Design and Analyze Secure Networked Systems 7

Prof. Edward Chow @ Colorado Univ.

Note by waegaein@github.com

Methods of Defense

- **Prevent** the intrusion from arriving or happening.
- **Deter** attacks by increasing the penalty of being caught, making it difficult and costly to close the hurdle.
- **Deflect** attackers attention.
- **Detect** to provide early detection of intrusion.
- **Recover** the system or mitigate the damage by deploying the layer of defenses.

Security Principles

- A collection of desirable system property behaviors, designs and implementation practice that can reduce the risk.
- Reduce either the likelihood of the harm occurrence or their impact.
- We can be aware of the threat to our system and ultimately derive a set of protection requirements.

1. Defense in Depth

- Layers of security mechanisms increase the security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system.

- For network and infrastructure attacks
  - Protect the local area network
  - Protect the wide area network
  - Deploy firewall
  - Deploy intrusion detection system
- For insider attacks
  - Deploy physical and personal security
  - Deploy authenticated access control and auditing procedure

2. Defense with Diversity

- Mono instruction architecture such as Intel 386 or 64 architecture used by current computer systems make it easier for attackers to develop just one malicious software and then attack vulnerabilities existing in all the system using the same ISA architectures.

- We should encourage the development of diversity in
  - System architectures
  - Operating systems
  - Library / Packages
  - Programming languages / Frameworks
- We should produce framework that allow real-time seamless service/application migration from one system which fails (or about to fail) to the others.

3. Cyber Resilience

- The ability of an architecture to support the function necessary for mission success in spite of those hostile action and adverse condition.

- An architecture is more resilient if it can provide these functions with
  - Higher probability
  - Shorter periods of reduced capability
  - Across a wider range of scenario/condition/threat.

4. Least Privileges

- Every program and user of the system should operate using the lest set of privileges necessary to complete the job.
- Unintentional, unwanted, or improper uses of privileges are less likely to occur.
- It limits the damage from error, accident, or break-in.

E.g.

- User's home directory
  - drwx------.
  - Only owner can access.
- Sharing documents with read-only permission
  - -rw-r--r--.
  - Only owner can write.
- Append-only permission for log file
  - drwxr-sr-x+
  - Logs cannot be overwritten.
  - Plus means extended access control like append-only.