Implementation and Management of Systems Security

158.738

A/Prof. Julian Jang-Jaccard
Massey University

INTRODUCTION TO SECURITY

Why Need Security?

- Day to day operations depend on the data and applications
- Reliance on the use of electronic-based information processing, storage, and communication
- Data is now recognized as the most valuable asset
  - Average value of organizational data and applications far exceeds cost of networks
- Organizations vulnerable due to dependency on computing and widely available Internet access to its resources

19 Online Cheating Site AshleyMadison Hacked

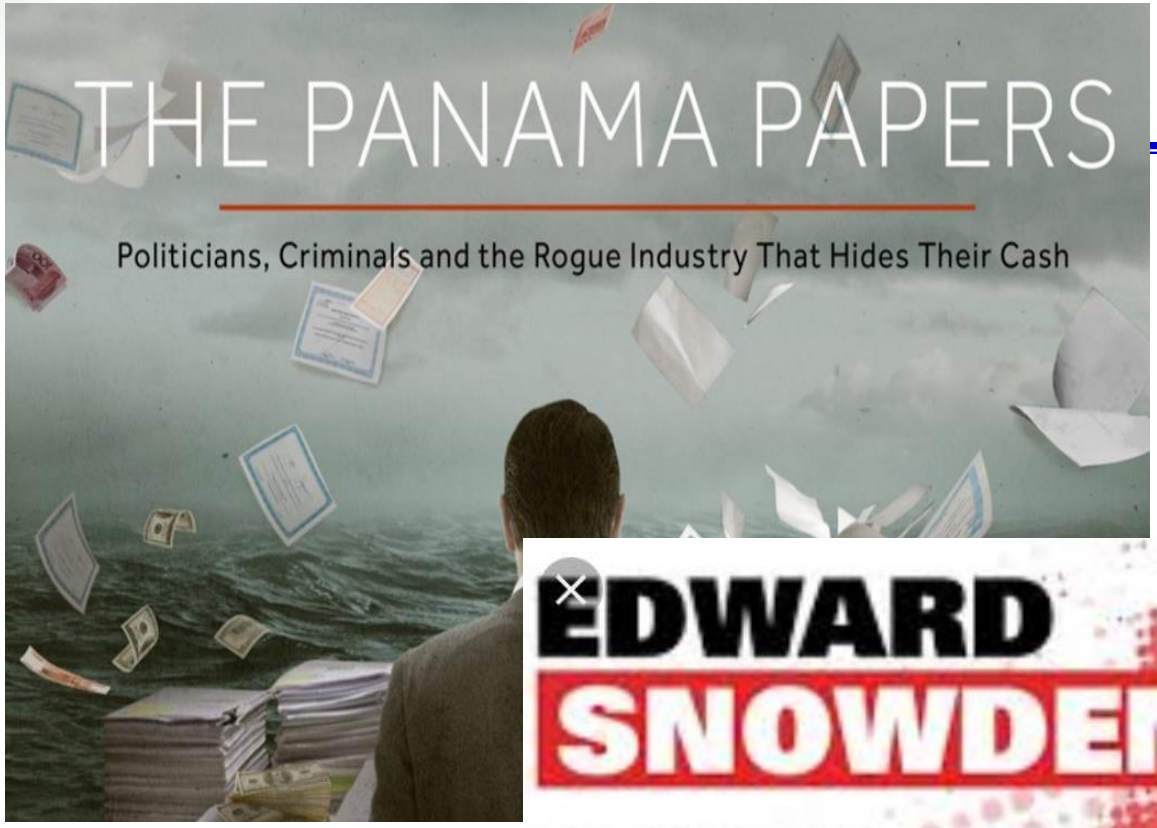
JUL 15

Large caches of data stolen from online cheating site **AshleyMadison.com** have been posted online by an individual or group that claims to have completely compromised the company's user databases, financial records and other proprietary information. The still-unfolding leak could be quite damaging to some 37 million users of the hookup service, whose slogan is "Life is short. Have an affair."

Anthem: Hacked Database Included 78.8 Million

Health insurer says data breach affected up to 70 million Anthem members

Anthem disclosed earlier this month that hackers had broken into a database containing personal information about 80 million customers and employees. *PHOTO: ASSOCIATED PRESS*


THE PANAMA PAPERS
Politicians, Criminals and the Rogue Industry That Hides Their Cash


EDWARD
SNOWDEN
HERO OR
TRAITOR?
BIO
GRAPHICS

IoT Hijacking

Source: Trendnet Webcam

Source: Jeep SUV hack

Difficulties in Defense I

- Faster detection of vulnerabilities
  - Weakness in hw/sw quickly uncovered
- Availability and simplicity of attack tools
  - Cheap & easy to use attack tools
- Increased speed of attacks
  - Can scan millions devices to find weaknesses
  - Automated attack possible without human

Difficulties in Defense II

- Universally connected devices
  - Distributed Attacks
- Delays in security updating (patches)
  - Speed of new & modified virus spread is faster than security updates
- User confusion
  - Little or no information to guide users to make security decisions

Security Definition

- Security = the necessary steps to protect a person or resource from harm
  - **C**onfidentiality : Protects data from unauthorized disclosure
  - **I**ntegrity: Protects data from alteration and deletion
  - **A**vailability: System resources are always available and accessible to authorized users

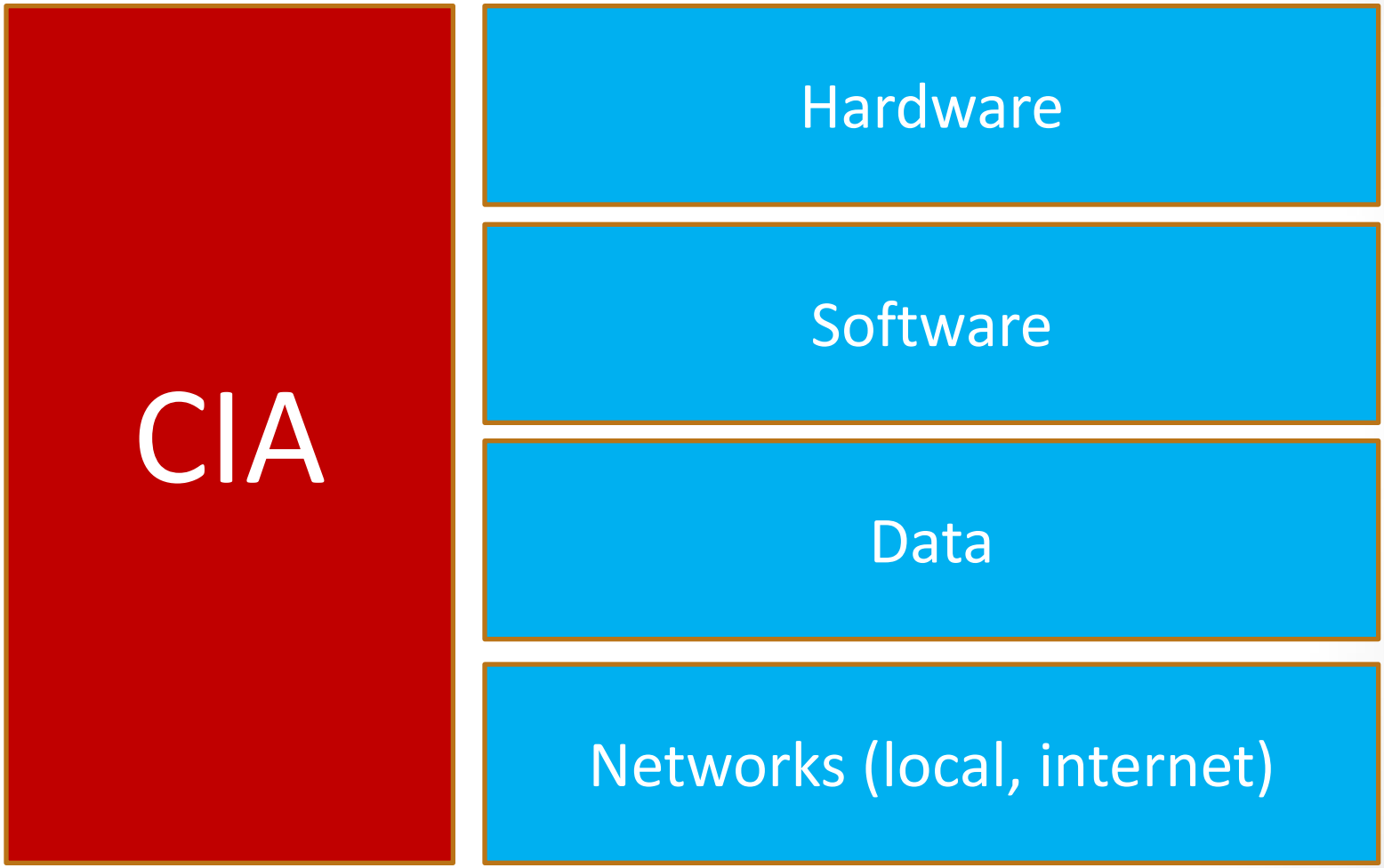
Related Terms

- Authentication – proving who you are
- Authorization – checking if allowed to access an asset usually based upon who you are, something you know or something you possess
- Non-repudiation - cannot deny knowledge of an action done by a user

Security Policy

- How do we know what is authorized or not?
- Role of security policy to specify:
  - Who (entity)
  - What (operation)
  - Which (system asset)
- Alice can read the exam.
- Bob can read and write to the exam.
- Carol can print the exam.

What are we trying to protect?



Vulnerabilities, Threats and Attacks

- Categories of system resource vulnerabilities
  - Corrupted (loss of Integrity)
  - Leaky (loss of Confidentiality)
  - Unavailable or very slow (loss of Availability)
- Security threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Security attacks
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Countmeasures

- Countermeasures are any means taken to deal with a security attack.
- Consider physical example of a bank.
  - *Prevention*: guard on the door.
  - *Detect*: CCTV cameras watching the tellers.
  - *Recovery*: police trace the bank robbers.
- Unsuccessful countermeasure leads to successful attack

Who are the attackers?

- Casual intruders
  - With Limited knowledge (“trying doorknobs”)
  - Script kiddies: Novice attackers using hacking tools
- Security experts (hackers)
  - Motivation: the thrill of the hunt; show off
  - Crackers: hackers who cause damage
- Professional hackers (espionage, fraud, etc.,)
  - Breaking into computers for specific purposes
- Organization employees
  - With legitimate access to the network
  - Gain access to information not authorized to use

Security Organizations

- Computer Emergency Response Team (CERT)
  - Responds and raises awareness of computer security issues across nation
  - NZ-CERT (operational since 2016) (https://www.cert.govt.nz/)
- APWG (Anti-phishing working group)
- Kaspersky Lab
- McAfee and Symantec

Importance of Security I

- Preventing data misuse
  - Stolen credit card numbers can easily & cheaply traded in the black market
- Thwarting Identity Theft
- Avoiding legal Consequences
  - Can be fined up to $50,000 for each violation (HIAPP)
  - $100,000 penalty not complying card transaction (PCI DSS)

Importance of Security II

- Maintaining Productivity
  - Cleaning up from attack diverts time, money and other resources away from normal activities
- Foiling Cyberterrorism
  - Prevent the cause to panic or provoke violence against citizens
  - Attackers increasingly target critical national infrastructure (banking, military, power plants, etc.,)

END