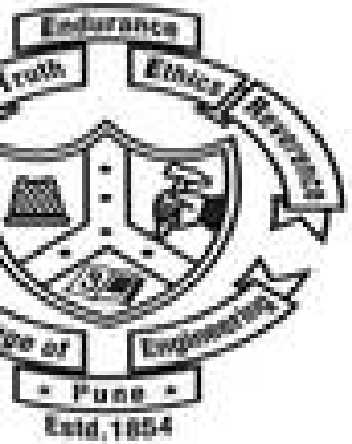


College of Engineering Pu

(An Autonomous Institute of the Govt. of Maharashtra)

Internet Fundamentals, Analysi of Threats and Risks

-- Dr. Sunil B. Mane, COl

Email: sunilbmane.comp@coep.a

UTLINES

- **nternet fundamentals**
- **nformation security**
- **Basics of Information security**
- **Analysis of threats and risks**
- **Difference between Information, IT and Network security**
- **Policies of Information Security**

ITERNET

t is the largest network in the world that connects hundreds of thousands of individual networks all over the world.

nternet service providers- A commercial organization with permanent connection to the Internet that sells temporary connections to subscribers.

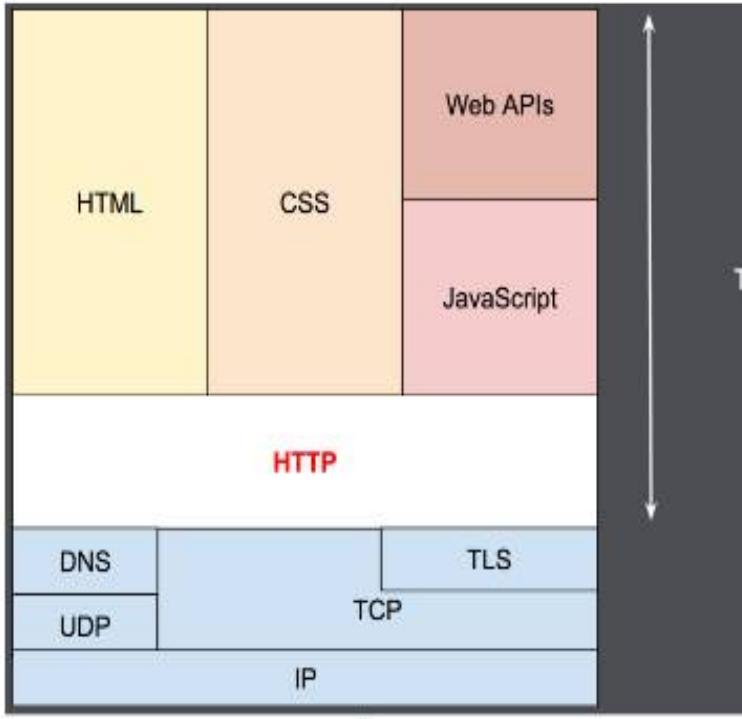
Examples: Prodigy, America Online, Microsoft network, AT&T Networks.

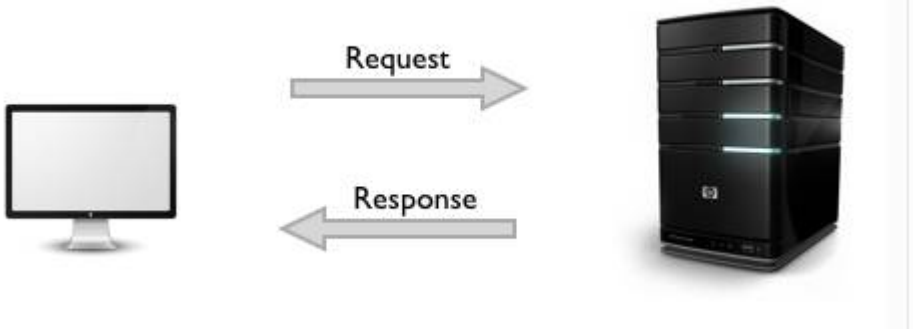
NDERSTANDING THE HTTP PROTOCOL

HTTP stands for Hypertext Transfer Protocol

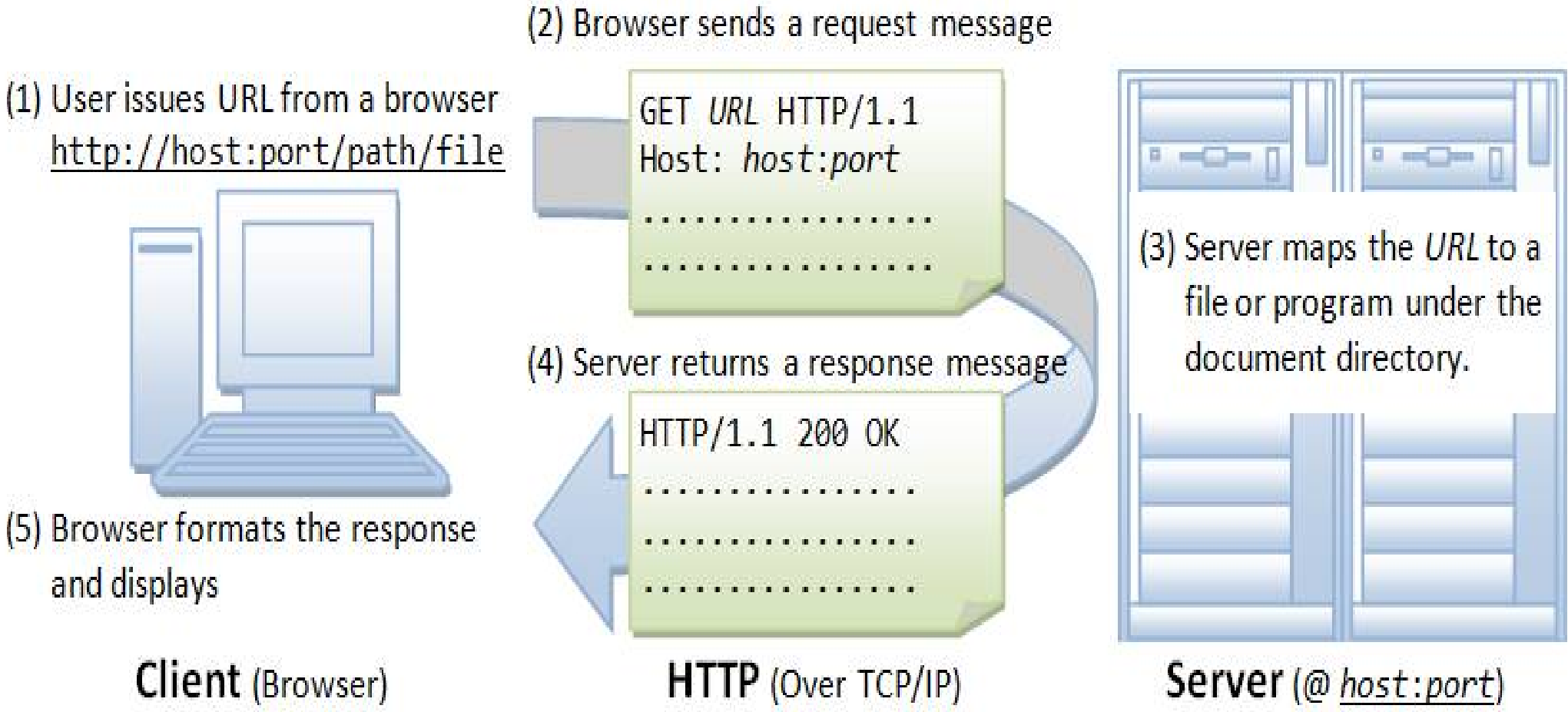
HTTP is simple, extensible

Stateless

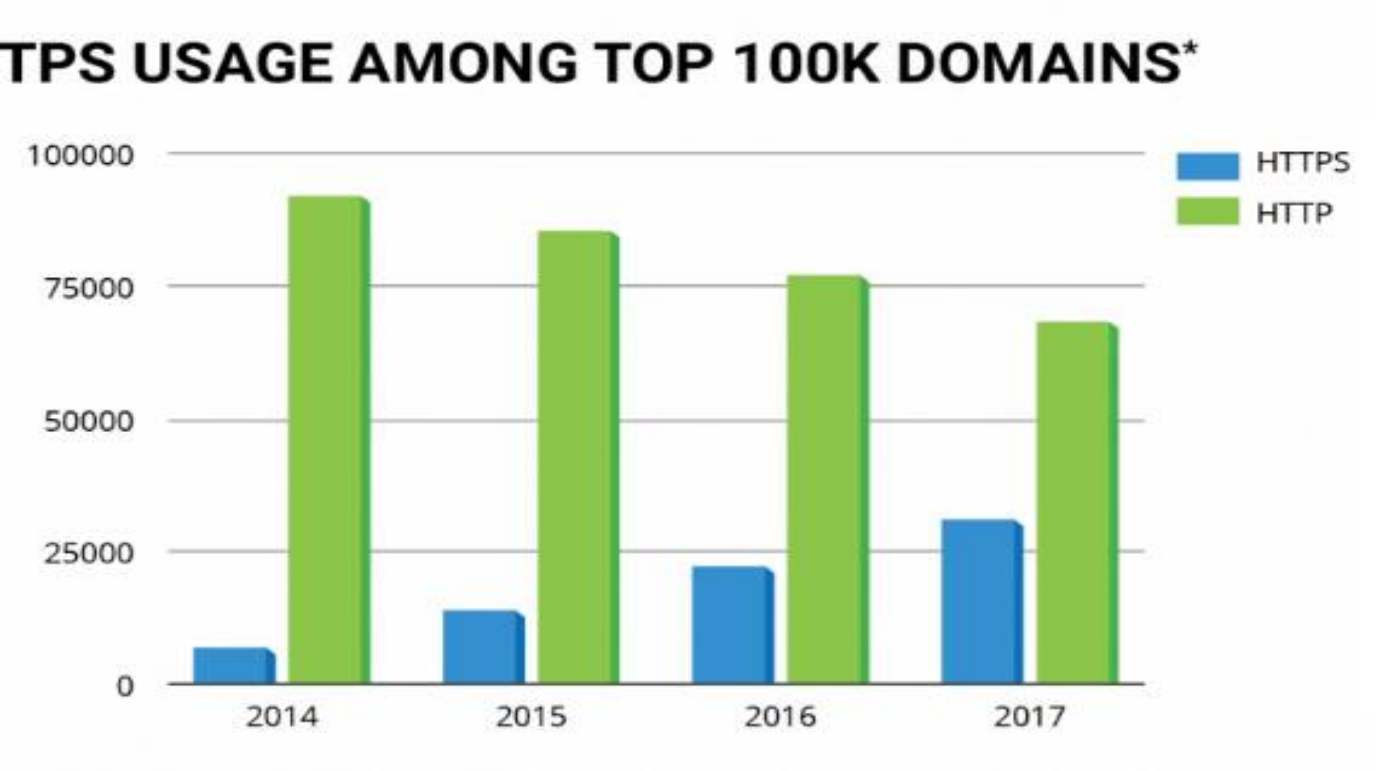


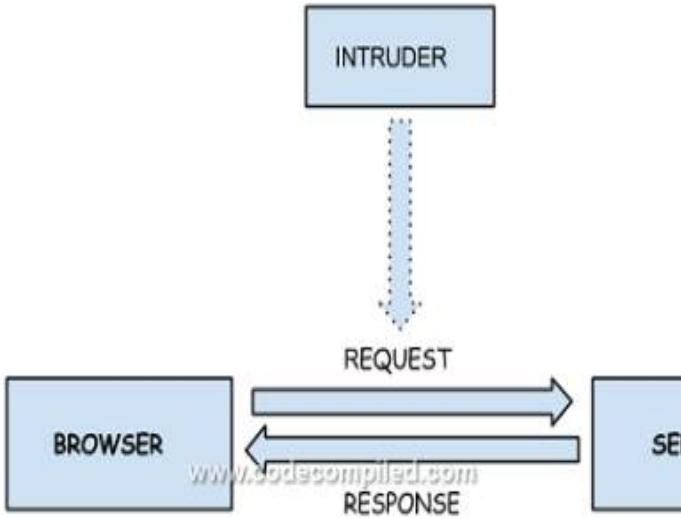


NDERSTANDING THE HTTP PROTOCOL



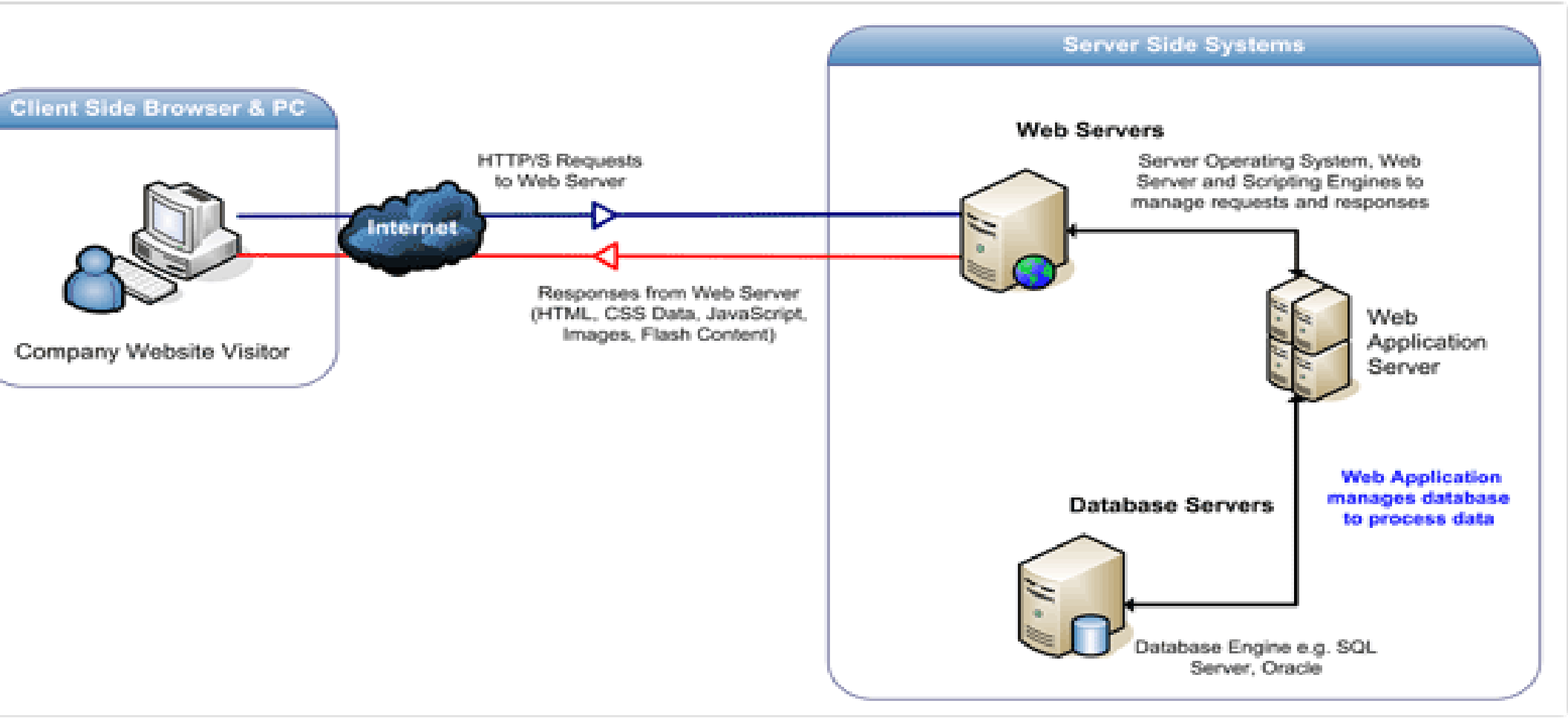
TP AND HTTPS



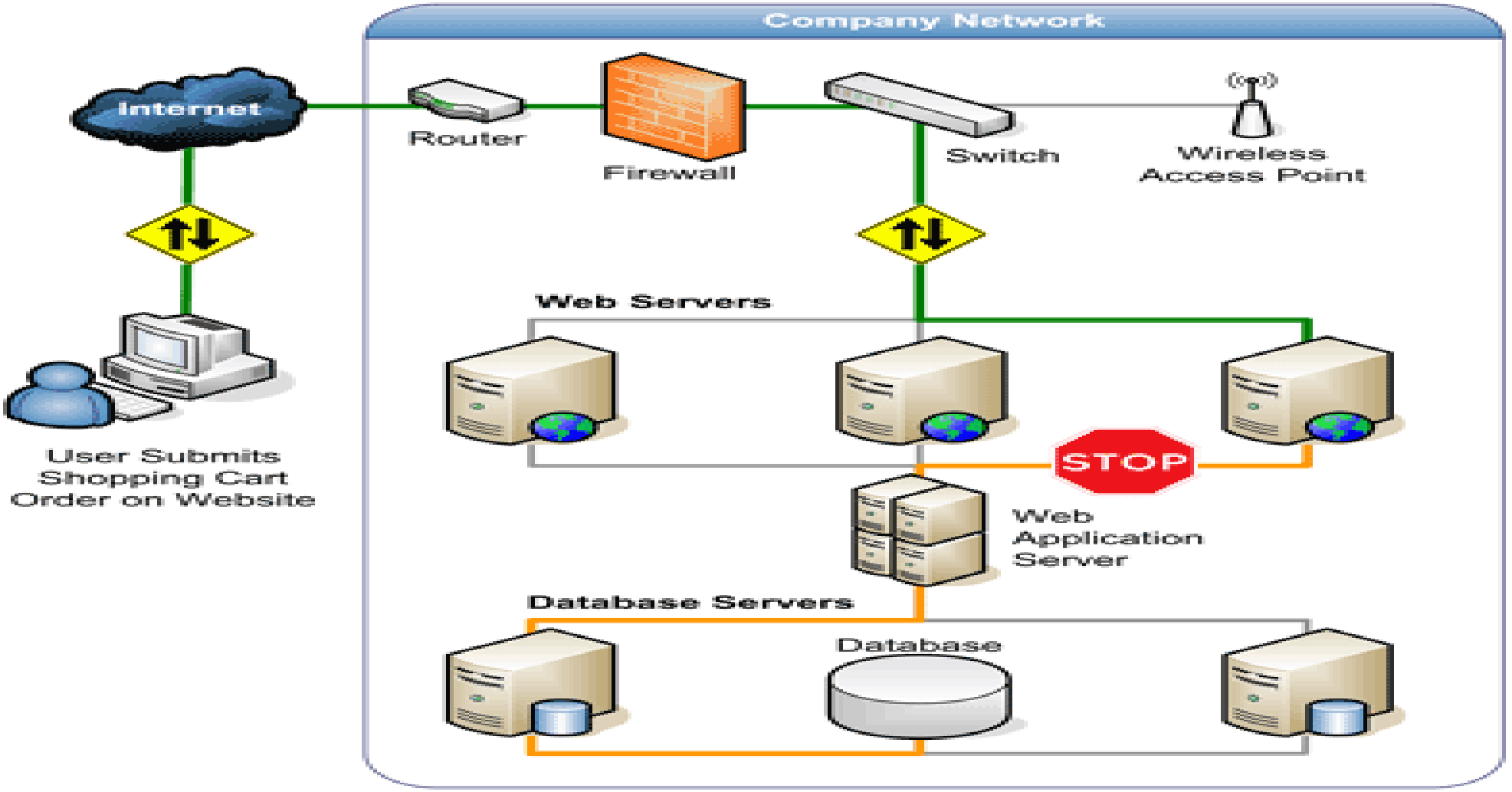


Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP to save the confidentiality by encryption.

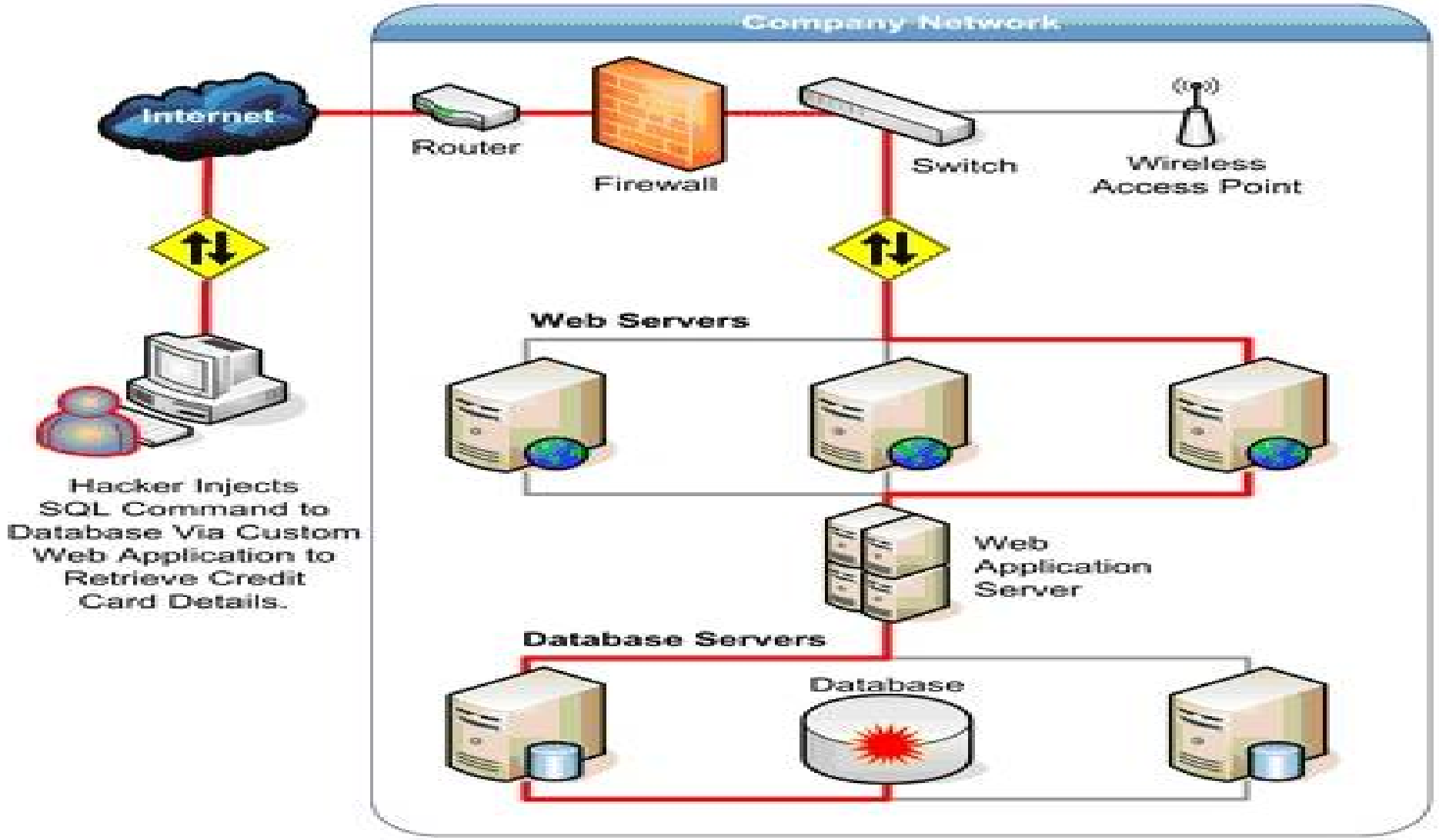
TERNET COMMUNICATION



OW A WEB APPLICATION WORKS

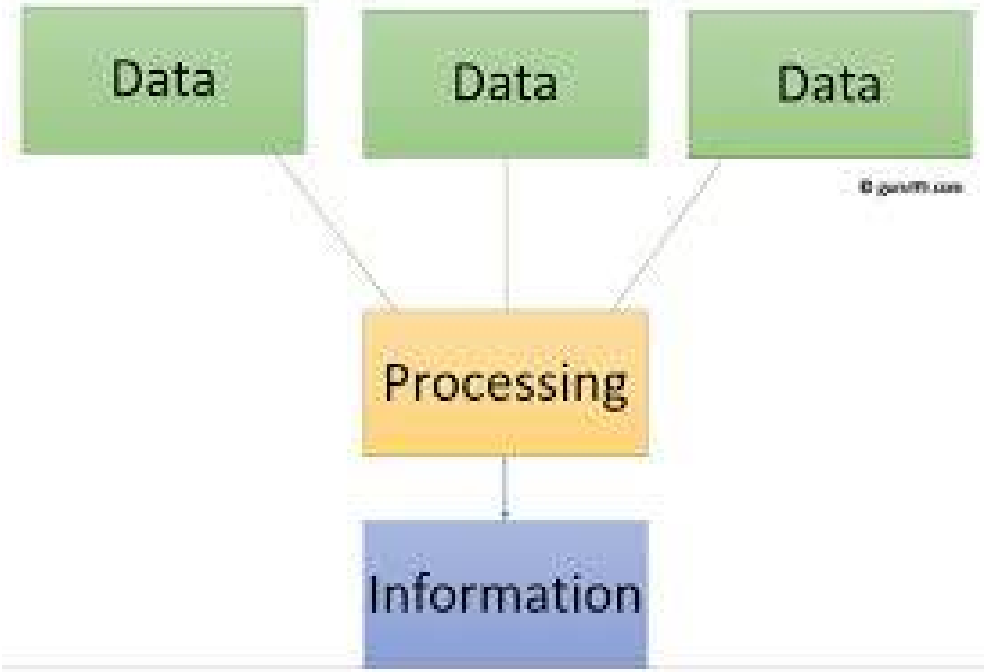


OW AN ATTACKER ATTACKS



ATA AND INFORMATION

- Data represent values
- Meaning associated with the data, it changes with the context



FORMATION SECURITY

- Information Security is “Organizational Problem” rather than “IT Problem”
  - More than 70% of Threats are Internal
  - More than 60% culprits are First Time fraudsters
  - Biggest Risk : People
  - Biggest Asset : People
  - Social Engineering is major threat

FORMATION AND INFORMATION SECURITY

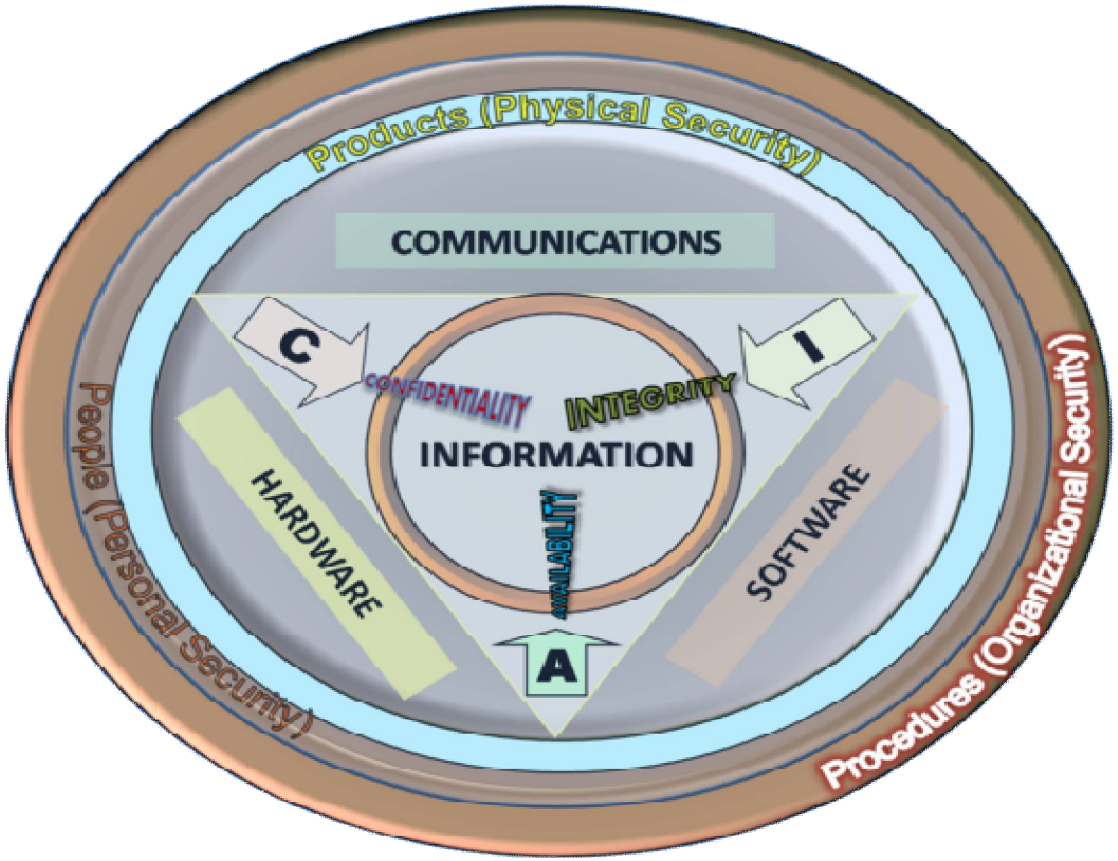
nformation is an asset which, like other important business assets, has value to organization and consequently needs to be suitably protected.

nformation Security is the process of protecting the intellectual property of organization.

nformation security is the protection of information and minimizes the risk of expos nformation to unauthorized parties.

Preservation of confidentiality, integrity and availability of information. Note: In additi other properties, such as authenticity, accountability, non-repudiation and reliability also be involved.

ASIC PRINCIPLES AND OBJECTIVES



The CIA triad of confidentiality, integrity, and availability is at t
heart of information security

HY INFORMATION SECURITY

- Ensure Availability of Business
- Take care of the risk of loss of Confidentiality, Integrity and Availabili of Information Assets
- Protect Data and Information Systems
- Brand and Reputation Loss
- Increased Productivity through best practices
- Higher levels of assurance
- Enable Business Continuity and Disaster Recovery

RMS

Threat:

- Any circumstance or factor with the potential to cause harm
- A motivated, capable adversary

Vulnerability:

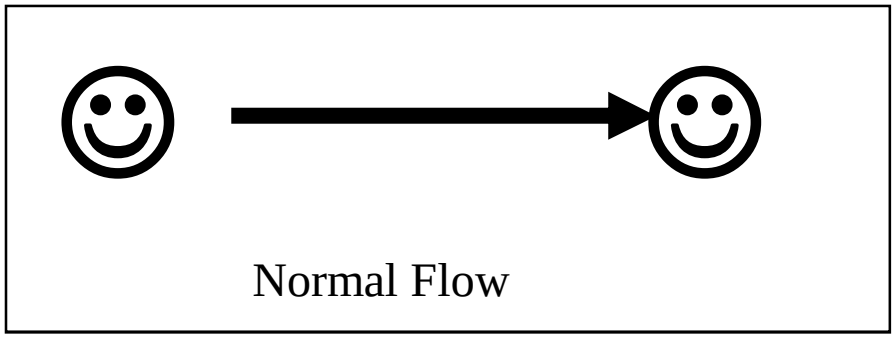
- A weakness in a system; in procedures, design, or implementation that can be exploited
  - Software bugs, design flaws, operational mistakes
  - Social engineering

- Risk=likelihood x consequence
  - Likelihood is the probability that particular vulnerability will occur
  - The severity(impact) of that occurrence

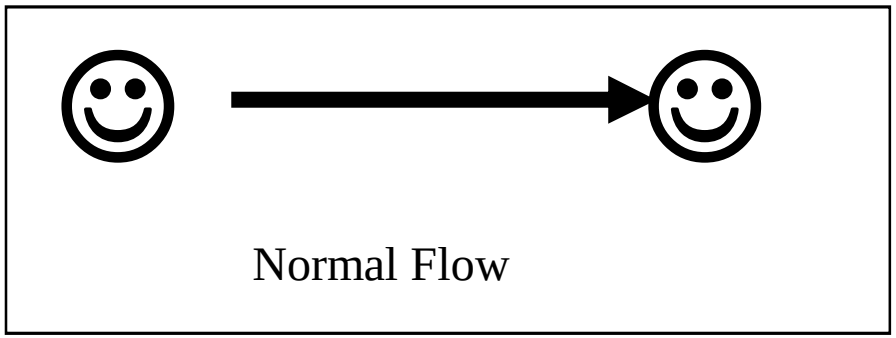
THREATS

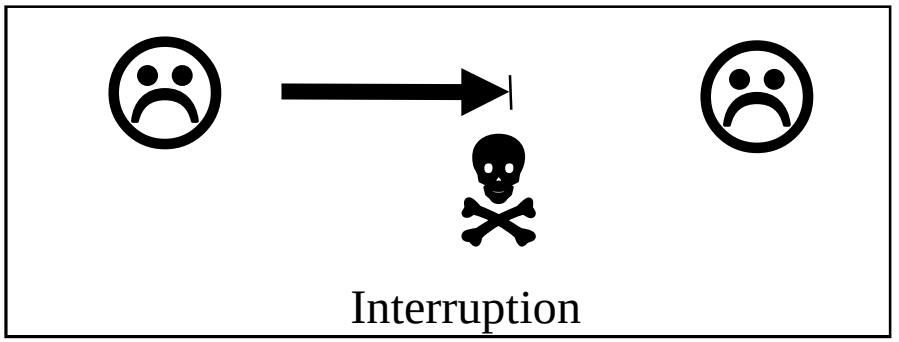
- Software Attacks,
- Theft of intellectual property,
- Identity theft,
- Theft of equipment or information,
- Sabotage, and
- Information extortion

ECURITY ISSUES

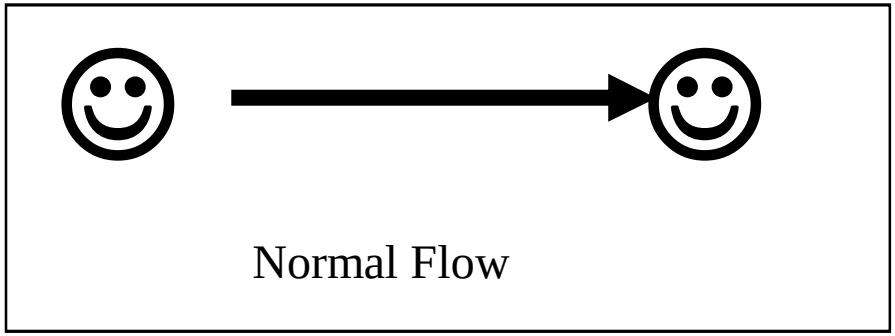


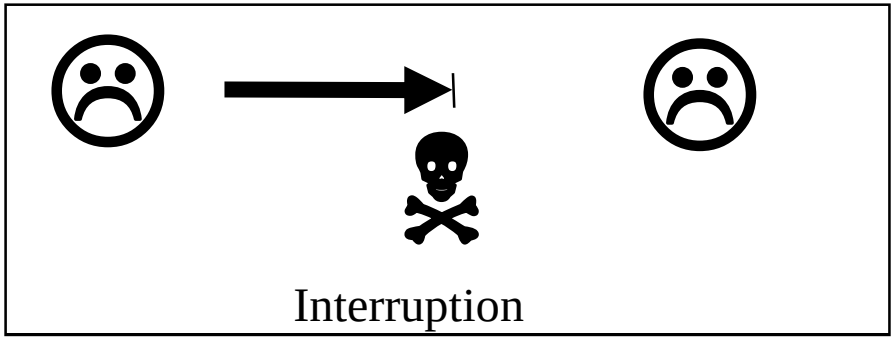
SECURITY ISSUES

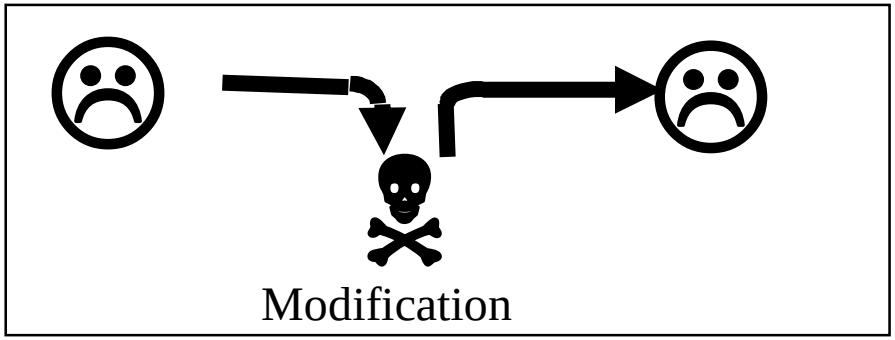




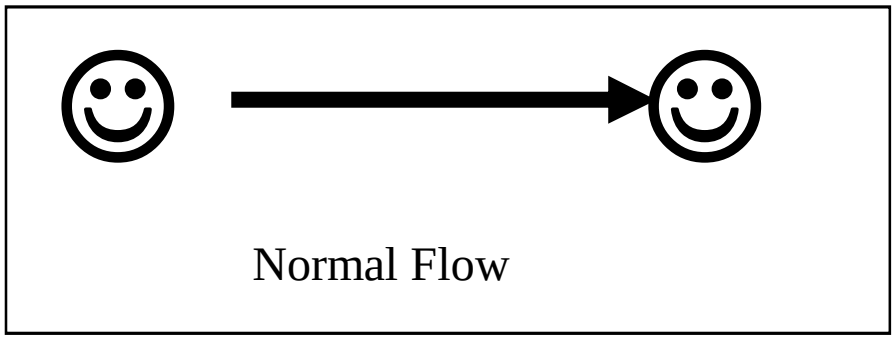
SECURITY ISSUES

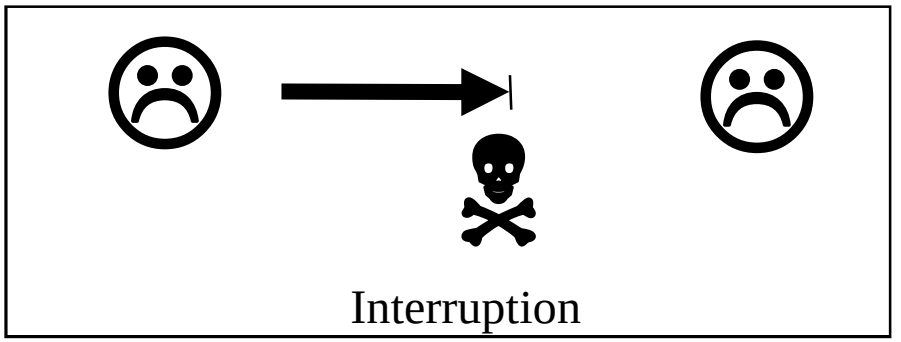


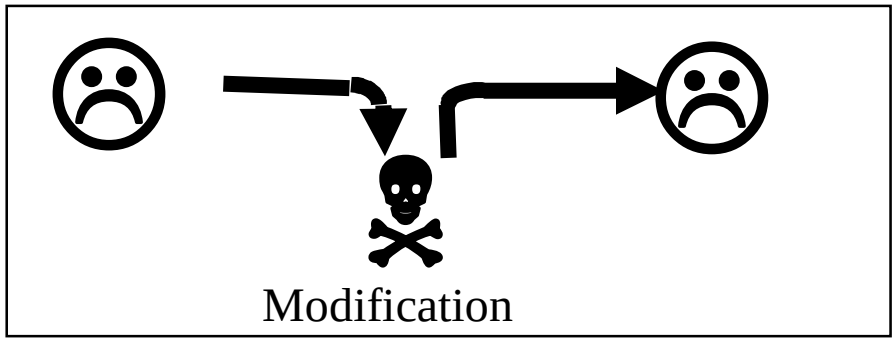


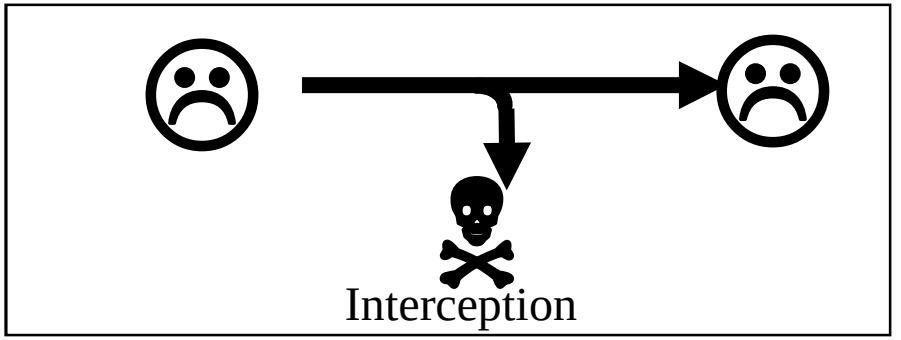


SECURITY ISSUES

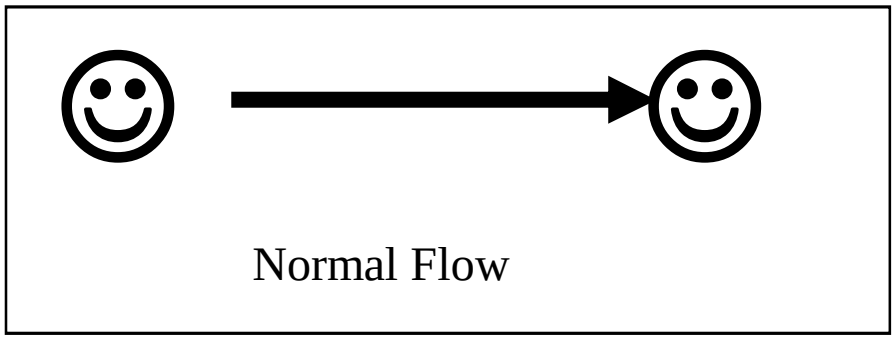


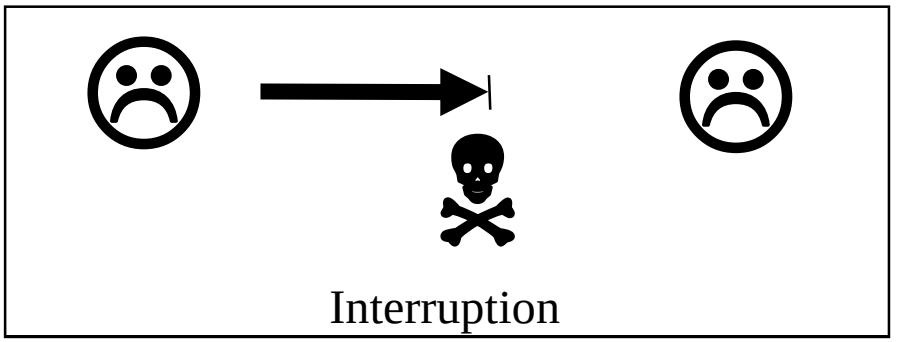


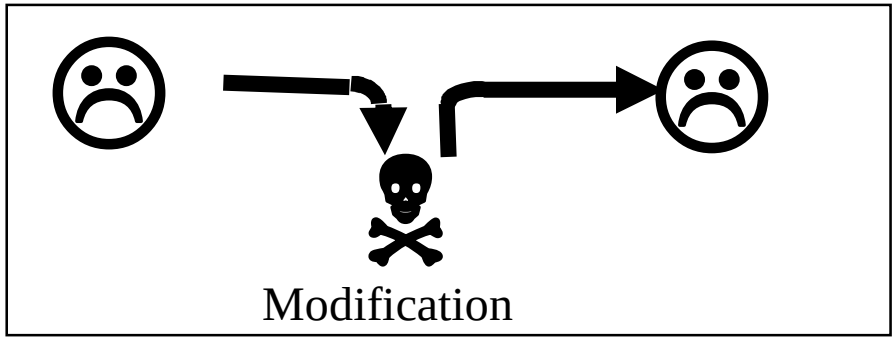


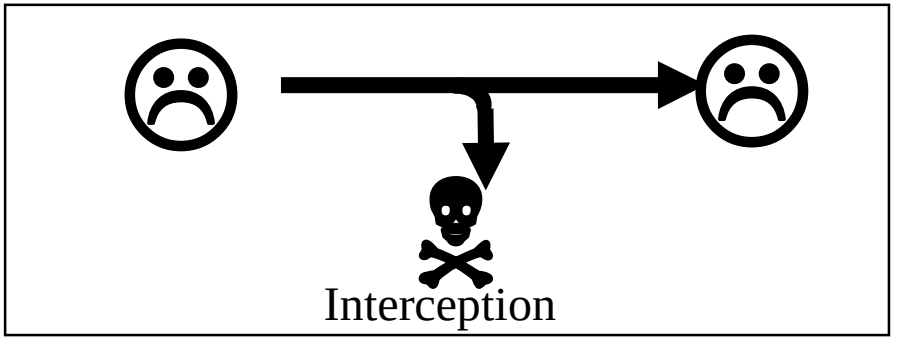


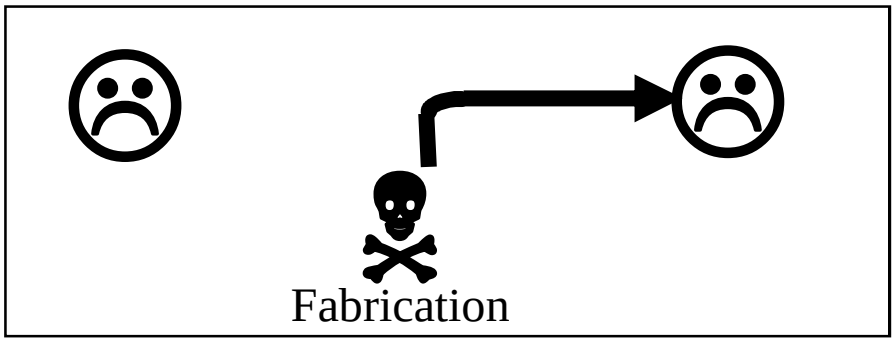
SECURITY ISSUES

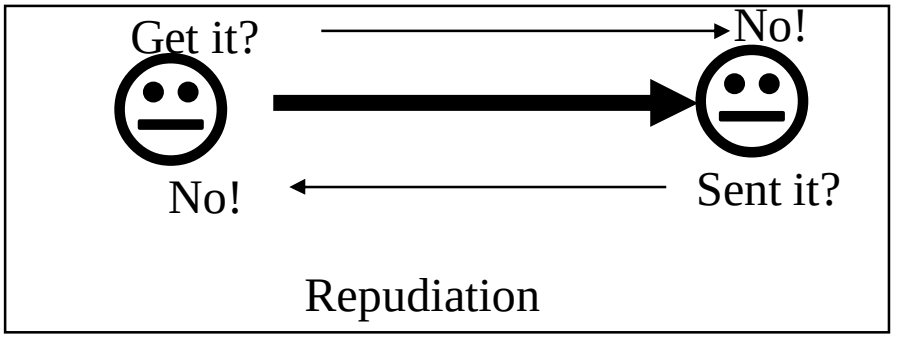




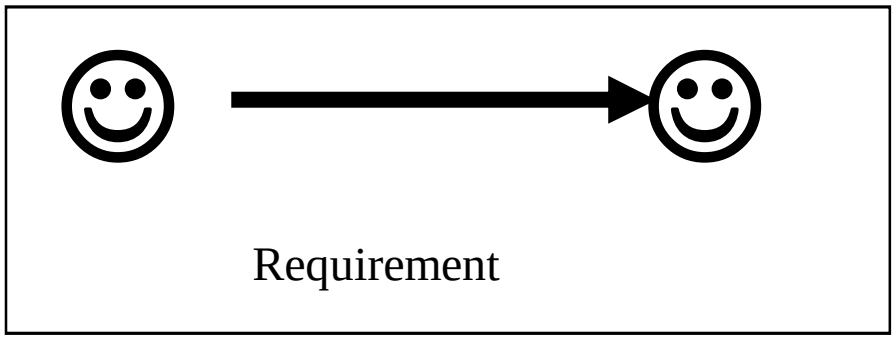


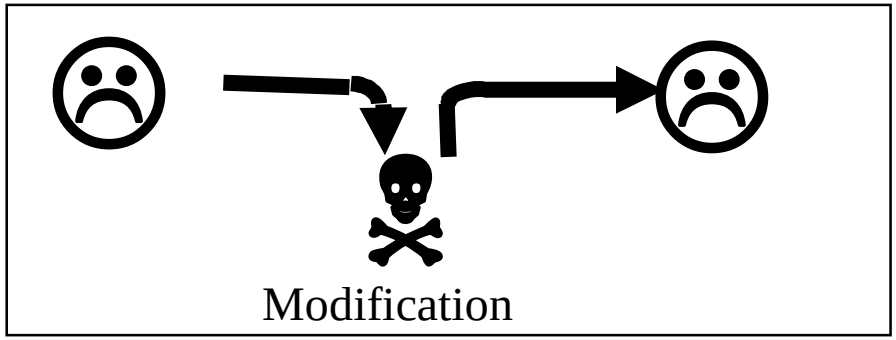


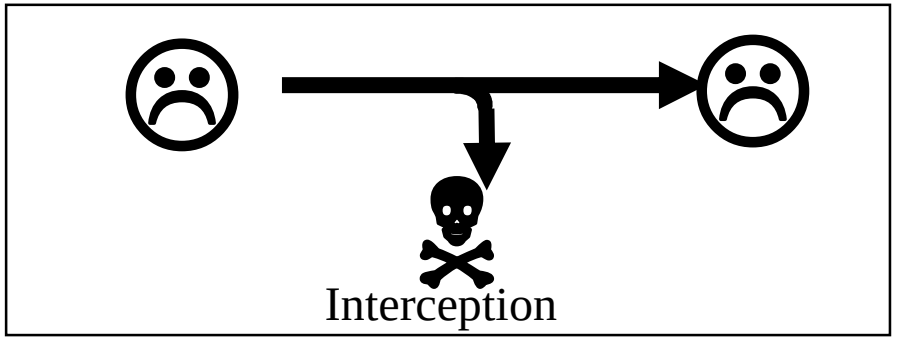


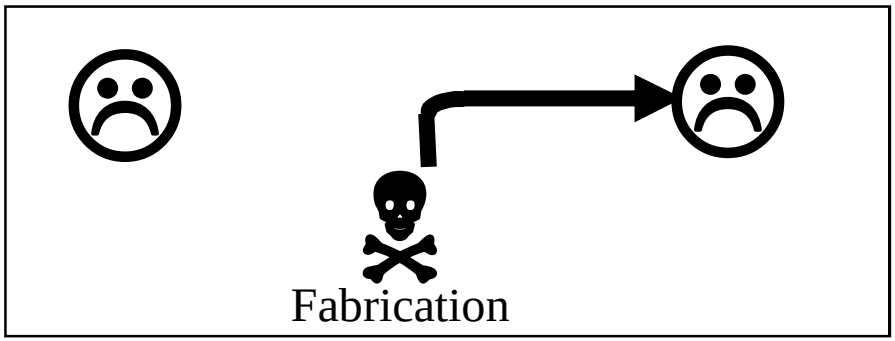


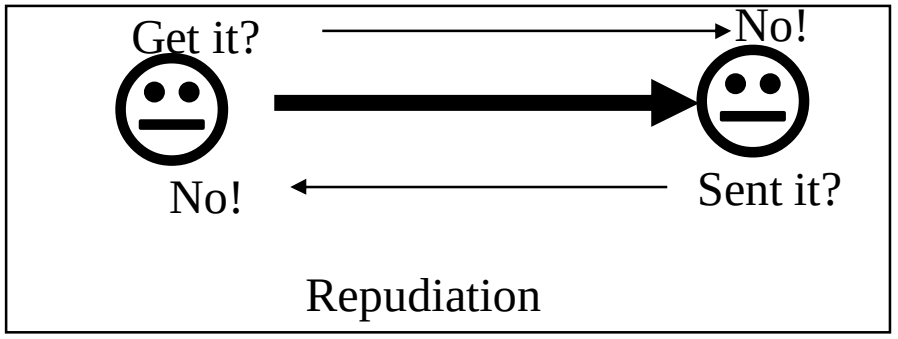
ECURITY ISSUES



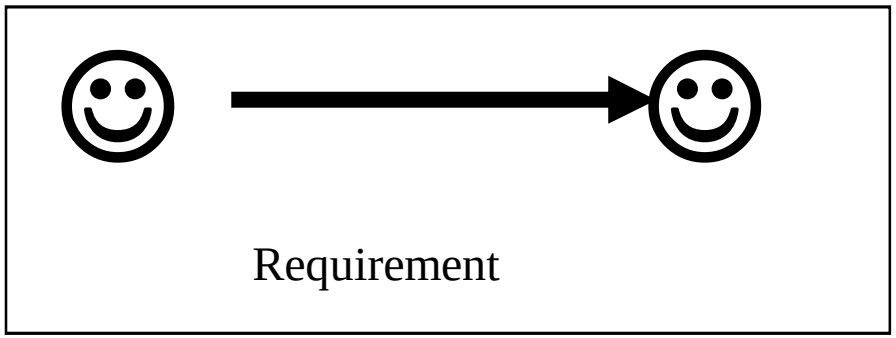






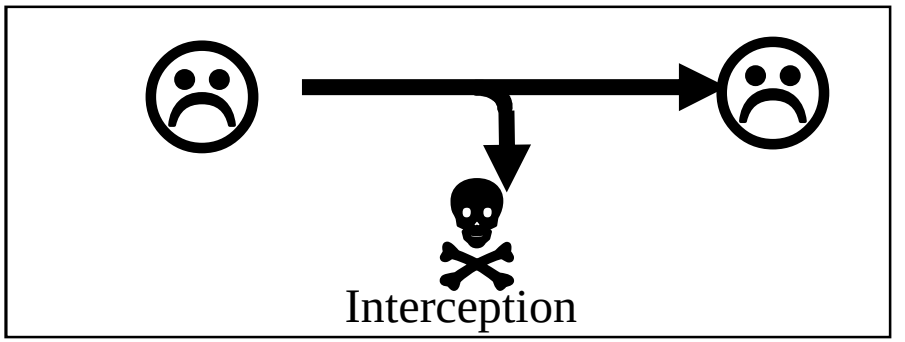


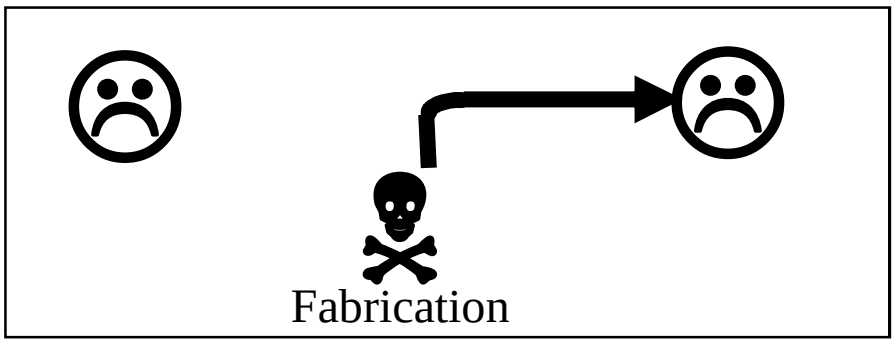
SECURITY ISSUES

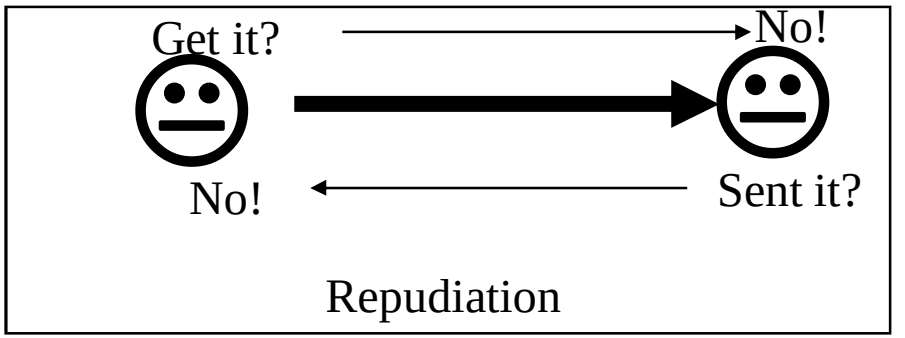


Availability

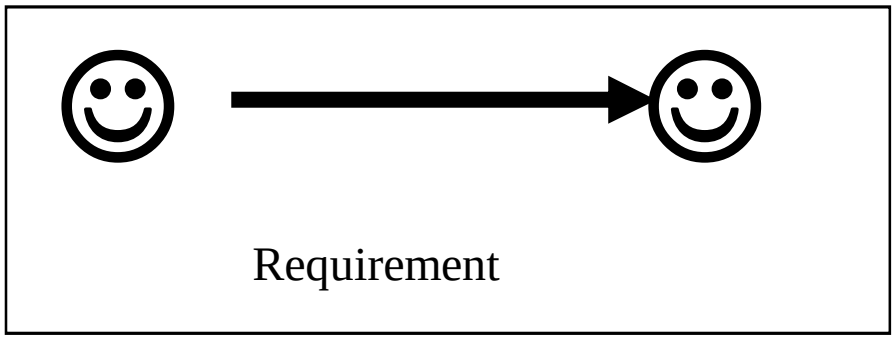
Integrity







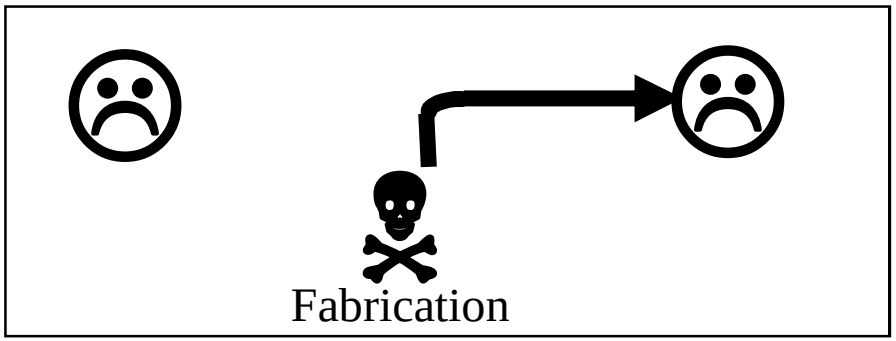
SECURITY ISSUES

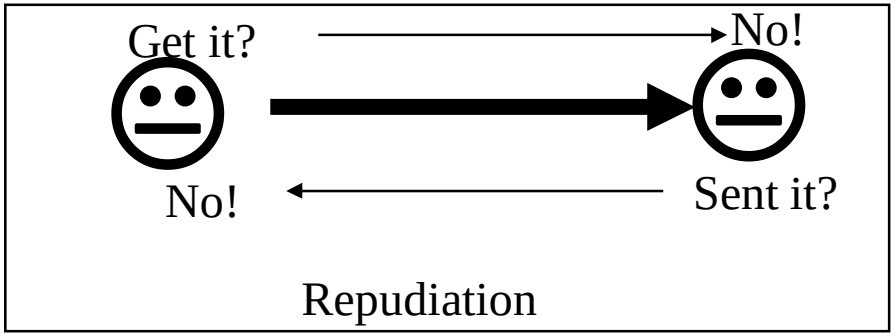


Availability

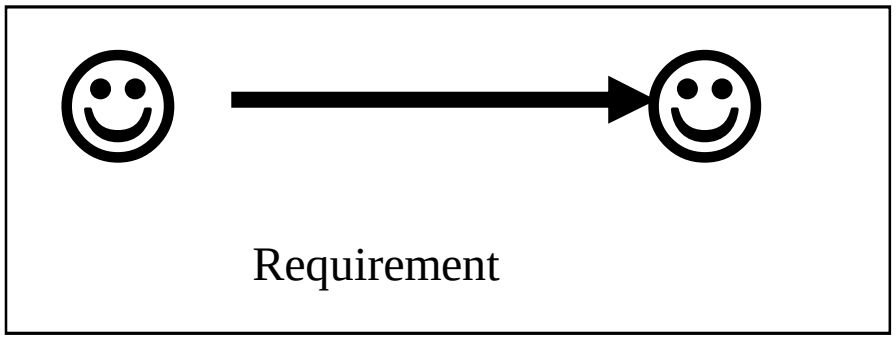
Integrity

Confidentiality





SECURITY ISSUES

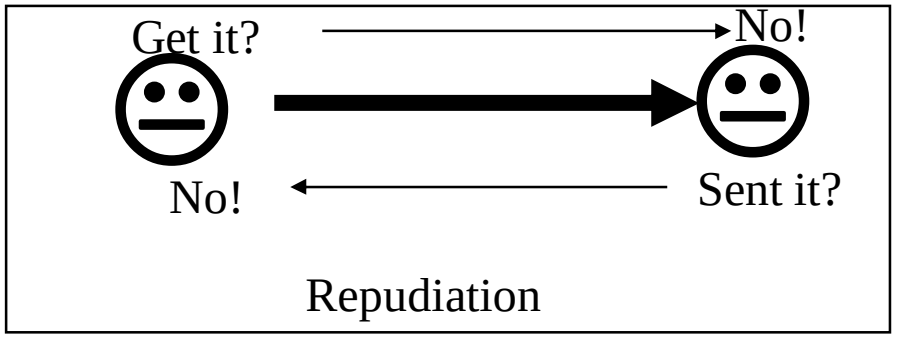


Availability

Integrity

Confidentiality

Authenticity



SECURITY ISSUES

Requirement

Availability

Integrity

Confidentiality

Authenticity

Non Repudiation

SECURITY MECHANISMS

- Confidentiality - Encryption
- Integrity - Hashing
- Authentication - Digital Certificates
- Non-Repudiation - Digital Signatures
- Cryptography plays a vital role in providing these services

BASIC TERMINOLOGY

Cryptology

Branch of mathematics and computer science that studies the mathematical foundation of cryptographic methods

Cryptography

Art of secret (crypto) writing (-graphy)

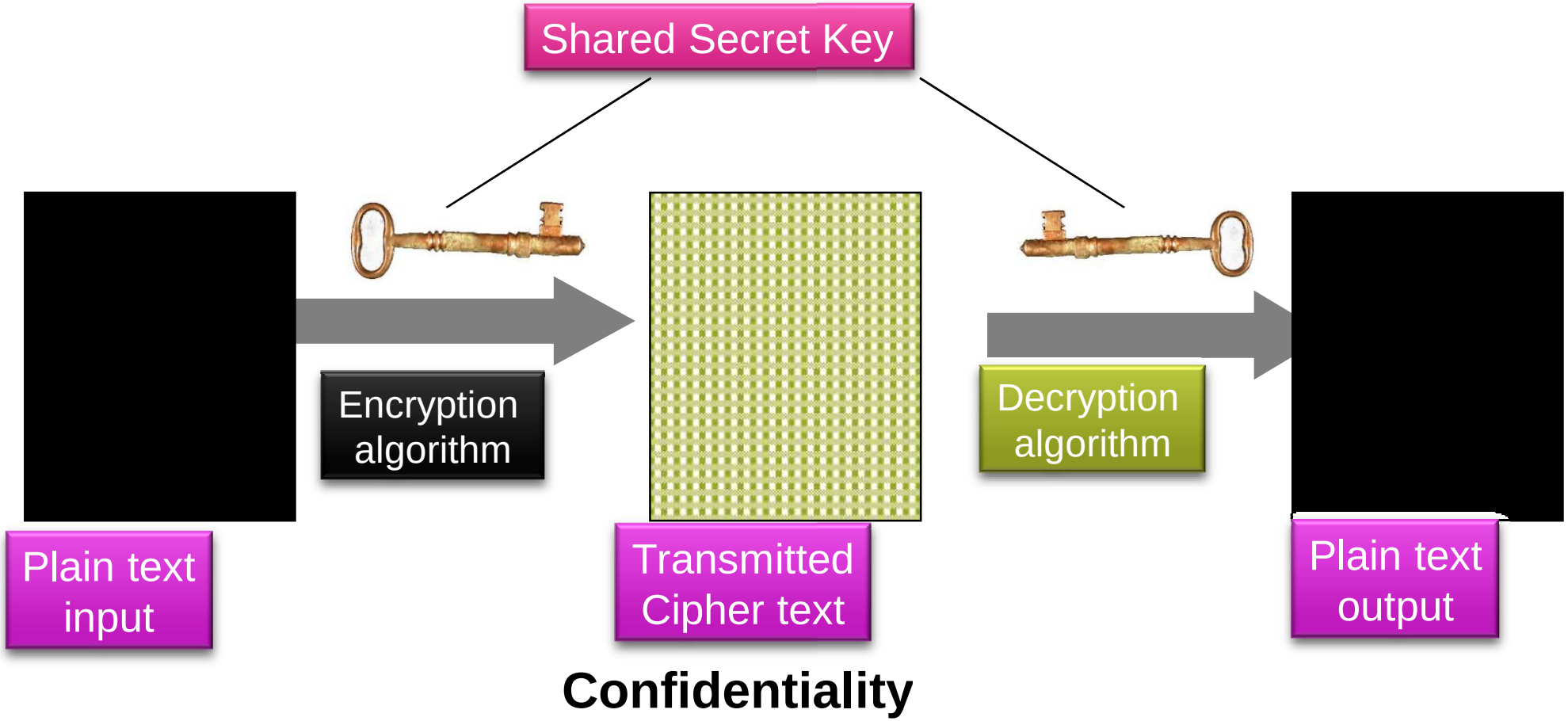
Cryptanalysis

Art of breaking ciphers

RYPTOGRAPHIC ALGORITHMS

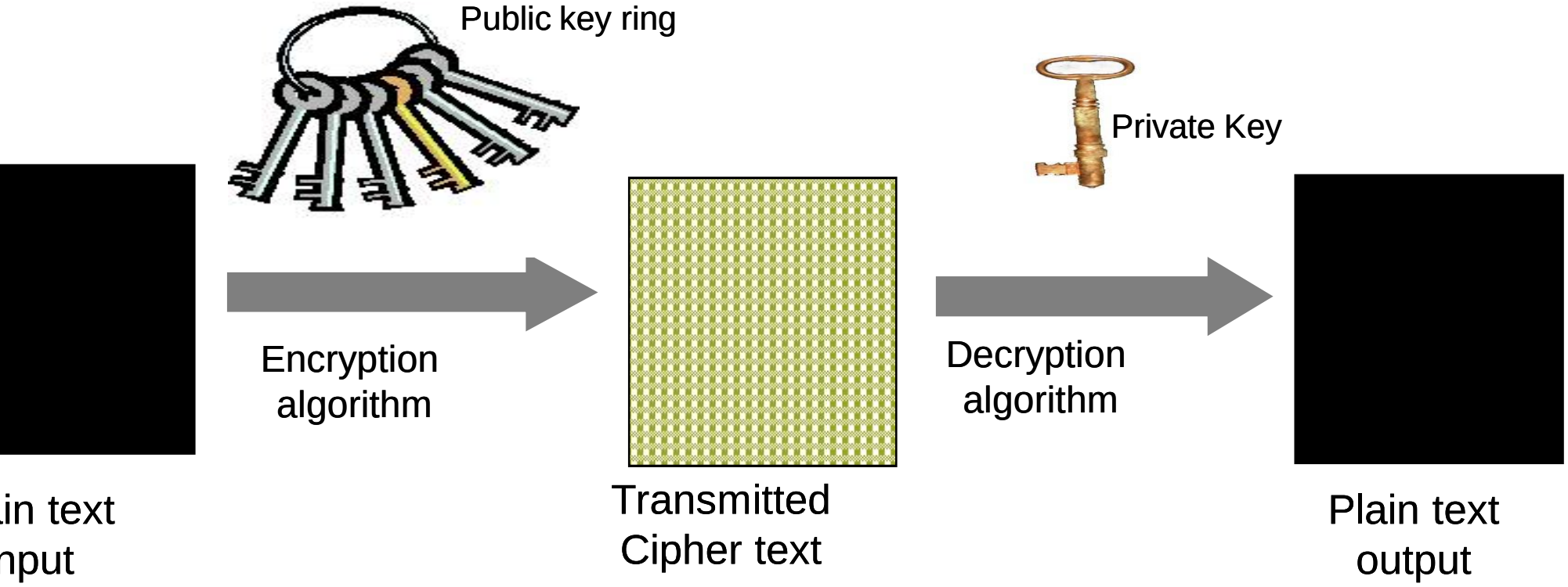
- Types of Cryptographic algorithms
  - Secret key cryptography or Symmetric Key
  - Public key cryptography or Asymmetric Key
  - Hash functions

CRET KEY ALGORITHMS



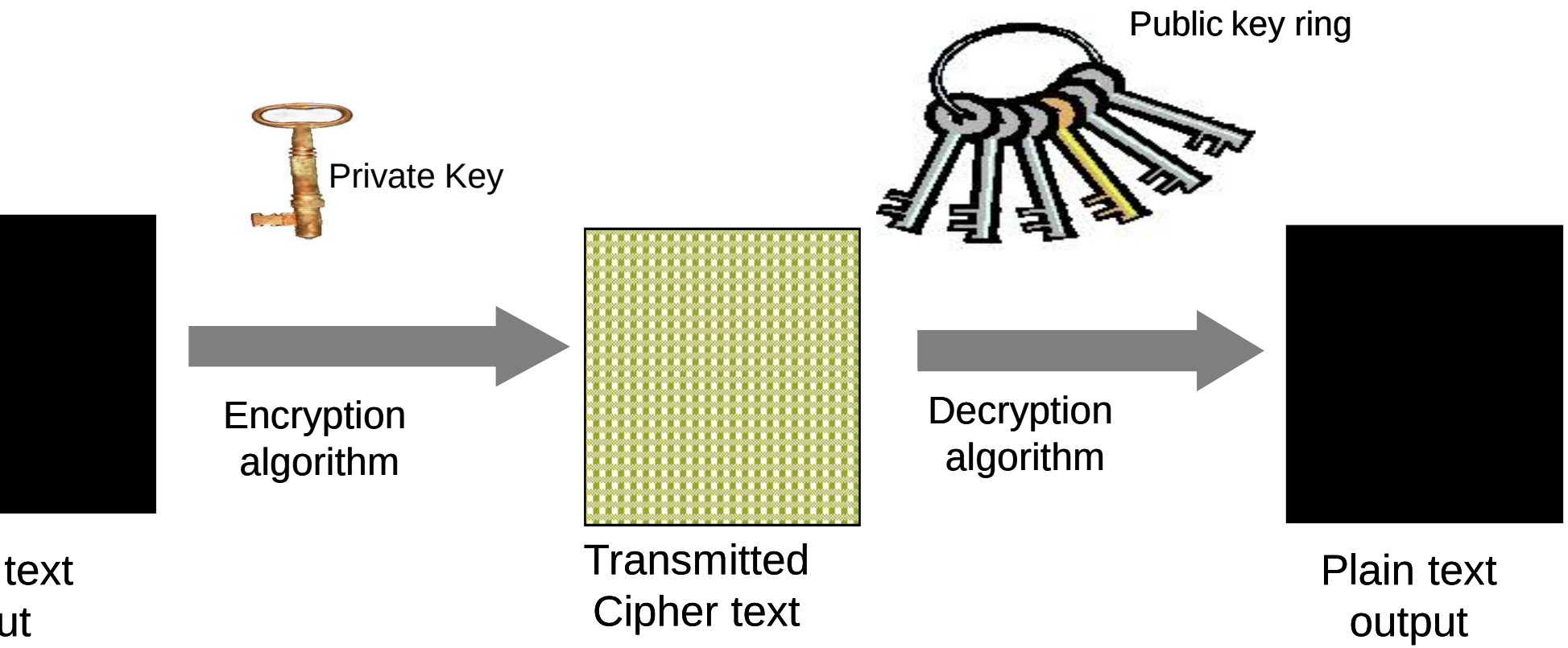
Confidentiality

UBLIC KEY ALGORITHMS



Confidentiality

UBLIC KEY ALGORITHMS



Authentication

PUBLIC KEY ALGORITHMS

Public key ring

Private Key

on
y

Encryption algorithm

encrypted key

Decryption algorithm

Shared session key

Key Exchange

HASH FUNCTIONS

- A public function that maps a plaintext message of any length into a fixed length hash value used as the authenticator
- Pros
  - One way transformation
  - Offers integrity without the cost of encryption
  - Message can be read when authentication is unnecessary
- Cons
  - No Confidentiality
  - Can be altered by attackers to match altered message

I UNEXPECTED SUCCESS...

- Evolution of technology, usage and value
- Evolution of security problems and solutions
- Evolution never stops...

E BIGGER PICTURE

YBER SECURITY

Cyber security policy which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks

Cyber security refers to the technologies and processes designed to protect computers, networks data from unauthorized access and attacks delivered via Internet by cyber criminals

YBER CRIME

It is a computer related crime, Internet crime, digital crime which uses high-technology tools comes under the cyber crime

People Vs. Technolog

STORY OF CYBER CRIME

First recorded cyber crime in 1820

The first spam email took place in 1978, when it was over ARPANET

First virus was installed on an Apple computer in 1982

OST COMMON CYBERCRIME

Debit/Credit Card Fraud – 38%

Compromised A/C Passwords – 34%

Online Purchase – 33%

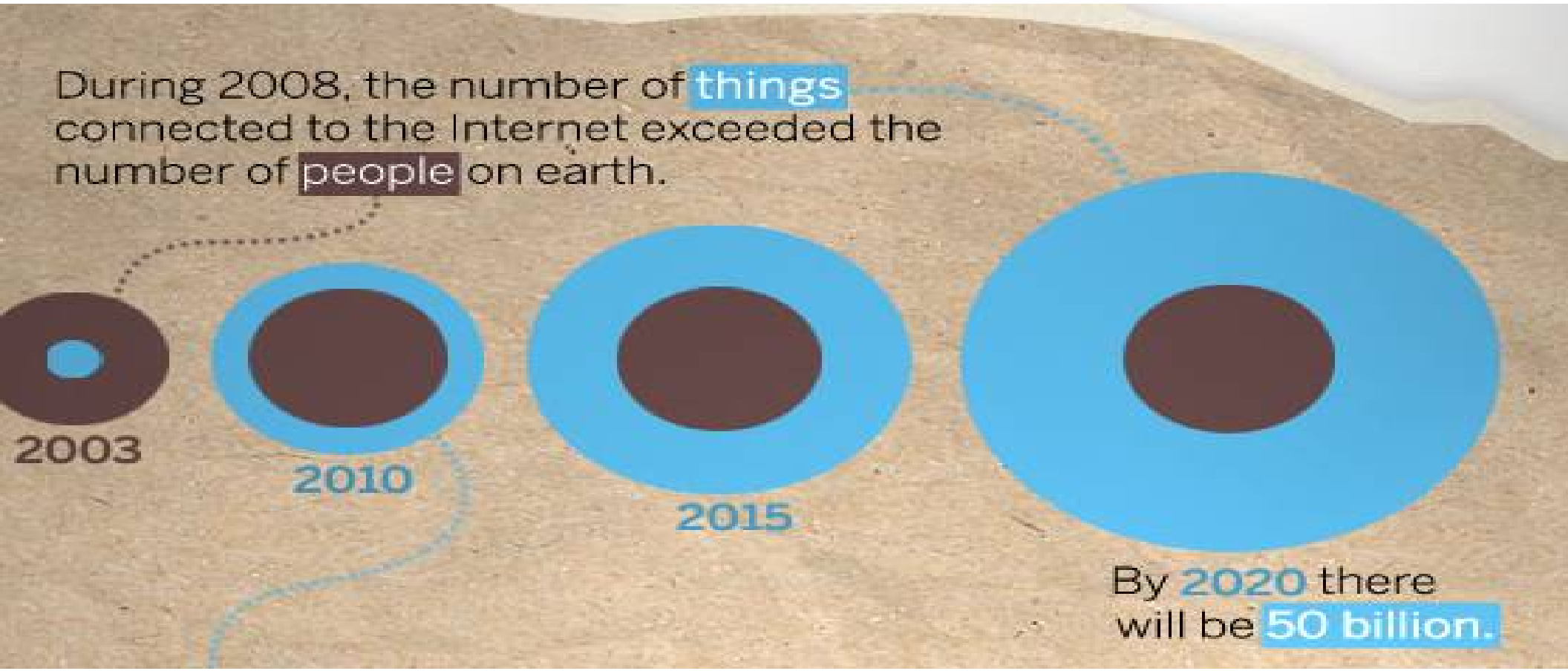
Unauthorized access or hacking of emails or social media A/C – 34%

Clicking on fraudulent email/ providing sensitive information – 32%

MOBILITY FACTS

erage People check their phones 150
day – That's once every 6.5 minutes

HINGS" CONNECTED TO THE INTERNET



rces: Cisco IBSG, Jim Cicconi, AT&T , Steve Leibson, Computer History Museum, CNN, versity of Michigan, Fraunhofer

mage Courtesy: : CISCO

BER ATTACKS AND DATA BREACHES

yber attack occurs when cybercriminals try to gain gal access to electronic data stored on a computer or etwork

e intent might be to inflict reputational damage or m to a business or person, or theft of valuable data

lata breach is a type of security incident. It occurs en information is accessed without authorization.

e information accessed could include personal rmation such as Aadhar numbers, passwords, and ancial account numbers

yber attack often happens first. A data breach might ow. Both incidents can have an impact on you

UTHENTICATION AND AUTHORIZATION

- **Access Control**
  - The ability to permit or deny the use of a resource by a user, through three essential services
- **Authentication**
  - To reliably identify the users
- **Authorization**
  - To control which users are allowed to do what with a resource
  - Representing trust, assuming reliable authentication

HISHING

- “Fishing“ for information such as usernames, passwords, credit card details, other personal information
- Forged emails apparently from legitimate enterprises, direct users to forged websites

IISHING

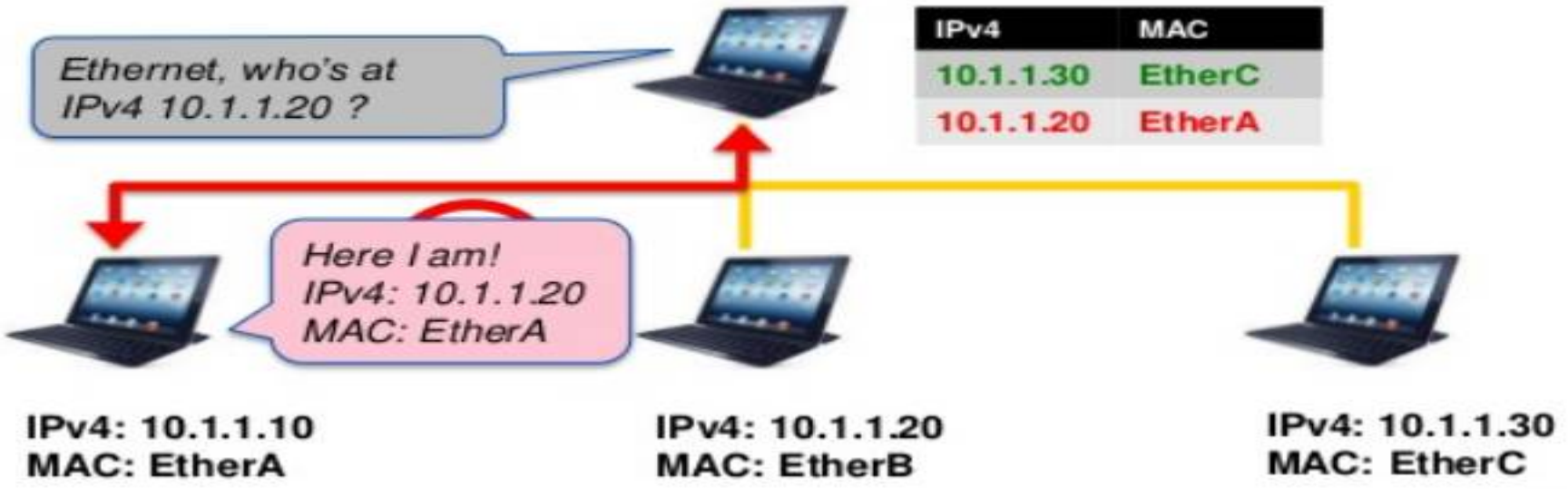

[redacted] @ icicibank . com [redacted]
[redacted]
bject: ICICI BANK : Please Update Your ICICI Bank detaild
Message | ICICI Netbanking Online Security Verfication.html (378 B)
ICICI Bank
Net Banking Upgrade Notifications.
Dear ICICI Net Banking User,
ICICI Bank is constantly striving to provide you with more convenience, control, and security to assist in managing your finances online. As part of our ongoing efforts to operate on ISO requirements, and create an enhanced security portal for your online banking services, we have upgraded the ICICI Electronic-Sign Consent and Online Access. To Upgrade your account security status it is mandatory that you kindly Login to your online banking using the link specified below to update us on your account information.
Do kindly update your account profile by downloading the attached file
Note
Failure to update your account details within seventy two (72) hours of receiving this notice could lead to account being suspended and online access restricted.
Thank you for your cooperation.
Sincerely,
ICICI Bank Ltd.
Online Banking Security Unit
Copyright 2014 ICICI Bank

ASQUERADING EXAMPLE: ARP

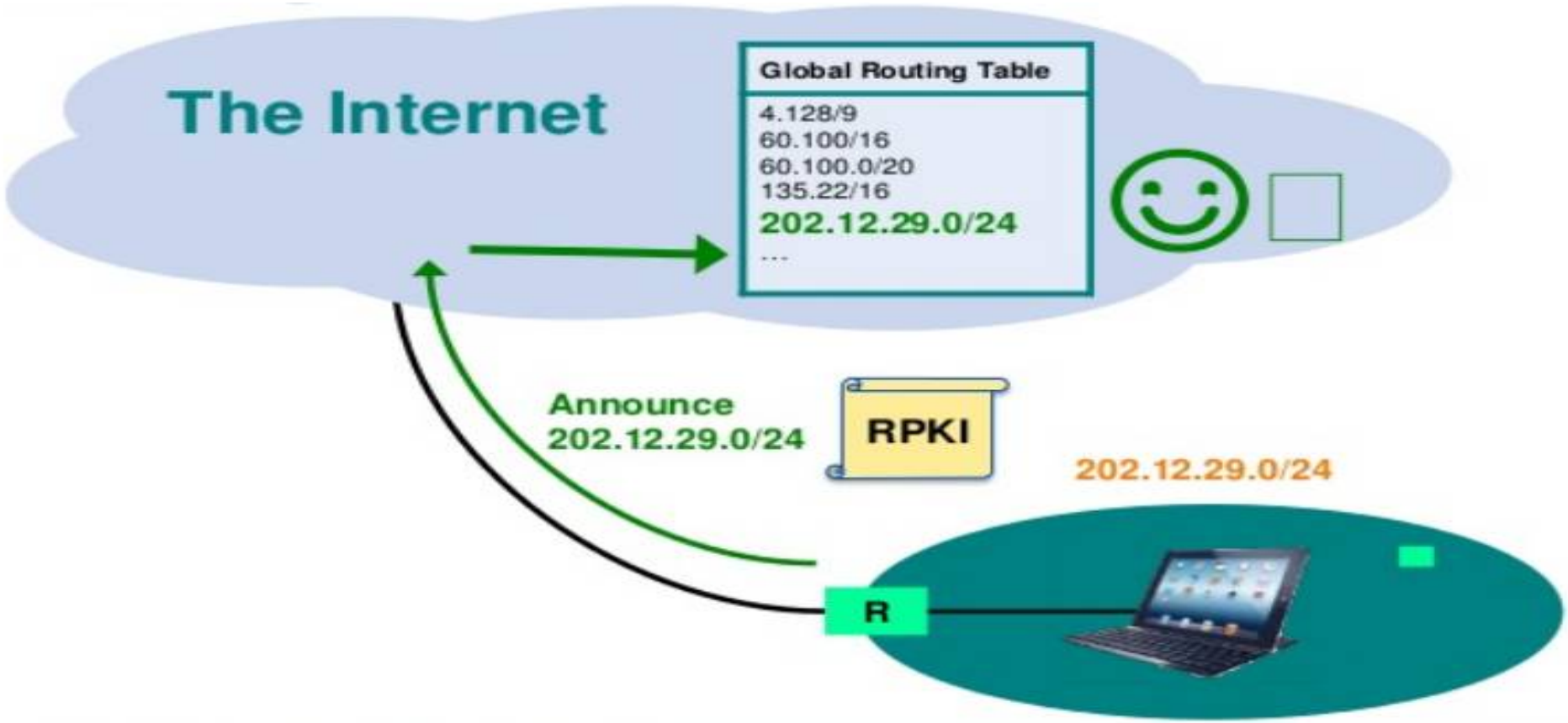
- Address Resolution Protocol
- Used by any TCP/IP device to discover the layer 2 address of an IPv4 address that it wants to reach

ASQUERADING EXAMPLE: ARP

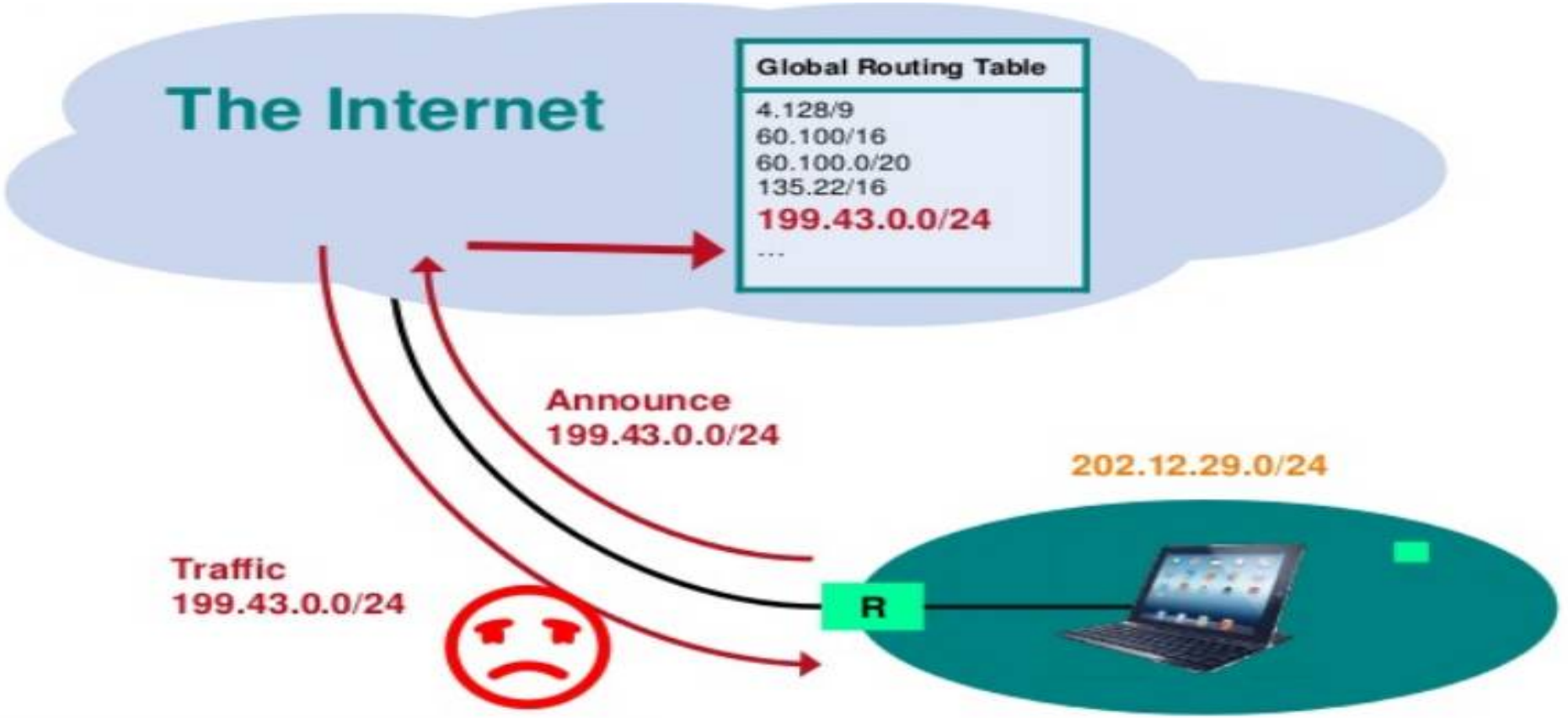
- Address Resolution Protocol
- SEND: IPv6 Secure Neighbour Discovery



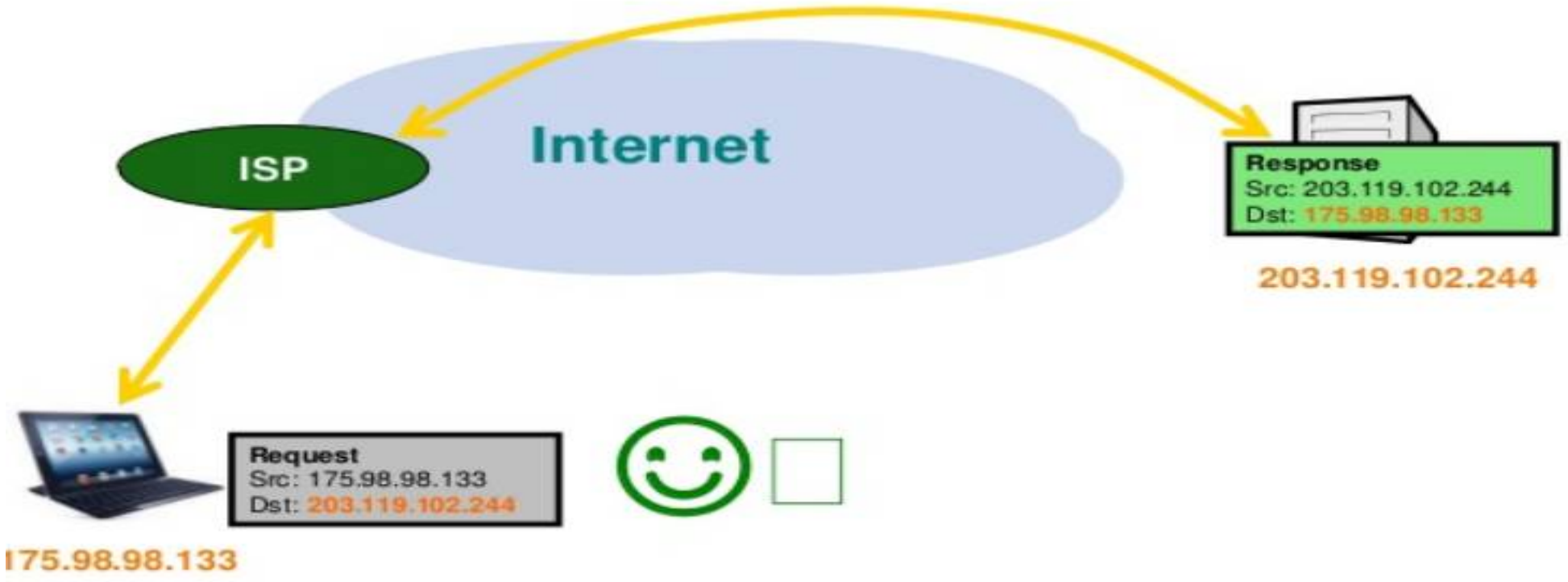
SUSING IP ADDRESSES



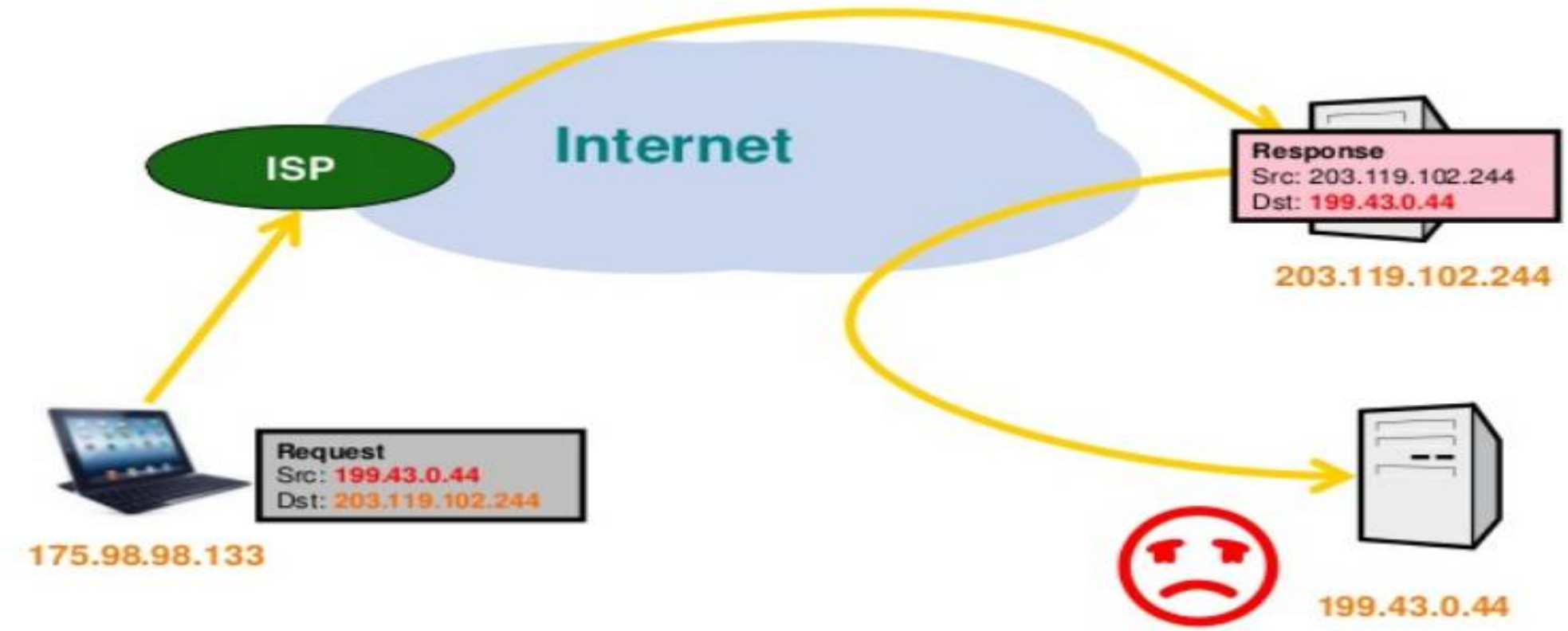
SUSING IP ADDRESSES



ASQUERADING AGAIN: IP SPOOFING



ASQUERADING AGAIN: IP SPOOFING



SECURING YOURSELF

- **Awareness**
  - What information you have
  - How important it is
  - How secure it is
- **Assess**
  - What could happen if lost or in the wrong hands
- **Adequate**
  - Precautions to protect it

CURING YOURSELF

Common Sense

Awareness

Regularly Update Patches

Anti Virus, anti spyware…

Be careful on P2P file sharing

what you download

Read the computer message(s)

- Don‘t blindly click next > next > next
- Be careful when you read email especially if it belongs to someone else
- Don‘t try to open every attachment
- Keep your password to yourself
- CyberSecurity – Cyberethics – Cybersafety

THANK YOU