جامعة الملك فهد للبترول والمعادن
King Fahd University of Petroleum & Minerals

Information Security: An Overview

Ahmad Almulhem
Assistant Professor
Computer Engineering Department, KFUPM

ITC Awareness Day – May 14, 2013

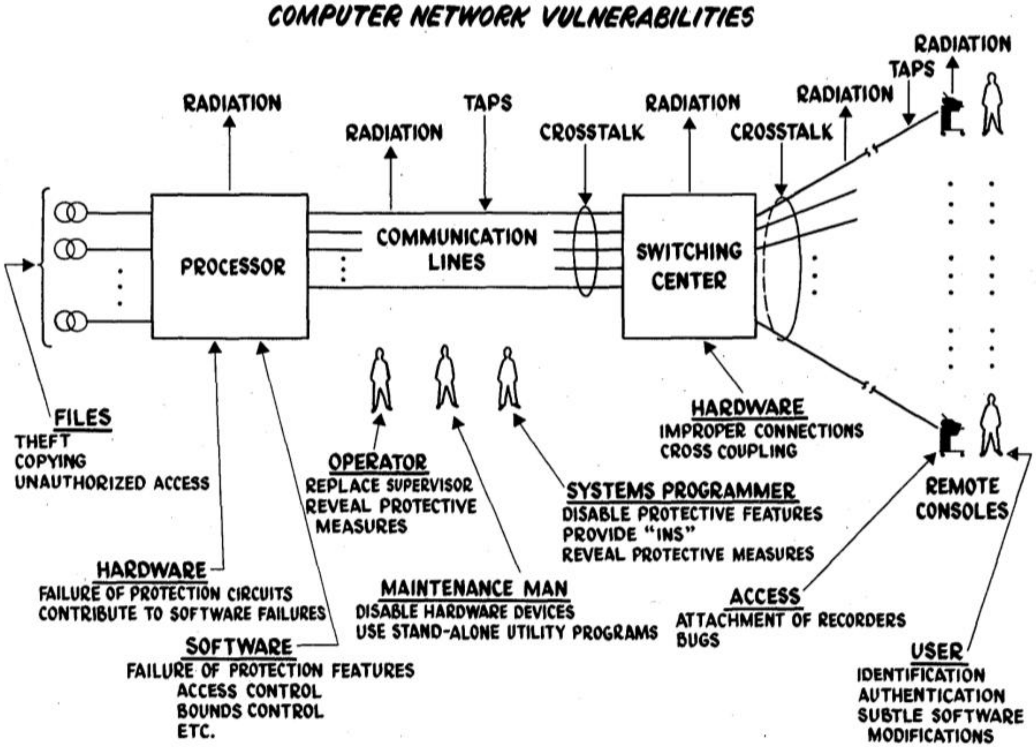
Outline

“A problem well put is half solved”

---- John Dewey (1859-1952)

- History
- Definition and important concepts
- Security design principles
- Conclusion

Information Security Origin

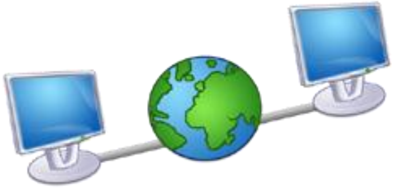


COMPUTER NETWORK VULNERABILITIES

- Rand Report R-609 (Willis Ware 1970) lays technical foundations
- “arguably” started computer security field
  - with Anderson Report-1972

Information Security History

40 years and counting



1970s

- mainframes
- multi-user
- multi-level policies
- access control
- encryption (DES, public-key)
- ....

1980s

- PCs
- single-user
- applications
- little security
- viruses (research to wild)

1990s

- Internet
- connected PCs
- web and browser
- remote attacks (DOS attacks)
- network security

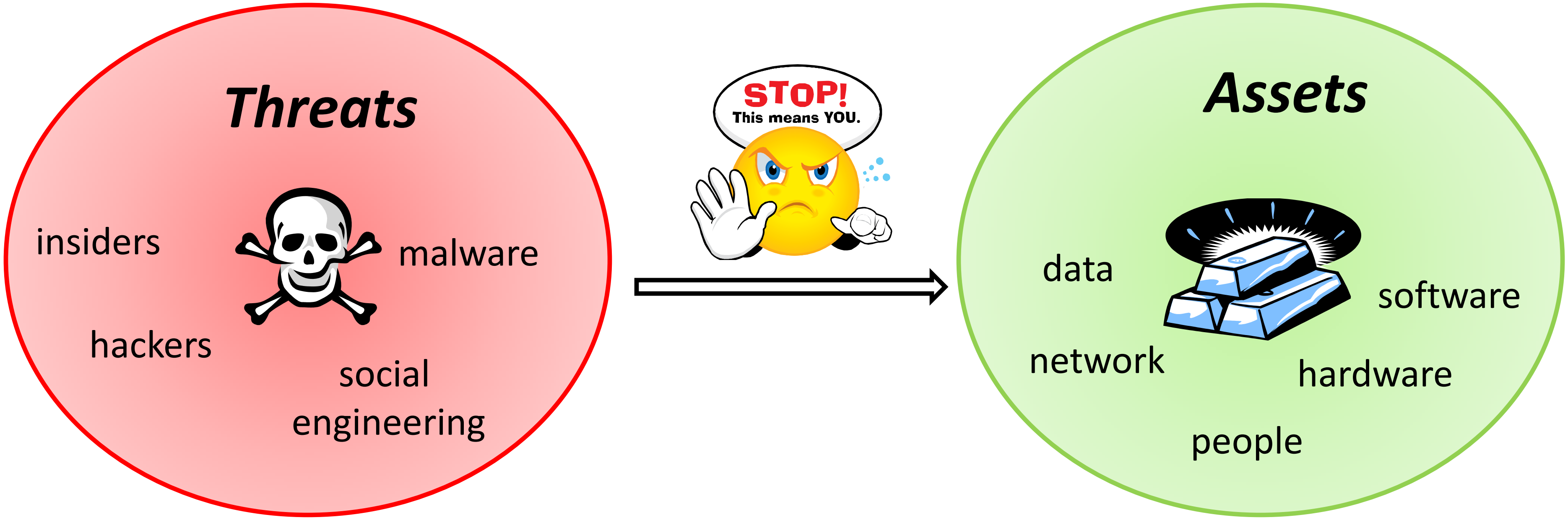
2000s

- Web
- server-side
- user base
- applications (airlines, banks)
- web attacks (SQL injection, cross-scripting)

???

What is Information Security?

"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" – *Glossary of Key Information Security Terms (NIST 2011)*



Threats

insiders

malware

hackers

social engineering

Assets

data

software

network

hardware

people

Why Information Security?

Information Value

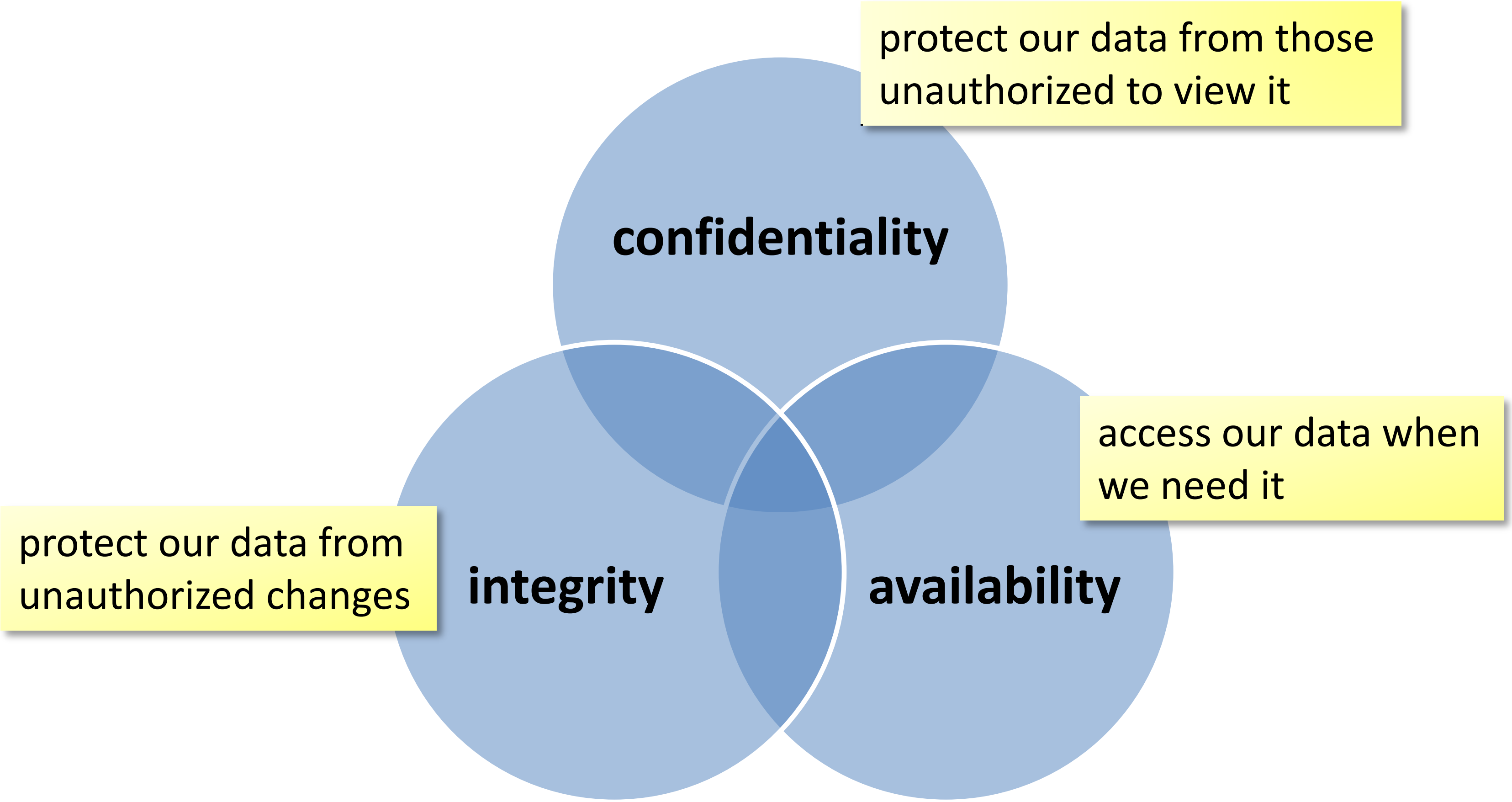
information is an important strategic and operational asset for most organization

- hardware, software, network, and even people may be replaced

Breaches Consequences

information leak/change/damage can be costly or even disastrous

Information Security Goals



confidentiality

protect our data from those unauthorized to view it

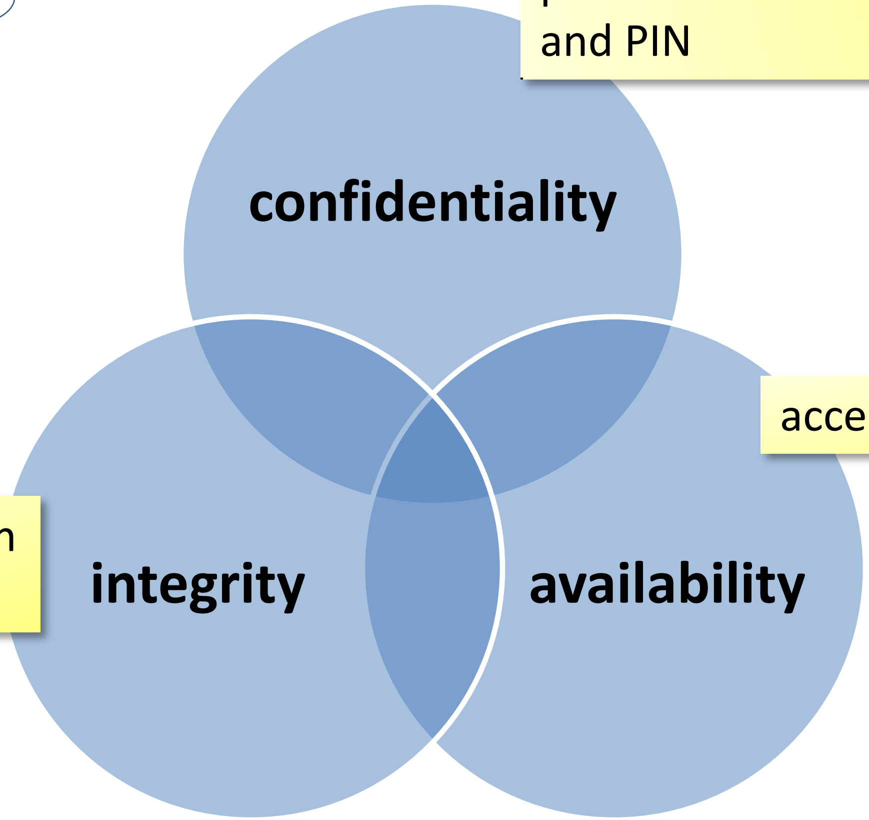
integrity

protect our data from unauthorized changes

availability

access our data when we need it

Information Security Goals



protect account information and PIN

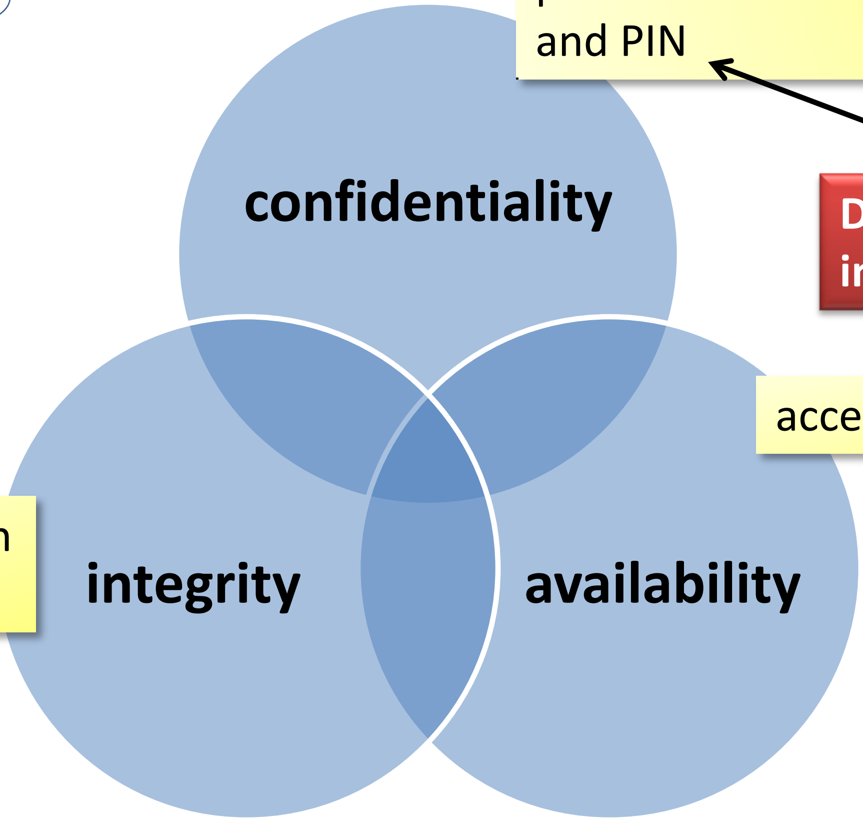
access any time 24/7

ensure transaction accuracy

Information vs. Data

- **Data** represents information, while **information** is the (subjective) interpretation of data
- protecting information is replaced by the more straightforward task of controlling access to data
- information may be leaked
  - covert channels
  - inference

Information vs. Data


confidentiality

integrity

availability

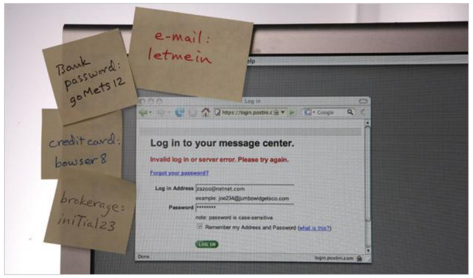
protect account information and PIN

Data: Number
information: PIN

access any time 24/7

ensure transaction accuracy

Security Design Principles



Log in to your message center.

Invalid log in or server error. Please try again.

Forgot your password?

Log in Address zazoo@netnet.com

example: joe234@jumbowidgetsco.com

Password *********

note: password is case-sensitive

☑ Remember my Address and Password (what is this?)

usability

security must be user-friendly
to end users and admin

open design

Security should not depend on
secrecy of design or implementation

simplicity

Keep it as simple as possible

more Security Design Principles

- Saltzer and Schroeder. "The protection of information in computer systems." (1975)
- Principles
  1. Least Privilege
  2. Fail-Safe Defaults
  3. Economy of Mechanism
  4. Complete Mediation
  5. Open Design
  6. Separation of Privilege
  7. Least Common Mechanism
  8. Psychological Acceptability

Conclusion

Bad News

- Security often not a primary consideration
  - performance and usability come first
- Many attacks are not technical in nature
  - Phishing, social engineering, etc.

Better News

- lots of defense mechanisms exist
- understanding technology limitations is important!
  - "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." ... Bruce Schneier

Thank you