Policy-Enhanced Linux

An Educational Tool

Paul C. Clark
clarkp@cs.nps.navy.mil

NPS CISR

Overview

- What ?
- Why ?!
- How ?

- Demonstration
- Questions

What Did I Do?

- Modified Linux to allow for the insertion of additional access control policies.
- In particular, I added two Mandatory Access Control policies.

Background

- 1 of the 7 computer security courses is *Introduction to Computer Security*
- Completion of 9 tutorials is required
- 3 of the 9 tutorials support classroom instruction of MAC policies

Problems in the Lab

- The MAC systems are getting old
- They are expensive to replace
- Few choices
- Cannot support distance learning sites
- Other universities cannot benefit from our work

Historical Background

- Research into MAC systems since ‘70s
- Orange Book required MAC beyond C2
- Some vendors built systems with MAC
- DoD did not buy many
- Such vendors did not fare well
- What IS available is very expensive

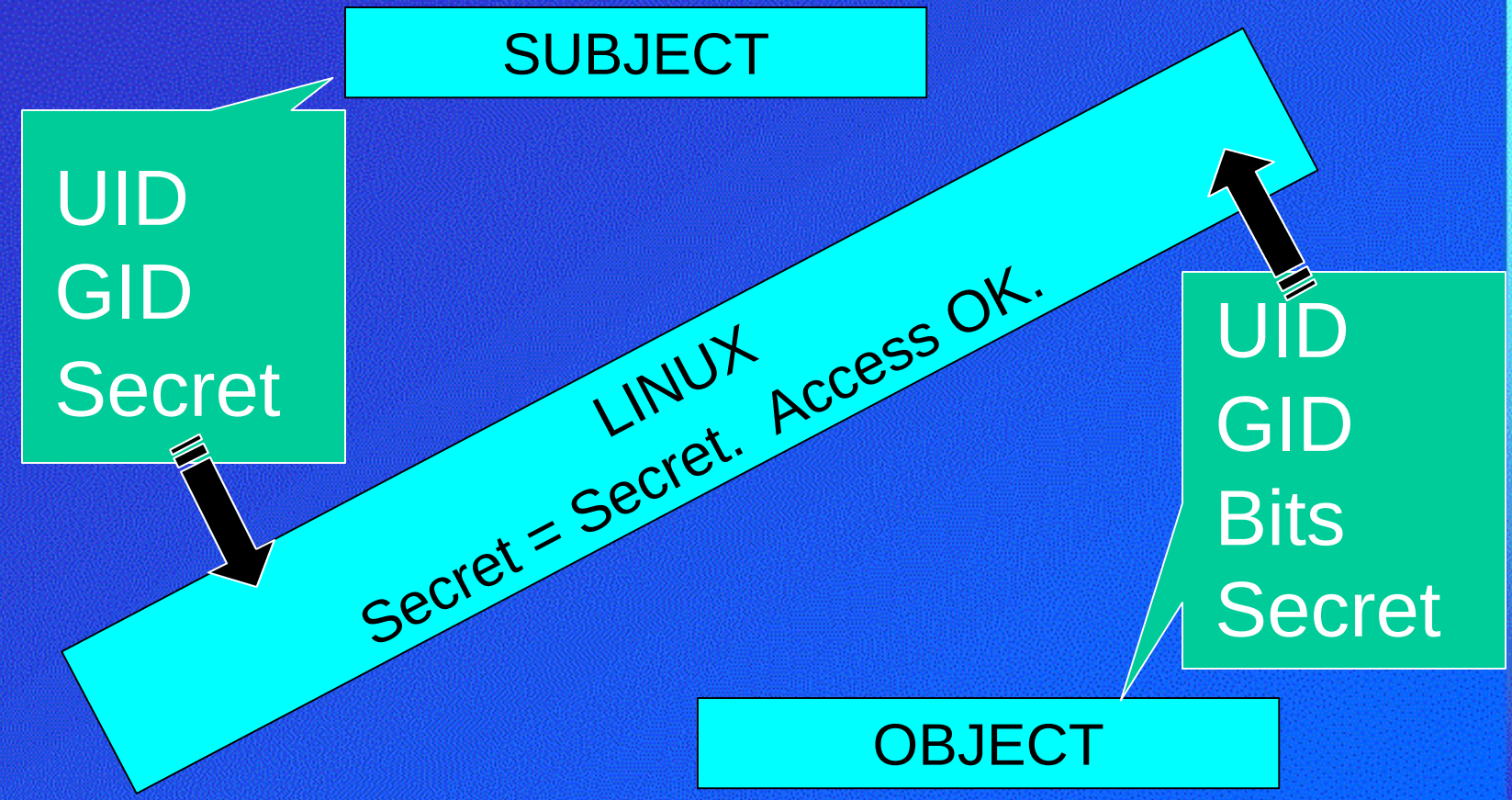
Requirements

- Inexpensive
- Runs on a PC
- Dual Boots
- “Easy” to Use
- Supports Secrecy & Integrity
- Supports a Session Level

Potential Side-Effects

- Inexpensive MAC systems
- Increased exposure
- Increased demand
- Increased availability

Access Control Decisions



Labels Were Attached

- Modified the inode (for objects)
- Modified task_struct (for subjects)
- 64-bit labels (only 36 used)

Introduced New Modules

Layer Name	Module Name
Control Layer	Clearance Manager, Range Manager, Meta-Policy Manager
Label Utility Layer	Label Manager
Clearance Layer	BLP Clearance, Biba Clearance
Range Layer	BLP Range, Biba Range
Label Layer	BLP Labels, Biba Labels
Policy Layer	BLP Policy, Biba Policy

Introduced Config. Files

- Human-readable labels
- User Clearances
- System Clearance

Some Design Choices

- Trusted Subjects
- Upgraded Objects
- Deflection Directories
- Restricted updates to object properties
- root is still unrestricted

How Much is Completed?

- Modifications to inodes & task_struct
- All new modules are implemented
- Some Linux code modified

How Much is Still Left?

- Several affected applications
- Deflection directories
- A lot of other modifications spread throughout Linux

Future Work

- Trusted Path (in progress)
- Robust Audit
- Administrative Interface
- Principal of Least Privilege
- Other Policies?

Reminder of Goal

- Intended for educational purposes
- No additional assurance is provided
- Not to be used in a “live” environment

Demonstration

Questions?