INTRODUCTION

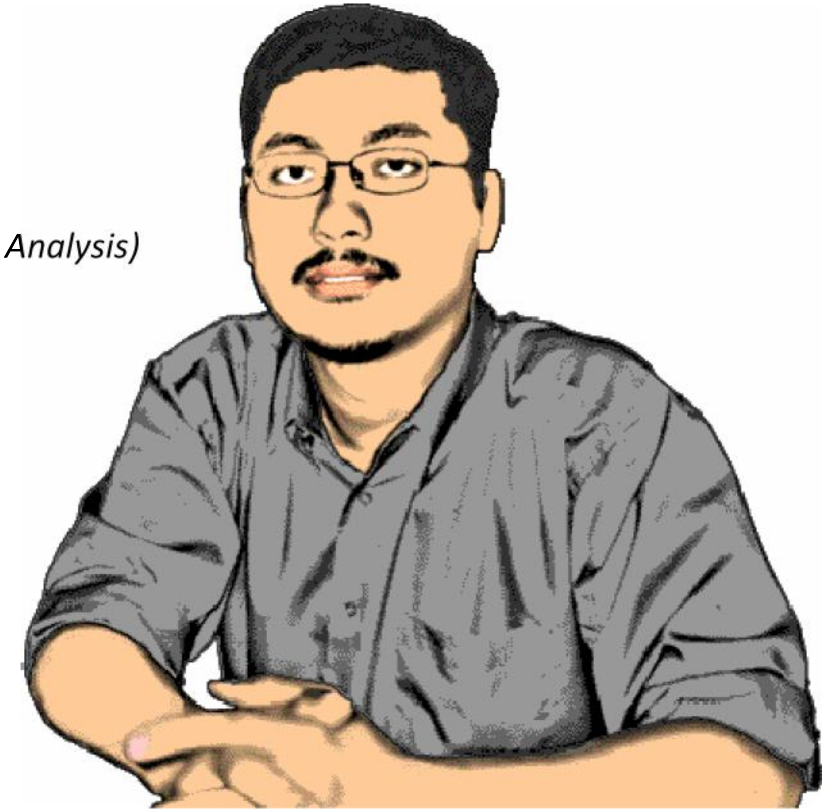
MALWARE ANALYSIS AND DIGITAL INVESTIGATION

BITS 3453

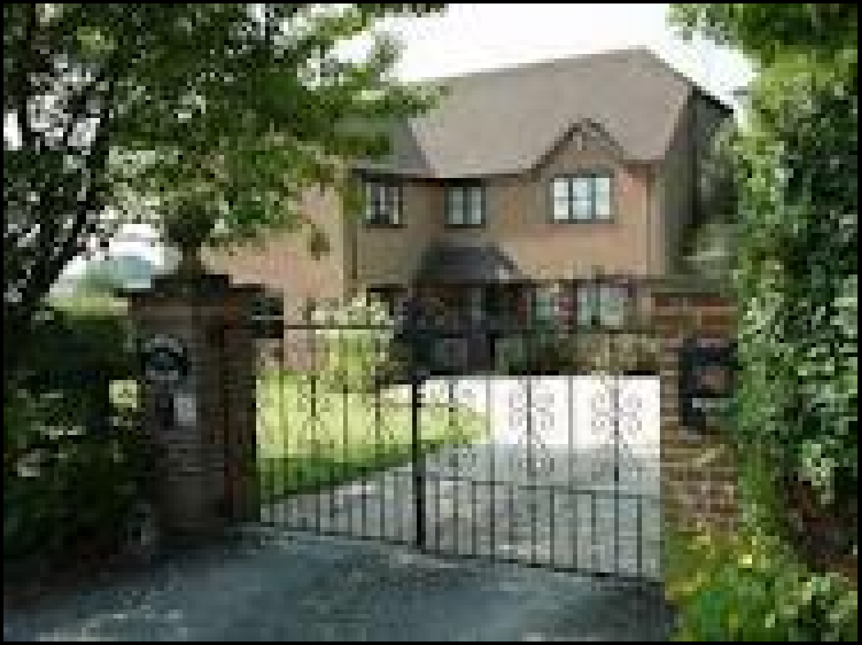
About Your Lecturer……

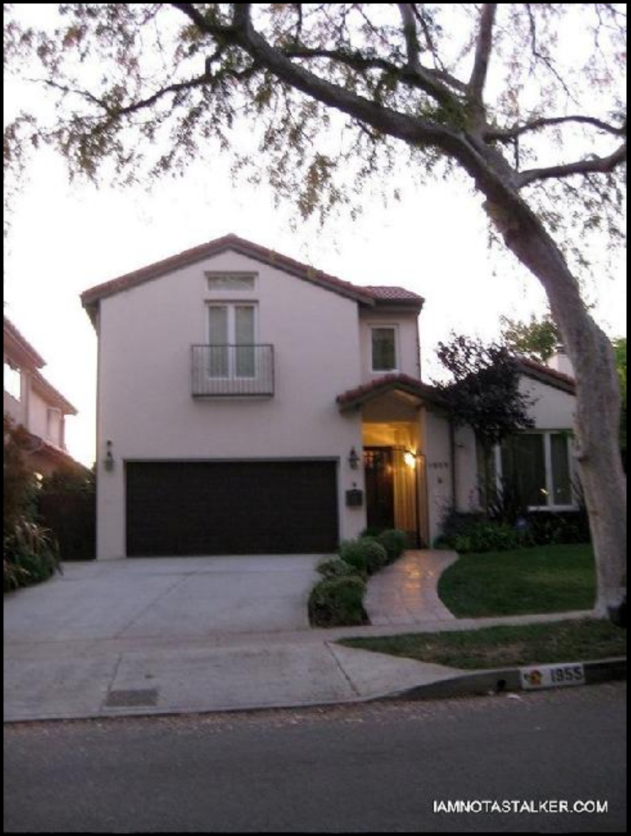
- Lecturer Name
  - Ts. Dr. Mohd *Zaki* Bin Mas'ud

    Senior Lecturer
    PhD (UTeM) Computer and Network Security (Malware Analysis)
    MIT(SC) (UKM) Science Computer
    B. Eng (Hons) Electronic (MMU) Electronic Engineering
    CHFI,CEH,CCNAI,CNE6
- Contact
  - 0133940912
  - zaki.masud@utem.edu.my
  - FTMK B2-20
- Consultation Hour
  - By appointment



Which one is easier to break into





THERE ARE NO SECURITY, THERE ARE ONLY OPPURTUNITY

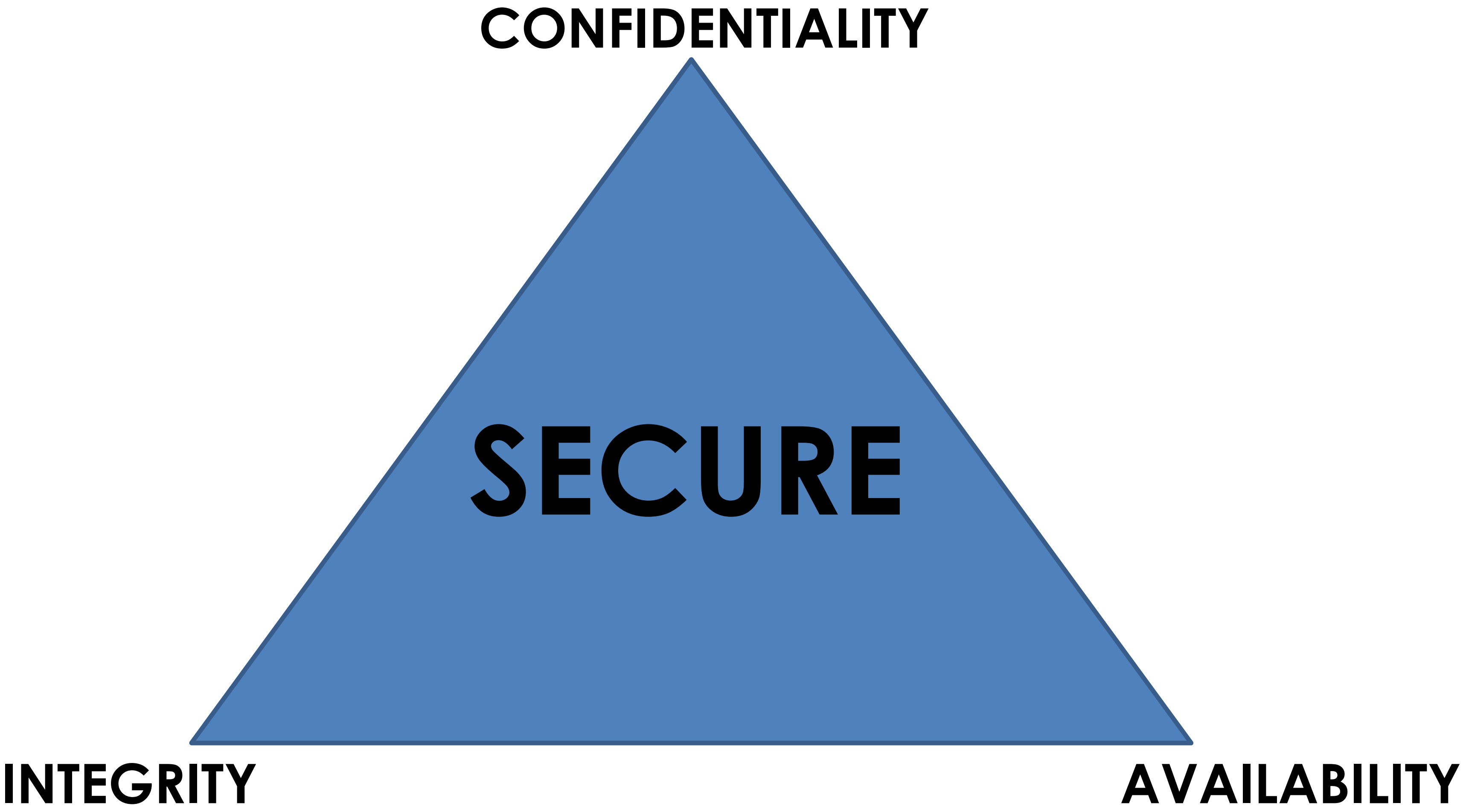
What is Security

- Dictionary.com says:
  - 1. Freedom from risk or danger; safety.
  - 2. Freedom from doubt, anxiety, or fear; confidence.
  - 3. Something that gives or assures safety, as:
    - 1. A group or department of private guards: Call building security if a visitor acts suspicious.
    - 2. Measures adopted by a government to prevent espionage, sabotage, or attack.
    - 3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant.
- Etc…

Why do we need security?

- Protect vital information while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- Provide authentication and access control for resources
  - Ex: AFS
- Guarantee availability of resources
  - Ex: 5 9’s (99.999% reliability)

What to achieve



What is the threat?

1 - Destruction (an attack on availability):

- Destruction of information and/or network resources

2 - Corruption (an attack on integrity):

- Unauthorized tampering with an asset

3 - Removal (an attack on availability):

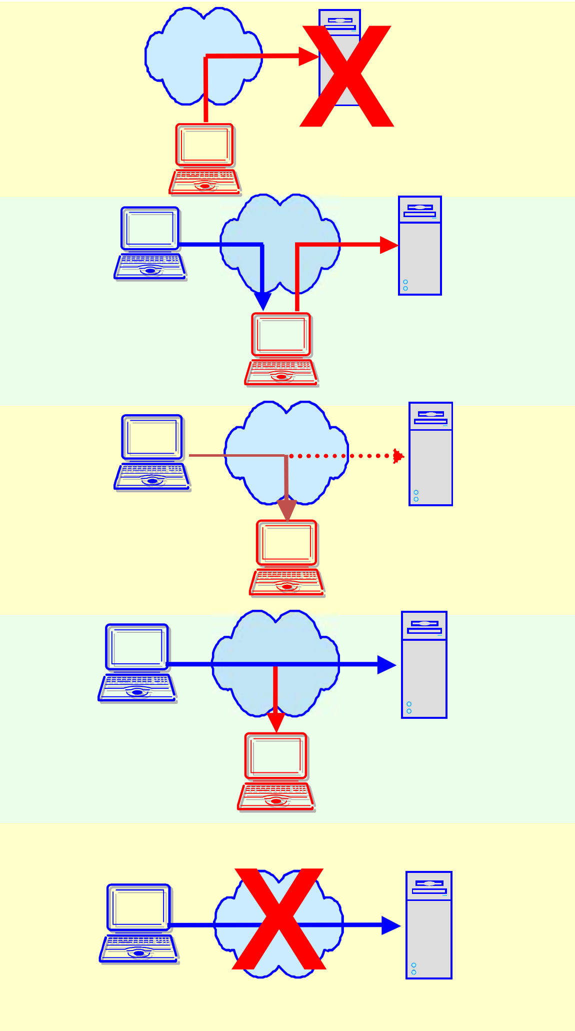
- Theft, removal or loss of information and/or other resources

4 - Disclosure (an attack on confidentiality):

- Unauthorized access to an asset

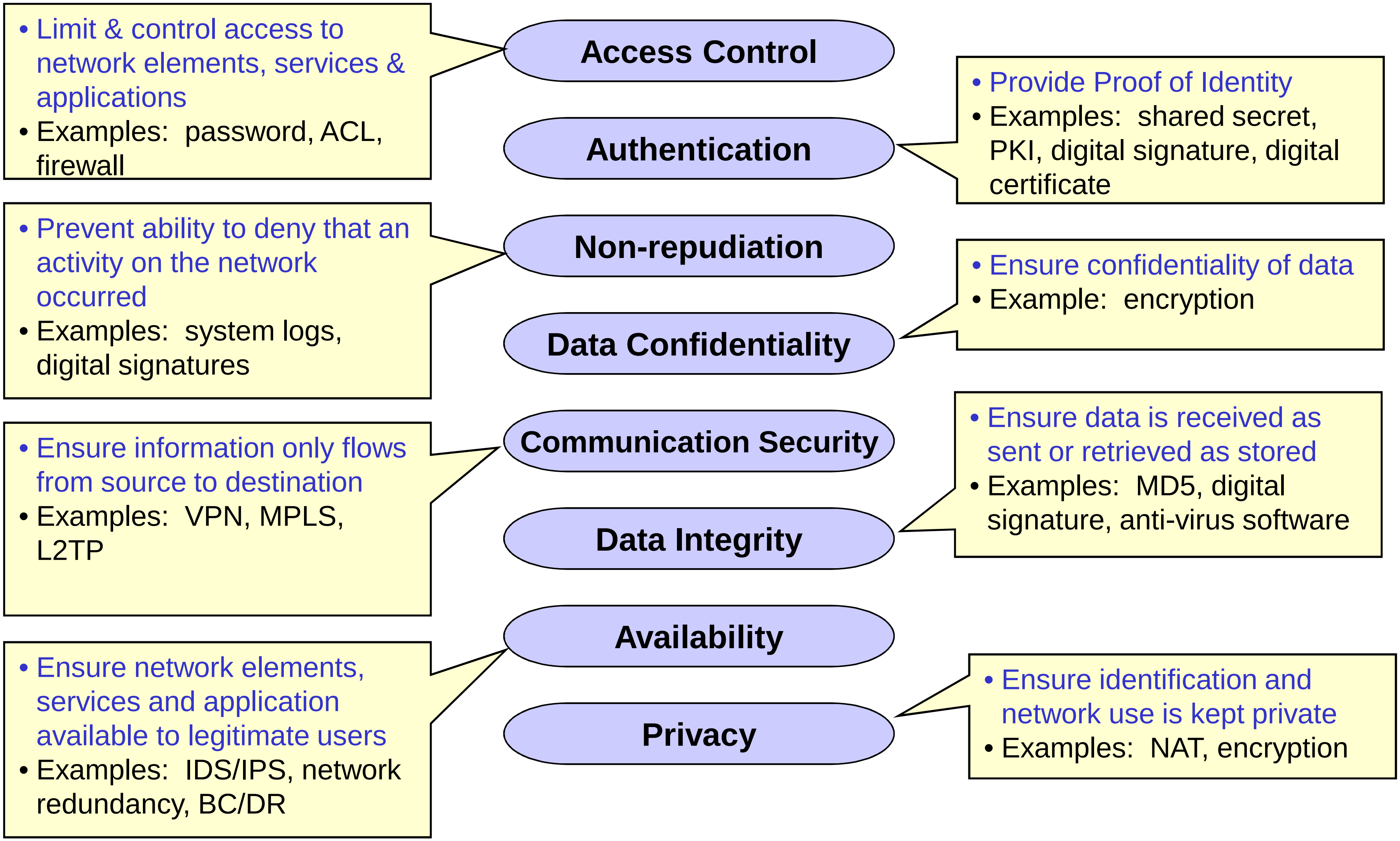
5 - Interruption (an attack on availability):

- Interruption of services. Network becomes unavailable or unusable



ITU-T X.800 Threat Model

Eight Security Dimensions Address the Breadth of Network Vulnerabilities



Access Control

- Limit & control access to network elements, services & applications
- Examples: password, ACL, firewall

Authentication

- Provide Proof of Identity
- Examples: shared secret, PKI, digital signature, digital certificate

Non-repudiation

- Prevent ability to deny that an activity on the network occurred
- Examples: system logs, digital signatures

Data Confidentiality

- Ensure confidentiality of data
- Example: encryption

Communication Security

- Ensure information only flows from source to destination
- Examples: VPN, MPLS, L2TP

Data Integrity

- Ensure data is received as sent or retrieved as stored
- Examples: MD5, digital signature, anti-virus software

Availability

- Ensure network elements, services and application available to legitimate users
- Examples: IDS/IPS, network redundancy, BC/DR

Privacy

- Ensure identification and network use is kept private
- Examples: NAT, encryption

Eight Security Dimensions applied to each Security Perspective (layer and plane)

Q
&
A