CS 3IS3 Fall 2007

08 Information Security Management

William M. Farmer

Department of Computing and Software
McMaster University

18 November 2007

Information Security Management: Overview

1. Security policy development.
2. Security strategy development.
3. Security mechanism development.
4. Vulnerability analysis.
5. Auditing.
6. Intrusion detection.
7. Physical security.
8. Human resources management.
9. Legal and business requirements.

Vulnerability Analysis

- A security vulnerability is a flaw in a security system that can be exploited to violate a security policy.
- Security vulnerabilities can arise from:
  - System design.
  - System implementation.
  - System operation.
  - System maintenance.
- Penetration testing is a testing technique to detect security vulnerabilities that consists of three steps:
  1. Put the system in a state that may contain a security vulnerability (precondition).
  2. Execute the system.
  3. Check the result of the test (postcondition).

Auditing

- Logging is the recording of events or statistics to provide information about system use and performance.
- Auditing is the analysis of log records to present information about the system in a clear and understandable manner.
- The goals for logging and auditing with respect to information security are determined by the security policy.
- An auditing system consists of three components:
  1. A logger that records information.
  2. A analyzer that analyzes logged data.
  3. A notifier that informs the system analyst of the results of the audit so that action can be taken if necessary.

Intrusion Detection

- An attack tool is an automated script designed to violate a security policy.
  - Example: A rootkit is a set of programs for taking control of an operating system.
- An intrusion detection system (IDS) looks for abnormal use of an information system.
- An IDS has four goals:
  1. Detect a wide variety of intrusions.
  2. Detect intrusions in a timely fashion.
  3. Present the analysis in a readily understandable format.
  4. Be accurate.
- There are three types of analyses that an IDS can provide:
  1. Anomaly detection: look for unusual states.
  2. Misuse detection: look for bad states.
  3. Specification-based detection: look for states that are known not to be good.