CSCI 331:
Introduction to Computer Security

Lecture 19: Locks

Instructor: Dan Barowy

Williams

Topics

Brute Force

Door Countermeasures

Locks

Your to-dos

1. Lab 7, **due Sunday 11/21**.
2. Last two reading responses:
   a. Reading response (Provos), **due Wed 12/1**.
   b. Reading response (Thompson/Stoll), **due Wed 12/8**.
3. Final project part 3, due Friday, **due 12/10**.

Congrats!

You are done (or nearly done) with this course's graded labs.

They are not easy.

Why did I choose these?

Why did I make them challenging?

The pandemic changed the way I thought about my job.

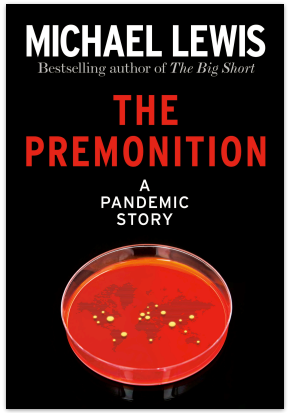
First reason: skills

Developing real skills.

You can **think adversarially**, identify **common** and **uncommon vulnerabilities**, **debug anything**, target **control flow weaknesses**, and most importantly, **write real exploit code**.

These are Hollywood-level hacking skills!

Second reason: competency



We need leaders who **know what they're talking about**.

You know how to recognize **threats** and **act**.

Remember: **know the limits** of your expertise and **listen carefully** when you are out of your depth.

Do the right thing.

This sometimes implies personal sacrifice.

Getting through doors…

Doors

Mostly “secure” only on one side: the outside

Motivations

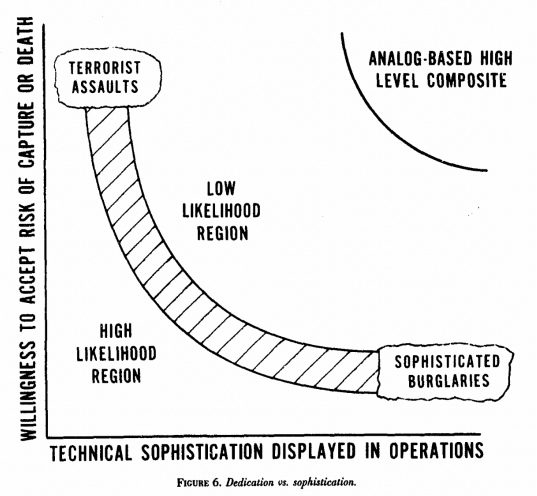


FIGURE 6. *Dedication vs. sophistication.*

Door countermeasures

Exterior doors often swing outward.
This is for safety (e.g., fire safety).

1942 Cocoanut Grove fire (Boston, MA): 492 deaths.
3rd deadliest fire in US history.
Profound effect on fire safety regulations.

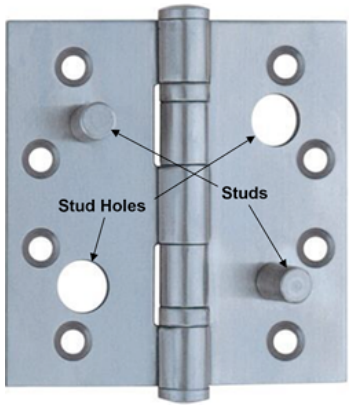
Door countermeasures

Exterior doors often swing outward.
This is for safety (e.g., fire safety).
How do we protect them?

Setscrew hinge

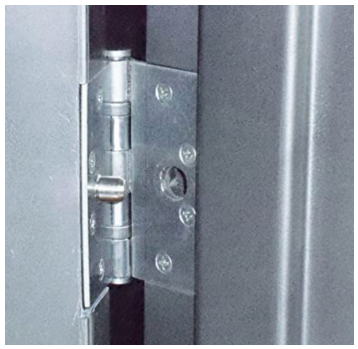
Screw locks hinge pin in place.
Screw only accessible when door is open.

Stud hinge



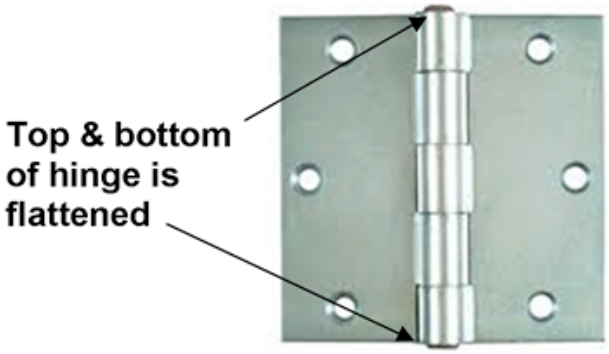
Holds door in place even when hinge pin is removed.
Existing hinges can be easily modified.

Stud hinge modification



Drill holes in both hinge leaves and in door.
On one side insert pin, on other side insert sleeve.

Non-removable hinge pins

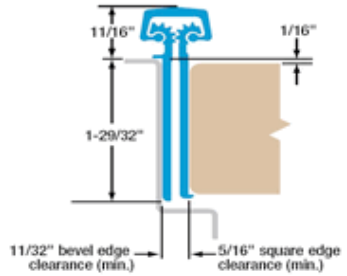


Hinge pin is riveted in place.
Door can only be removed by unscrewing hinge.

Continuous ("geared") hinge

No hinge pins. Much more difficult to attack.
Often used in embassies, correctional facilities,
commercial buildings (and, oddly, bathroom stalls).

Continuous (“geared”) hinge



Leaves (and leaf screws) are concealed when door is shut.

Screw vulnerability

Notice screws are almost always on the *inside*.

Drop ceiling vulnerability

Walls frequently end at drop ceiling!

Brute force

Lock vulnerability: brute force

Lock vulnerability: brute force

https://www.youtube.com/watch?v=dBSSA5ot0tA

Lock vulnerability: (extreme) brute force

https://www.youtube.com/watch?v=P0gksOCqp4I

Latch vulnerability

https://www.youtube.com/watch?v=-Bazy3Ew6D4

Latch guard

Prevents “card” attack

What is the advantage of lockpicking?

Don’t forget!

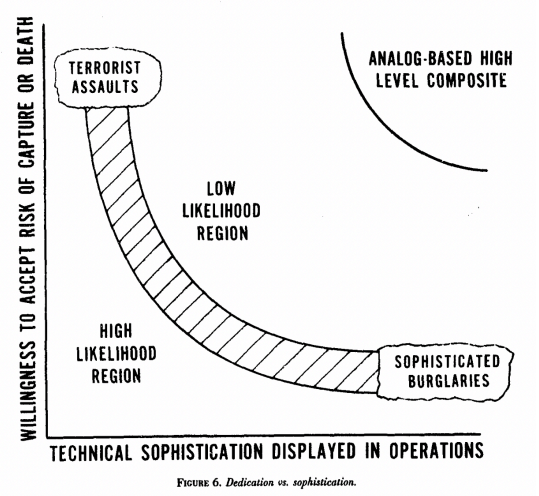
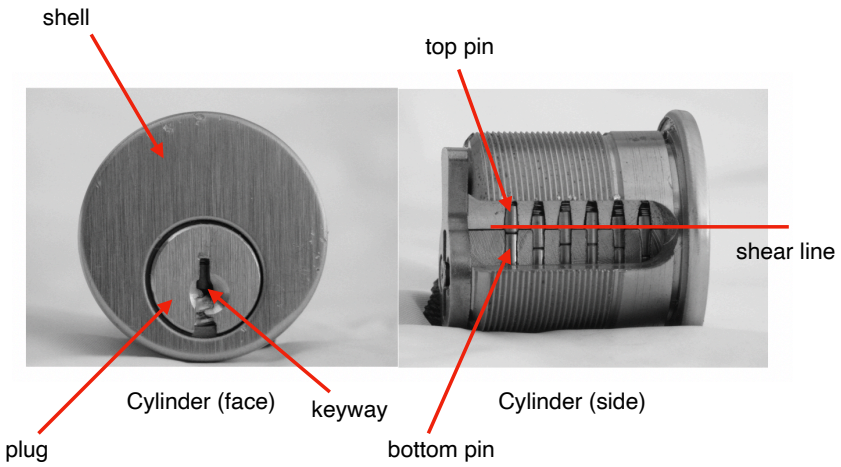


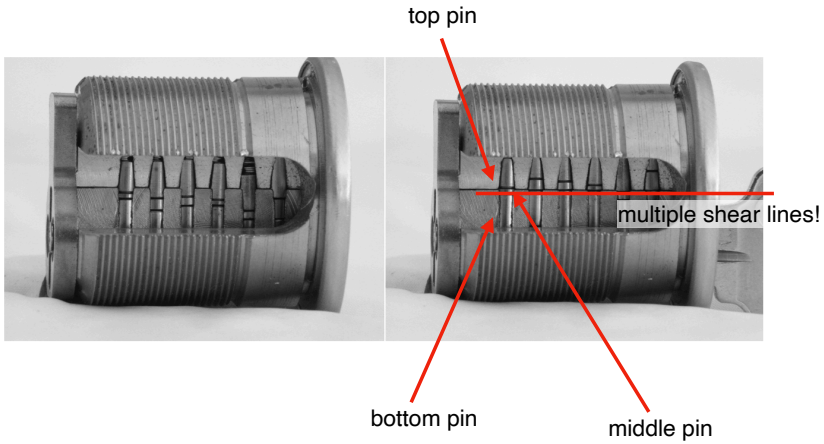
FIGURE 6. *Dedication vs. sophistication.*

How do locks work?

Pin tumbler lock



Master-keyed pin tumbler lock



Paper discussion (Blaze)

Common vulnerabilities

Single-pin picking

hook pick

diamond pick

ball pick

Single-pin picking is fun but is often a waste of time.

Multi-pin picking

rake

Multi-pin picking (“raking”) is usually more effective.

Demos

Lockpicking has limited practicality.

Recap & Next Class

Today we learned:

More common physical vulnerabilities

Locks

Next class:

Something fun