Lockpicking: A Problem Statement on the Illusion of Security

By

Vibhuti Naik
Intern ID: 2046

Lockpicking

The fundamental problem in lockpicking (from a security perspective) is the asymmetry between perceived security and actual physical resistance. Most consumers believe a locked door is a barrier, whereas a locksmith or penetration tester views it as a timed delay.

Here are few problem statements for simulating various lock types.

1. Wafer Tumbler Locks
Commonly found in cars, cabinets, and desks, these use flat wafers instead of cylindrical pins.

- **The Simulation Challenge:** Unlike pins, wafers are single pieces of metal that must be moved to a specific window in the center. The simulation must account for double-sided wafers, where the picker must tension the lock while navigating both the top and bottom of the keyway.
- **Key Variable:** "Over-setting" is much easier here because the wafers are thin and can easily slip past the shear line.

2. Lever Tumbler Locks
Often used in safes and older European doors, these rely on a set of flat levers that must be lifted to a specific height to allow a "bolt stump" to pass through a gate.

- **The Simulation Challenge:** This requires simulating non-linear tension. As you lift one lever, it may bind another. The simulation must accurately model the "gate" (the notch the bolt slides through) and "false gates" designed to trap the picker.
- **Key Variable:** The friction between the lever surfaces and the pressure of the internal springs.

3. Disc Detainer Locks
Popularized by brands like Abloy, these use rotating discs instead of reciprocating pins or wafers.

- **The Simulation Challenge:** This is a rotational problem rather than a height problem. The simulation must track the angular position of each disc.

- **Key Variable:** The "False Gate" mechanic is critical here. If the simulation doesn't perfectly model the tactile "click" of a disc falling into a false notch versus a true notch, the simulation loses its realism.

4. Tubular Locks

Frequently seen on vending machines and bike locks, these are essentially pin tumblers arranged in a circle.

- **The Simulation Challenge:** The difficulty here is simultaneous manipulation. While they can be picked one pin at a time, most simulations focus on the "tubular pick" tool which applies equal pressure to all pins.
- **Key Variable:** Spring tension variance. In high-security tubular locks, each pin might have a different spring weight, making a standardized tool fail.

5. Magnetic Locks (Passive)

Some high-security locks use small magnets embedded in the key to repel or attract internal rotors.

- **The Simulation Challenge:** This shifts from mechanical physics to magnetic field simulation. The picker (user) must move a magnetic probe and feel the "pull" or "push" to identify the polarity of the internal components.

6. Dimple Locks

Dimple locks are essentially pin tumblers where the pins are oriented horizontally and interacted with using the flat side of the key.

- **The Simulation Challenge:** The movement is rotational. Instead of lifting a pin, the picker must "flick" or rotate a flag-shaped pick to move the pins. The simulation must account for the extremely tight tolerances and the "warding" (the shape of the keyway) that limits the pick's range of motion.
- **Key Variable: Side Pins.** High-security dimple locks often have interactive elements on the side of the plug that must be set simultaneously with the main stack.

7. Combination (Rotary) Locks

Used primarily on safes and lockers, these rely on a series of "wheels" with notches (gates) that must align to allow a fence to drop.

- **The Simulation Challenge:** This is an exercise in acoustics and vibration. The simulation focuses on the contact points between the "drive cam" and the "wheels." The user must detect minute changes in resistance (friction) or sound as the dial turns.
- **Key Variable: Contact Points.** The physics engine must calculate the exact degree on the dial where the lever hits the cam to allow for "graphing"—a technique used to visualize the internal wheel shapes.

8. Warded Locks

These are the simplest and oldest types of locks, found on padlocks or old house doors. They use a series of static metal plates (wards) to block the wrong key.

- **The Simulation Challenge:** This is not a "picking" simulation in the traditional sense, but a geometry and bypass simulation. The "puzzle" is finding a tool (skeleton key) that is thin enough to bypass the wards entirely and hit the back spring.
- **Key Variable:** Obstacle collision detection. The simulation focuses on the "pathing" of the tool through a maze-long keyway.

9. Cruciform (Cross) Locks

These are essentially four pin tumbler locks arranged in a cross (+) shape.

- **The Simulation Challenge:** The primary difficulty is tension management. Applying tension to one "arm" of the cross can bind the pins in the other three arms unevenly. The simulation must track four independent pin stacks and how they interact with a single rotating plug.
- **Key Variable:** Shear line synchronization. If one stack is picked but another is over-set, the plug will not turn, requiring the player to "feel" which arm is causing the bind.

10. Slider Locks

Often found as secondary locking mechanisms in high-security cylinders, sliders move back and forth along a track rather than up and down.

- **The Simulation Challenge:** Sliders often have "false gates" that are extremely shallow. The simulation must model the subtle feedback of a slider moving 0.5mm into a false notch versus 2.0mm into a true gate.

- **Key Variable:** Interaction with a "Sidebar." Most slider locks use a sidebar that won't retract until every slider is perfectly aligned.

11. Biometric Systems (Fingerprint & Facial Recognition)

Modern biometric locks no longer just "match a picture." They use liveness detection to verify that the biological sample is part of a living human.

- **The Simulation Challenge:** Instead of "picking," the player must simulate Spoofing (physical fakes) or Injection (digital bypass).
  - Physical: Simulating the creation of a 3D-printed mask or a "gummy finger" with the correct thermal and capacitive properties.
  - Digital: Simulating an "Injection Attack" where the player intercepts the camera's ribbon cable and injects a pre-recorded video stream or a synthetic "Deepfake" directly into the processor.
- **Key Variable: False Acceptance Rate (FAR).** The simulation should model the probability that a "near-match" or high-quality fake trick the sensor based on environmental lighting or sensor degradation.

12. Electronic Smart Locks (IoT & Connectivity)

These locks rely on Bluetooth Low Energy (BLE), Wi-Fi, or protocols like **Matter** (a unified smart home standard in 2026).

- **The Simulation Challenge:** This is a Side-Channel Attack simulation. The "picker" isn't moving pins; they are performing "sniffing."
  - Replay Attack: Simulating the capture of an encrypted "unlock" packet from a smartphone and attempting to play it back to the lock.
  - Power Analysis: Monitoring the lock's power consumption to determine when the processor is performing a "successful" vs. "failed" credential check.
- **Key Variable: Firmware Latency.** Some simulations model the "30-second lockout" after four wrong attempts, forcing the player to simulate a "Power Cycle" to reset the timer (a known bypass for certain 2020-era budget smart locks).

13. Cloud-Based Access Control

Often used in commercial buildings, these locks don't store "keys"; they check a remote database via the cloud for every entry request.

- **The Simulation Challenge:** This moves the simulation into Network Topology. The player must simulate a "Man-in-the-Middle" (MitM) attack between the lock and its cloud server.
- **The "Offline Mode" Exploit:** A common simulation scenario involves jamming the lock's Wi-Fi signal to force it into "fail-secure" or "fail-safe" mode, then exploiting the local override protocol which is often less secure than the cloud one.
- **Key Variable: API Vulnerability.** Simulating the exploitation of an unencrypted API endpoint to send an "Emergency Open" command.

14. Smart Safes & Multi-Layered Hybrids

High-security units in 2026 often feature "Electronic Front, Mechanical Back" systems. You might use a fingerprint to activate a motor, which then allows you to turn a physical dial.

- **The Simulation Challenge: Layered Logic.** The player must first solve a digital puzzle (hacking the keypad) to unlock the physical dial's movement, then solve the mechanical puzzle (manipulating the wheels).
- **Key Variable: Solenoid Interaction.** In many "smart" safes, an electronic solenoid acts as the final gate. A common simulation involves using a high-powered Neodymium magnet to physically pull the solenoid pin without ever touching the electronics—a classic "magnet bypass."