Multi Level Security

Introduction

Petr Jirásek © 2013
petr.jirasek@cybersecurity.cz

What is MLS?

A class of system that has system resources at more than one security level and that permits concurrent access by users who differ in security clearance and need-to-know, but is able to prevent each user from accessing resources for which the user lacks authorization.

General definition (open source)

The MLS History

- 1960 – 1970 Introduction to MLS
- 1973 Bell-LaPadula Model
- 1983 US DoD Standard 5200.28-STD
- 1988 IBM MVS, JES2, JES3, TSO, PSF met B1
- 1990 Common Criteria (CC) introduced (EAL7, …)
- 1999 CC approved as ISO 15408
- 2003 Linux: Fedora, RHEL, …

Bell-LaPadula (BLP)

- The principles:
  - Suggested scheme
  - Subject has a **security clearance** level
  - Object has a **security classification** level
  - Class control how subject may access an object
  - Discretionary access control
    - No read up
    - No write down
- BLP give formal theorems

MLS Granularity

- Infrastructure level
- HW level
- Partitioning & Virtualization
- Operating System
- File system level
- Database level
- Application level
- Presentation level

Computer Security Models

- Fundamental facts:
  - All complex software systems have bugs
  - Is extraordinarily difficult to build computer (HW/SW) system not vulnerable to attack
- Computer security is essentially a software security problem

Recent trends in MLS

- **Virtualization**
  - DELL
  - VMware (EAL4 NIAP/CC)
  - Etc.
- **Multi-Network Access**
- **MLS-based firewall products**
- **MLS in Cloud**

Recent trends in MLS

- **MLS in Big Data**
  - **Hadoop**
  - **MLS-Aware**
    - A component is considered MLS-Aware if it executes without privileges in an MLS environment, and yet takes advantage of that environment to provide useful functionality.

(Cynthia E. Irvine, Ph.D. - Center for Information Systems Security Studies and Research Department of Computer Science, Naval Postgraduate School, Monterey, CA, USA)

New trends in MLS ??

Industry	Sensitivity Label
Public Sector	Top Secret Secret Confidential Unclassified ▪ *FOUO* ▪ *Public*
Business to Business	Trade_Secret Company_Confidential Public
HR and other systems	Highly_Sensitive Sensitive HR_Confidential Public