Authorization

- **Chapter 3**

Authentication vs Authorization

- Authentication — Who goes there?
  - Restrictions on who (or what) can access system
- **Authorization** — Are you allowed to do that?
  - Restrictions on actions of authenticated users
- Authorization is a form of **access control**
- Authorization enforced by
  - Access Control Lists
  - Capabilities

Lampson's Access Control Matrix

- **Subjects** (users) index the rows
- **Objects** (resources) index the columns

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

Are You Allowed to Do That?

- **Access control matrix** has all relevant info
- But how to manage a large access control (AC) matrix?
- Need to check this matrix before access to any resource is allowed

Access Control Lists (ACLs)

- ACL: store access control matrix by **column**
- Example: ACL for **insurance data** is in **blue**

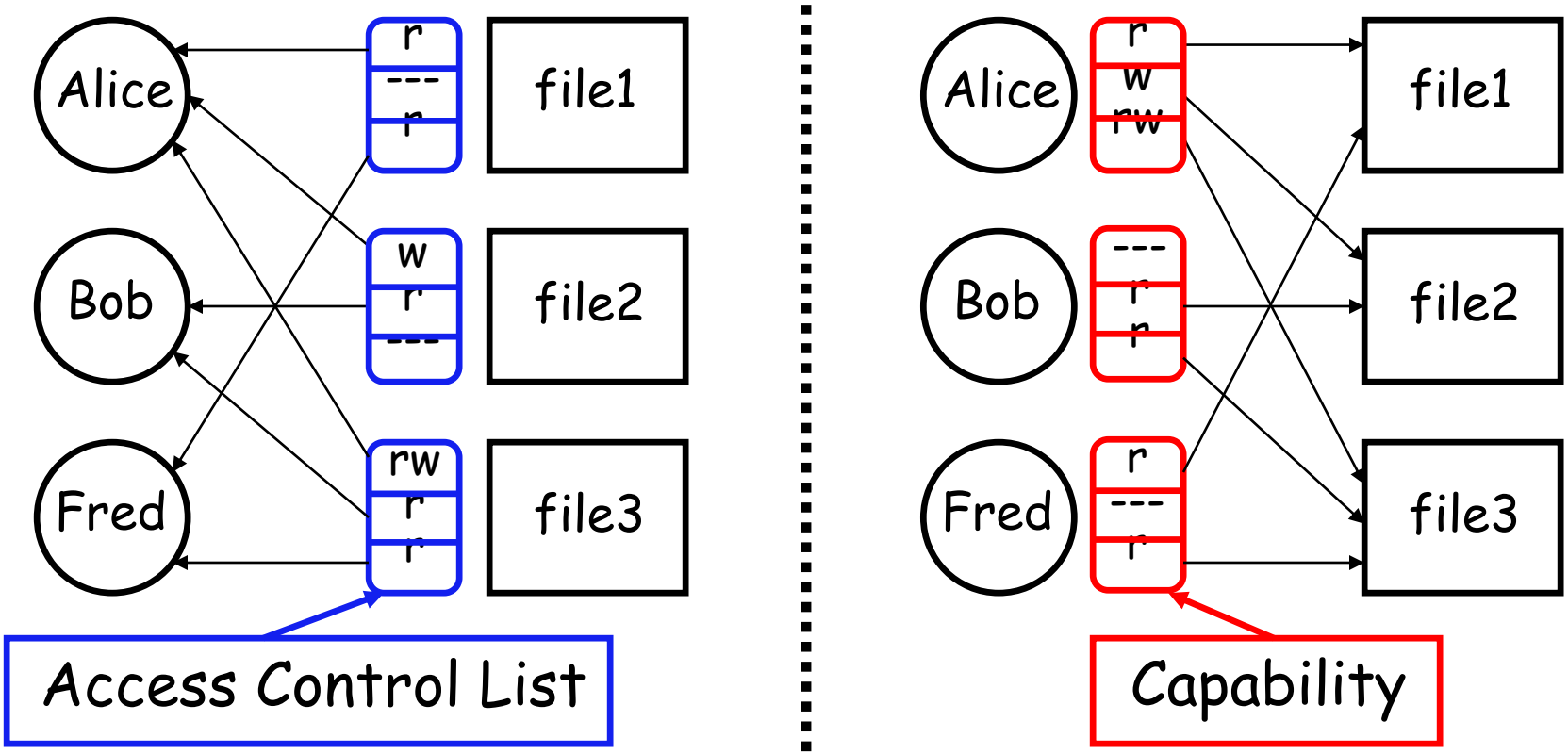
	OS	Accounting program	Accounting data	**Insurance data**	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

Capabilities (or C-Lists)

- Store access control matrix by **row**
- Example: Capability for **Alice** is in **red**

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

ACLs vs Capabilities



- Note that arrows point in opposite directions!
- With ACLs, still need to associate users to files

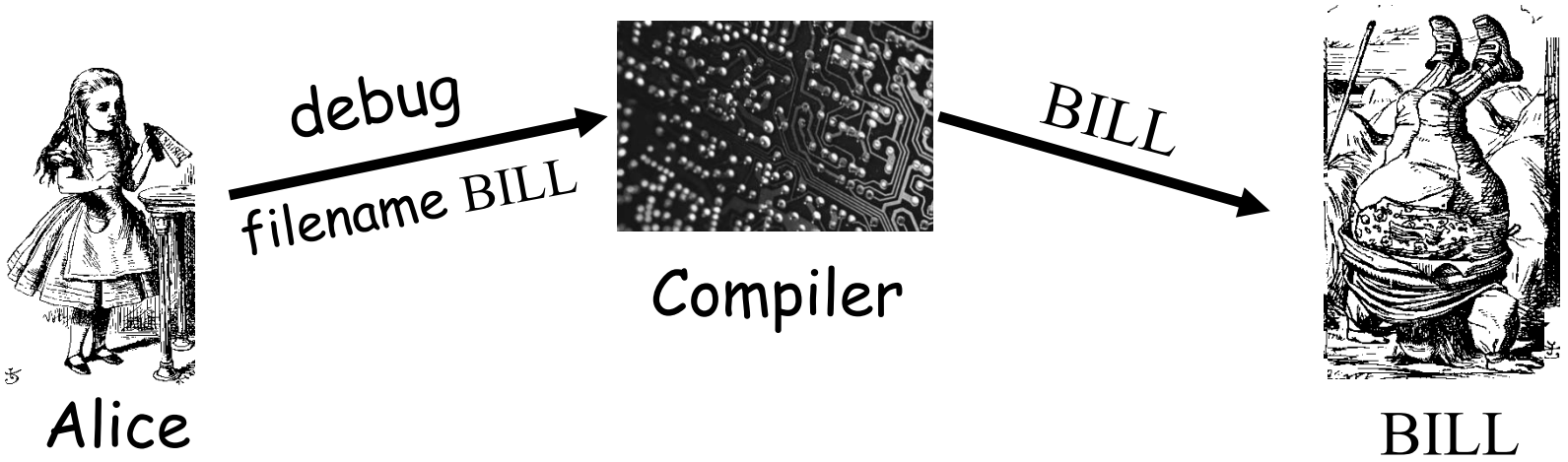
Confused Deputy

- Two resources
  - Compiler and BILL file (billing info)
- Compiler can write file BILL
- Alice can invoke compiler with a debug filename
- Alice not allowed to write to BILL

- Access control matrix

	Compiler	BILL
Alice	x	---
Compiler	rx	rw

ACL's and Confused Deputy



- Compiler is **deputy** acting on behalf of Alice
- Compiler is **confused**
  - Alice is not allowed to write BILL
- Compiler has confused its rights with Alice's

Confused Deputy

- Compiler acting for Alice is confused
- There has been a separation of **authority** from the **purpose** for which it is used
- With ACLs, difficult to avoid this problem
- With Capabilities, easier to prevent problem
  - Must maintain association between authority and intended purpose
  - Capabilities make it easy to **delegate** authority

ACLs vs Capabilities

- ACLs
  - Protection is data-oriented
  - Easy to change rights to a resource
- Capabilities
  - Easy to delegate
  - Easy to add/delete users
  - Easier to avoid the confused deputy

Multilevel Security (MLS) Models

Classifications and Clearances

- **Classifications** apply to **objects**
- **Clearances** apply to **subjects**
- US Department of Defense uses 4 levels of classifications/clearances

  TOP SECRET

  SECRET

  CONFIDENTIAL

  UNCLASSIFIED

Clearances and Classification

- To obtain a **SECRET** clearance requires a routine background check
- A **TOP SECRET** clearance requires extensive background check

Multilevel Security (MLS)

- MLS needed when subjects/objects at different levels use same system
- MLS is a form of **Access Control**
- Military/government interest in MLS for many decades
  - Lots of funded research into MLS
  - Strengths and weaknesses of MLS relatively well understood (theoretical and practical)
  - Many possible uses of MLS outside military

MLS Applications

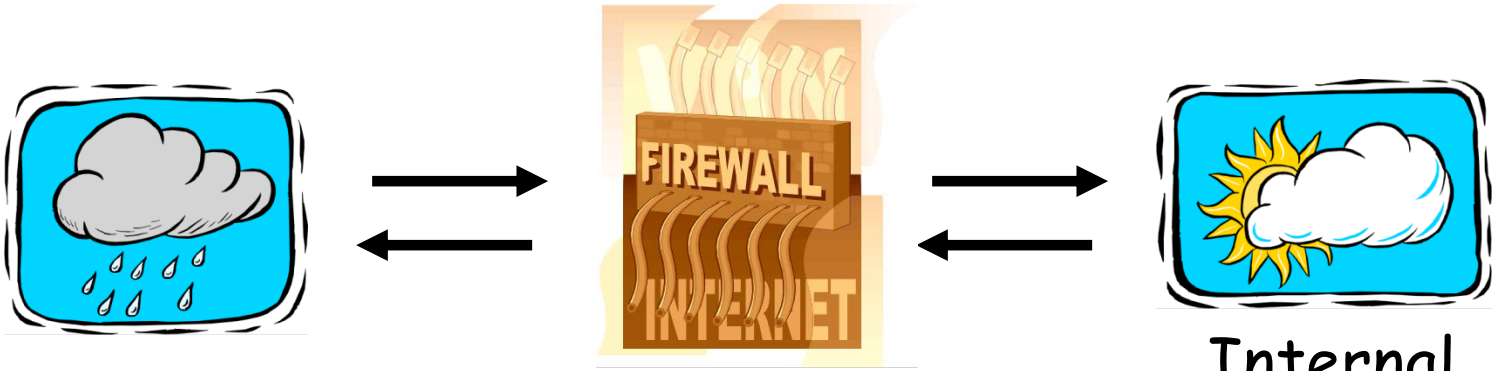
- Classified government/military information
- **Business example:** info restricted to
  - Senior management only
  - All management
  - Everyone in company
  - General public
- Network firewall
  - Keep intruders at low level to limit damage
- Confidential medical info, databases, etc.

MLS Security Models

- MLS models explain **what** needs to be done
- Models do **not** tell you **how** to implement
- Models are descriptive, not prescriptive
  - High level description, not an algorithm

Firewalls

Firewalls



- Firewall must determine what to let in to internal network and/or what to let out
- **Access control** for the network

Firewall as Secretary

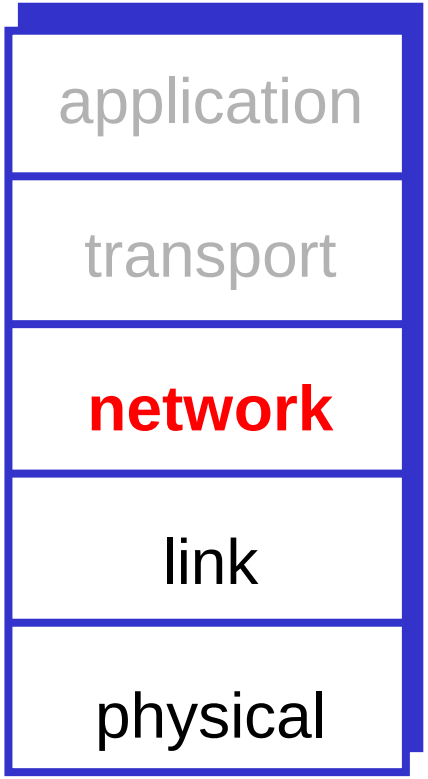
- A firewall is like a **secretary**
- To meet with an executive
  - First contact the secretary
  - Secretary decides if meeting is reasonable
  - Secretary filters out many requests
- You want to meet chair of CS department?
  - Secretary does some filtering
- You want to meet President of US?
  - Secretary does lots of filtering!

Firewall Terminology

- No standard terminology
- Types of firewalls
  - **Packet filter** — works at network layer
  - **Stateful packet filter** — transport layer
  - **Application proxy** — application layer
  - Personal firewall — for single user, home network, etc.

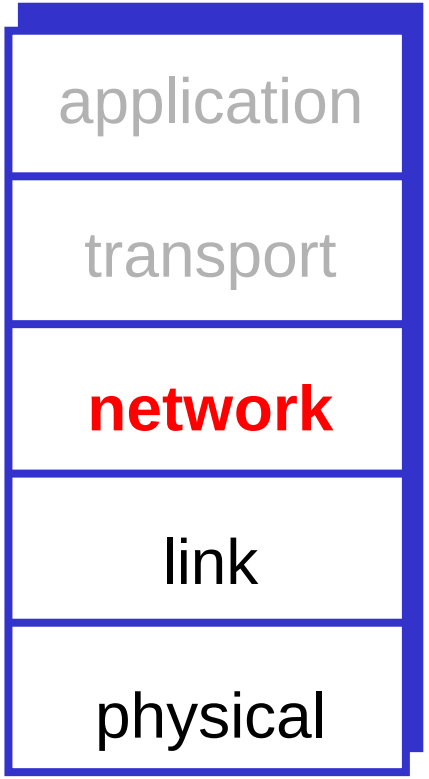
Packet Filter

- Operates at network layer
- Can filters based on
  - Source IP address
  - Destination IP address
  - Source Port
  - Destination Port



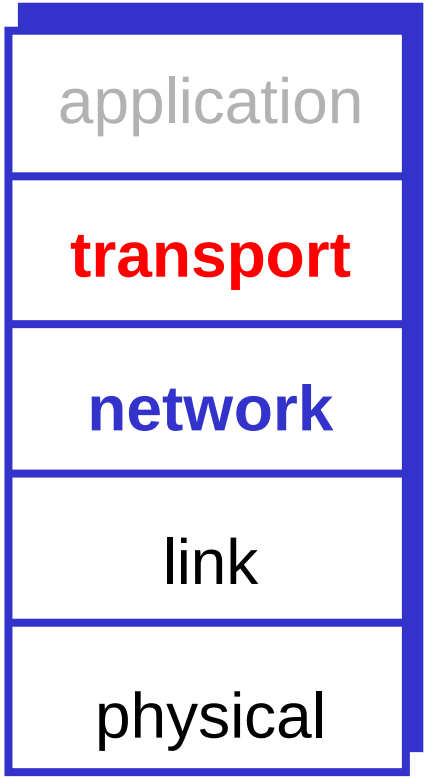
Packet Filter

- Advantage
  - Speed
- Disadvantages
  - No state
  - Cannot see TCP connections



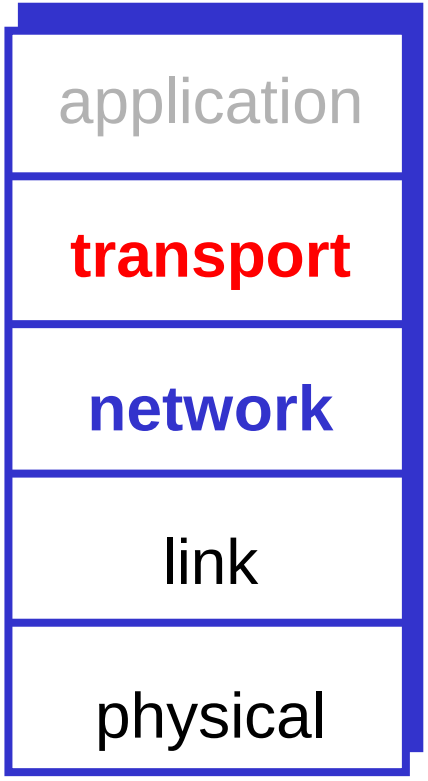
Stateful Packet Filter

- Adds **state** to packet filter
- Operates at transport layer
- Remembers TCP connections
- Can even remember UDP packets (e.g., DNS requests)



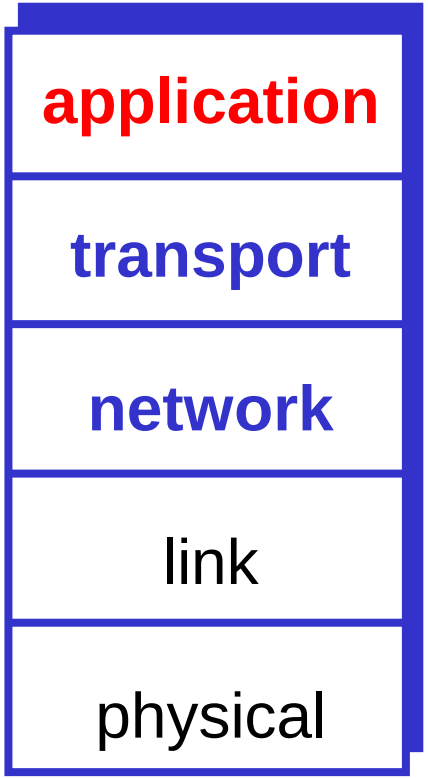
Stateful Packet Filter

- Advantages
  - Can do everything a packet filter can do plus…
  - Keep track of ongoing connections
- Disadvantages
  - Cannot see application data
  - Slower than packet filtering



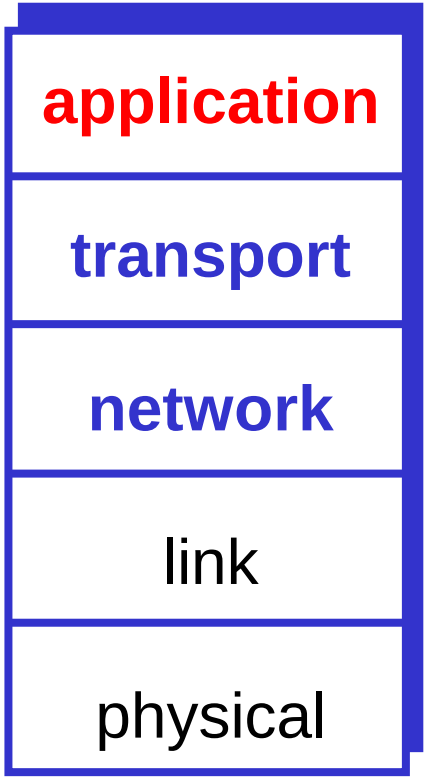
Application Proxy

- A **proxy** is something that acts on your behalf
- Application proxy looks at incoming application data
- Verifies that data is safe before letting it in



Application Proxy

- Advantages
  - Complete view of connections and applications data
  - Filter bad data at application layer (viruses, Word macros)
- Disadvantage
  - Speed

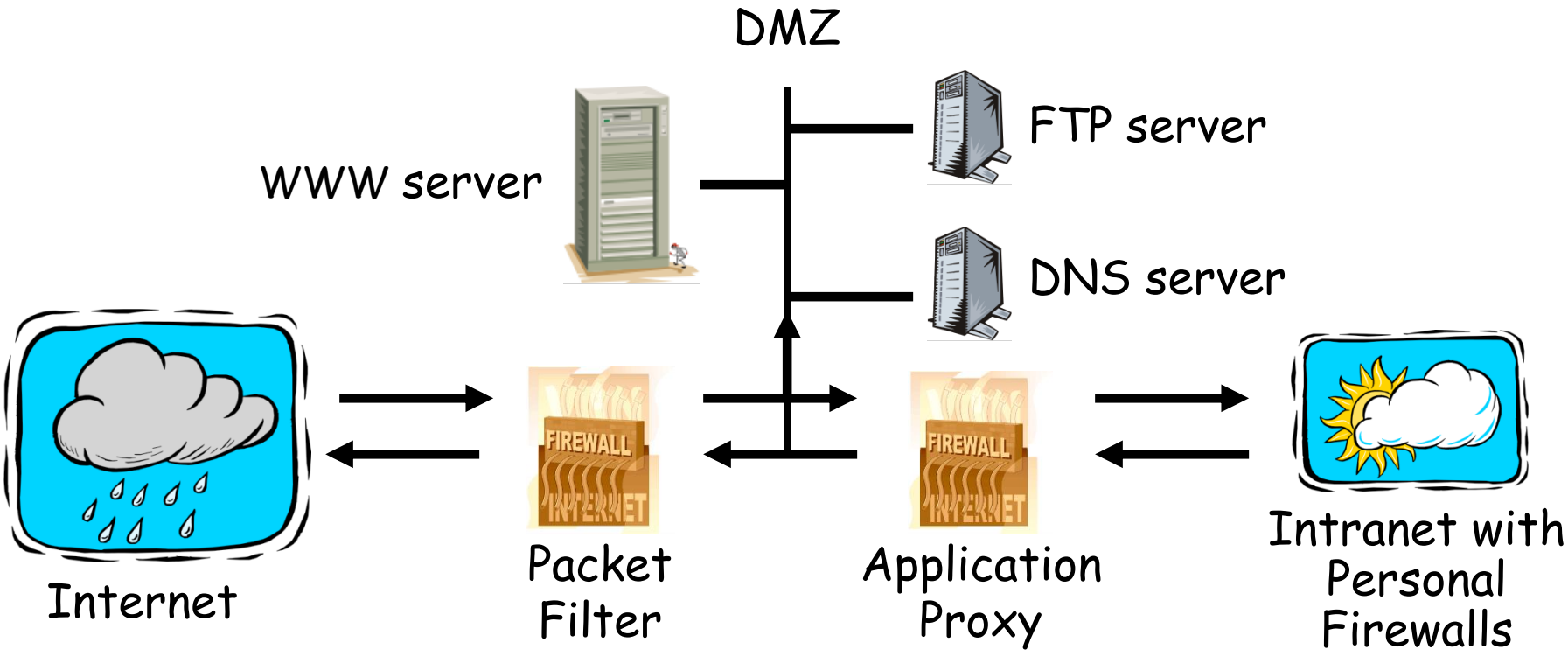


Personal Firewall

- To protect one user or home network
- Can use any of the methods
  - Packet filter
  - Stateful packet filter
  - Application proxy

Firewalls and Defense in Depth

- Example security architecture



Intrusion Detection Systems

Intrusion Prevention

- Want to keep bad guys out
- **Intrusion prevention** is a traditional focus of computer security
  - Authentication is to prevent intrusions
  - Firewalls a form of intrusion prevention
  - Virus defenses also intrusion prevention
- Comparable to locking the door on your car

Intrusion Detection

- In spite of intrusion prevention, bad guys will sometime get into system
- Intrusion detection systems (IDS)
  - Detect attacks
  - Look for "unusual" activity
- IDS developed out of log file analysis
- IDS is currently a very **hot** research topic
- How to respond when intrusion detected?
  - We don't deal with this topic here

Intrusion Detection Systems

- Who is likely intruder?
  - May be outsider who got thru firewall
  - May be evil insider
- What do intruders do?
  - Launch well-known attacks
  - Launch variations on well-known attacks
  - Launch new or little-known attacks
  - Use a system to attack other systems
  - Etc.

How to Measure Normal?

- How to measure normal?
  - Must measure during "representative" behavior
  - Must not measure during an attack…
  - …or else attack will seem normal!
  - Normal is statistical mean
  - Must also compute variance to have any reasonable chance of success

Access Control Summary

- Authentication and authorization
  - Authentication — who goes there?
    - Passwords — something you know
    - Biometrics — something you are (or "you are your key")

Access Control Summary

- Authorization — are you allowed to do that?
  - Access control matrix/ACLs/Capabilities
  - MLS
  - Firewalls
  - IDS