Distributed Applications

Information security

BS Doherty

b.s.doherty@aston.ac.uk

Aston University

Contents

- Concepts, issues and terminology
- Threats and vulnerabilities
- Technologies

1 Suggested reading

- [Pfleeger and Pfleeger, 2003], [Schneier, 2000], [Anderson, 2001].
- [Summers, 1997], [Abrams et al., 1995], [Neumann, 1995] and Carroll [Carroll, 1996]

What is security?

- Security is protection of (information) assets.

1.1 Protection provides:

- Confidentiality, secrecy, and privacy
- Integrity,
- Availability

A useful mnemomic is CIA - Confidentiality, Integrity, Availability

Assets include:

- information,
- hardware
- software
- peripherals
- people
- communication media
- processing capabilities
- financial assets.

Assets protected against "threats"

- Threats are posed by adversaries or by mishaps.

Adversaries are:

- spies
- terrorists
- warfare
- criminals: organised or individuals,
- people: malicious, disgruntled, curious or mischievious.

Mishaps include:

- accidents
- mistakes or ’acts of God’
  For example:
  - hardware failures,
  - software errors,
  - communication loss,
  - incorrect operation,
  - or ’natural’ events:
    - fire, flood, storm, lightning, earthquake.

Security measures:

- are needed where assets are vulnerable.

Vulnerabilities

- are paths through which assets are exposed to threat.

Protective measures

- are security features that are incorporated to minimise vulneralbility and/or risk [Cooper, 1989].
- these might include:
  - physical security
  - backups and disaster recovery
  - authentication controls
  - use of encryption
  - use of digests

An incident

- is an occurrence of a threat.
- Responses
- Responses are measures taken after an incident.

Approaches to security

These factors suggest an approach to security

- Identify assets to protect
- Identify threats to those assets
- Identify vulnerabilities
- Estimate risk
- Select protective measures
- Monitor security related events to take responsive action

Threats to Information

- Threats arise in a security context
- *malicious threats*
- *non-malicious threats*
- Alternatively threats by *adversaries* and threats by *mishap*.
- Threat model

Non-malicious threats

- external threats
- internal threats
- unintended consequence threats
- unintended inadequacy threats.

Malicious threats

- Malicious threats are deliberate acts to threaten assets in some way.
- criminal purposes
- act of information warfare or terrorism.
- internal or external

Threat Assessment

- A rational assessment of threats is an imprecise activity.
- Risk analysis makes use of probabilities of threats occurring and uses this in conjunction with the cost of defending against risks and value of loss to provide a quantitative view of risk management.

Vulnerabilities

- Hardware
  - The processing unit and ancillary equipment
- Software
  - Operating system
  - Application
- Data
- Communications

How is computer misuse carried out

- access or connection to the system is required
- terminal or a network connection.
- access to the input or output information is needed.

Who carries out misuse

There are a number of ways of classifying

- by purpose
- by position of intruder relative to information

Purpose

- mischief
- curiousity
- for personal gain
- for commercial gain
- for law enforcement
- for national security

Relative position of intruder

- internal attacker
- an ex-employee
- a random attacker
- a spy

Methods of computer misuse

- Physical scavenging
- Piggybacking and tailgating
- Spying
- Masquerading
- Entering false data
- Theft

requiring computing skills

- System scavenging
- Eavesdropping
- Piggybacking and tailgating
- Trojan Horse attack, Virus attacks
- Salami attacks
- Using trapdooors
- Using logic bombs
- Pirating
- Repudiation
- Key exchange

Addressing Threats

There are a number of approaches:

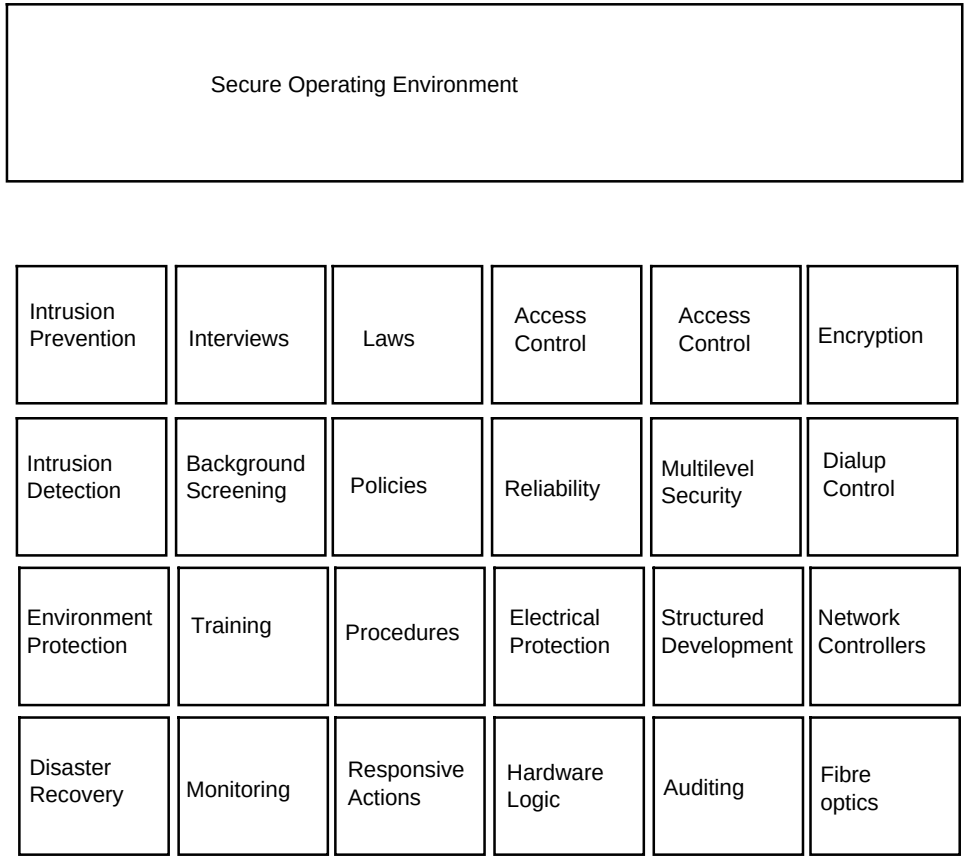
- real-world policy [Summers, 1997]
- building block security support structure [Cooper, 1989]

Real-world policy

[Summers, 1997].

- individual accountability
- authorisation
- least privilege
- separation of duty
- auditing
- redundancy
- risk reduction

Building block security



Cryptography

- Cryptography
- steganography

Terminology and Definitions

- plaintext
- ciphertext
- encryption or *enciphering*
- decryption or *deciphering*
- cryptosystem.
- key

Categories of cryptosystems

- symmetric
- asymmetric

Cryptographic strength

[Pfleeger and Pfleeger, 2003]

- Confusion
- Diffusion.

Stream and Block Ciphers

- Stream ciphers
- Block ciphers

Symmetric Cryptography

- Monoalphabetic Substitution
  - The Caesar Cipher
  - Other Monoalphabetic Substitutions
- Transposition
  - Columnar Transposition
  - The Vigenère Substitution
- Stream Ciphers
  - One-Time Pads: The Vernam Cipher

Block Ciphers

- permutations
- substitutions
- Cryptographic Composition or product ciphers
- The Data Encryption Standard
- The International Data Encryption Algorithm, IDEA

symmetric cryptography limitations

- key distribution problem
- N-square problem
- authenticity

Asymmetric Cryptography

- public key cryptography
- public key cryptosystem, PKC
- encryption key available to all - the public key
- the decryption key is secret or private key

Examples of asymmetric systems

- The RSA cryptosystem
- The ElGamal cryptosystem
- The Rabin cryptosystem
- Elliptic curve cryptosystems

Public-Key Certificates

- Each user has to send his public key to a CA
- the CA produces a certificate for him.
- The certificate consists at least of a user's ID, a time stamp and the user's public key.
- All signed by the CA, that means the CA encrypts the information with it's private key.
- X.509 certificate.
- The user has to have the CA's public key in order to verify signatures.

Authentication process

One-Way Authentication In this protocol information is sent from Alice to Bob. The following is ensured:

1. Identity of Alice
2. The message was generated by Alice
3. The message was supposed to be for Bob
4. Integrity
5. Non repetition

Authentication process

1.2 Two-Way Authentication

1. Identity of Alice
2. The message was generated by Alice
3. The message was supposed to be for Bob
4. Integrity
5. Non repetition
6. Identity of Bob
7. The message was generated by Bo
8. The message was supposed to be for Alice
9. Integrity of the reply

1.3 Three-Way Authentication

This protocol follows the two-way authentication but additionally a final message is sent from Alice to Bob again.
Reply attacks can be detected.

Security should provide: CIA

- Confidentiality
- Integrity
- Availability

Services

- Privacy,confidentiality.
- Secure distribution of keys
- Secure online transactions
- Limiting access to paying customers

Key distribution

- Merkle's puzzle
- Shamir's method
- Diffie■Hellman key exchange
- Public key cryptosystems

Authentication

- Digital Signature
- Authentication of Files or Documents
  Message Digests or hash function.
  MD5
  Secure Hash Algorithm (SHA)
- PGP

Society Press.

[Anderson, 2001] Anderson, R. (2001). *Seurity Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

[Carroll, 1996] Carroll, J. (1996). *Computer Security*. Butterworth-Heinemann, third edition.

[Cooper, 1989] Cooper, J. (1989). *Computer and Communications Security: Strategies for the 1990s*. McGraw-Hill.

[Neumann, 1995] Neumann, P. (1995). *Computer Related Risks*. ACM Press, New York.

[Pfleeger and Pfleeger, 2003] Pfleeger, C. P. and Pfleeger, S. L. (2003). *Security in Computing*. Prentice Hall, third edition.

[Schneier, 2000] Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc.