CS 563 - Advanced Computer Security: Foundations I

Professor Adam Bates
Fall 2018

Administrative

Learning Objectives:

- Understand the genesis and significance of Multics and the Reference Monitor Concept

Announcements:

- E-Ink tablets approved for class use
- Reaction paper was due today (and all subsequent classes)
  - No penalties for late submission this week as people add/drop.
- Questions about writing reaction papers?
- 3 seats open for class this morning — talk to me if you can't register

Reminder: Please put away (backlit) devices at the start of class

Anderson Report, 1972

… thoughts?

Anderson Report, 1972

What's in the report?

- Historical context of computer security
- Foundational operating system security primitive
- Budgeting + Administrative Minutia >_<

Anderson Report, 1972

Anderson Report, 1972

What computer security problems were the Air Force facing in 1972?

Anderson Report, 1972

What computer security problems were the Air Force facing in 1972?

- *"there is a growing requirement to provide shared use of computer systems containing information of different classification levels and need-to-know requirements in a user population not uniformly cleared or access-approved."*

Anderson Report, 1972

What computer security problems were the Air Force facing in 1972?

- *"there is a growing requirement to provide shared use of computer systems containing information of different classification levels and need-to-know requirements in a user population not uniformly cleared or access-approved."*
- *"… users with different clearances and data of different classifications share primary storage simultaneously…"*

Anderson Report, 1972

What computer security problems were the Air Force facing in 1972?

- *"there is a growing requirement to provide shared use of computer systems containing information of different classification levels and need-to-know requirements in a user population not uniformly cleared or access-approved."*
- *"… users with different clearances and data of different classifications share primary storage simultaneously…"*
- *"It is generally true that contemporary systems provide limited protection against accidental violation of their operating systems… it is equally true that virtually none of them provide any protection against deliberate attempts to penetrate the nominal security controls provide."*

Anderson Report, 1972

What computer security problems were the Air Force facing in 1972?

- *"there is a growing requirement to provide shared use of computer systems containing information of different classification levels and need-to-know requirements in a user population not uniformly cleared or access-approved."*
- *"… users with different clearances and data of different classifications share primary storage simultaneously…"*
- *"It is generally true that contemporary systems provide limited protection against accidental violation of their operating systems… it is equally true that virtually none of them provide any protection against deliberate attempts to penetrate the nominal security controls provide."*
- *"A final trend… is the movement toward the establishment of large dispersed networks of related computer systems…"*

What's old is new

Many of the problems forecast in the Anderson report have defined the next 50 years of security research…

What's old is new

Many of the problems forecast in the Anderson report have defined the next 50 years of security research…

- *"an unsuccessful penetration attempt would not show grounds for certification, since the possibility of a yet undiscovered route into a large existing system is ever"*

What's old is new

Many of the problems forecast in the Anderson report have defined the next 50 years of security research…

- *"an unsuccessful penetration attempt would not show grounds for certification, since the possibility of a yet undiscovered route into a large existing system is ever"*
- *"Attempts to 'patch' an off-the-shelf system for security tend to obscure penetration routes, but have little impact on underlying security problems."*

What's old is new

Many of the problems forecast in the Anderson report have defined the next 50 years of security research…

- *"an unsuccessful penetration attempt would not show grounds for certification, since the possibility of a yet undiscovered route into a large existing system is ever"*
- *"Attempts to 'patch' an off-the-shelf system for security tend to obscure penetration routes, but have little impact on underlying security problems."*
- *"We have identified this threat as that of a malicious user… we do not need to distinguish between a foreign agent or the misguided/ disgruntled actions taken by an individual against the "establishment".*

What's old is new

Many of the problems forecast in the Anderson report have defined the next 50 years of security research…

- *"an unsuccessful penetration attempt would not show grounds for certification, since the possibility of a yet undiscovered route into a large existing system is ever"*
- *"Attempts to 'patch' an off-the-shelf system for security tend to obscure penetration routes, but have little impact on underlying security problems."*
- *"We have identified this threat as that of a malicious user… we do not need to distinguish between a foreign agent or the misguided/ disgruntled actions taken by an individual against the "establishment".*
- *"In contemporary systems, the attacker attempts to find design or implementation flaws that will give him supervisory control of the system."*

How to fix?

"In order to provide a base upon which a secure system can be designed and built, we recognize the need for a formal statement of what is meant by a secure system - that is a model or ideal design. The model must incorporate in an appropriate and formal way the intended use of a system, the kind of use environment it will exist in, a definition of authorization, the objects (system resources) that will be shared, the kind of sharing required, and the idea of controlled sharing described above. "

How to fix?

"In order to provide a base upon which a secure system can be designed and built, we recognize the need for a formal statement of what is meant by a secure system - that is a model or ideal design. The model must incorporate in an appropriate and formal way the intended use of a system, the kind of use environment it will exist in, a definition of authorization, the objects (system resources) that will be shared, the kind of sharing required, and the idea of controlled sharing described above. "

1) Define a formal Security Model

How to fix?

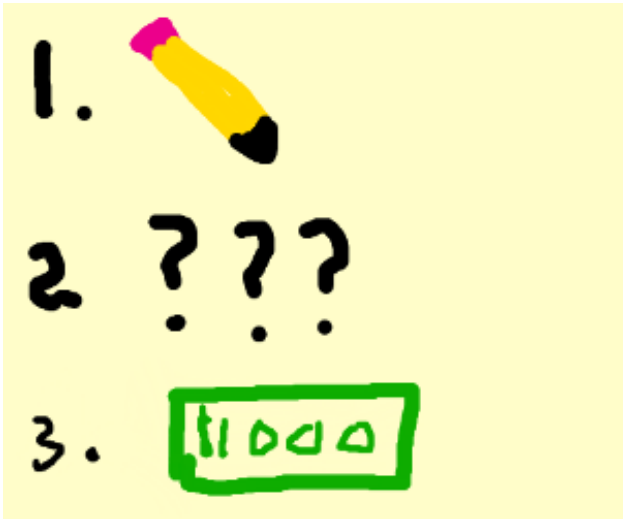
"In order to provide a base upon which a secure system can be designed and built, we recognize the need for a formal statement of what is meant by a secure system - that is a model or ideal design. The model must incorporate in an appropriate and formal way the intended use of a system, the kind of use environment it will exist in, a definition of authorization, the objects (system resources) that will be shared, the kind of sharing required, and the idea of controlled sharing described above. "

1) Define a formal Security Model
2) Enforce security model (???????)

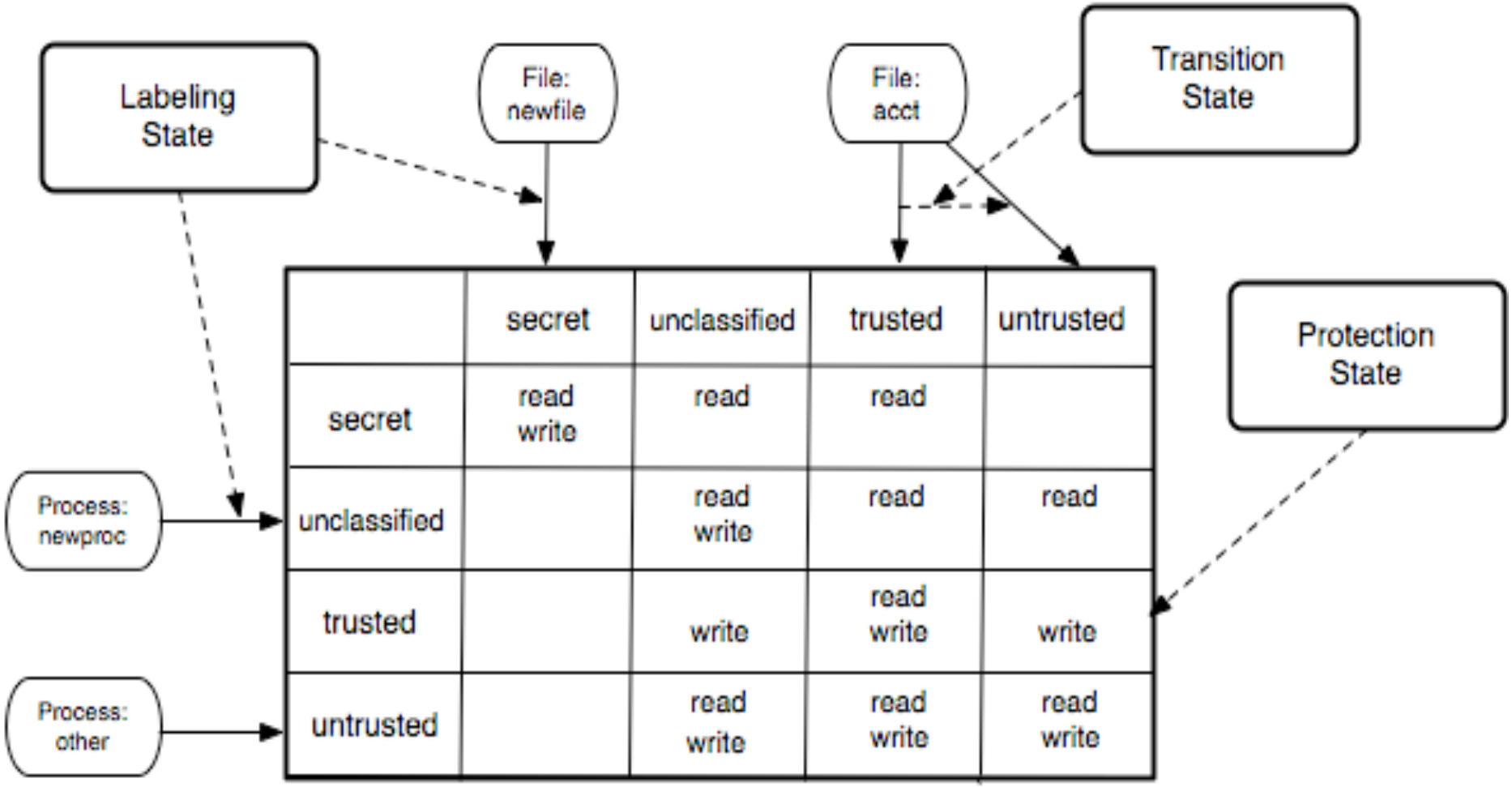
How to fix?

"In order to provide a base upon which a secure system can be designed and built, we recognize the need for a formal statement of what is meant by a secure system - that is a model or ideal design. The model must incorporate in an appropriate and formal way the intended use of a system, the kind of use environment it will exist in, a definition of authorization, the objects (system resources) that will be shared, the kind of sharing required, and the idea of controlled sharing described above. "

1) Define a formal Security Model
2) Enforce security model (???????)
3) $$$$ Profit $$$$$



Mandatory Protection System



	secret	unclassified	trusted	untrusted
secret	read write	read	read	
unclassified		read write	read	read
trusted		write	read write	write
untrusted		read write	read write	read write

Mandatory Protection System

- Immutable table of
  - Subject labels
  - Object labels
  - Operations authorized for former to perform upon latter
- Example: MPS for Operating System
  - Allow media player to communicate with browser, exec certain files
  - No network access
- Example: MPS for Media Player
  - Play only trusted input

Labeling State

- Immutable rules mapping
  - Subjects to labels (in rows)
  - Objects to labels (in columns)
- Example: Labeling State of OS
  - Browser, Media Player have own subject labels
  - Label inputs from network (network connection)
  - Root and TCB program files have labels based on their trust
- Example: Labeling State of Web Application
  - Content – untrusted; Prevent integrity violation

Transition State

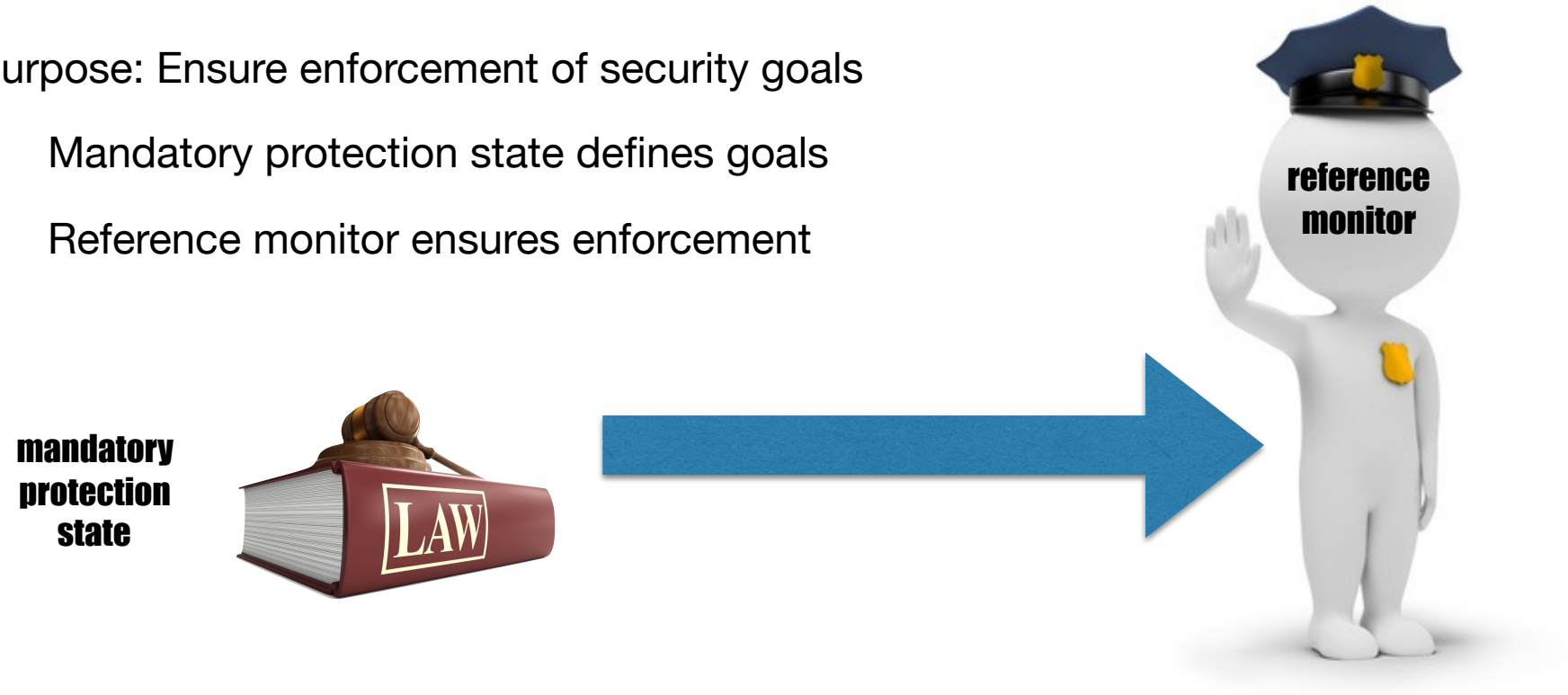
- Immutable rules mapping
  - Processes to conditions that change their subject labels
  - IPC to conditions that change their object labels
- Example: Transition State of OS
  - Change label of processes that receive untrusted input
  - Change label of outputs of these processes
- Example: Transition State of Programs
  - Server, Browser, Media Player change labels of their internal objects (threads and variables)
  - Server, Browser, Media Player may be trusted to change their labels (down only?)

Managing MPS

- Challenge
  - Determining how to set and manage an MPS in a complex system involving several parties
- Parties
  - What does programmer know about deploying their program securely?
  - What does an OS distributor know about running a program in the context of their system?
  - What does an administrator know about programs and OS?
  - Users?

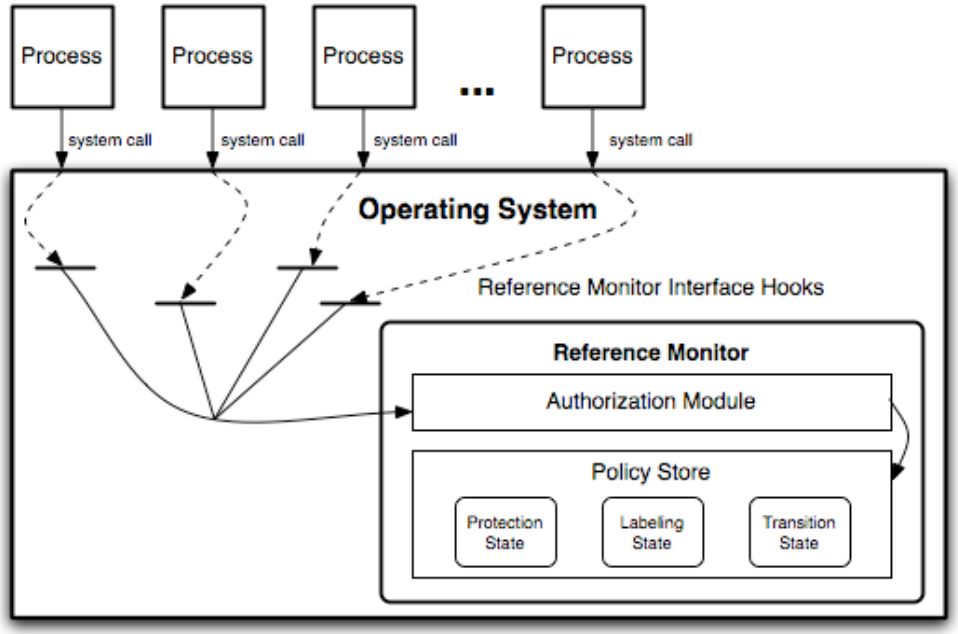
Reference Monitor Concept

- Purpose: Ensure enforcement of security goals
  - Mandatory protection state defines goals
  - Reference monitor ensures enforcement



- **Every component that you depend upon to enforce your security goals must be a reference monitor**

Reference Monitor Concept



- Components
  - Reference monitor interface
  - Authorization module
  - Policy store
- Examples of each available today?

Reference Monitor Guarantees

- **Complete Mediation**
  - The reference validation mechanism must always be invoked
- **Tamperproof**
  - The reference validation mechanism must be tamperproof
- **Verifiable**
  - The reference validation mechanism must be subject to analysis and tests, the completeness of which must be assured

Complete Mediation

- Every security-sensitive operation must be mediated
  - What's a "security-sensitive operation"?
  - Operation that enables a subject of one label to access an object that may be a different label
- How do we validate complete mediation?
  - Every such operation must be identified
  - Then we can check for dominance of mediation
- **Mediation:** Does interface mediate correctly?
- **Mediation:** On all resources?
- **Mediation:** Verifably?

Tamperproof

- Prevent modification by untrusted entities
  - Interface, mechanism, policy of reference monitor
  - Code and policy that can affect reference monitor mods
- How to detect tamperproofing?
  - Transitive closure of operations
  - Challenge: Often some untrusted operations are present
- **Tamperproof:** Is reference monitor protected?
- **Tamperproof:** Is system TCB protected?

Verification

- Test and analyze reference validation mechanism
  - And tamperproof dependencies
  - And what security goals the system enforces
- Determine correctness of code and policy
  - What defines correct code?
  - What defines a correct policy?
- **Verifiable:** Is TCB code base correct?
- **Verifiable:** Does the protection system enforce the system's security goals?

Evaluation

- **Mediation:** Does interface mediate correctly?
- **Mediation:** On all resources?
- **Mediation:** Verifably?
- **Tamperproof:** Is reference monitor protected?
- **Tamperproof:** Is system TCB protected?
- **Verifiable:** Is TCB code base correct?
- **Verifiable:** Does the protection system enforce the system's security goals?

What is Multics?

- Multiprocessing system that developed many major concepts in operating systems, including security
- Began in 1965, development continued until the mid-1970s
- Last deployment decommissioned in 2000
- Initial partners: MIT, Bell Labs, GE/Honeywell
- Unprecedented amount of money and effort to develop ($10M in 1960s dollars, research staff peaked at 400)

What is Multics?

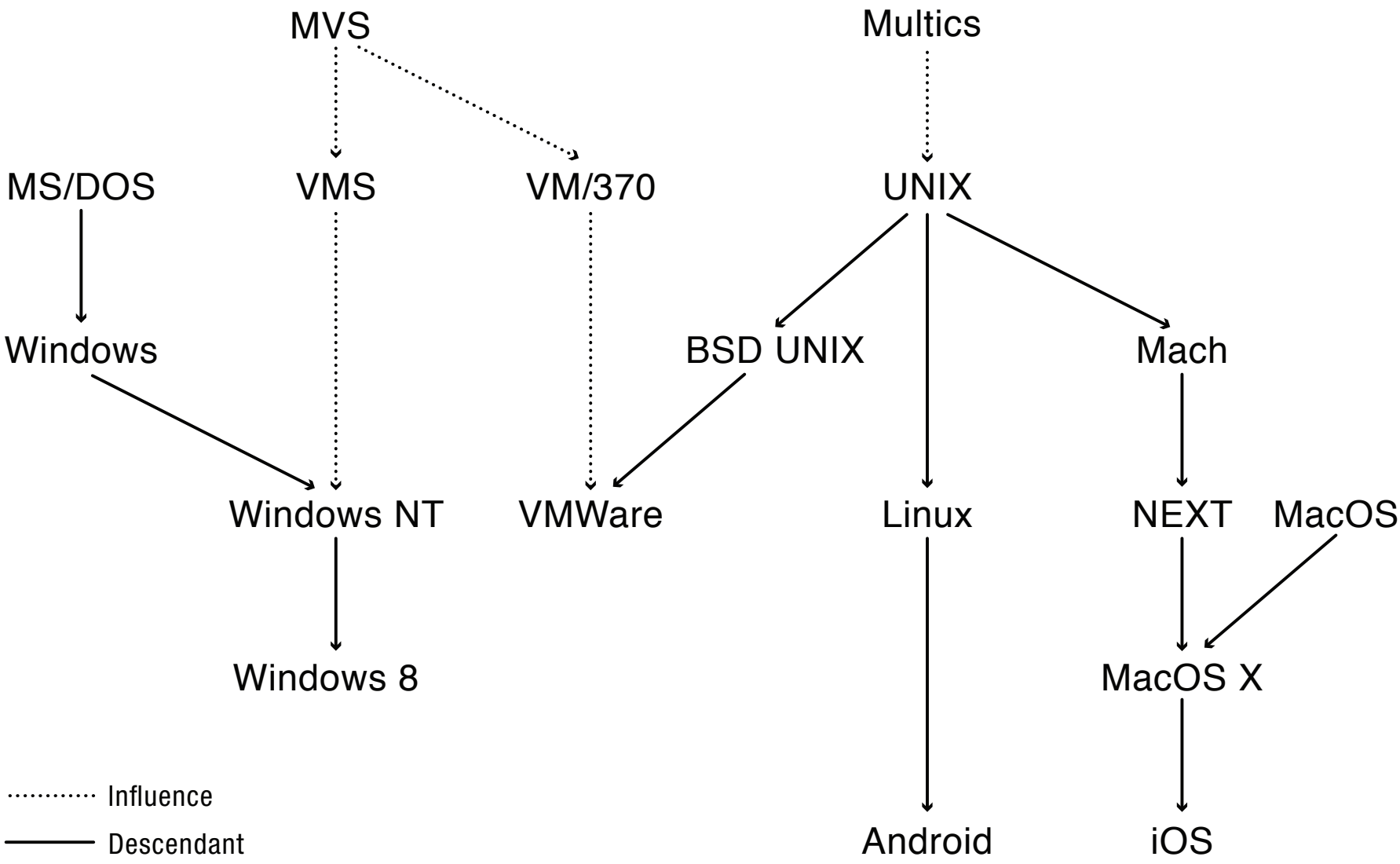
Multics Achievements

- Virtual memory and memory segmentation
- Hierarchical file system
- Including symbolic links and removable devices
- Shared-memory symmetric multiprocessing
- Dynamic linking
- Security in the design phase

Multics Achievements

- Virtual memory and memory segmentation
- Hierarchical file system
- Including symbolic links and removable devices
- Shared-memory symmetric multiprocessing
- Dynamic linking
- Security in the design phase

Multics Achievements



Multics Security

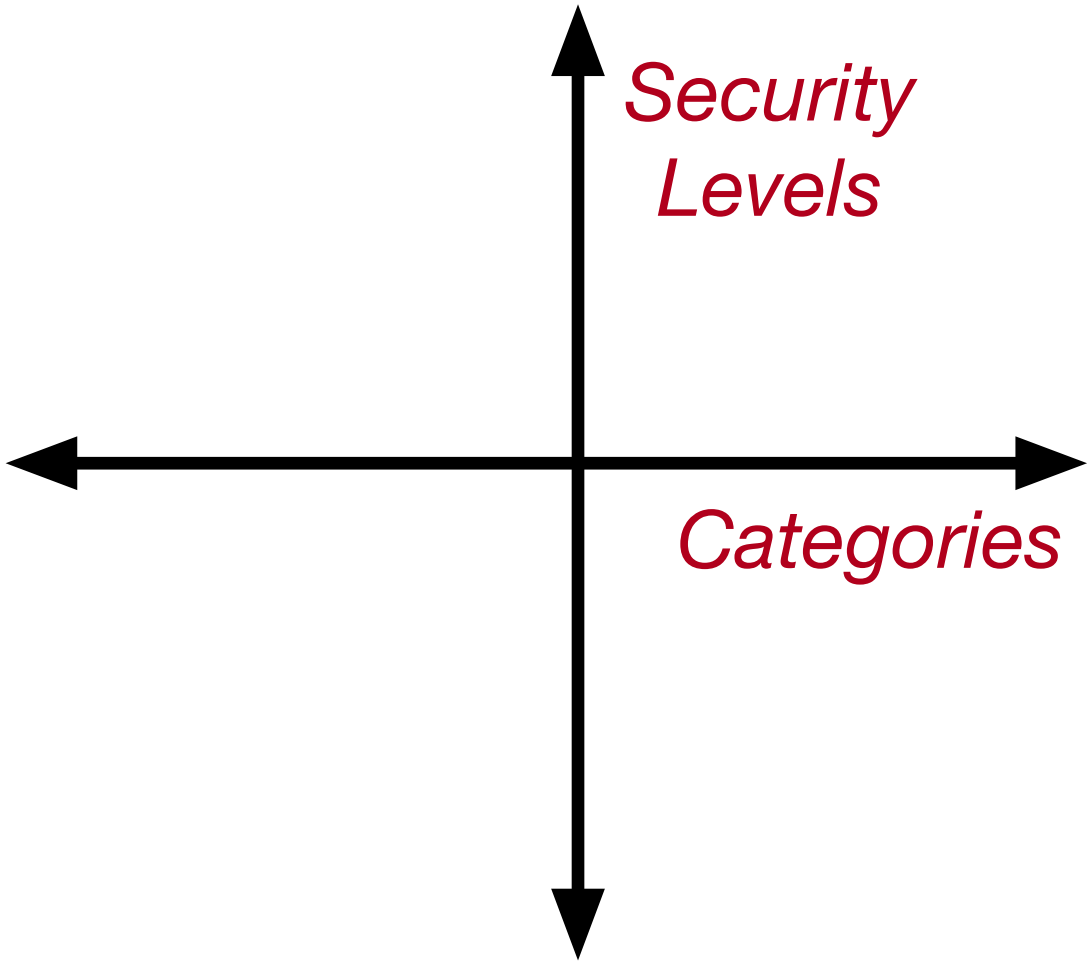
- What were the security goals for Multics?
  - Evolved as the system design evolved
  - First system design to consider such goals
- Secrecy
  - Prevent leakage – even if running untrusted code
- Integrity
  - Prevent unauthorized modification – layers of trust
- Comprehensive control (enforce at lowest level)

Multics Security

- Secrecy goal
  - Implemented as multilevel security
- Integrity goal
  - Implemented as rings of protection
- Reference monitor
  - Mediated segment crossing and all ring crossing activity (gates)
- Resulting system: considered a high point in secure system design

Multics MLS

- A multilevel security system tags all objects and subjects with security tags, classifying them in terms of sensitivity and access level.
- We formulate access policy based on these levels
- We can also add other dimensions called categories that horizontally partition the rights space (similar to roles)



US DoD Policy

- Used by the US military (and many others), the **lattice** model uses MLS to define policy; the levels are:
  - UNCLASSIFIED < CONFIDENTIAL < SECRET < TOP SECRET
- Categories are represented as an unbounded set:
  - NUC(lear), INTEL(ligence), CRYPTO(graphy)
- These levels are used for physical government documents as well

Aside: What do these levels mean?

The New York Times | https://nyti.ms/2FIsusf

POLITICS

Ex-C.I.A. Officer Suspected of Compromising Chinese Informants Is Arrested

查看简体中文版
查看繁體中文版

By ADAM GOLDMAN JAN. 16, 2018

WASHINGTON — A former C.I.A. officer suspected by investigators of helping China dismantle United States spying operations and identify informants has been arrested, the Justice Department said on Tuesday. The collapse of the spy network was one of the American government's worst intelligence failures in recent years.

Aside: What do these levels mean?

- From a CIA affadavit for an arrest warrant:
  - **Confidential** = "unauthorized disclosure could reasonably result in damage to the national security"
  - **Secret** = "unauthorized disclosure could reasonably result in serious damage to the national security"
  - **Top Secret** = "unauthorized disclosure could reasonably result in exceptionally grave damage to the national security"
  - **Sensitive Compartmented Information (SCI):** special category that provides exceptionally sensitive access (highest level of clearance considered TS/SCI)
    - Requires "numerous security clearance briefs" during employment and a lifetime binding non-disclosure agreement
    - "I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparably injury to the United states or be used to advantage by a foreign nation…"

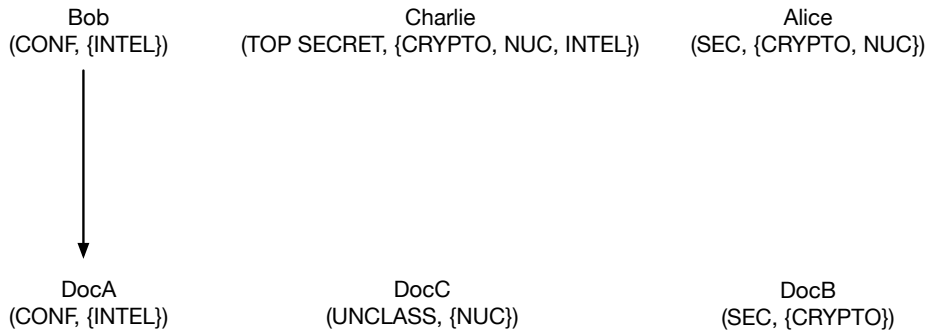
Assigning Security Levels

- All subjects are assigned clearance levels and compartments
  - Alice: (SECRET, {CRYPTO, NUC})
  - Bob: (CONFIDENTIAL, {INTEL})
  - Charlie: (TOP SECRET, {CRYPTO, NUC, INTEL})
- All objects are assigned an access class
  - DocA: (CONFIDENTIAL, {INTEL})
  - DocB: (SECRET, {CRYPTO})
  - DocC: (UNCLASSIFIED, {NUC})

How MLS Works

Evaluating Policy

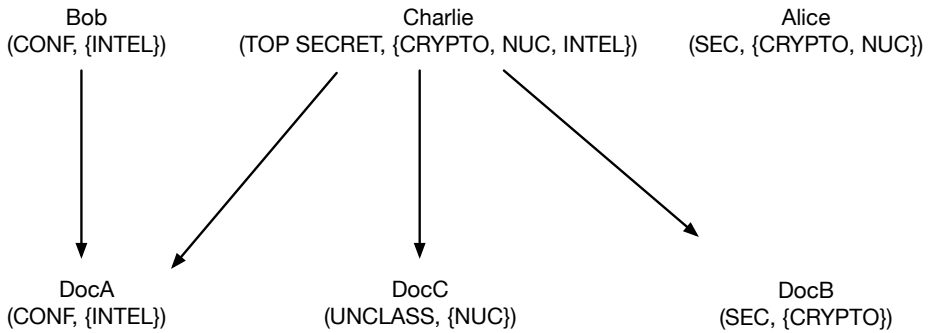
- Access is allowed if:
  - subject clearance level ≥ object sensitivity level and
  - subject categories ⊆ object categories (**read-down** property)



How MLS Works

Evaluating Policy

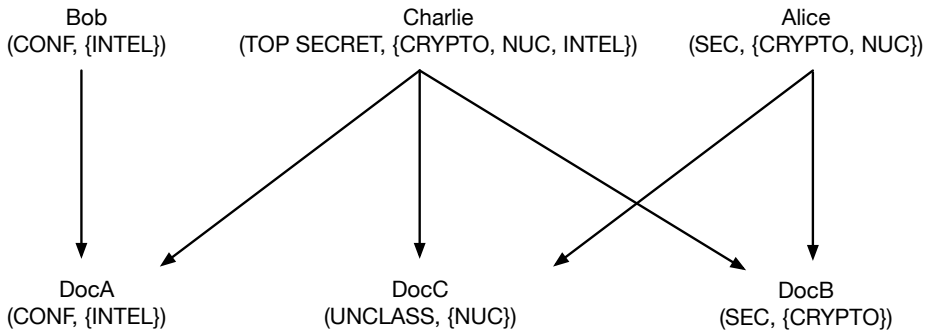
- Access is allowed if:
  - subject clearance level ≥ object sensitivity level and
  - subject categories ⊆ object categories (**read-down** property)



How MLS Works

Evaluating Policy

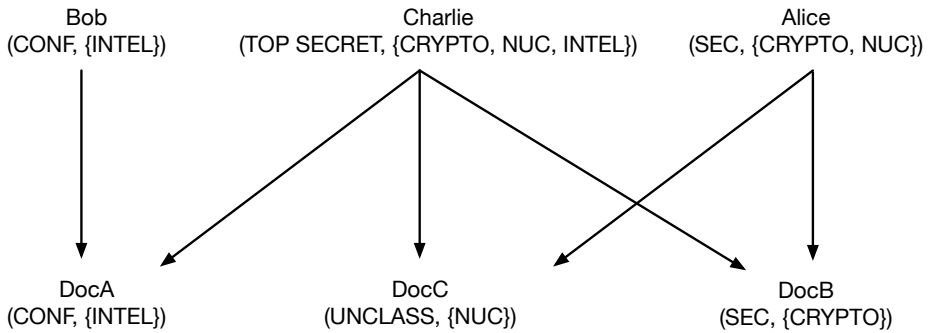
- Access is allowed if:
  - subject clearance level ≥ object sensitivity level and
  - subject categories ⊆ object categories (**read-down** property)



How MLS Works

Evaluating Policy

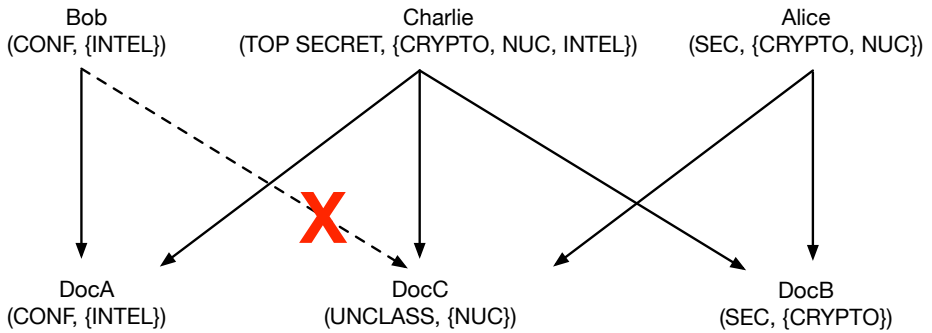
- Access is allowed if:
  - subject clearance level ≥ object sensitivity level and
  - subject categories ⊆ object categories (**read-down** property)
- Can Bob access DocC?



How MLS Works

Evaluating Policy

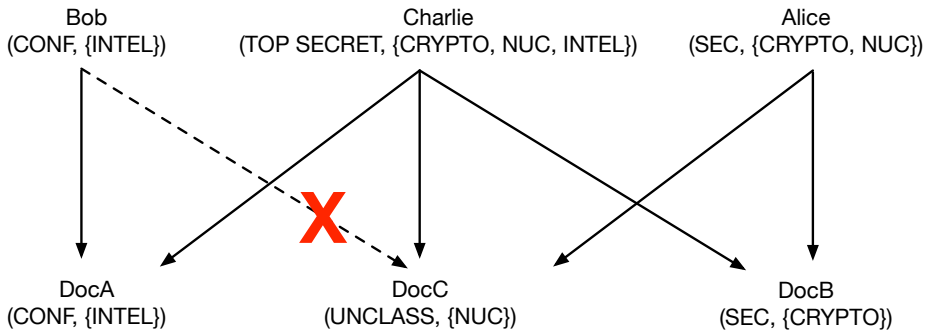
- Access is allowed if:
  - subject clearance level ≥ object sensitivity level and
  - subject categories ⊆ object categories (**read-down** property)
- Can Bob access DocC?



How MLS Works

Evaluating Policy

- Access is allowed if:
  - subject clearance level ≥ object sensitivity level and
  - subject categories ⊆ object categories (**read-down** property)
- What would a **write-up** property be?



How MLS Works

(More) Formal Definitions

— Ability to access a resource because of greater level of rights is called a dominance relationship: if A can access C then it dominates

— $(A, C)\ dom\ (A', C') \iff A' \geq A \cap C' \subseteq C$

Examples:

— (SECRET, {NUC, CRYPTO} dom (CONF {NUC, CRYPTO})

— (TOP SECRET, {NUC} $\neg dom$ (CONF {NUC, CRYPTO})

How MLS Works

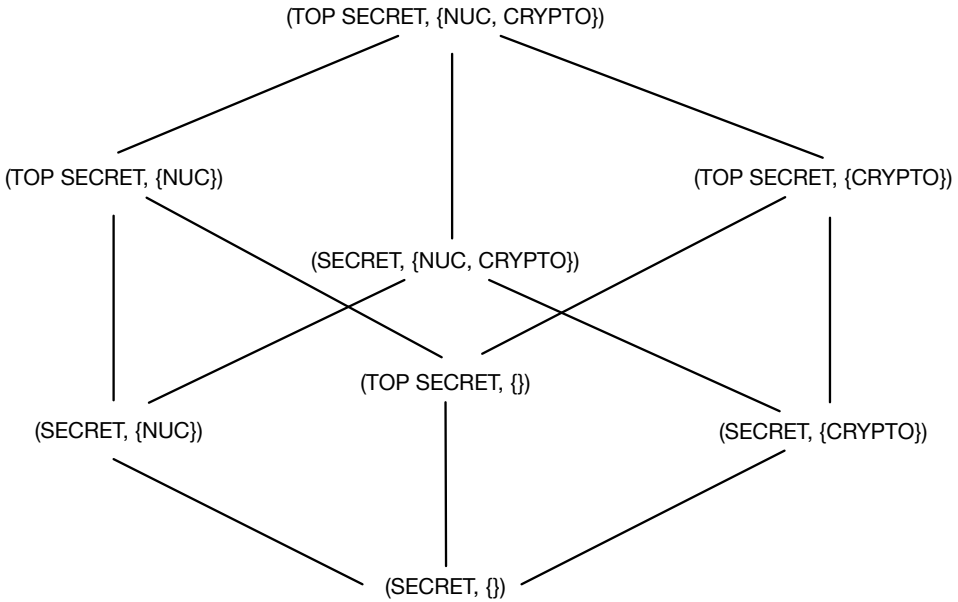
Security Lattices

- Given a set of classifications C and categories K
- Set of security levels $L = C \times K$, dom forms a lattice
- Security levels defined in terms of **least upper bound** (lub, called supremum in lattice theory) and **greatest lower bound** (glb, called an infimum in lattice theory)
  - $lub(L) = (max(A, C))$
  - $glb(L) = (min(A, \varnothing))$
- Security levels form a partially ordered set (poset) and every element has a security level and corresponding supremum and infimum, therefore describing a lattice

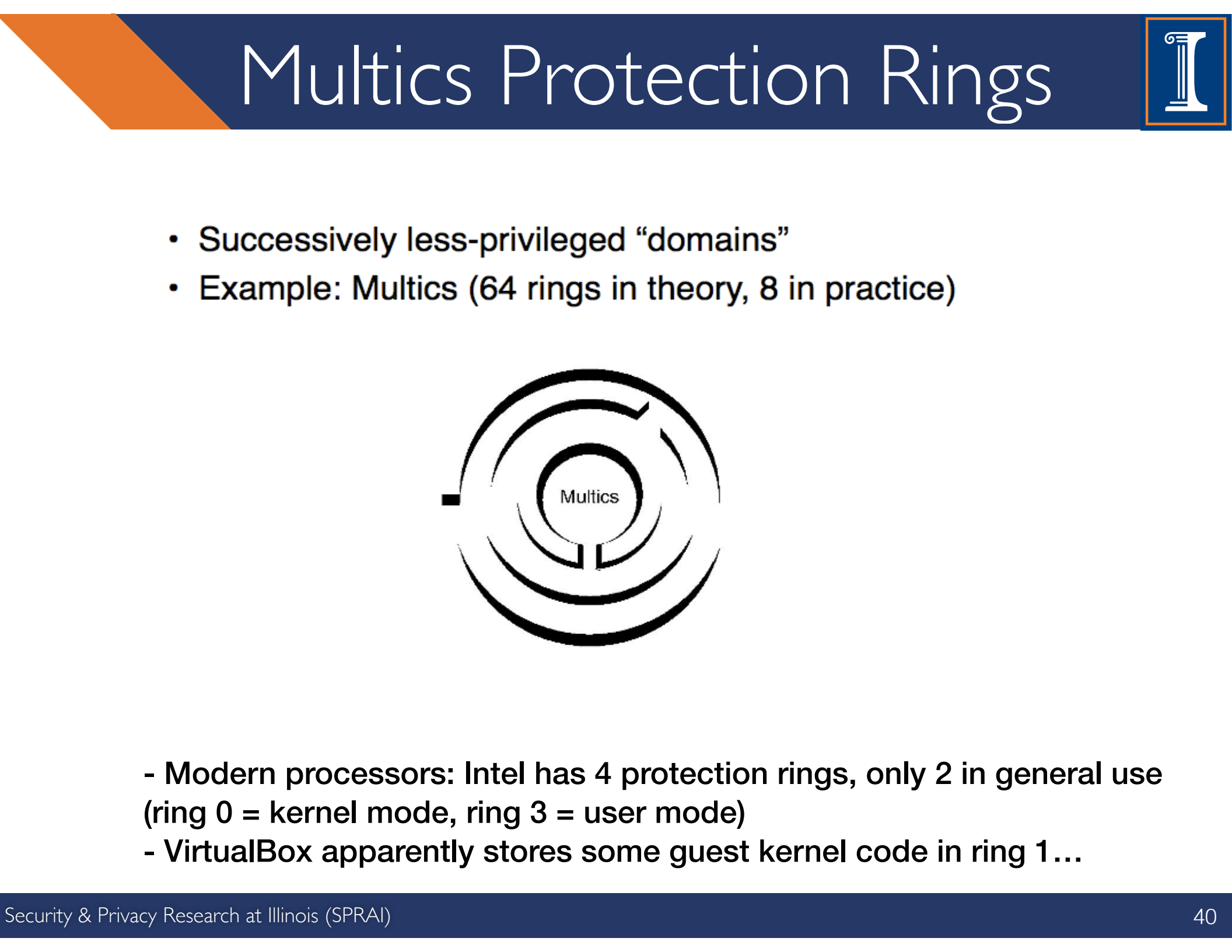
How MLS Works

Lattice Representation

- Security lattices can be represented by a Hasse diagram
- Represents a finite poset as a directed graph of its transitive reduction (minimum representation of edges)



Multics Protection Rings



- Successively less-privileged “domains”
- Example: Multics (64 rings in theory, 8 in practice)

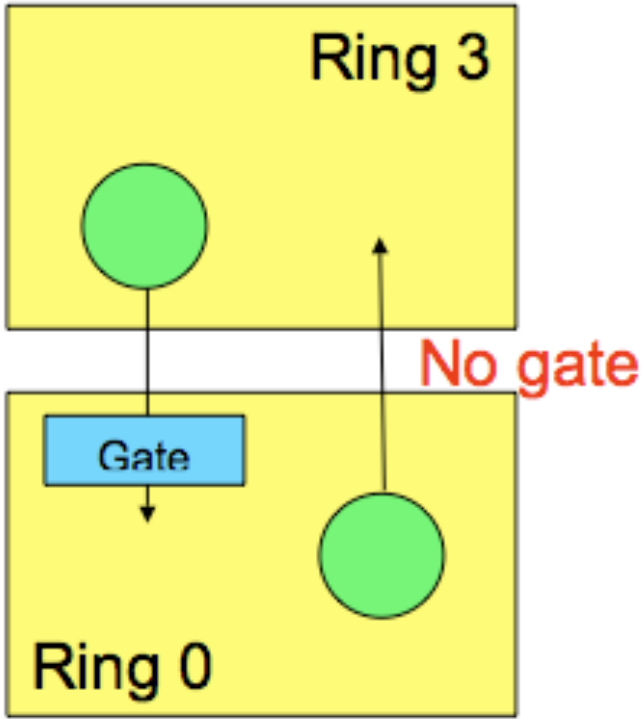
- Modern processors: Intel has 4 protection rings, only 2 in general use (ring 0 = kernel mode, ring 3 = user mode)
- VirtualBox apparently stores some guest kernel code in ring 1…

Multics Ring Brackets

- Kernel resides in ring 0
- Process runs in a ring r
  - Access based on current ring
- Process accesses data (segment)
  - Each data segment has an *access bracket*: (a1, a2)
    - a1 <= a2
  - Describes read and write access to segment
    - r is the current ring
    - r <= a1: access permitted
    - a1 < r <= a2: r and x permitted; w denied
    - a2 < r: all access denied

Multics Process Invocation

- Program cannot call code of *higher privilege* directly
  - Gate is a special memory address where lower-privilege code can call higher
    - Enables OS to control where applications call it



Multics Process Invocation Brackets

- Also different procedure segments
  - with *call brackets*: (c1, c2)
    - c1 <= c2
  - and access brackets (a1, a2)
  - Rights to execute code in a new procedure segment
    - r < a1: access permitted with ring-crossing fault
    - a1 <= r <= a2 = c1: access permitted and no fault
    - a2 < r <= c2: access permitted through a valid gate
    - c2 < r: access denied
- What's it mean?
  - case 1: ring-crossing fault changes procedure's ring
    - increases from r to a1
  - case 2: keep same ring number
  - case 3: gate checks args, decreases ring number

Multics Brackets Examples

Authorized or not?

- Process in ring 3 accesses data segment
  - access bracket: (2, 4)
  - What operations can be performed?
- Process in ring 5 accesses same data segment
  - What operations can be performed?
- Process in ring 5 accesses procedure segment
  - access bracket (2, 4) and call bracket (4, 6)
  - Can call be made? How do we determine the new ring? Can new procedure segment access the data segment above?

Multics Reference Monitor

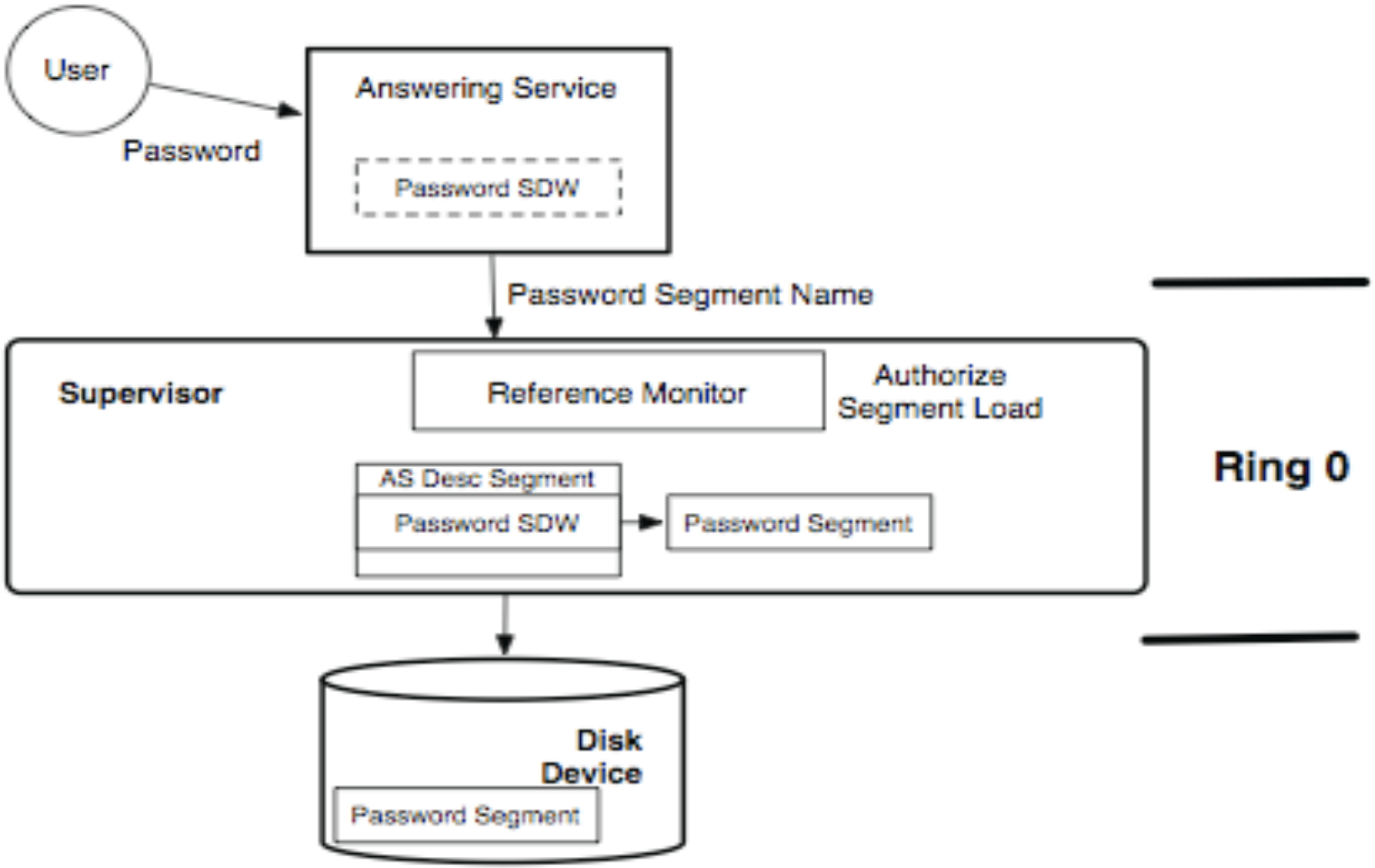


Figure 3.2: The Multics login process. The user's password is submitted to the Multics *answering service* which must check the password against the entries in the *password segment*. The Multics *supervisor* in the privileged *protection ring 0* authorizes access to this segment and adds a SDW for it to the answering service's descriptor segment. The answering service cannot modify its own descriptor segment.

Multics SDW Format

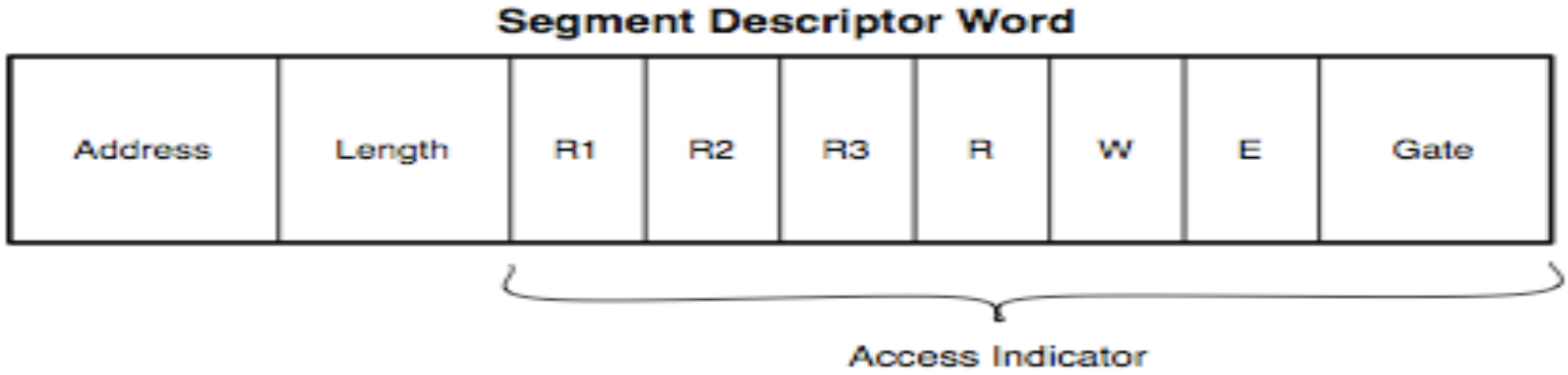


Figure 3.3: Structure of the Multics *segment descriptor word* (SDW): in addition to the segment's address and length, the SDW contains access indicators including *ring brackets* (i.e., *R1*, *R2*, *R3*), the process's ACL for the segment (i.e., the *rwe* bits), and the *number of gates* for the segment.

- Process uses SDW to access a segment
  - Directory stores a mapping between segments and secrecy level
  - Each segment has a ring bracket specification: Copied into SDW
  - Each segment has an ACL: Authorized ops in RWE bits

Multics SDW Examples

Authorized or not?

- Secrecy
  - Clearance of process = secret
  - Access class of segment = confidential
- Brackets
  - Process in ring 2
  - Access bracket (2-3); Call bracket (4-5)
- Access control list
  - RWE

Multics Questions

Multics Questions

- Where do we see Multics concepts and mechanisms in use today?

Multics Questions

- Where do we see Multics concepts and mechanisms in use today?
- What concepts and mechanisms haven't made the cut? Why?

Multics Questions

- Where do we see Multics concepts and mechanisms in use today?
- What concepts and mechanisms haven't made the cut? Why?
- Why aren't we still using Multics-based systems?

Multics Questions

- Where do we see Multics concepts and mechanisms in use today?
- What concepts and mechanisms haven't made the cut? Why?
- Why aren't we still using Multics-based systems?

so, was it secure?