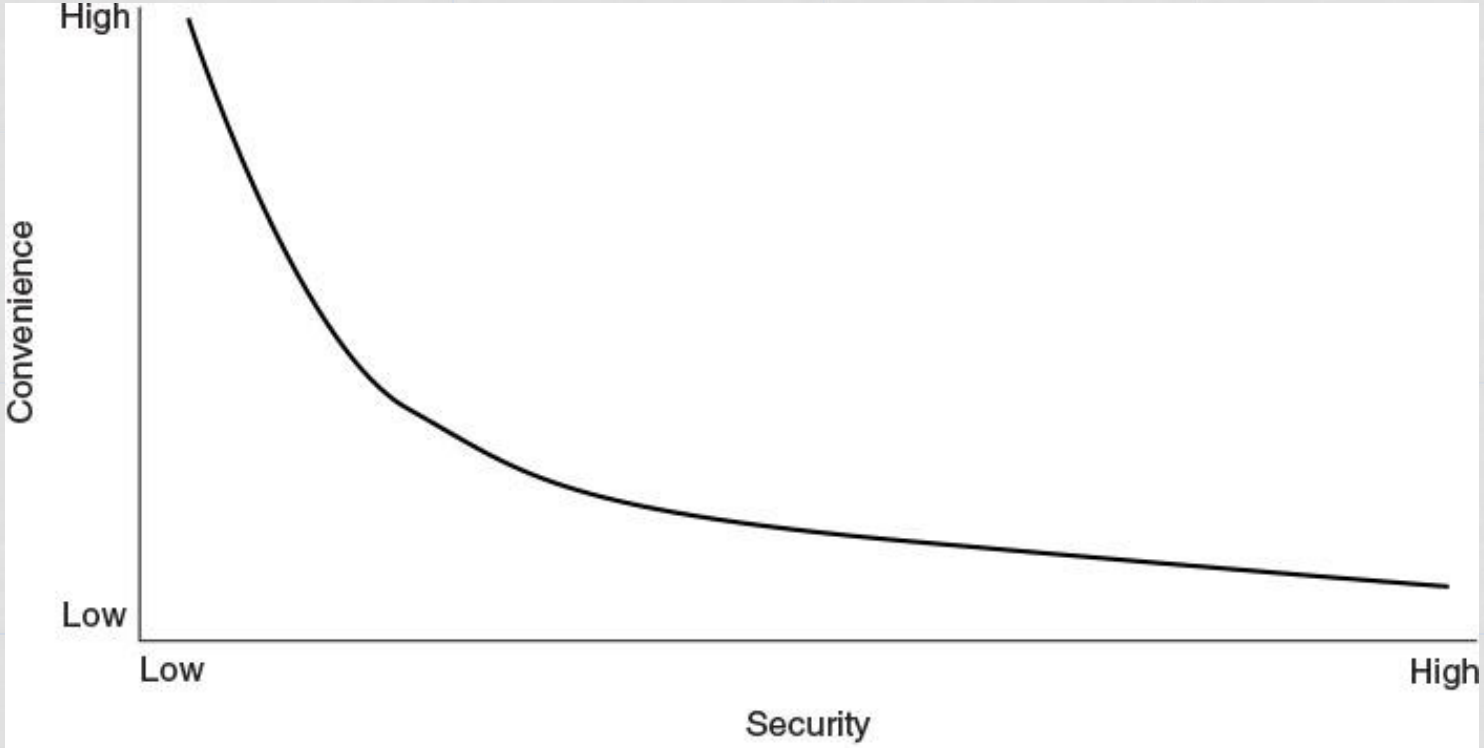


Figure 1-2 Relationship of security to convenience

Security is often described as sacrificing convenience for safety

3. SECURITY OBJECTIVES

SECURITY OBJECTIVES

- **Confidentiality**

  Assures that private or confidential information is not made available or disclosed to unauthorized individuals

- **Integrity**

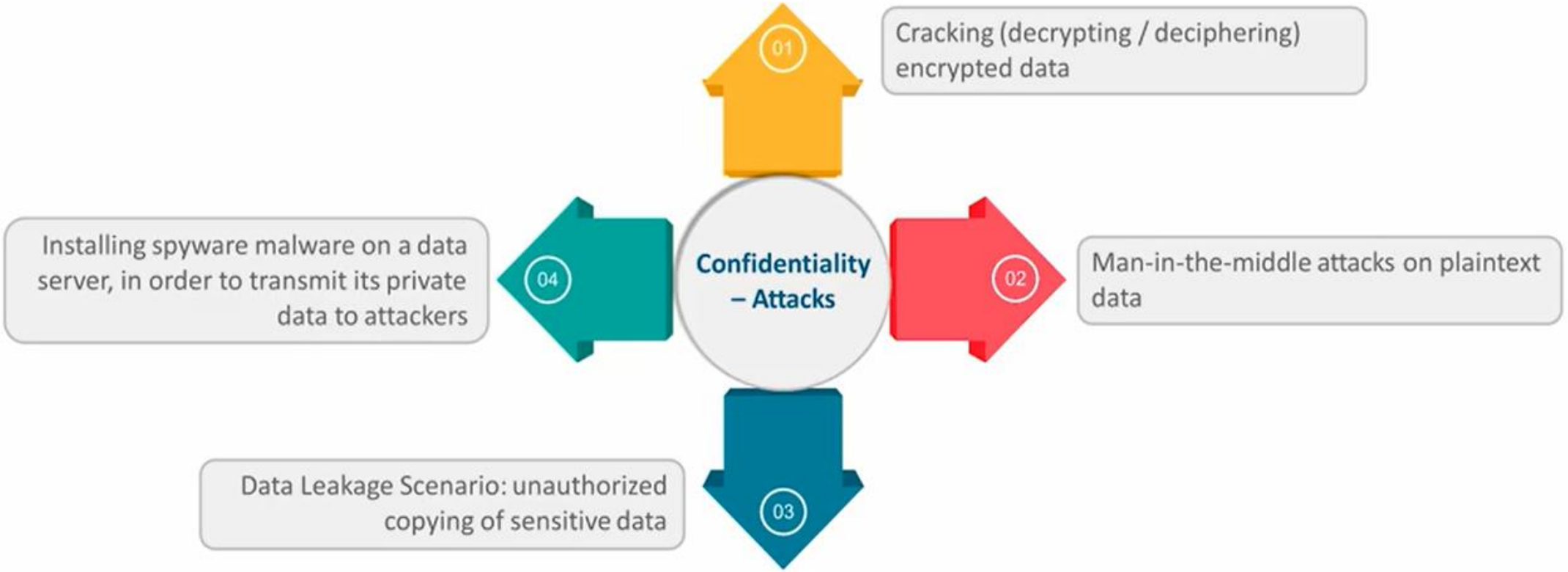
  Assures that information and programs are changed only in a specified and authorized manner

- **Availability**

  Assures that systems work promptly and service is not denied to authorized users

Confidentiality

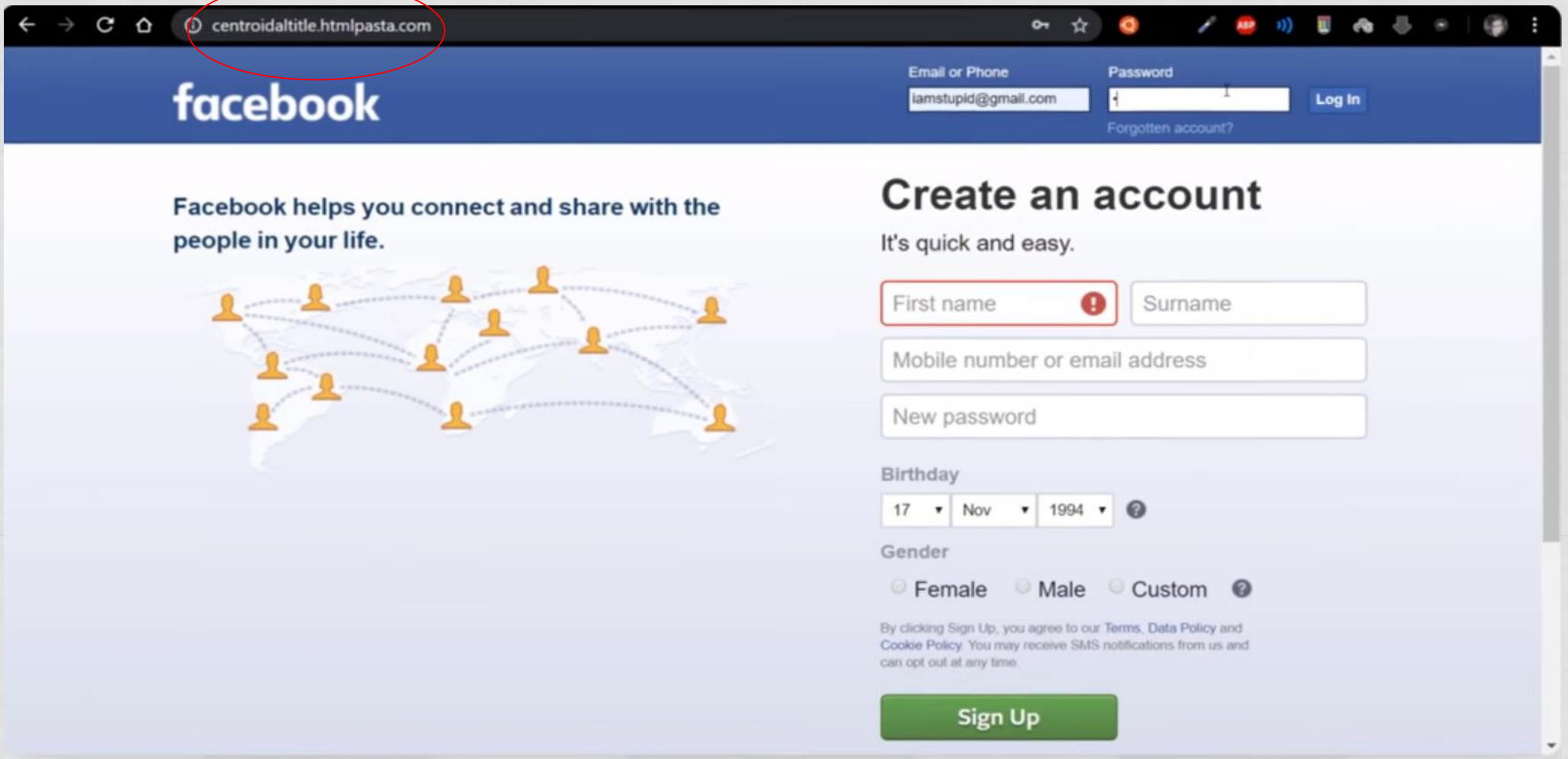
Confidentiality is all about making sure that data is accessible only to its intended (authorized) individual



A classic data breach

- Employee is sent a phishing email with a link to a realistic looking internal site.
- Employee opens the email, clicks the link, and types her user name and password.
- Malicious site collects the password and shows the user that everything is actually fine so they are not suspicious.
- Malicious actor uses user name and password to download sensitive files.

Do you see any problem here



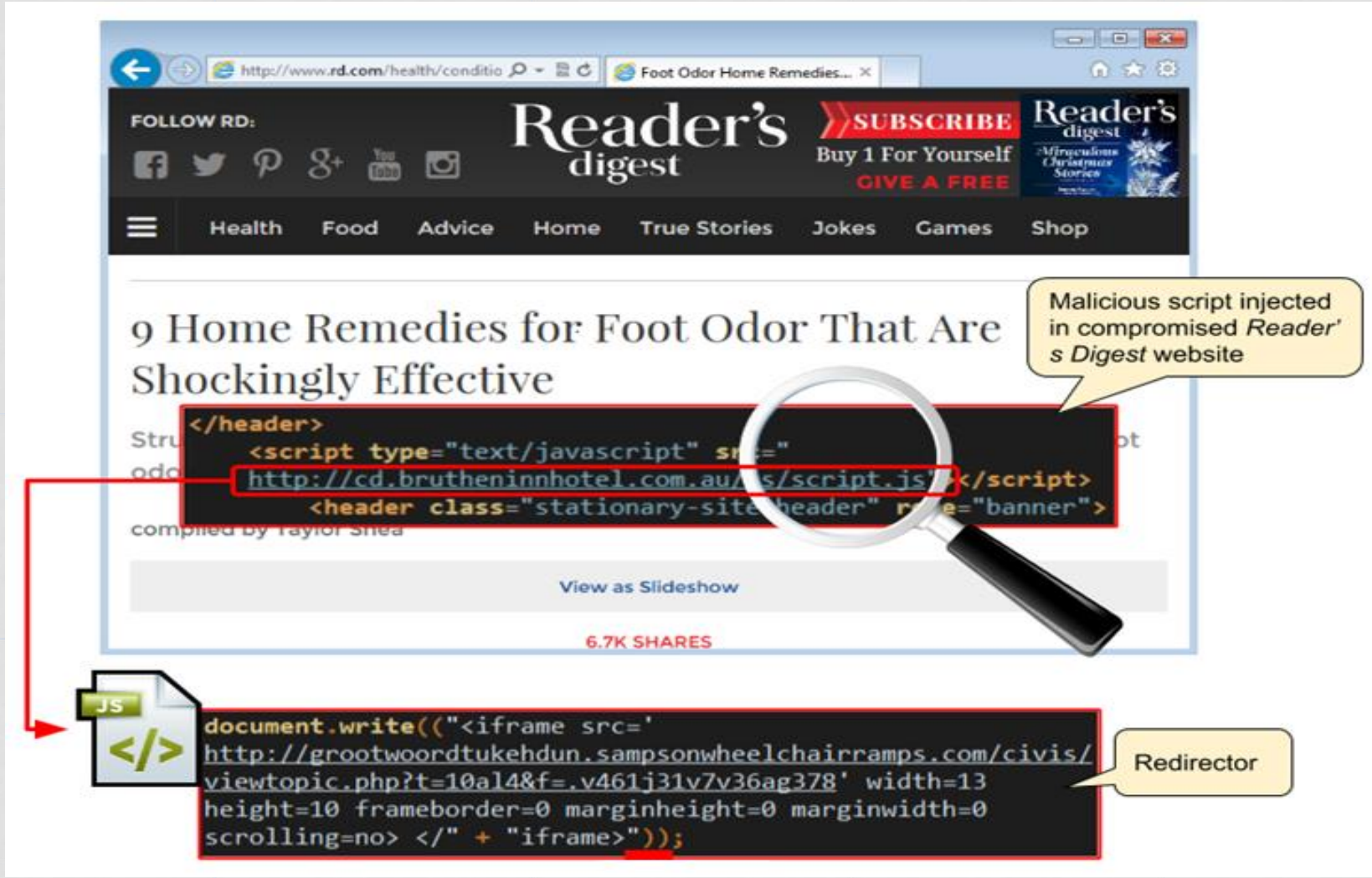
A classic data breach

- **Prevention:**
  Detect phishing URLs and mark as spam, train employees to notice phishing, identify offsite access of sensitive files and block, encrypt files so it will become useless if leaked.

- **Detection**:
  Identify that sensitive files have been accessed from off site

- **Response**:
  Change employee's password, notify CTO, notify insurer, begin post-breach plan.

Sites are sometimes the last to know they have been compromised



Quiz

- **Question: Confidentiality: Suppose you are making an online purchase and want to pay for it with your credit card. What is the best way to preserve confidentiality of your credit card information?**

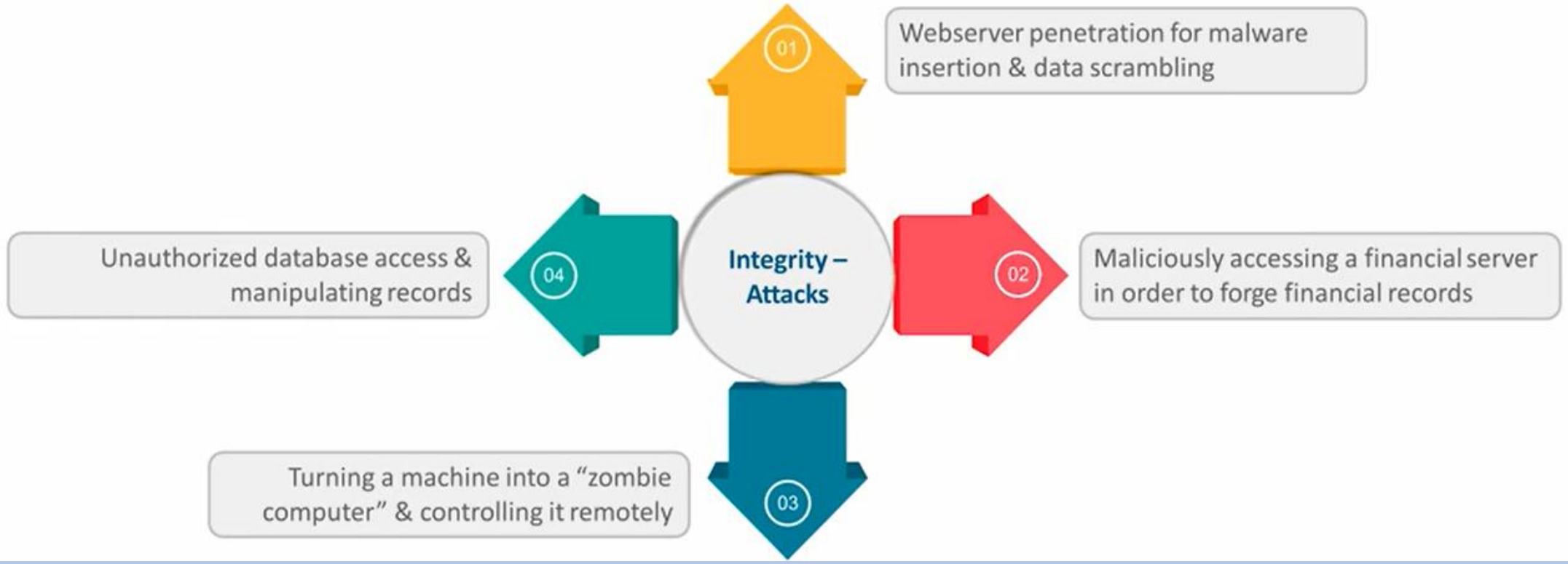
Quiz

- **Question: Confidentiality: Suppose you are making an online purchase and want to pay for it with your credit card. What is the best way to preserve confidentiality of your credit card information?**

Check if the online connection is secured with SSL or TLS, you can then enter the credit card information.

Integrity

Integrity is all about making sure that data is kept properly intact without it being meddled with in an unauthorized way



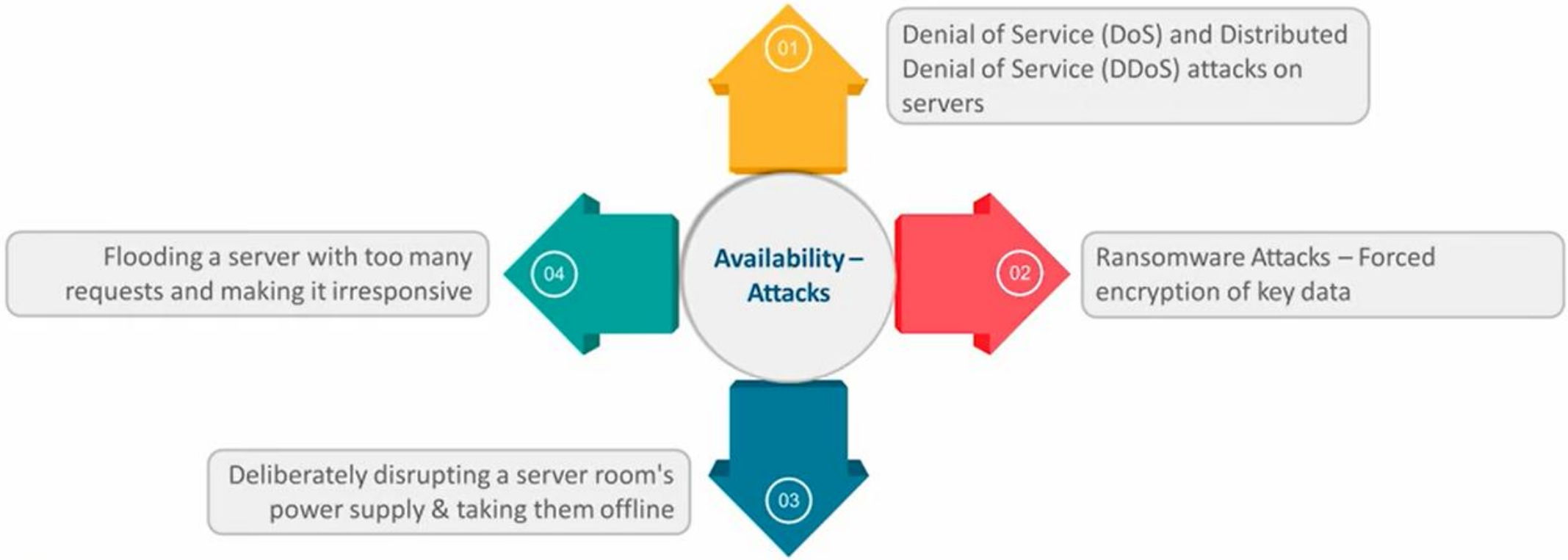
Integrity

- Events that lead to integrity breaches include (non-intentional)
  - Accidentally deleting files
  - Entering invalid data
  - Altering configurations

- Countermeasures
  - Hashing (data integrity)
  - Configuration management (system integrity)
  - Access control (physical and technical)

Availability

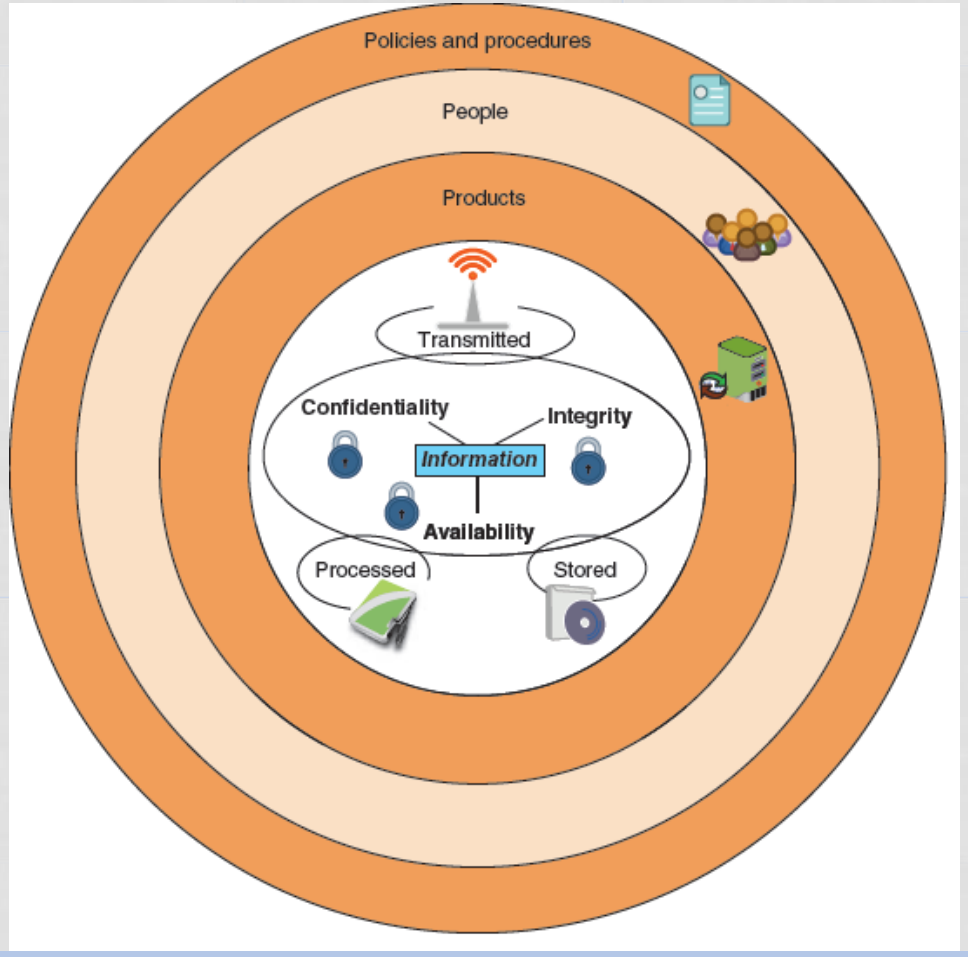
Availability is all about making sure that data and computers are available as needed by authorized parties

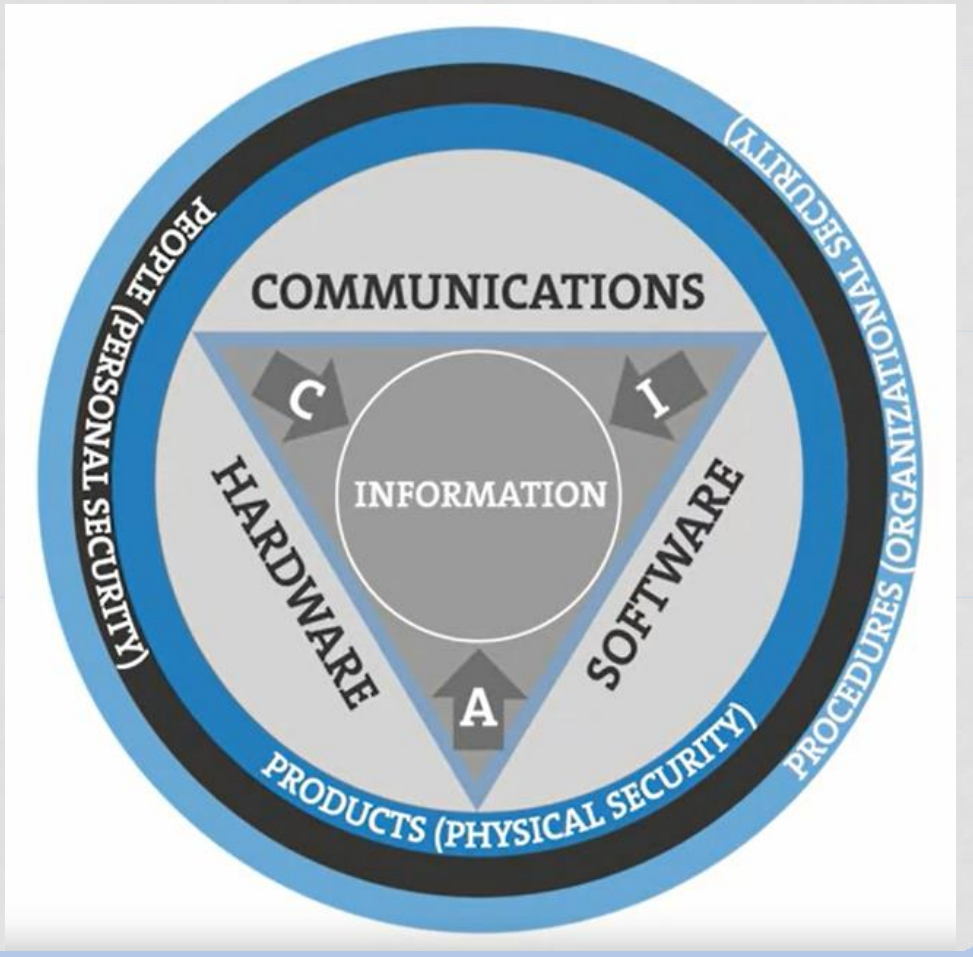


Availability

- **Countermeasures**
  - **Redundant array of independent disks (RAID)**
  - **Load balancing**
  - **Redundant data and power lines**
  - **Software and data backups**
  - **Co-location and offsite facilities**
  - **Rollback functions**
  - **Failover configurations**

Information Security in an Organization





4. SECURITY SERVICES ITU-T (X.800)

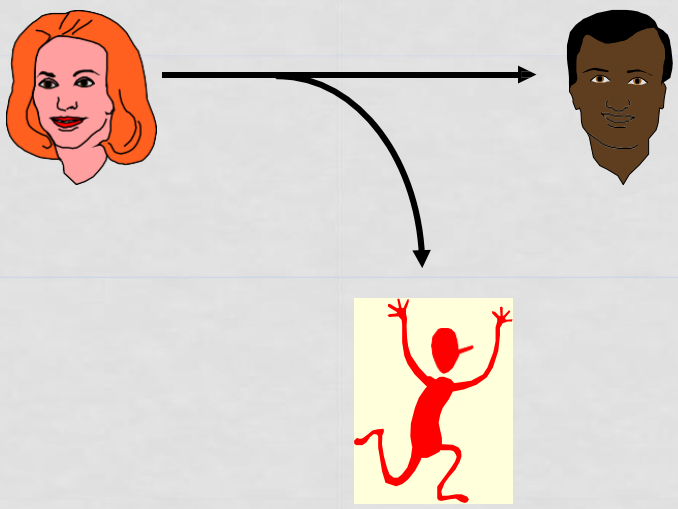
SECURITY SERVICES ITU-T (X.800)

- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Availability
- Access Control

CONFIDENTIALITY (SECRECY)

- Protect transmitted data
- Protect against traffic analysis

- **INTERCEPTION**
  Unauthorised party gains access to data

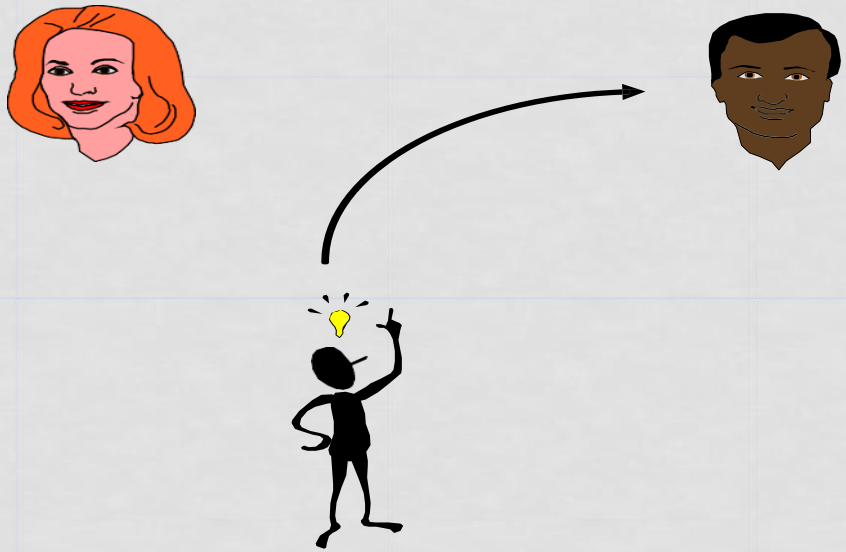


AUTHENTICATION

- Assurance that message is from proper source
- Protect from third party masquerade

Mutual Authentication

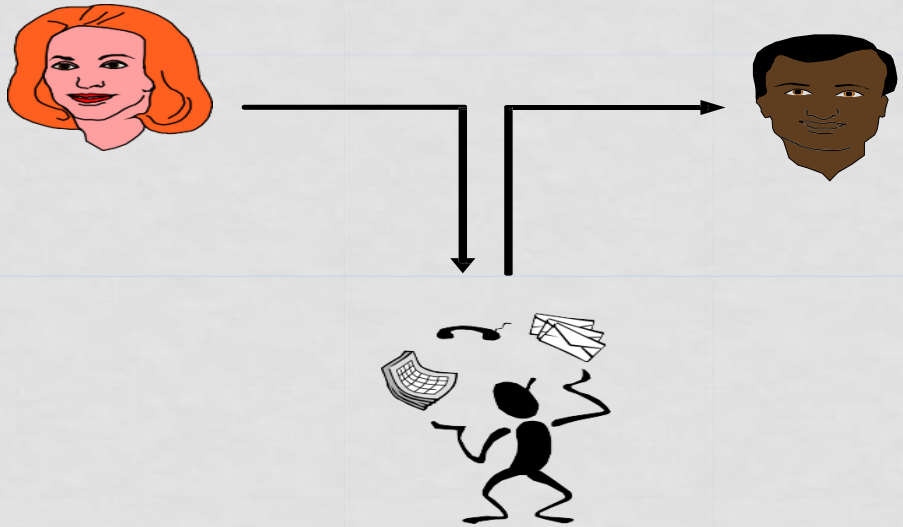
- **FABRICATION**
  Insertion of “counterfeit” messages



INTEGRITY

- Message is received as sent
- Modification
- Also interested in replay, re-ordering, deletion, delay

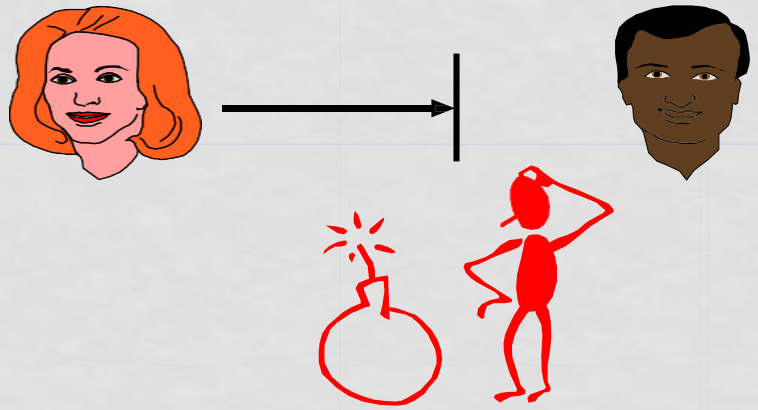
- **MODIFICATION**
  Gain access and “tampers” with messages



AVAILABILITY

- Availability of information/resources
- Complete loss of availability
- Reduction/Degradation in availability

- **INTERRUPTION**
  Loss of communication (cut the cable)
- **DENIAL OF SERVICE**
  Noisy comms (physical noise, spurious messages)



NON-REPUDIATION

- Prevents parties from denying they sent or received a message; i.e. concerned with protecting against legitimate protocol participants, not with protection from external source
- Receiver can verify and prove who sent a message
- Sender can verify and prove who received a message

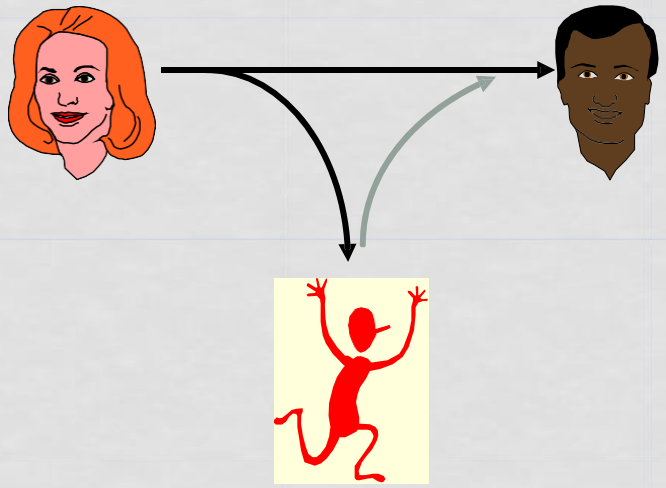
- **REPUDIATION ATTEMPT**
  Party anonymously publishes his or her message/key(s) and falsely claims that they were stolen.

ACCESS CONTROL

- Limit & control access to host system/services
- Limit & control access to networks
- Authenticate each party so that access rights can be assigned
- More fine-grained solutions, e.g. Digital Rights Management

Auditing Service

- **REPLAY**
  Record a legitimate message
  e.g. a login, and replay later



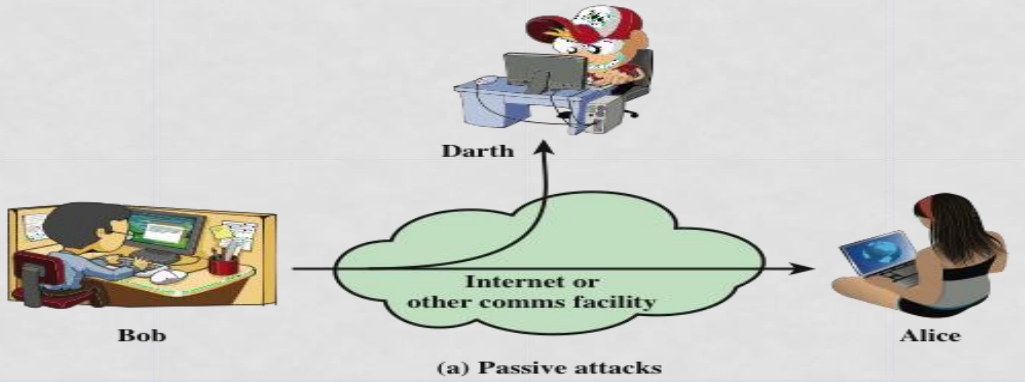
Quiz

Suppose XYZ bank has launched online portal to facilitate its customers. By using the online portal, the bank's customers can perform all types of banking transactions online and can also check different information related to their account such as current balance, transaction history, personal information etc. By keeping in mind CIA triangle, you are required to briefly explain the confidentiality, integrity, and availability with respect to the said banking application.

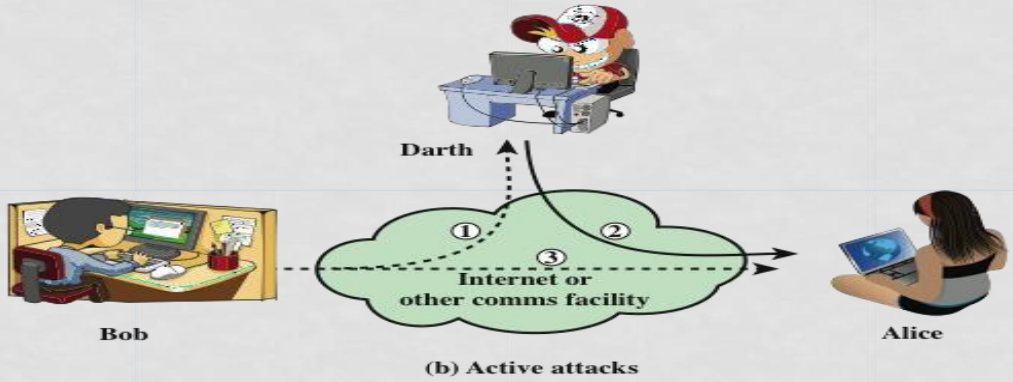
6. Active Vs. Passive Attacks

SECURITY ATTACKS

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation



(a) Passive attacks



(b) Active attacks

Figure 1.2 Security Attacks

PASSIVE ATTACKS

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

ACTIVE ATTACKS

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

7. Information Security Terminologies

Information Security Terminologies

- **Asset**
  - Item of value
  - Data contained in an information system; or a service provided by a system; or a system capability; or an item of system equipment (i.e., a system component—hardware, firmware, software, or documentation).

SECURITY TERMINOLOGIES

- **Vulnerability:**
  A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
- **Threat:**
  A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- **Threat agent**
  Person or element with power to carry out a threat
- **Attack:**
  An attack is a threat that is carried out (threat action)

SECURITY TERMINOLOGIES

- **Risk:**
  An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result

- **Countermeasure:**
  An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

- **Security Policy:**
  A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

ASSETS

- Data including archives
- Computers, Disks, Tapes
- CPU time, Storage, Net capacity
- Comms (routers, switches, firewalls, modems, patch panels, bandwidth), Phones, Faxes
- Air-conditioning systems/alarm systems, Physical Security
- Manuals, guides
- Printouts: reports, letters, emails, contracts
- Configuration information
- Passwords
- Staff
- Safety and health of personnel
- Privacy of users
- Public image and reputation
- Customer/client goodwill
- Share price
- Intellectual property
- Domain name

THREATS

- Hardware errors
- Terrorists
- Theft, Malicious file
- Industrial espionage, Government
- Malicious software
- Pirating
- Password cracking
- Denial of Service
- Misuse of resources
- Social engineering
- Reverse engineering

- Fire, Earthquakes,
- Disaffected employees
- Human error
- Illness & Injury
- Economic downturns

THREATS

- Unreliable software, bugs
- Viruses, worms, trojan horses, bombs, trap doors, spoofs, artificial life-forms, password crackers, Cryptanalysis, Microsoft
- Disgruntled, blackmailed, bribed, greedy employees or ex-employees
- Hackers
- Government agencies, military spies, industrial spies, criminals, terrorists
- ISPs, Backbone Providers

COUNTERMEASURES

- Protect buildings, equipment and people from unauthorised access, natural disasters
- Use fibre optic cabling, Shield equipment & cabling
- Use reliable H/W & S/W, Shredder
- Keep backups & standby systems
- Use “good” cryptography
- Use firewalls, simulated attacks
- Use good password admin, virus checkers, intrusion detection s/w, auditing software, biometrics
- Isolate network
- Counter-intelligence, Ethical hackers, Security guards, Lawyers
- Employ trustworthy staff, background checks
- Train/educate staff
- Keep staff happy
- Insure
- Good legal backup
- Take security seriously (planning, administration, risk assessment, cost/benefit analysis, paranoia level)
- Splendid Isolation

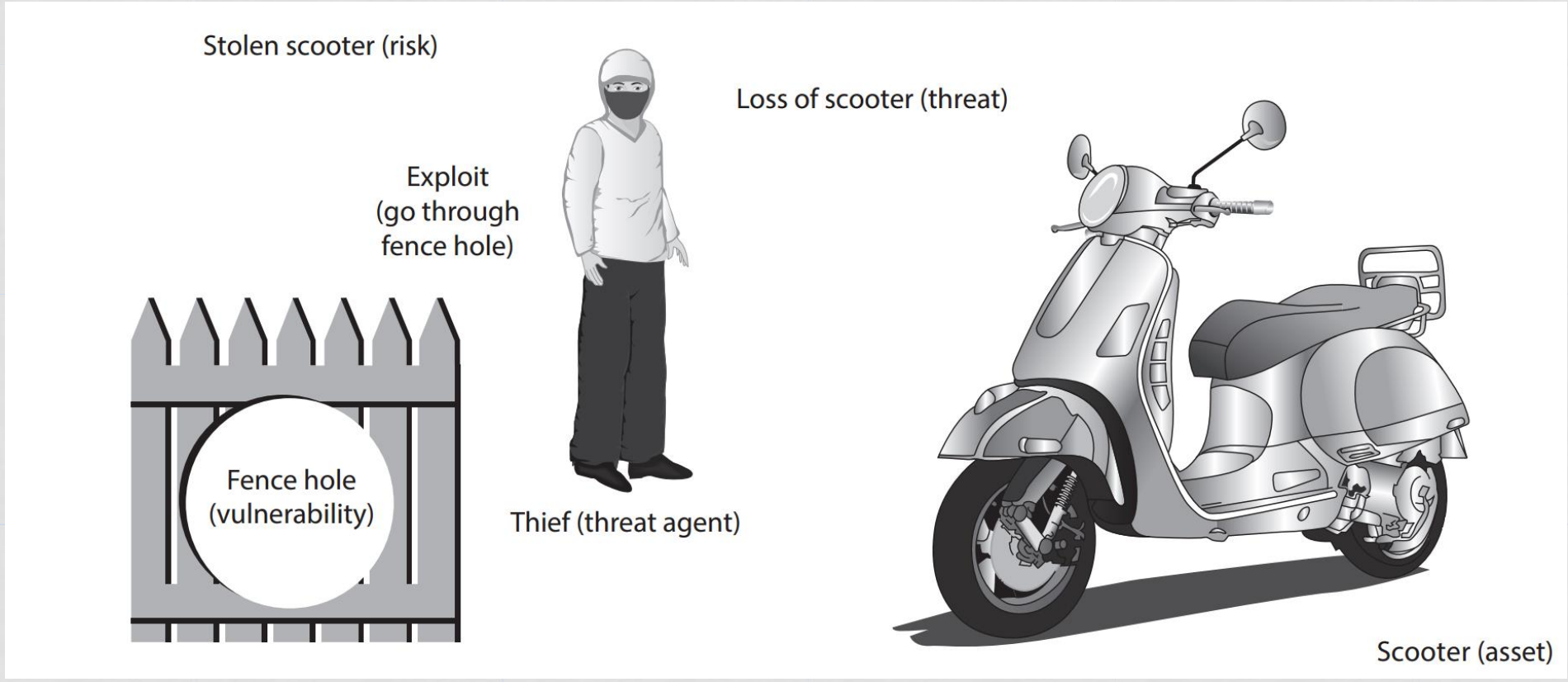
POLICIES

- Set of well-defined, consistent and implementable rules (security requirement). Policies should be general and change little over time.
- Consider an online auction company such as E-bay which allows most users to buy and sell goods online. Sellers can post details of their goods on E-Bay's web site and interested buyers can bid for the goods.
- What policies might the users of the system want applied?

Example: In a system that allows weak passwords,

- Vulnerability---password is vulnerable for dictionary or exhaustive key attacks
- Threat---An intruder can exploit the password weakness to break into the system
- Risk---the resources within the system are prone for illegal access/modify/damage by the intruder.


Imbalance is weakness
i.e. VULNERABILITY
Possibility of falling
down is the RISK
Crocodiles are
The THREATS


Stolen scooter (risk)
Exploit
(go through
fence hole)
Loss of scooter (threat)
Fence hole
(vulnerability)
Thief (threat agent)
Scooter (asset)

Risk Management

- Options to deal with risk:
  - **Risk avoidance** - involves identifying the risk but not engaging in the activity (i.e. not to buy the scooter)
  - **Acceptance** - risk is acknowledged but no steps are taken to address it (i.e. ignore the risk and buy the scooter any way)
  - **Risk mitigation** - the attempt to address the risks by making risk less serious (i.e. request the management to fix the fence by making the risk less serious)
  - **Deterrence** - understanding the attacker and then informing him of the consequences of his actions (i.e. put a sign board to warn the attacker of the consequences of stealing)
  - **Transference** - transferring the risk to a third party (i.e. insurance)

NETWORK ACCESS SECURITY MODEL

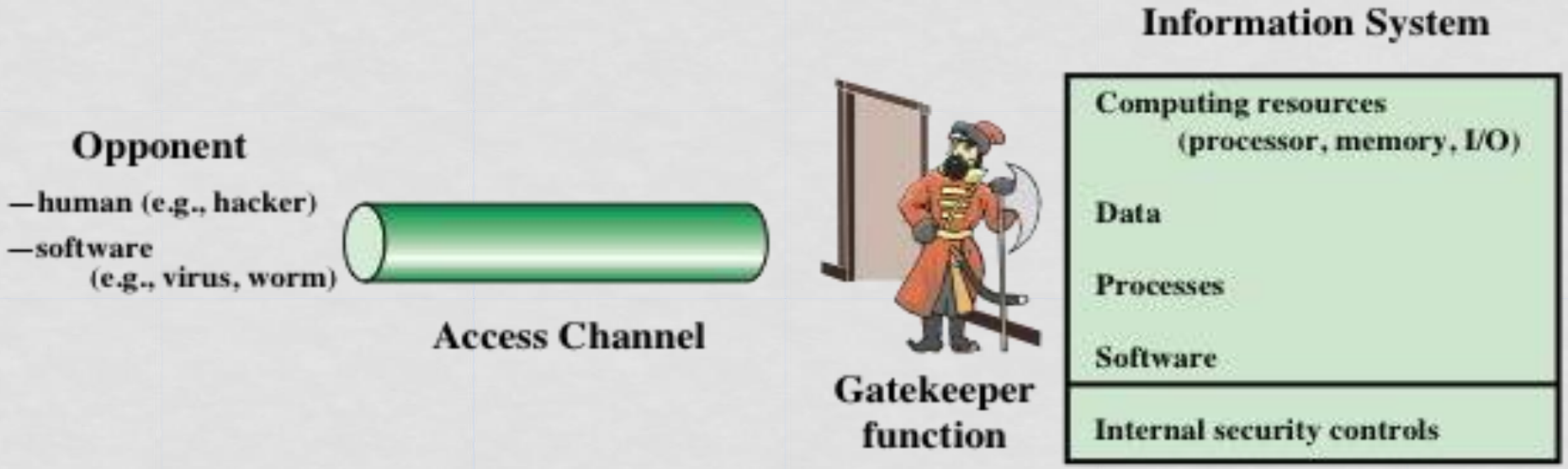


Figure 1.6 Network Access Security Model

INFORMATION SECURITY IS CHALLENGING

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

References

- CompTIA **Security+ Guide to Network Security Fundamentals**, Fifth Edition by Mark Ciampa

- **Corporate Computer Security,** by Randall J. Boyle, 3th Edition

- Cherdantseva Y. and Hilton J. **"A Reference Model of Information Assurance & Security,"** Accepted to SecOnt 2013 workshop which will be held in conjunction with the 8th International Conference on Availability, Reliability and Security (ARES) 2013, University of Regensburg, Germany. September 2nd - 6th, 2013.

Data Breaches

- Study the world's biggest data breaches in various industry sectors
- Filter the data based on methods of leak and number of records stolen

Use the link:

https://informationisbeautiful.net/visualizations/worldsbiggest-data-breaches-static/

Internet Threat Scenario

- Monitor the global cyber threat scenario including hacking, bots, and malware attacks using live threat maps
- Identify hacking attempts or cyber-attacks from different parts of the world as they happen in real time

Use the link:

https://www.fireeye.com/cyber-map/threat-map.html


The End