FA2022 Week 09

Physical Security & Lockpicking

Thomas Quig and Sam Ruggerio

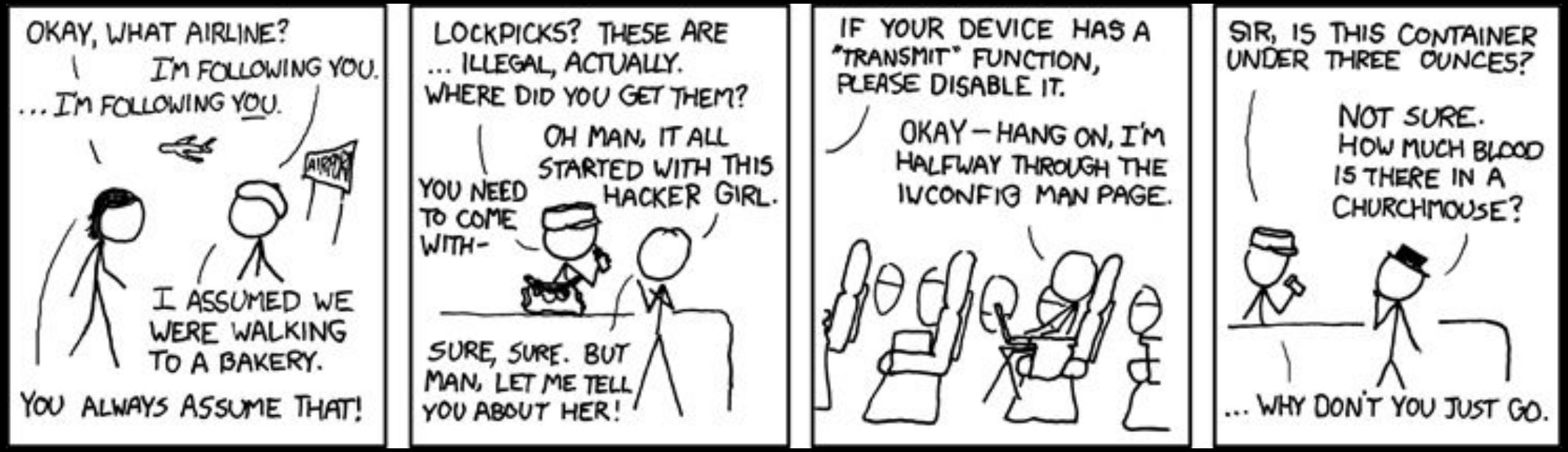
Announcements

- Halloween Party!

- CSAW soon!

ctf.sigpwny.com

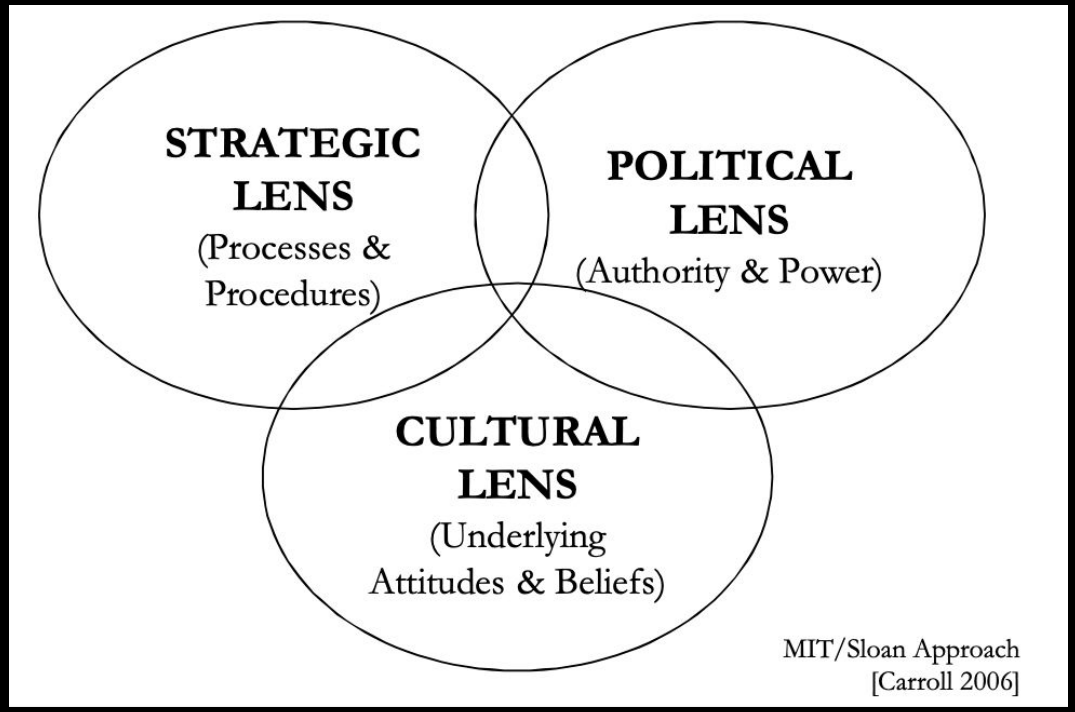
sigpwny{keys_picks_cameras_safes}



Physical Security

- Still extends the fundamentals of security, just in the physical world

- What you need personally versus a corporation versus a government lab are usually wildly different.
  - unless your net worth is that as of a company.
  - traditional mentality "gates, guards, guns" doesn't really hold up anymore



What is Physical Security?

- protecting the most vulnerable path
- *f*(system theory, organizational theory, control theory)
- Emergent Across Hierarchical Levels
- communication of control actions
- recurrent human actions over time
- eliminating migration of facility into vulnerable or insecure states

(Sandia National Laboratory talk)

Access Control

- Allowing the people that you want within your living area

- Fences, gates, walls are all deterrents

- Keys and locks are what most people have, but is basically equal to just closing your door.
- RFID/NFC keycards is stronger, global access control for your business or home.

Surveillance

- If you have something to steal, most people will weigh the risk of just breaking a window instead of picking the door.

- Cameras that are recording to a secure server allows you to track poorly prepared adversaries.
- Doorbell cameras are also nice, although cloud based solutions could be insecure.

- At a corporate level, you may see heat/motion sensors or patrol guards

Detection

If someone gets in, can we make sure we know they’re there.

Difficult, one point of entry can lead to failure.

Cameras, Sensors on points of entry etc.

Legal Warning

- Picking locks that you don't have permission to pick is illegal

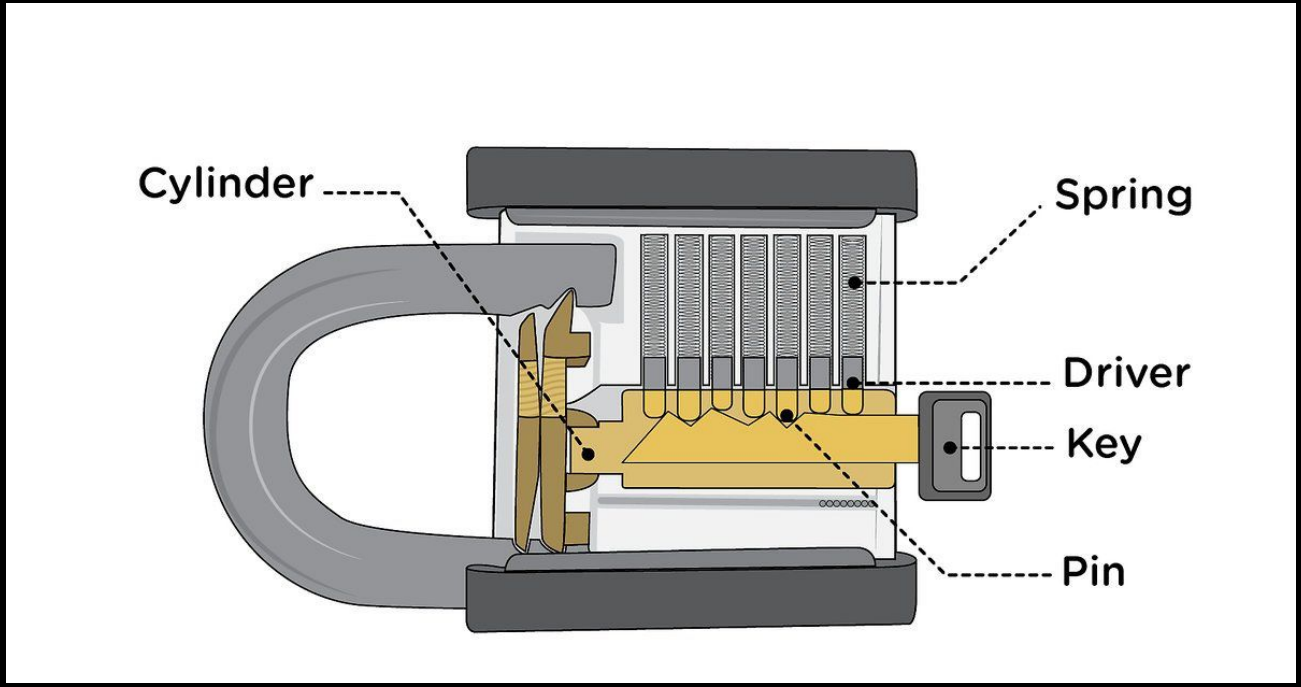
- In Illinois, it is illegal to carry lockpicks with an intent to commit crime. It is illegal to carry bump keys.

- Explicitly Illegal to possess in NV, OH, VA
- Check state laws for specific regulations.

- Please be smart. This is a controlled environment with explicit permission

Locks

Surprisingly used everywhere, despite being incredibly weak to most attacks.



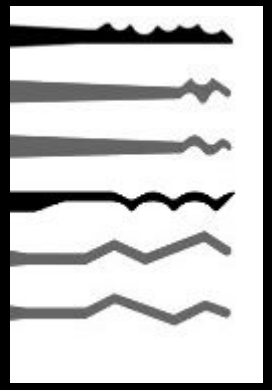
Lockpicking a Cylinder Lock

- Apply torque to the cylinder
- Try every pin until one "binds"
- Due to manufacturing errors, pins will bind and you'll be able to move a pin to the break line and keep it there.
- Repeat until you have picked every pin, the cylinder will follow with the torque.

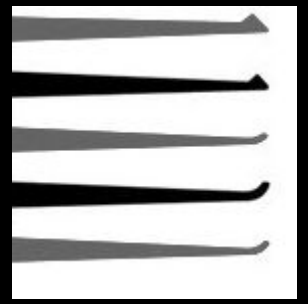
- Pins not staying at the break line? Apply more torque.
- No pins are binding? Apply less torque.

Methods

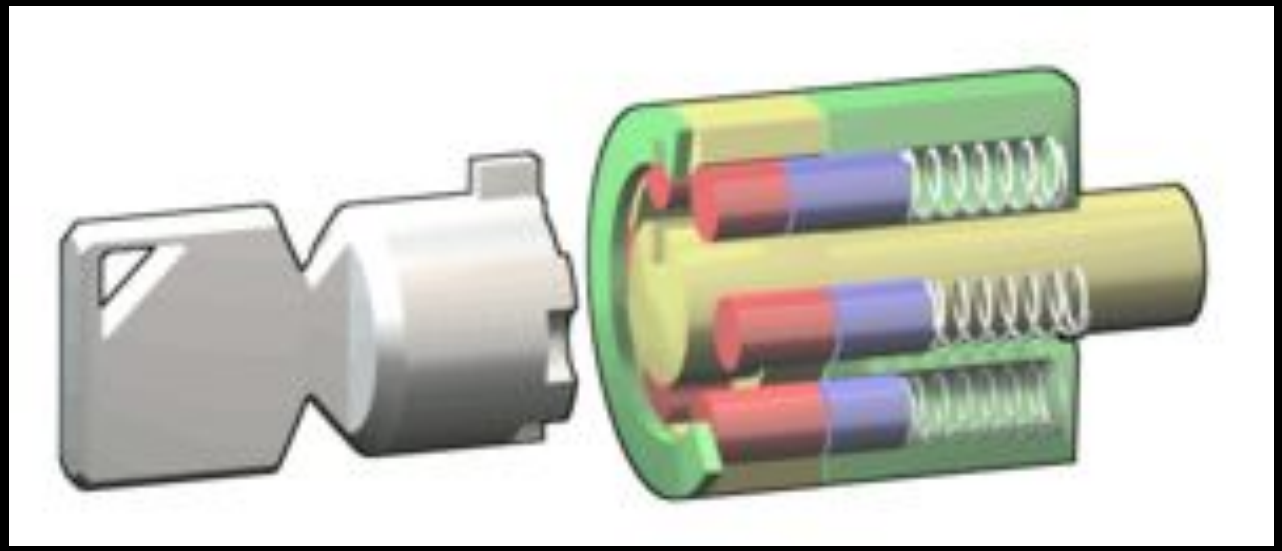
- Rake Picking



- Single Pin Picking



Bonus: Tubular Lock



Demo!!!

Next Meetings

2022-10-30 - Social

- Social
- Halloween party :) Amogus

2022-11-03 - Operational Security (Tentative)

- Keep yourself secure online!
- Very approachable

SIGPwny