Network Security

Dr. Ihsan Ullah

Department of Computer Science & IT
University of Balochistan, Quetta
Pakistan

March 19, 2015

Network Security

Reference Books

- “Corporate Computer Security (3rd Edition)” by Randy J Boyle and Raymond R. Panko, Prentice Hall Press, 2012.
- “Security in Computing fifth Edition”, by Charles P. Pfleeger, Shari Lawrence Pfleeger and Jonathan Margulies, Publisher: Printice Hall Press, 2015
- “Network Security Essentials: Applications and Standards, 4th edition” by William Stallings, Prentice Hall Press, Upper Saddle River, NJ, USA, , 2010.

Computer Security

- The generic name for the collection of tools designed to protect data and to thwart hackers [Sta10]
- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications) [GA95] [1]

[1] National Institute of Standards & Technology

Network Security

- Provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources [Wikipedia]
- Network security measures are needed to protect data during their transmission [Sta10]

Security terms

Vulnerabilities

- A weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm
- A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access

Security terms

Threats

- A set of circumstances that has the potential to cause loss or harm

Security terms

Attacks

- A human who exploits a vulnerability perpetrates an attack on the system
- An attack can also be launched by another system

Security terms

Compromises

- When a threat succeeds in causing harm to a system
- Also called incident or breach

Security terms

Controls

- An action, device, procedure, or technique that removes or reduces a vulnerability
- A threat is blocked by control of a vulnerability
- Also called safeguards, protections, and countermeasures
- Preventive, Detective, Corrective

Security requirements (CIA)

Confidentiality

The ability of a system to ensure that an asset is viewed only by authorized parties

Integrity

The ability of a system to ensure that an asset is modified only by authorized parties

Availability

The ability of a system to ensure that an asset can be used by any authorized party

CIA + AN

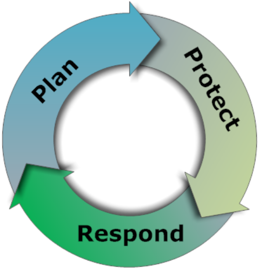
Authentication

The ability of a system to confirm the identity of a sender

Nonrepudiation

- The ability of a system to confirm that a sender cannot convincingly deny having sent something
- Actions of an entity to be traced uniquely to that entity

Security management process



[BP12]

Planning & policy

- The cycle begins with planning
- All three activities take place simultaneously and constantly feed into one another
- New threats and business conditions, feedback

Security management process

Protection

- Plan-based creation and operation of countermeasures
- cryptographic protections, access control, host operating system security, application security

Response

- Recovery from an incident according to plan
- Complex due to different levels of attacks require different response approaches

Randy J Boyle and Raymond R. Panko.
Corporate Computer Security (3rd Edition).
Prentice Hall Press, 3rd edition, 2012.

Barbara Guttman and Edward A.Roback.
An introduction to computer security: The NIST Handbook, special publication: 800-12.
Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 1995.

William Stallings.
Network Security Essentials: Applications and Standards.
Prentice Hall Press, Upper Saddle River, NJ, USA, 4th edition, 2010.