CSci 5271
Introduction to Computer Security
Day 12: OS security: higher assurance

Stephen McCamant
University of Minnesota, Computer Science & Engineering

Outline

Multilevel and mandatory access control, cont'd

Side and covert channels

Announcements intermission

OS trust and assurance

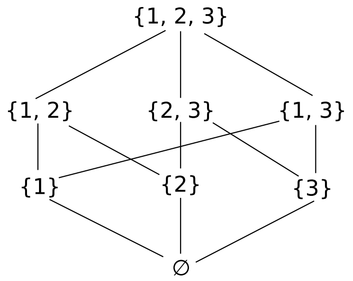
Multilateral security / compartments

- In classification, want finer divisions based on need-to-know
- Also, selected wider sharing (e.g., with allied nations)
- Many other applications also have this character
  - Anderson's example: medical data
- How to adapt BLP-style MAC?

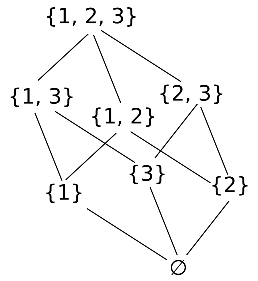
Partial orders and lattices

- $\leq$ on integers is a *total order*
  - Reflexive, antisymmetric, transitive, $a \leq b$ or $b \leq a$
- Dropping last gives a *partial order*
- A *lattice* is a partial order plus operators for:
  - Least upper bound or join $\sqcup$
  - Greatest lower bound or meet $\sqcap$
- Example: subsets with $\subseteq$, $\cup$, $\cap$

Subset lattice example



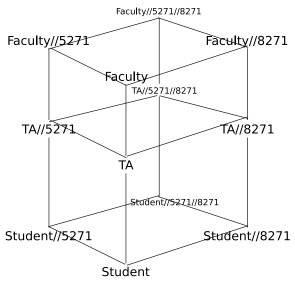
Subset lattice example



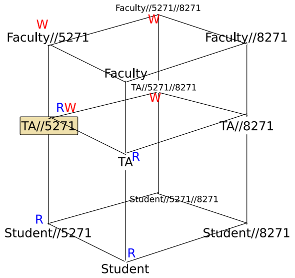
Lattice model

- Generalize MLS levels to elements in a lattice
- BLP and Biba work analogously with lattice ordering
- No access to incomparable levels
- Potential problem: combinatorial explosion of compartments

Classification lattice example



Lattice BLP example



Another notation

Faculty
→ (Faculty, $\emptyset$)
Faculty//5271
→ (Faculty, $\{5271\}$)
Faculty//5271//8271
→ (Faculty, $\{5271, 8271\}$)

MLS operating systems

- 1970s timesharing, including Multics
- "Trusted" versions of commercial Unix (e.g. Solaris)
- SELinux (called "type enforcement")
- Integrity protections in Windows Vista and later

Multi-VM systems

- One (e.g., Windows) VM for each security level
- More trustworthy OS underneath provides limited interaction
- E.g., NSA NetTop: VMWare on SELinux
- Downside: administrative overhead

Air gaps, pumps, and diodes

- The lack of a connection between networks of different levels is called an *air gap*
- A *pump* transfers data securely from one network to another
- A *data diode* allows information flow in only one direction

Chelsea Manning cables leak

- Manning was an intelligence analyst deployed to Iraq
- PC in a T-SCIF connected to SIPRNet (Secret), air gapped
- CD-RWs used for backup and software transfer
- Contrary to policy: taking such a CD-RW home in your pocket `http://www.fas.org/sgp/jud/manning/022813-statement.pdf`

Outline

Multilevel and mandatory access control, cont'd

Side and covert channels

Announcements intermission

OS trust and assurance

Unintentional information flow

- Generalizing from the last section, want to secure all ways information can get revealed
- It is important to consider all the ways this can happen, even unintentional
- This is a never-ending area of security research, and sometimes a serious vulnerability

Side channel

- A *side channel* is an unexpected way in which a system reveals information
  - Different from how information is intentionally output
- These can pop up in many different ways

Analog side channels

- Mediated by the physical world outside the machine:
  - Sound of the hard-disk running
  - Power usage
  - E-M radiation

Digital side channels

- Reveal information while staying inside the computer abstraction:
  - You can't read a file, but the error message reveals that it exists
  - Running time of an operation depends on what else is running

Covert channels

- In a side channel, the source of information is an unsuspecting victim
- In a covert channel, the source and receive work together to transmit information (contrary to a policy)
- Sometimes the channel can be the same, it's just a matter of usage

Exam analogy

- Side channel: the sound of many people erasing indicates that an exam question is difficult
- Covert channel: cough once if the answer is "true", twice if it is "false"

Timing channels

- One common source of side/covert channels is effects on the amount of time operations take
- Lots of factors affect performance of computer operations
- There are many ways to measure the passage of time
  - E.g., with parallel operations even without a clock

Classic: SSH keystroke timing

- When typing your password, keys are sent one by one but encrypted
- Longer delays may mean that keys are farther apart
- Statistics and machine learning are often used in decoding

Outline

Multilevel and mandatory access control, cont'd

Side and covert channels

Announcements intermission

OS trust and assurance

Exercise set 2

- Exercise set 2, covering more memory safety and OS security, is now available on the course public web site
- Due Friday night at 11:59pm
- Last question relates to the lattice model we just covered

Lecture topics and the midterm

- This set of slides are the last material that will be covered on the midterm
- Recall that the midterm will be on Wednesday, October 23rd, in class
- (More info/reminders about the midterm will be upcoming)

Outline

Multilevel and mandatory access control, cont'd

Side and covert channels

Announcements intermission

OS trust and assurance

Trusted and trustworthy

- Part of your system is trusted if its failure can break your security
- Thus, OS is almost always trusted
- Real question: is it trustworthy?
- Distinction not universally observed: trusted boot, Trusted Solaris, etc.

Trusted (I/O) path

- How do you know you're talking to the right software?
- And no one is sniffing the data?
- Example: Trojan login screen
  - Or worse: unlock screensaver with root password
  - Origin of "Press Ctrl-Alt-Del to log in"

Minimizing trust

- Kernel → microkernel → nanokernel
- Reference monitor concept
- TCB size: measured relative to a policy goal
- Reference monitor $\subseteq$ TCB
  - But hard to build monitor for all goals

How to gain assurance

- Use for a long time
- Testing
- Code / design review
- Third-party certification
- Formal methods / proof

Evaluation / certification

- Testing and review performed by an independent party
- Goal: separate incentives, separate accountability
- Compare with financial auditing
- Watch out for: form over substance, misplaced incentives

Orange book OS evaluation

- Trusted Computer System Evaluation Criteria

D. Minimal protection

C. Discretionary protection
   - C2 adds, e.g., secure audit over C1

B. Mandatory protection
   - B1<B2<B3: stricter classic MLS

A. Verified protection

Common Criteria

- International standard and agreement for IT security certification
- Certification against a *protection profile*, and *evaluation assurance level* EAL 1-7
- Evaluation performed by non-government labs
- Up to EAL 4 automatically cross-recognized

Common Criteria, Anderson's view

- Many profiles don't specify the right things
- OSes evaluated only in unrealistic environments
   - E.g., unpatched Windows XP with no network attacks
- "Corruption, Manipulation, and Inertia"
   - Pernicious innovation: evaluation paid for by vendor
   - Labs beholden to national security apparatus

Formal methods and proof

- Can math come to the rescue?
- Checking design vs. implementation
- Automation possible only with other tradeoffs
   - E.g., bounded size model
- Starting to become possible: machine-checked proof

Proof and complexity

- Formal proof is only feasible for programs that are small and elegant
- If you honestly care about assurance, you want your TCB small and elegant anyway
- Should provability further guide design?

Some hopeful proof results

- seL4 microkernel (SOSP'09 and ongoing)
   - 7.5 kL C, 200 kL proof, 160 bugs fixed, 25 person years
- CompCert C-subset compiler (PLDI'06 and ongoing)
- RockSalt SFI verifier (PLDI'12)