Cyber Crimes

M. A. Taherkhani

Dec. 2013

Agenda

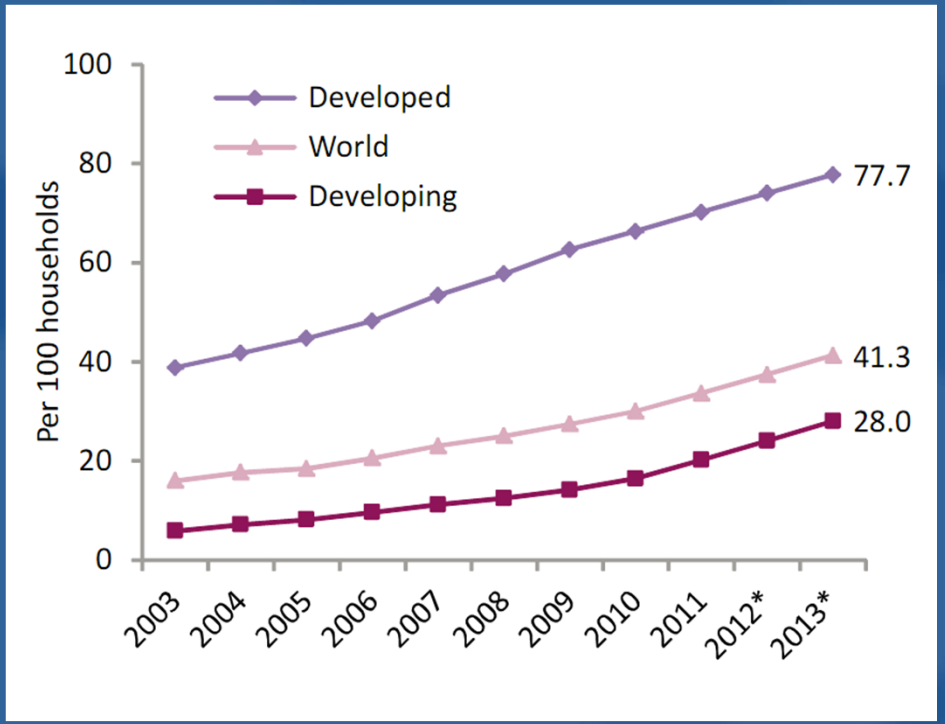
- Concept & Definitions
- Theoretical Aspects of Attacks
- Cyber Attacks: A Case Study
  - Identity Theft
  - Social Engineering
  - Malwares
  - Denial of Services
- References

Concepts & Definitions

- Cyber Crime: Any crime conducted via cyber infrastructures
  - computer networks: Internet
  - some other inter-communication networks

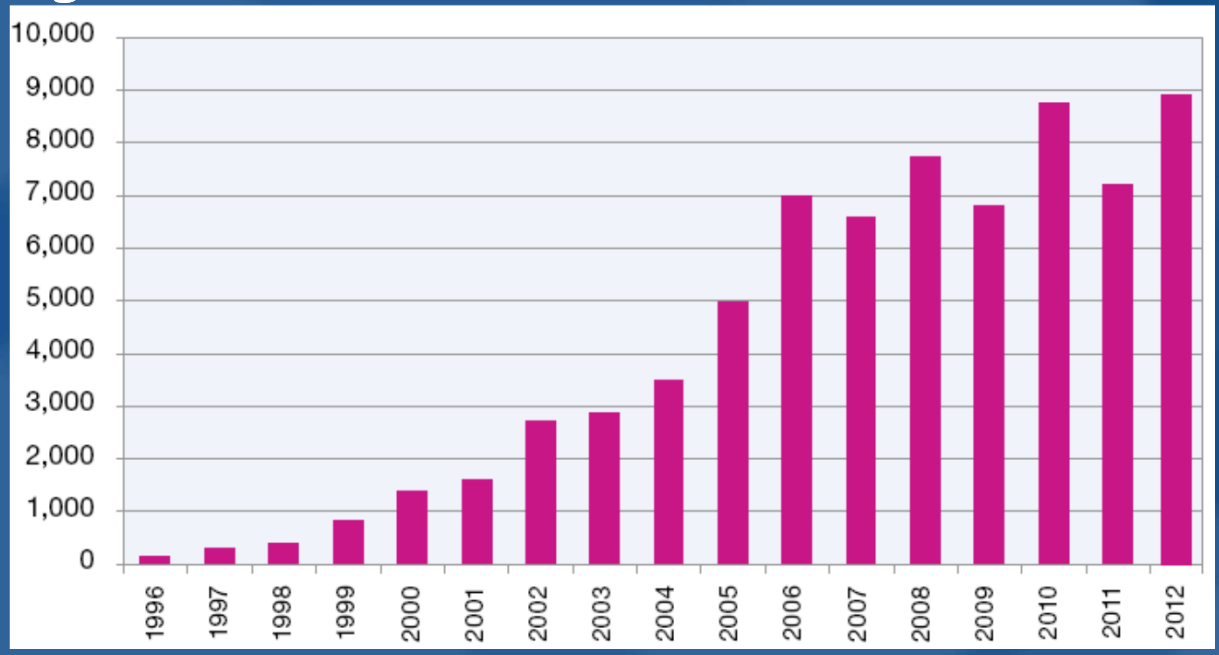
Concepts & Definitions

- Current Trends (Technical):
  - Household with Internet Access:
    (Ref: ITU: Annual Report. 2013)



Concepts & Definitions

- Current Trends (Technical):
  - Household with Internet Access
  - Increasing no. Vulnerabilities (Ref: Xforce-2012)

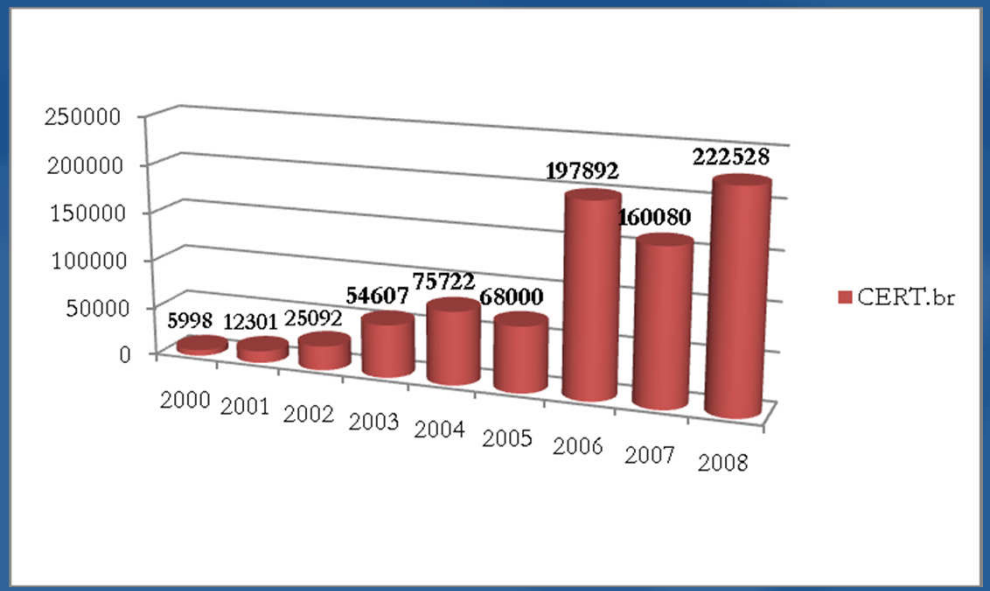


Vulnerability:

An error or weakness in design, implementation or operation

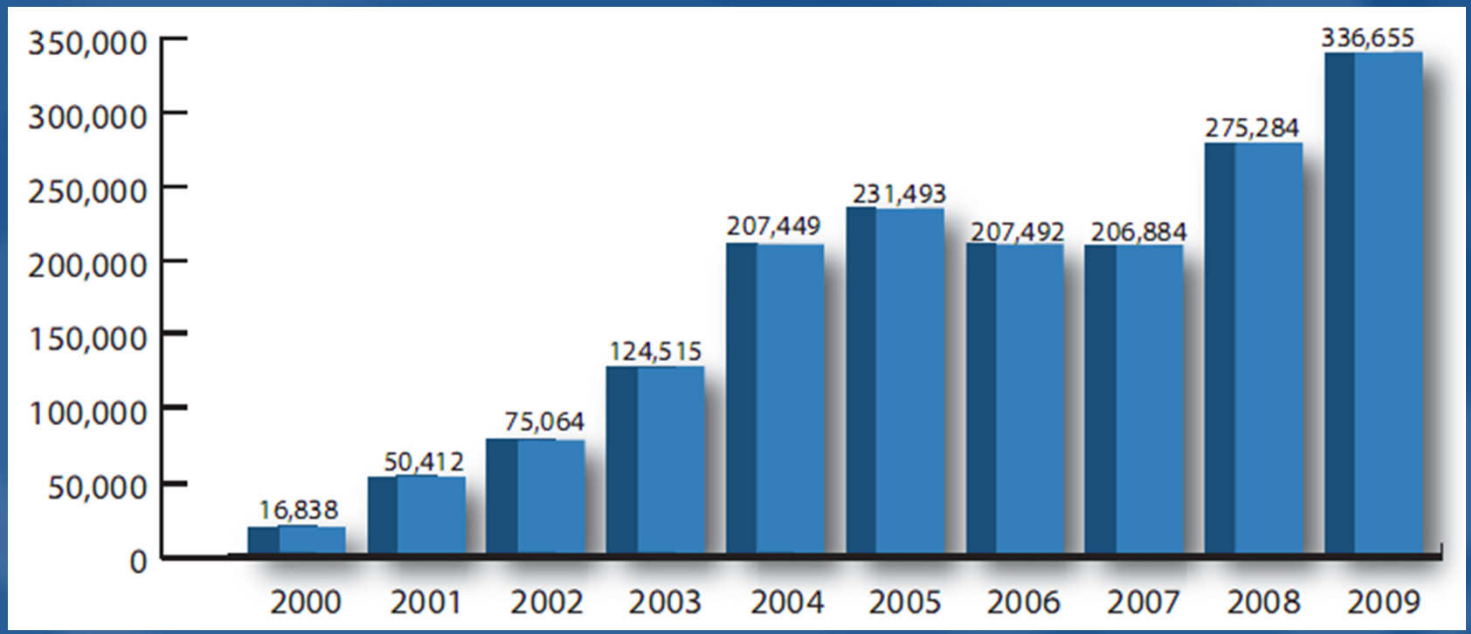
Concepts & Definitions

- Current Trends (Technical):
  - Household with Internet Access
  - Increasing no. Vulnerabilities
  - Increasing no. of Security Incidents
    - CERT/CC, CSIRT



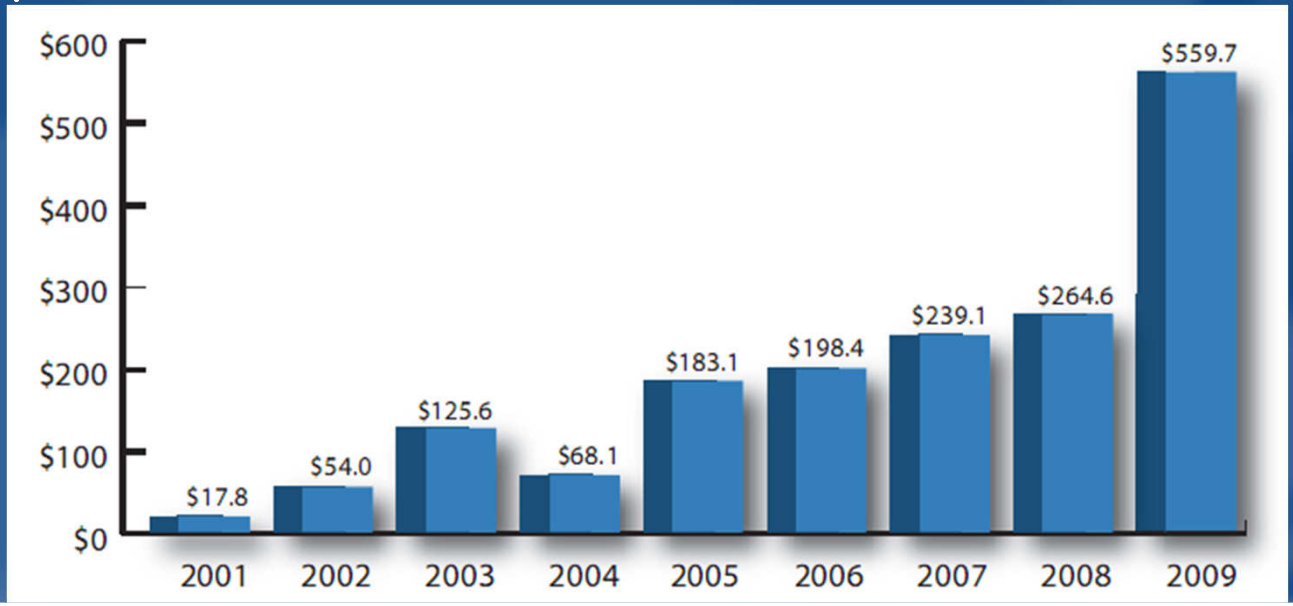
Concepts & Definitions

- Current Trends (Case Study)
  - Internet Crime Compliant Center: IC3
    - Yearly Comparison Complaints Received via the IC3 Web site:



Concepts & Definitions

- Current Trends (Case Study)
  - Internet Crime Compliant Center: IC3
    - Yearly Comparison Complaints Received via the IC3 Web site
    - Yearly Dollar Loss (in millions) of Referred Complaints



Concepts & Definitions

- Current Trends (Case Study)
  - Internet Crime Compliant Center: IC3
    - Yearly Comparison Complaints Received via the IC3 Web site
    - Yearly Dollar Loss (in millions) of Referred Complaints
  - FBI Report (2005)
    - 9 out of 10 businesses affected by cybercrime
    - $67.2 billion per year is lost to cybercrime in the USA

Concepts & Definitions

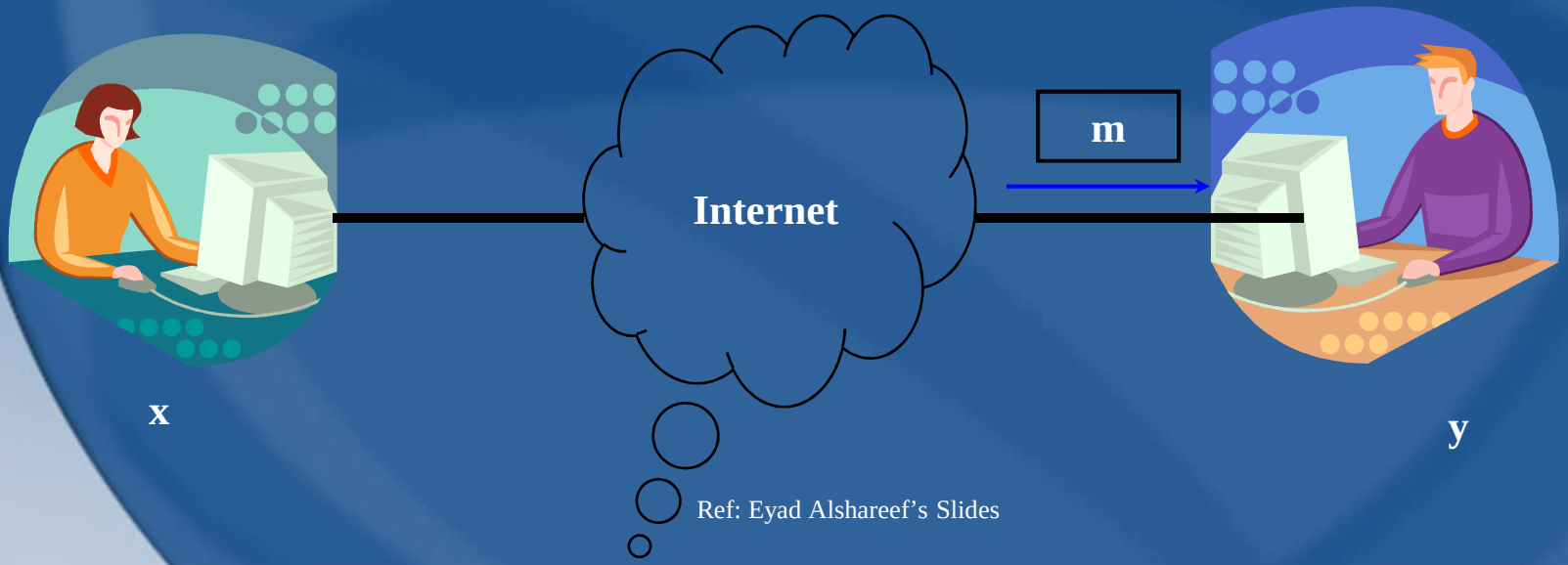
- Security Metrics
  - Confidentiality
    - The asset can only be viewed by authorized entities
  - Integrity
    - The asset is protected from accidental or deliberate modification
  - Availability
    - The asset is available for legitimate entities
  - Non-Repudiation
    - proves the origin of the data/service

Agenda

- Concept & Definitions
- Theoretical Aspects of Attacks
- Cyber Attacks: A Case Study:
  - Identity Thefts
  - Social Engineering
  - Malwares
  - Denial of Services
- Security Mechanism
- References

Theoretical Aspects of Attacks

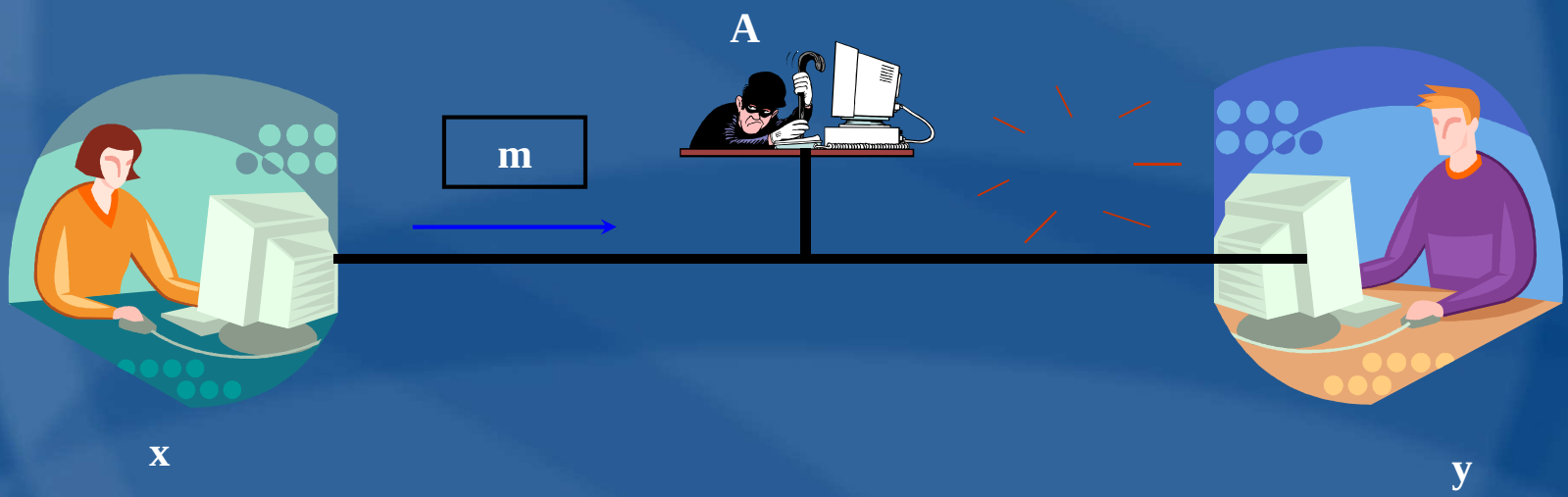
- Theoretical aspects of Attacks
  - Waiting for receiving message m (Ref: Eyad Alshareef)



Ref: Eyad Alshareef's Slides

Theoretical Aspects of Attacks

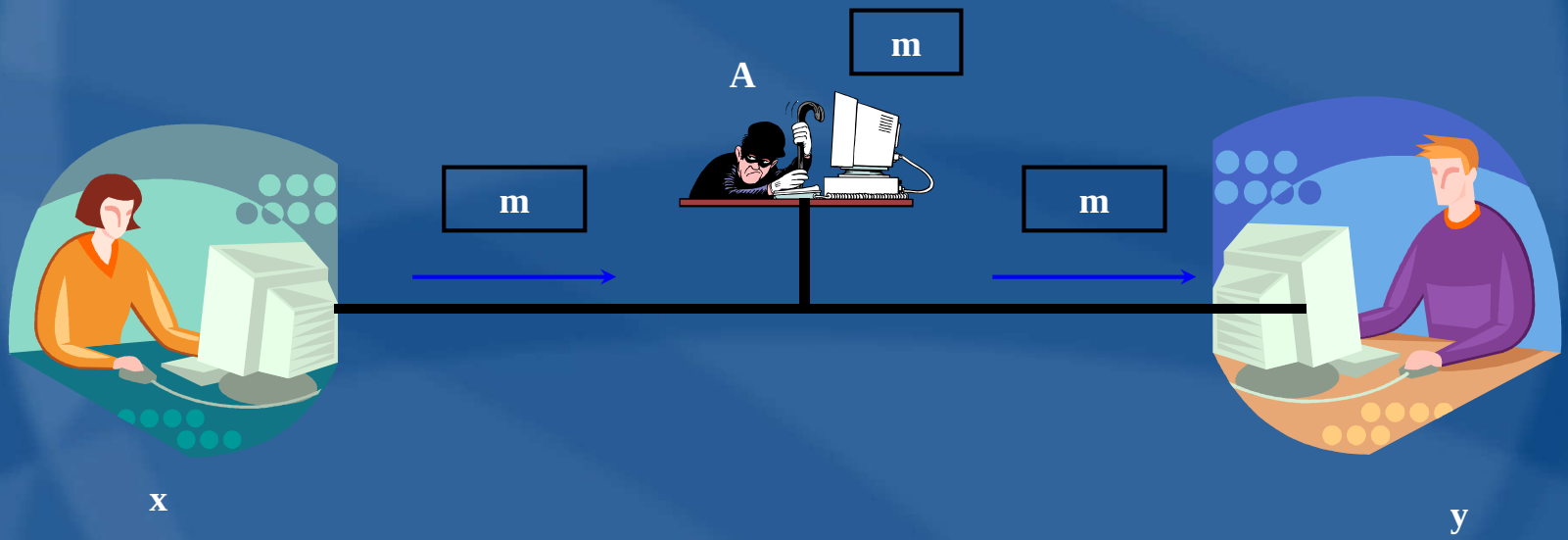
- Interruption:
  - Adversary (A) can discard (m) in its transit



Ref: Eyad Alshareef's Slides

Theoretical Aspects of Attacks

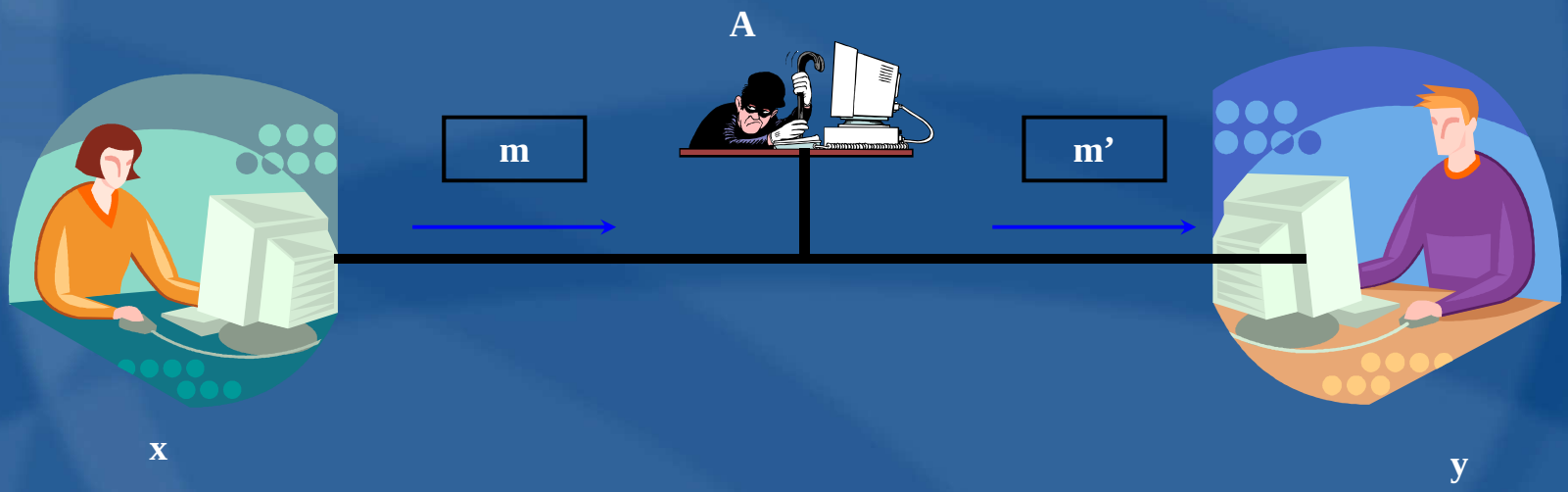
- Interception:
  - Adversary (A) can get a copy of (m) when (m) passes by



Ref: Eyad Alshareef's Slides

Theoretical Aspects of Attacks

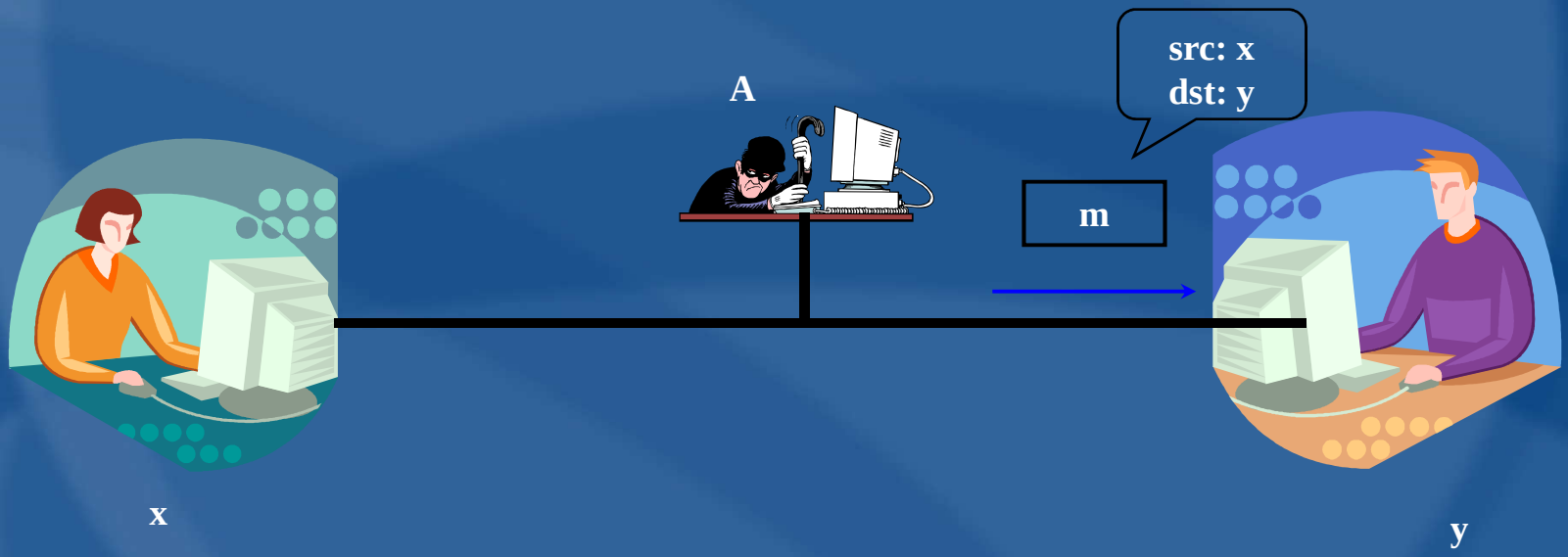
- Modification:
  - Adversary (A) can arbitrarily modify the content of (m) to become (m')



Ref: Eyad Alshareef's Slides

Concepts & Definitions:

- Fabrication:
  - Adversary (A) can arbitrarily fabricate a message (m), pretending that (m) was sent by (x)

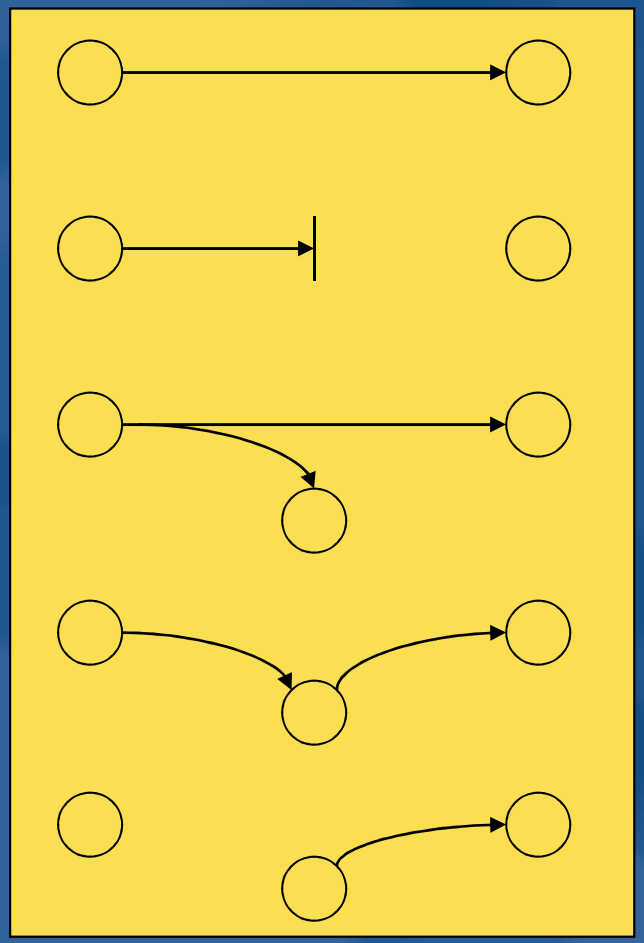


Ref: Eyad Alshareef's Slides

Concepts & Definitions:

- Normal Flow:

- Interruption:
  - Attack on Availability
- Interception:
  - Attack on Confidentiality
- Modification:
  - Attack on Integrity
- Fabrication:
  - Attack on Non-Repudiation



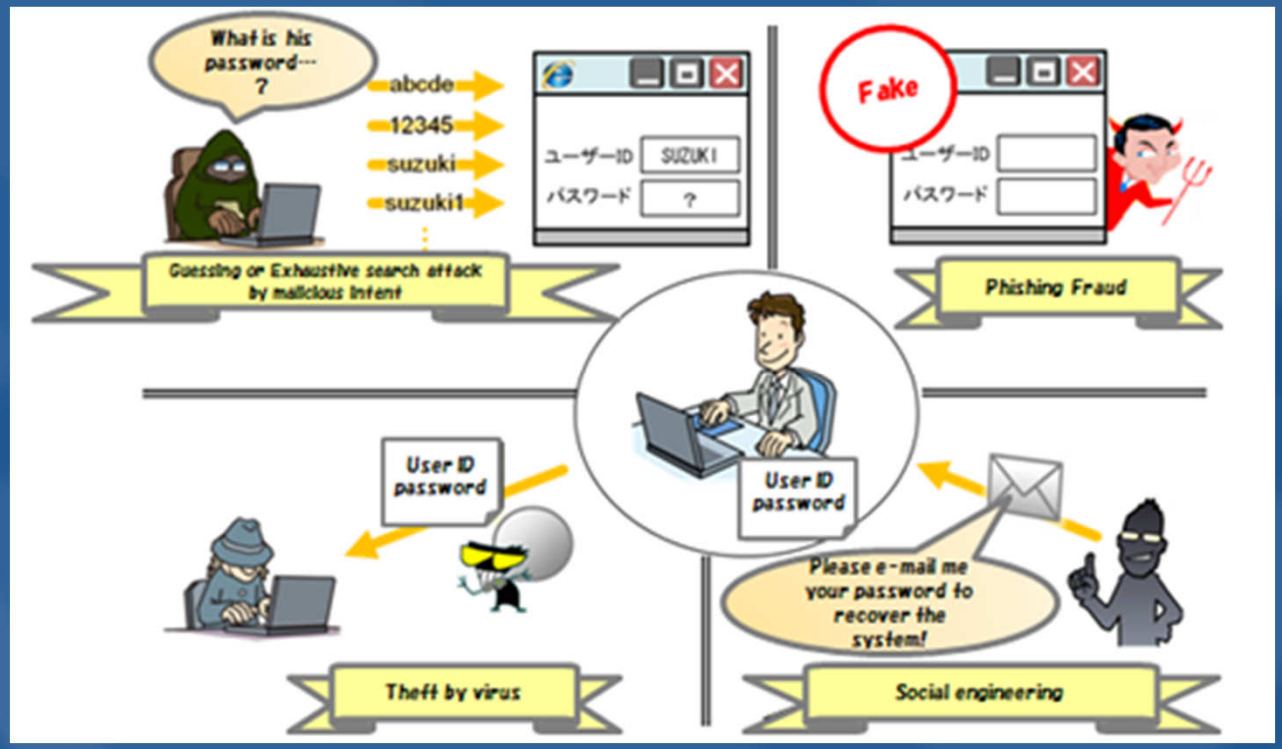
Ref: Eyad Alshareef's Slides

Agenda

- Concept & Definitions
- Theoretical Aspects of Attacks
- Cyber Attacks: A Case Study:
  - Identity Theft
  - Social Engineering
  - Malwares
  - Denial of Services
- References

Cyber Attacks

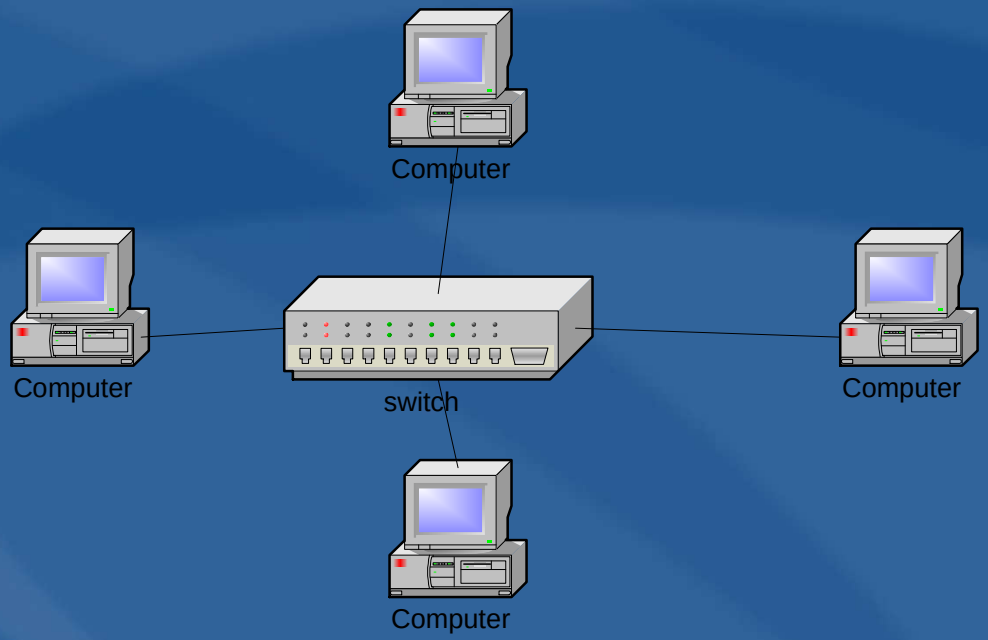
- Case Study
  - Target: Your User Account



Ref: http://www.ipa.go.jp

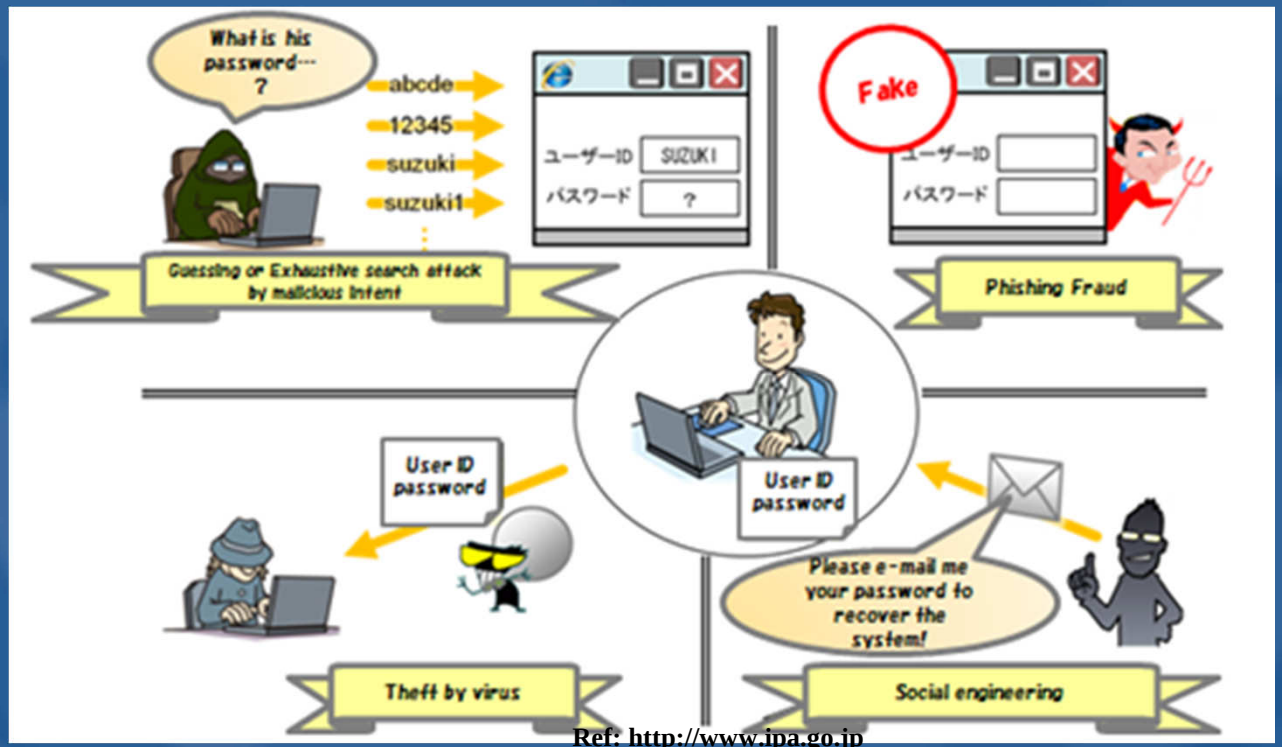
Cyber Attacks

- Identity Theft:
  - Password Sniffing
    - Eavesdropping network traffic
  - Password Cracking



Cyber Attacks

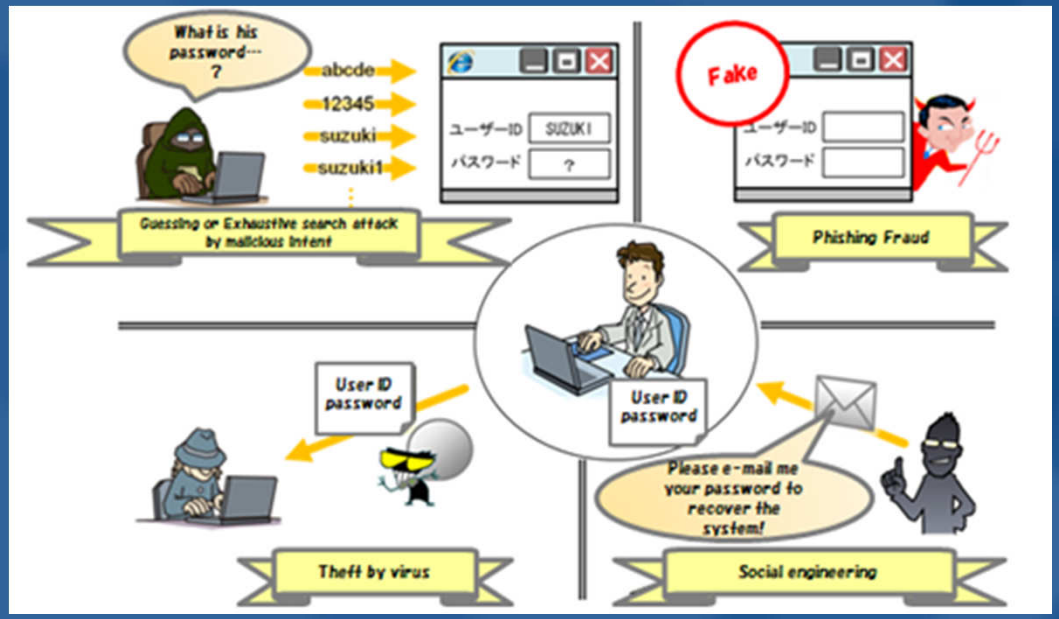
- Social Engineering Attacks
  - Phishing
  - Pharming



Ref: http://www.ipa.go.jp

Cyber Attacks

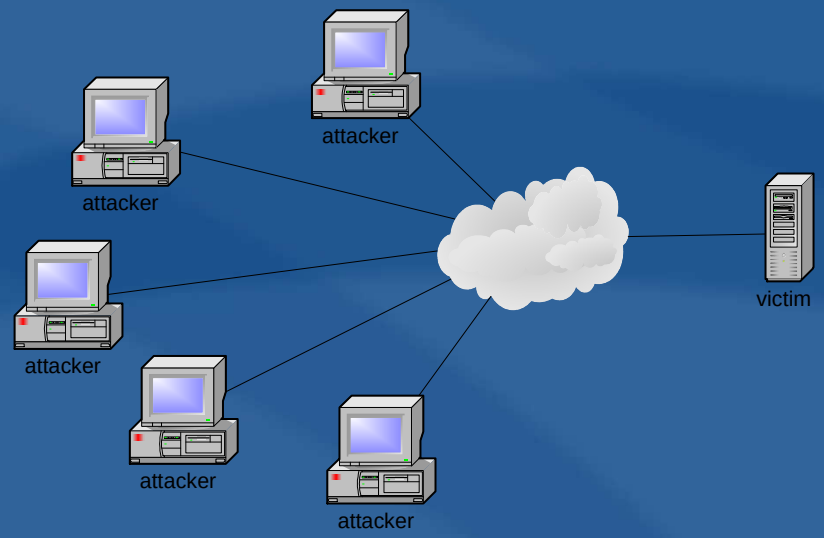
- Malware
  - Virus
  - Worms
  - Rootkits
  - Trojan Horses
  - Etc.



Ref: http://www.ipa.go.jp

Cyber Attacks

- Denial of Service
  - Distributed DoS



References

- ITU Annual Report (2012)
- IC3 Report (2009)
- FBI Cyber Report (2005)
- Network Security Essentials