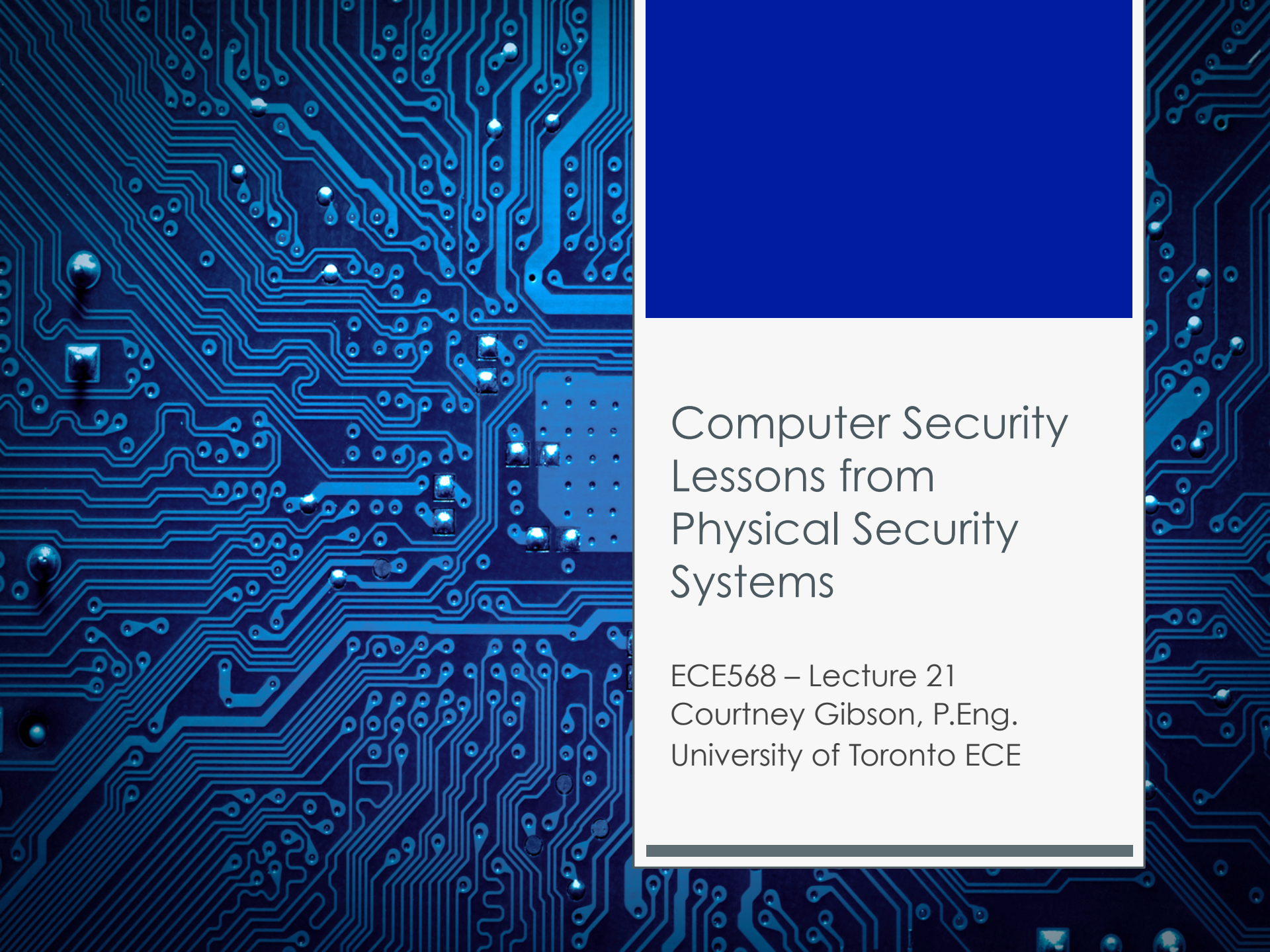
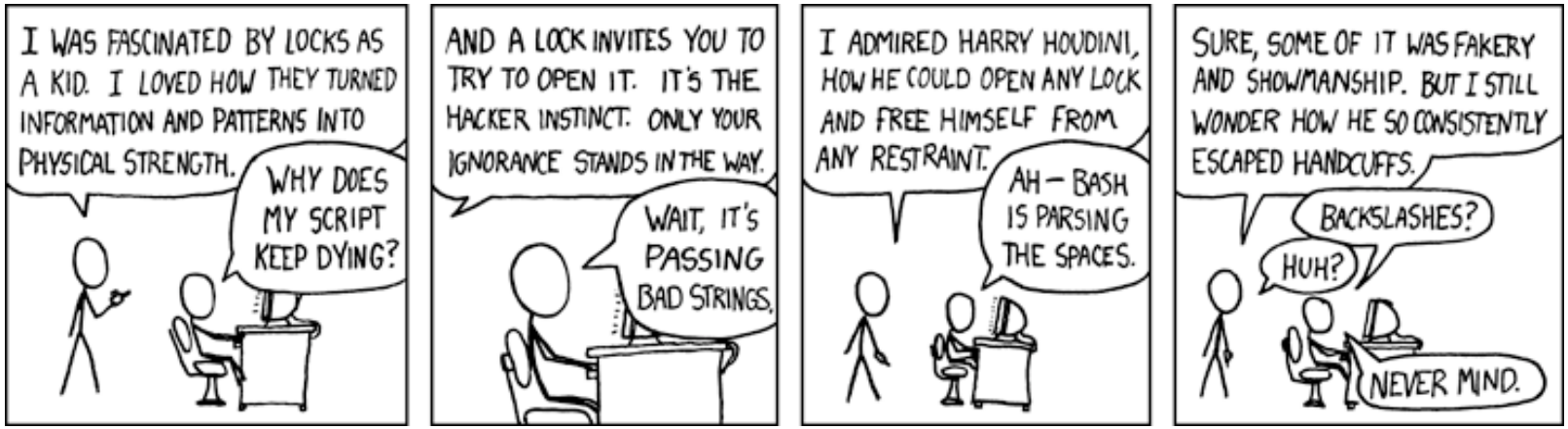


Computer Security Lessons from Physical Security Systems

ECE568 – Lecture 21

Courtney Gibson, P.Eng.
University of Toronto ECE



Source: xkcd.com

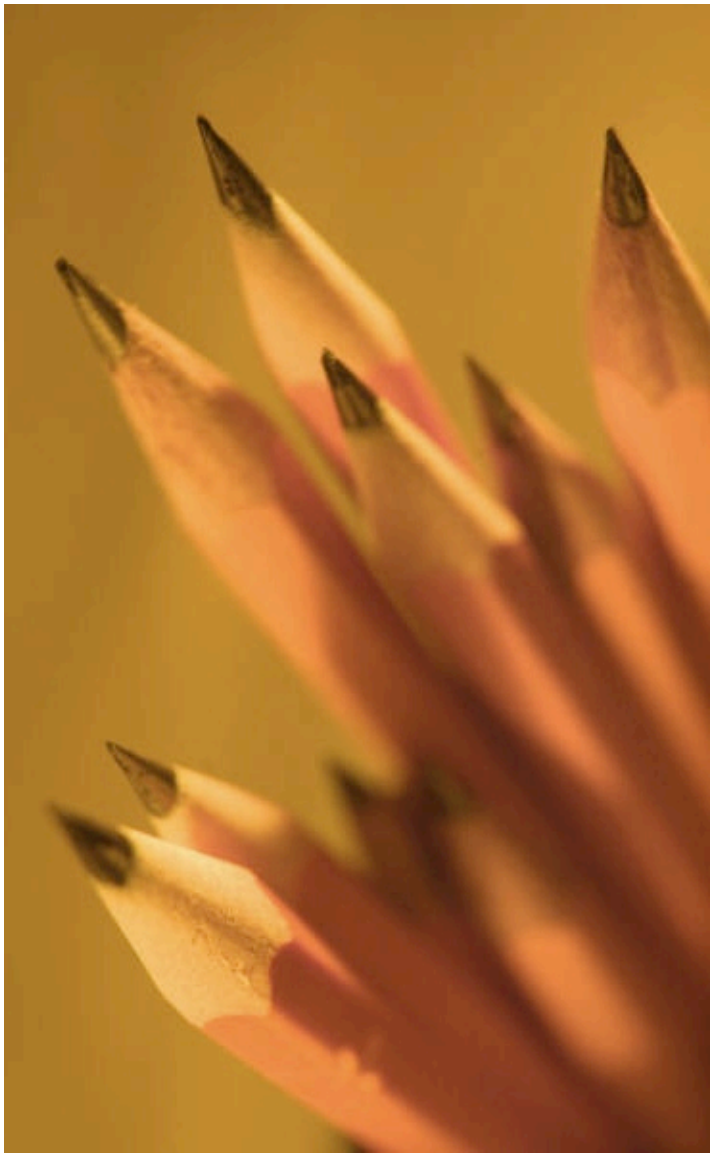
Outline

Background

- Technological Evolution
- Different Approaches to Disclosure

Lessons from the Physical Security World

Thinking about System Design



Background

Why Locks?

Presents an interesting opportunity to look at the evolution of a security design goal that has remained unchanged for over 4,000 years:

> "*Do not let the bolt move until someone presents a valid token*"

Opportunity to practice design and discover weaknesses on discrete, well-understood, physical systems.

Negative Goals

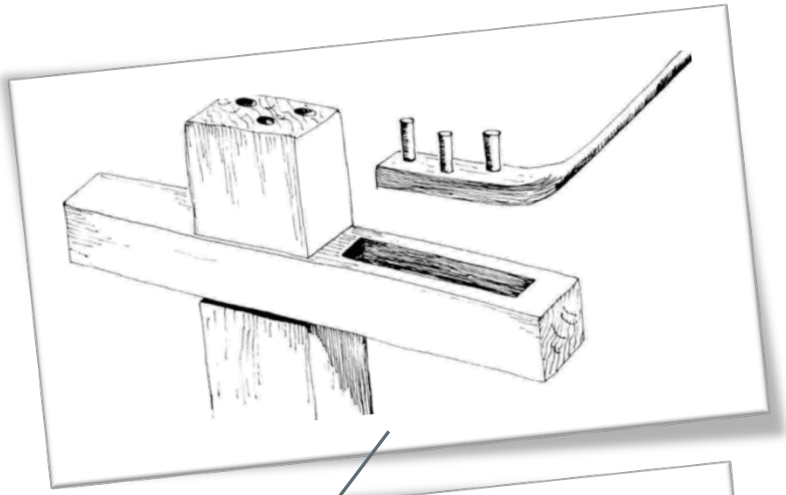
Recall: much of what makes security hard to implement/verify is related to negative goals.

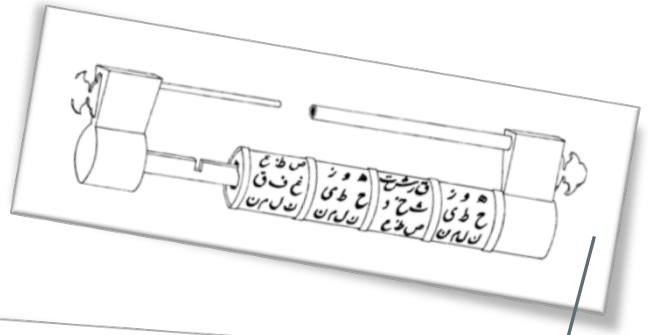
- Computer security goals:
  - Alice cannot read the file
  - Charlie cannot forge a message from Bob
- Physical security goals:
  - Alice cannot open the door
  - Charlie cannot copy a key belonging to Bob

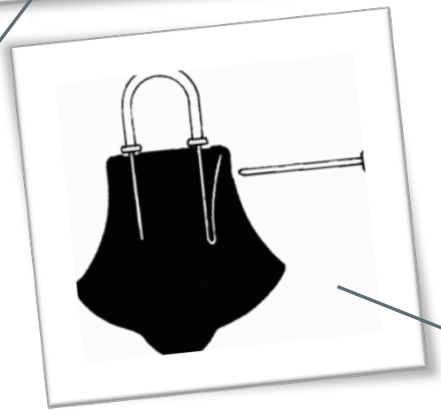
Before Locks

Before we began to create devices to protect our wealth, there were limited options:

- Hiding it
- Encasing it
- Guarding it







2000 BCE
Egypt

79
Rome

800
Persia

1300
China

1500
Persia

Today

Roman-Era Bronze Lock Latch, Bolt and Keys (circa 200AD)

Hand-Forged Spring-Barb Padlock (circa 19th-century, India)

Source: Die Hausbücher der Nürnberger Zwölfbrüderstiftungen (1451)

Banbury Lock (circa 17th-century, Canterbury, UK)

History of Development

Slow, steady design improvements matched pace with advances in materials and tooling

- Earliest examples are wooden construction
- Early advances came out of Persia and China, from roughly the 9th to 16th century
- Craftsmanship improved dramatically, but few technical changes in 16th - 17th century
- Industrialization in the 19th century ushered in many changes; tooling and mass-production of complex locks for houses, vaults
- Future: electronic/mechanical "smart keys"

Vulnerability Disclosure

Physical security differs from computer security in some important ways that impact the ethics of vulnerability disclosure.

Upgrades are hard:

- Manufacturers: retooling production lines
- Consumers: locks are expensive to replace

Consequence of exploits can be huge:

- Property
- Lives

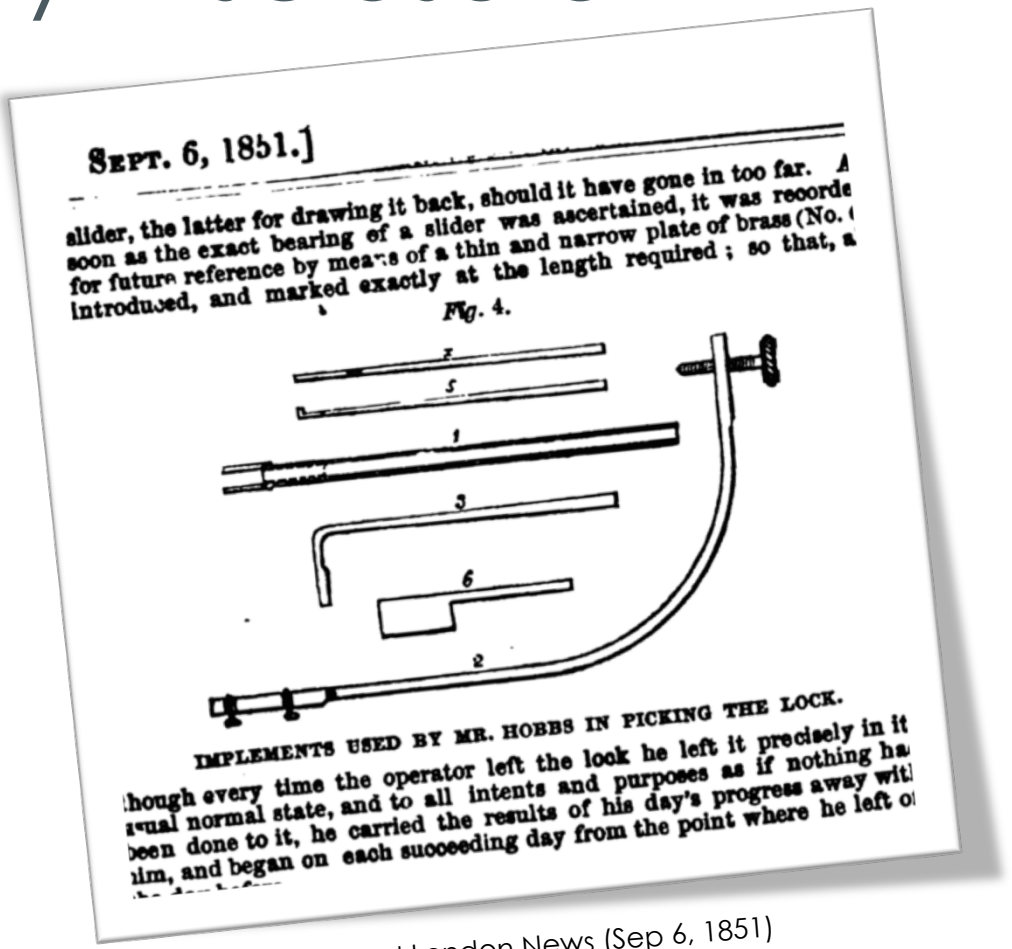
Vulnerability Disclosure

This has often led to a culture of secrecy:

- Historically, manufacturers and locksmiths have protected their secrets
- As a consequence, many of the lessons of past design failures are not well known
  - Many new lock companies start business every year: many are making mistakes that were fixed in designs over 100 years ago
- Very hard to educate consumers about risks if the technology isn't understood

Vulnerability Disclosure

Interesting exception was England, from roughly 1850-1880, when public interest in locks and security flourished



SEPT. 6, 1851.]

slider, the latter for drawing it back, should it have gone in too far. A
soon as the exact bearing of a slider was ascertained, it was recorde
for future reference by means of a thin and narrow plate of brass (No.
introduced, and marked exactly at the length required; so that, a

Fig. 4.

IMPLEMENTS USED BY MR. HOBBS IN PICKING THE LOCK.

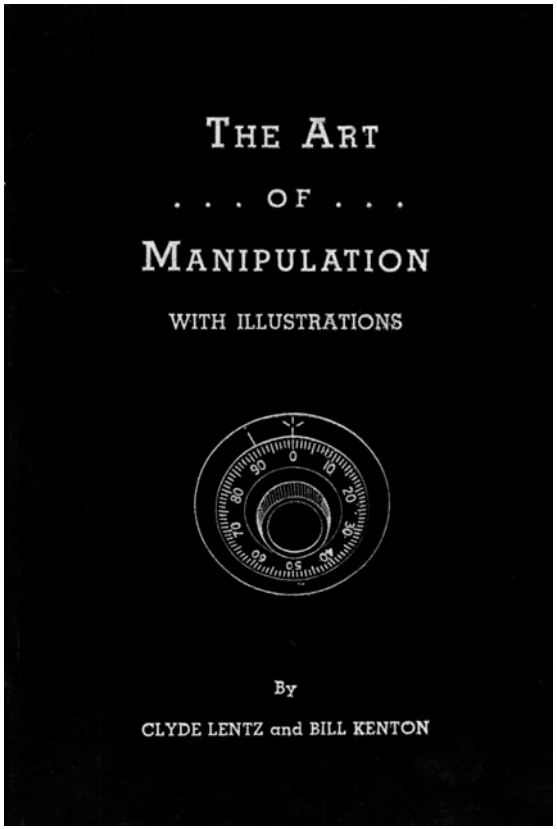
though every time the operator left the lock he left it precisely in it
ual normal state, and to all intents and purposes as if nothing ha
been done to it, he carried the results of his day's progress away wit
him, and began on each succeeding day from the point where he left o

Source: The Illustrated London News (Sep 6, 1851)

Vulnerability Disclosure

Quick return to secrecy, from the early 1900's to present:

> *"It is extremely important that the information contained in this book be faithfully guarded so as not to fall into the hands of undesirables.*
>
> *We also suggest after you have become proficient […] to destroy this book completely, so as to protect yourself and our craft."*



Source: *The Art of Manipulation*, Lentz and Kenton (1955)

Lessons from the Physical Security

Physical Security Lessons

- Establishing Key / Password Strength
- Design vs. Implementation
- Input Validation
- Replay Attacks
- Privilege Escalation
- Side-channel Attacks

Key / Password Strength

As technology advances, attackers have much easier access to powerful tools

- Need for increased key complexity, systems using multi-factor auth for increased entropy

Protection Until	Bits Required
2010	1024-bit key
2011 – 2030	2048-bit key
> 2030	3072-bit key
>> 2030	7680-bit key
>>> 2030	15360-bit key

2011 NIST recommendations: minimum key length required for asymmetric encryption

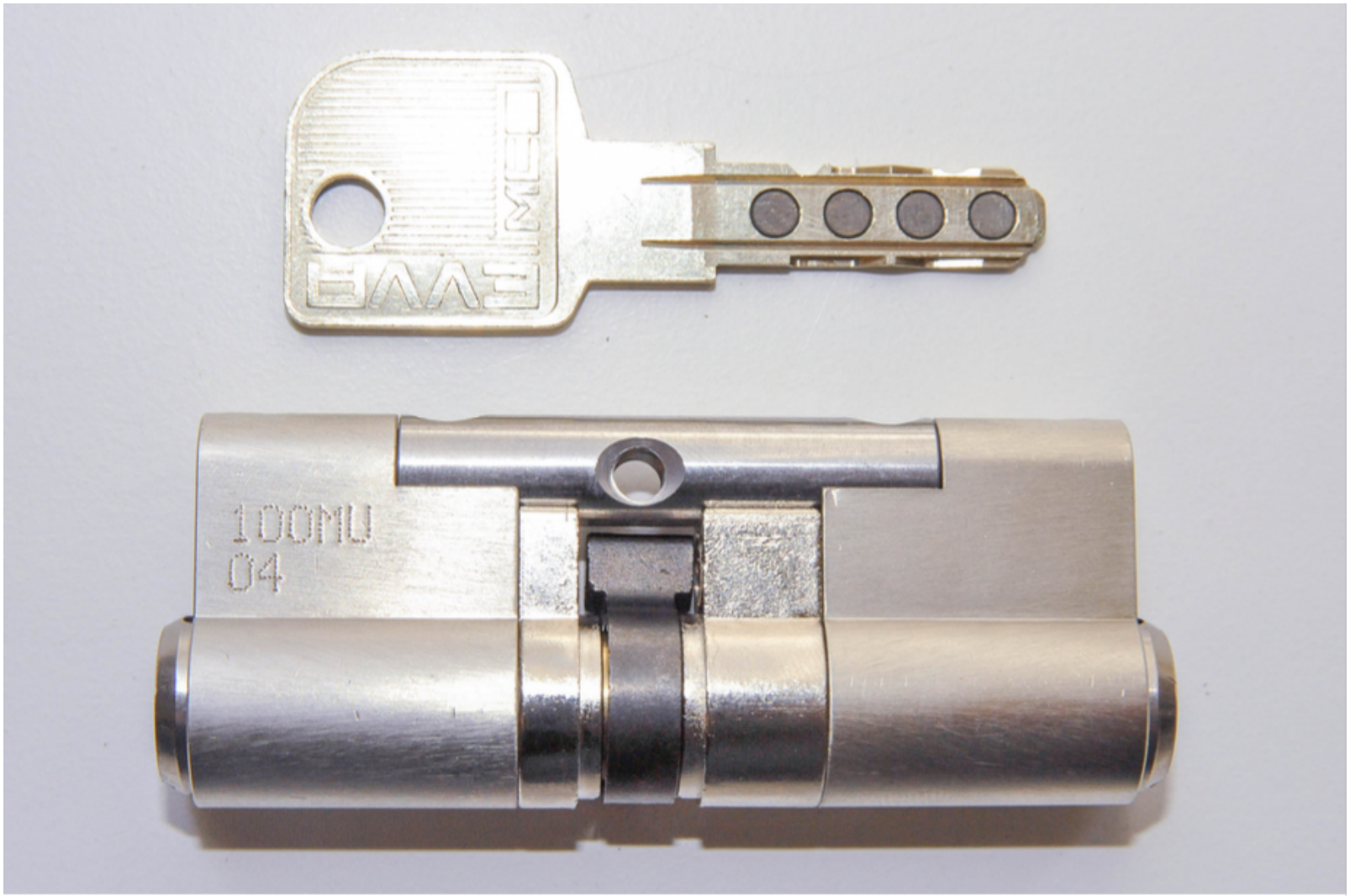
Key Complexity

Physical keys have followed a similar complexity growth, as attackers gained access to increasingly-sophisticated lock-picking equipment

6-Lever Push-Key Padlock cut-away

DOM D Euro-Profile Cylinder

DOM Diamant Euro-Profile Cylinders



EVVA MCS Euro-Profile Cylinder

Multi-Factor Authentication

High-security systems now typically use locks that test multiple different factors: something you have, something you are, something you can do, something you know

Design vs. Implementation

The Pen Is Mightier Than the Lock

A Ballpoint Trick Infuriates Bicyclists

By LYDIA POLGREEN

The cunning bicycle thieves of New York City always seem to be one step ahead of lockmakers. Design a more sophisticated lock and the thieves make a better pick. Make a sturdier chain and they get bigger bolt cutters. And if all else fails, they just dig up the parking meter or stop sign to unshackle the bike from it. But to open some of the toughest locks on the market, a thief needs only to flick his Bic pen.

Many cyclists erupted in disbelief and anger this week after videos were posted on the Internet showing how a few seconds of work could pick many of the most expensive and common U-shaped locks, including several models made by Kryptonite, the most recognized brand.

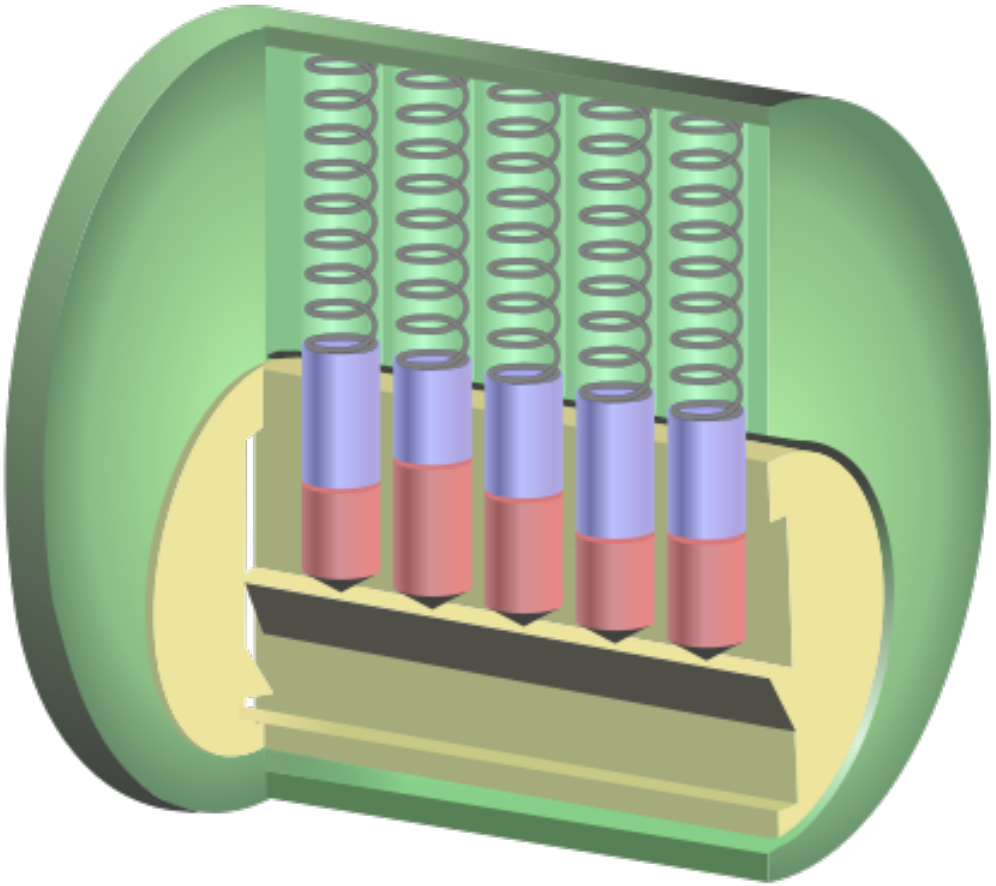
Mashing the empty barrel of a ballpoint pen into the cylindrical keyhole and turning it clockwise does the trick that has struck fear into the hearts of bicycle owners, especially those in New York, where thousands of bikes are stolen each year.

"There was murmuring on various Web sites, and so I decided to go home and pick up a pen and see if it works," said Benjamin Running, a graphic designer who lives in downtown Brooklyn. "Sure enough, within 30 seconds I had broken into my $90

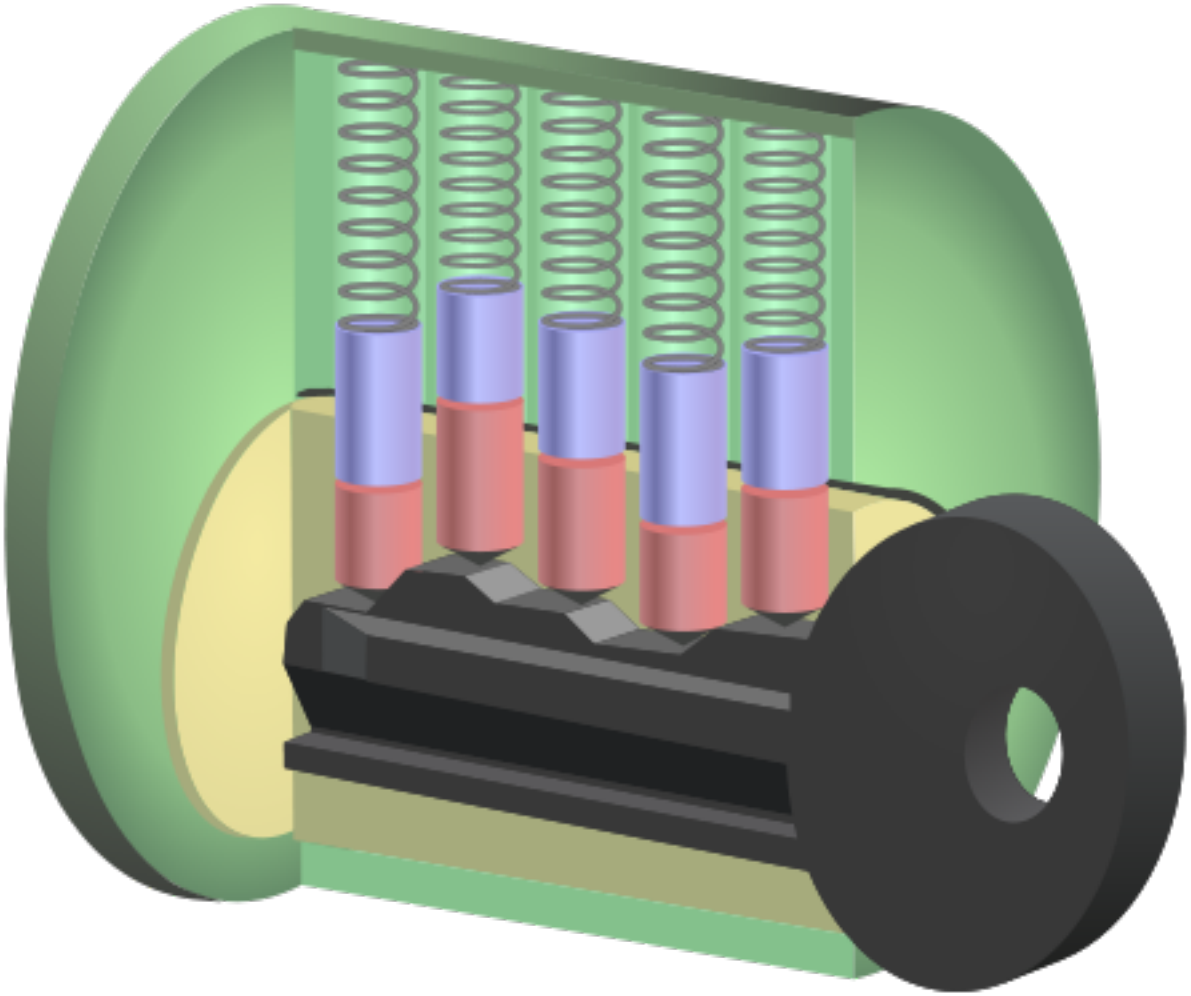
Source: New York Times (Sep 14, 2004)

Majority of security vulnerabilities come from implementation decisions, rather than design decisions

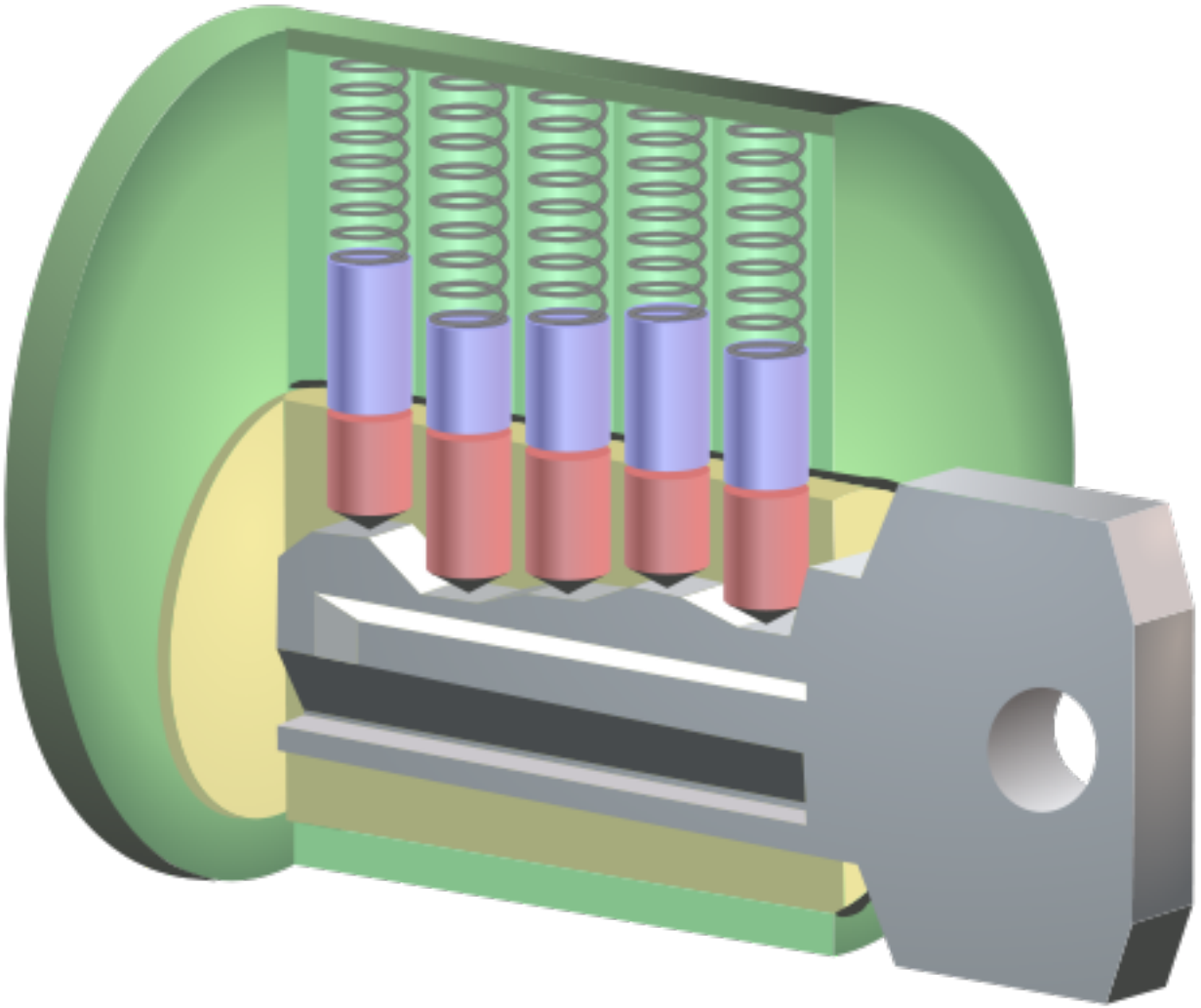
- True for computer and physical security systems alike



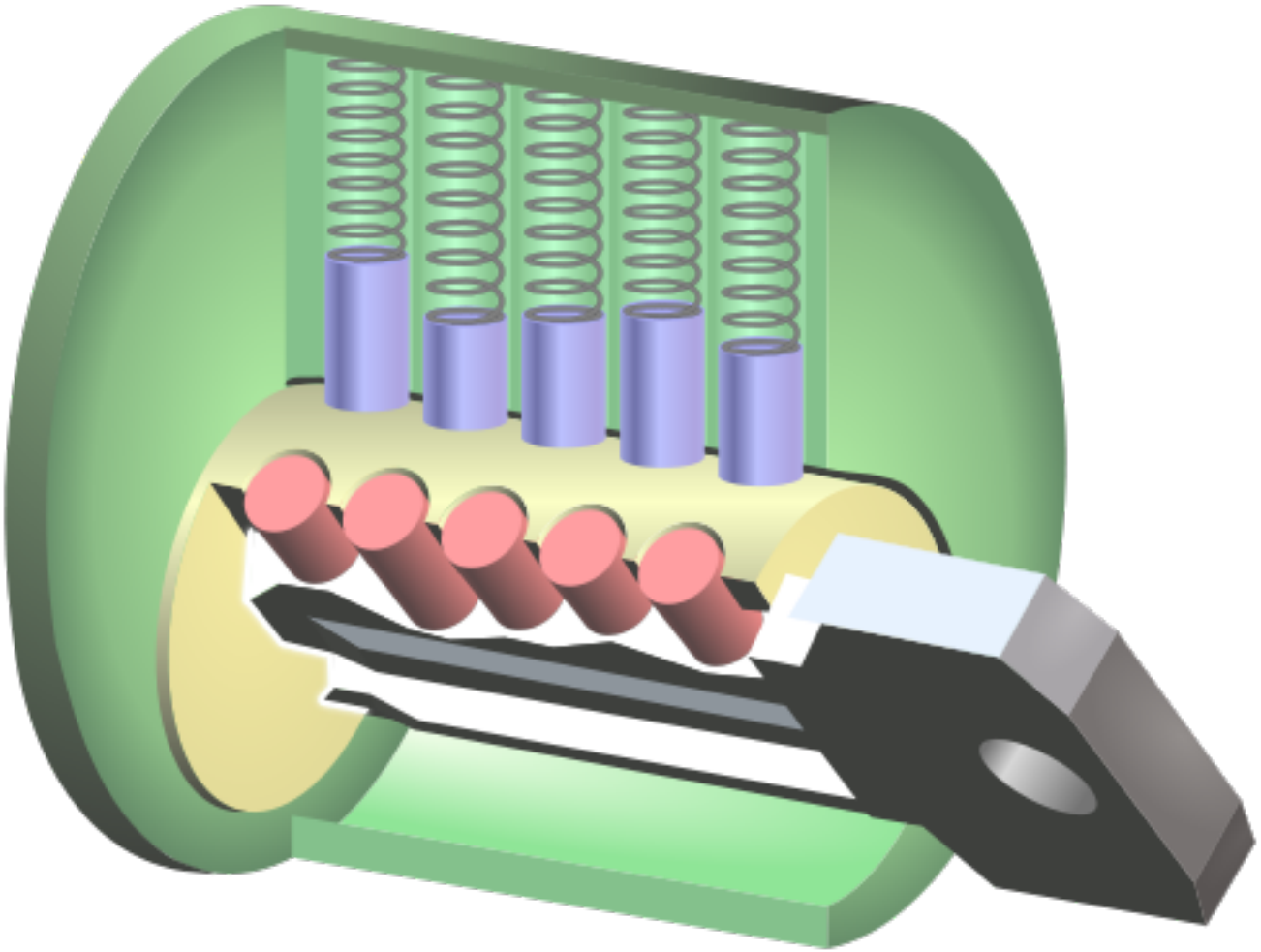
Source: WikiMedia Commons



Source: WikiMedia Commons



Source: WikiMedia Commons

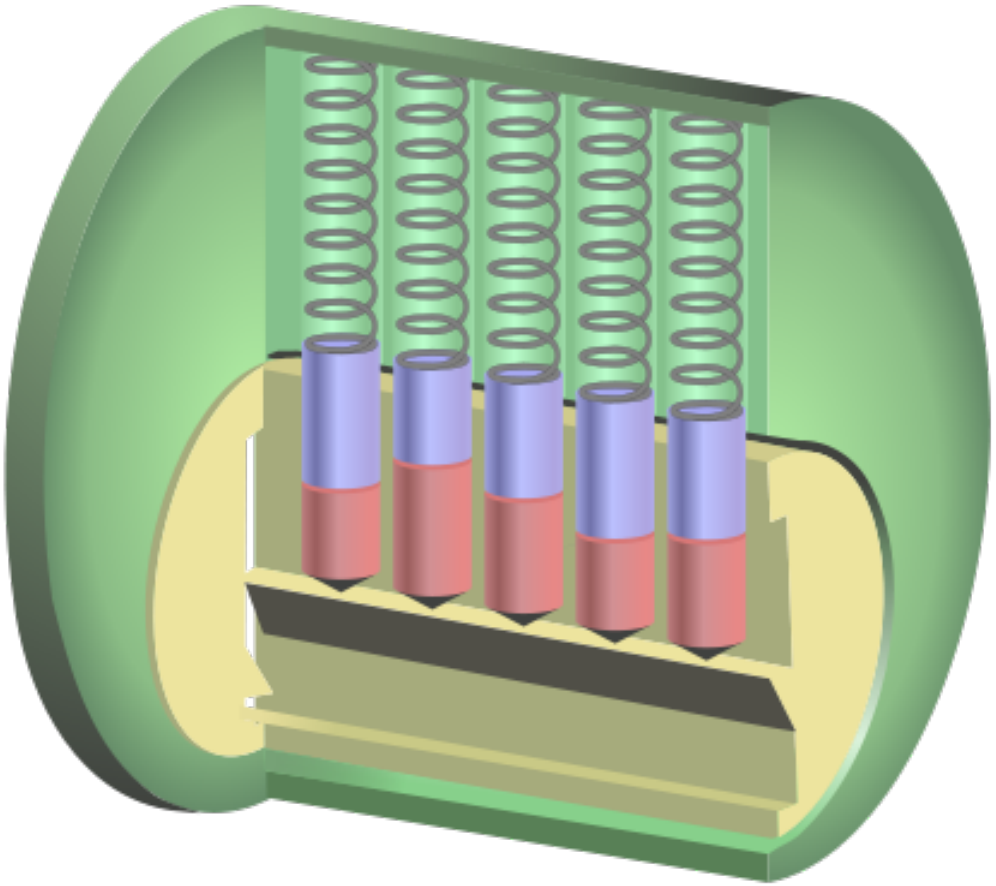


Source: WikiMedia Commons

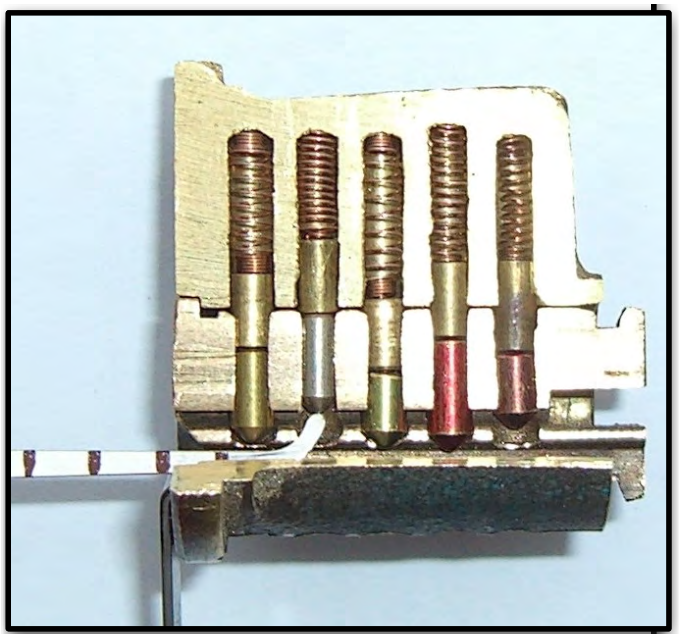
Manufacturing Tolerances

Most lock designs are secure *in theory*, but it is not cost-effective to manufacture every part to perfect tolerances

- Differences in **implementation** (*i.e.*, tiny differences in part dimensions) lead to a product that is not as secure as its **design**
- Important lesson for software designers



Source: WikiMedia Commons



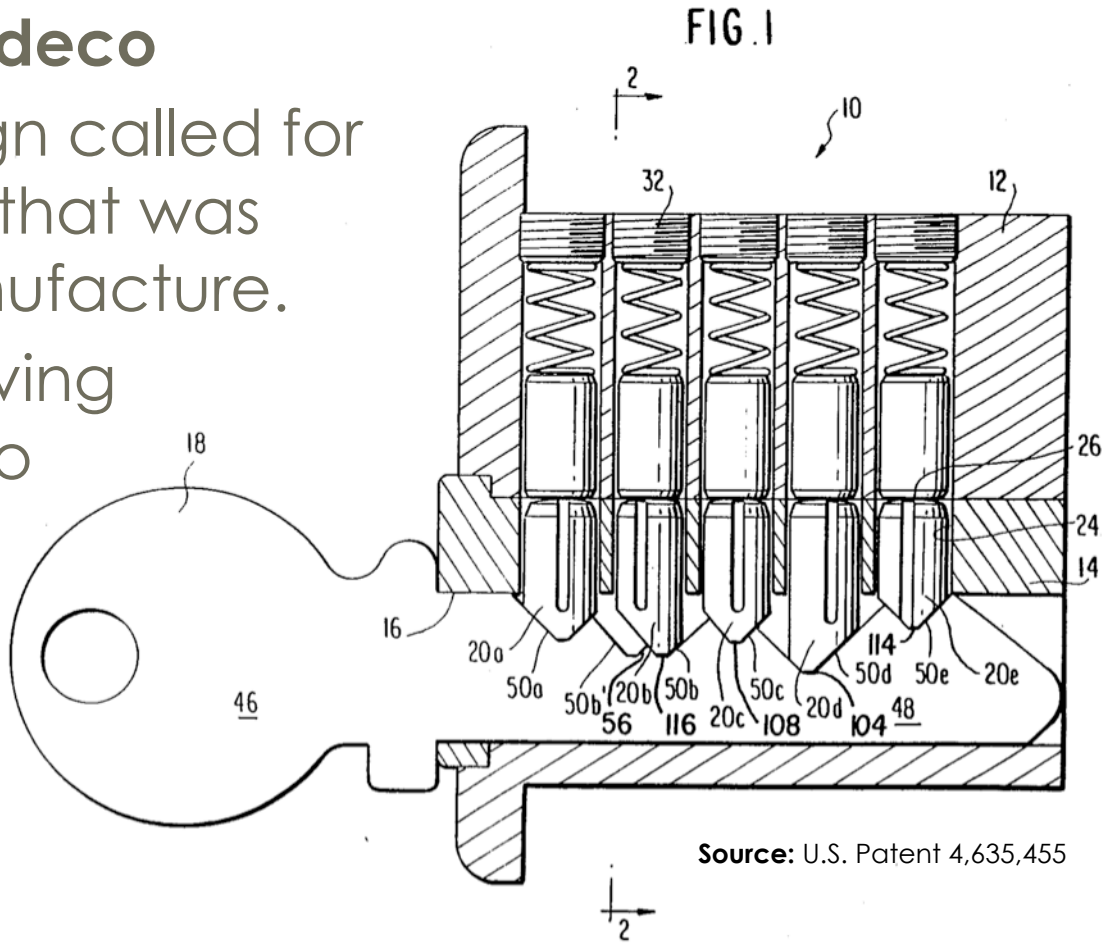
Source: LSI Guide to Lockpicking

Design vs. Implementation

Example: Medeco

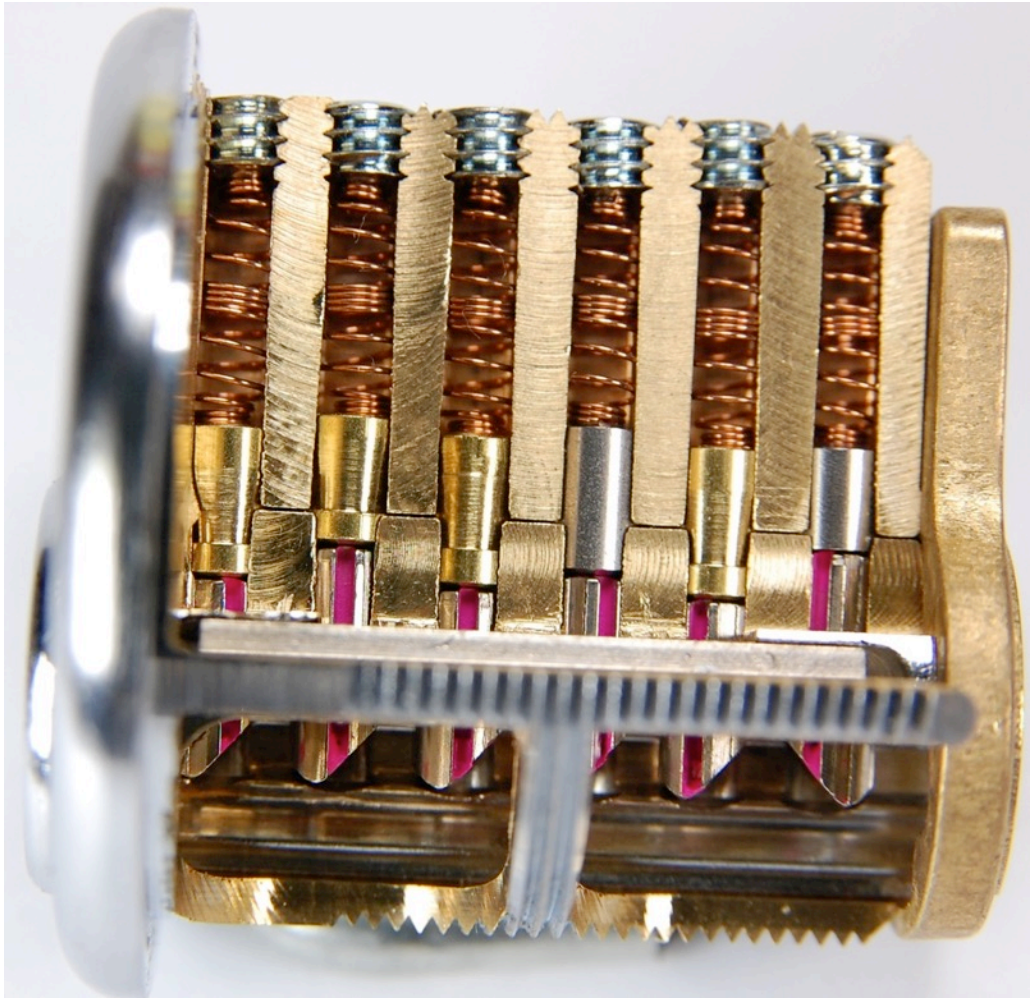
Original design called for a style of pin that was costly to manufacture.

Small cost-saving change led to a major production vulnerability

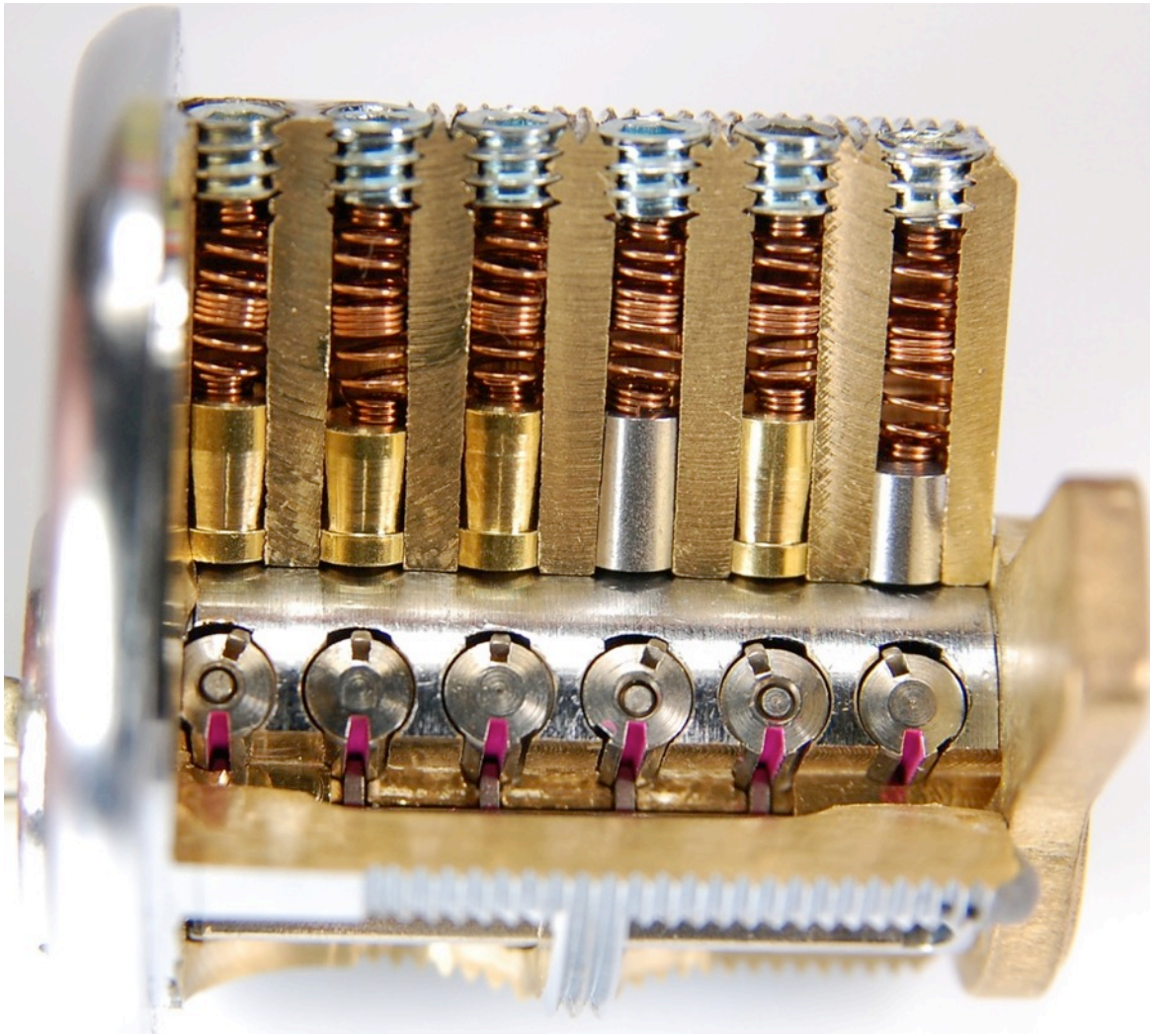


Source: U.S. Patent 4,635,455

Source: LockWiki



Source: MitchCapper



Source: MitchCapper

Design vs. Implementation

Example: Medeco

The decision was made to use a design that is cheaper to manufacture and, as a result, the security of the design was compromised

- Jon King: Medecoder

Source: NDE Magazine

Design vs. Implementation

Example: Medeco

Corrected the design problem: now selling the non-vulnerable version as an added-cost upgrade to military and high-value clients

- ARX (Attack Resistance eXtended) pins

Source: LockWiki

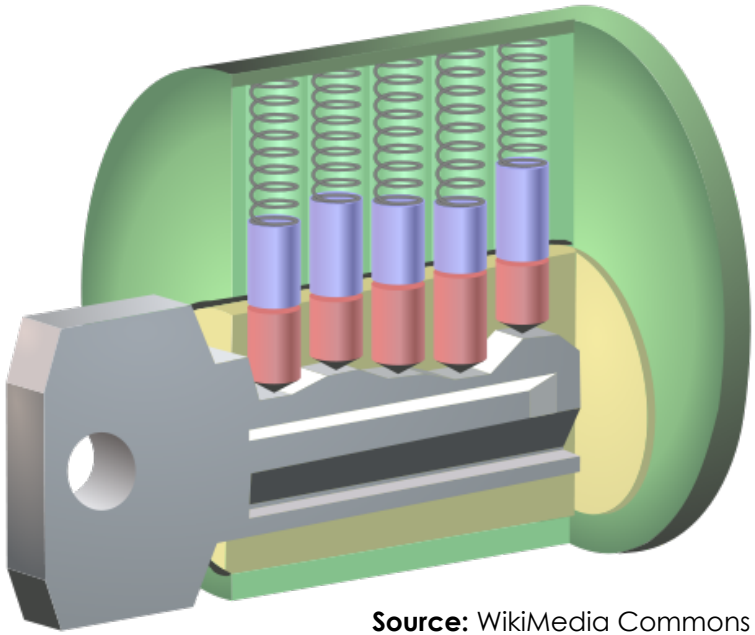
Design vs. Implementation

Implementation trade-offs that lead to vulnerabilities are a substantial, costly risk in the physical security world:

- Unlike software, you cannot push a component upgrade out to clients when an implementation defect is found
- Same costs (money and logistics) can apply to patching hardware and many embedded systems

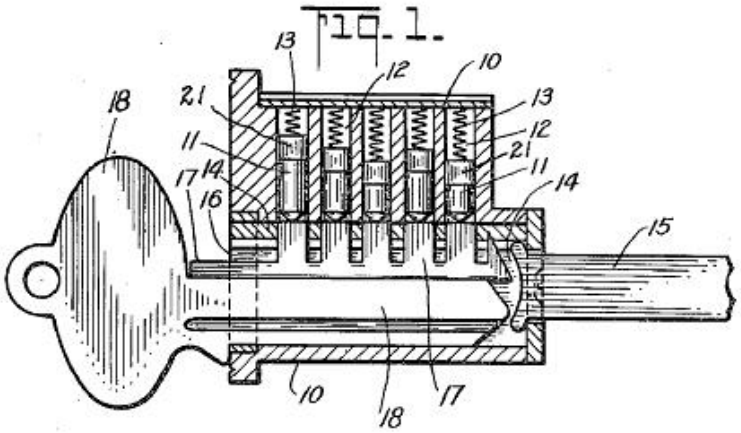
Validating User Input

What could go wrong when the user provides an input that we're not expecting?



Source: WikiMedia Commons

Overlifting Attack



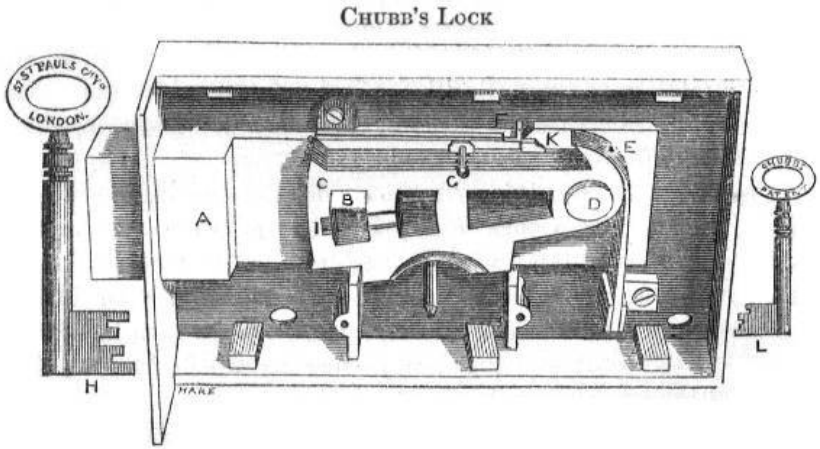
Source: U.S. Patent 2,064,818 (1934)

Source: LockWiki

Overlifting Attack

In 1818, British lock manufacturer Chubb designed a mechanism to detect if an attacker has overlifted a lever; jams the lock in a locked state

- Interesting parallel to buffer overflow and stack canaries



Overlifting Attack

Variants of similar keyway attacks have been popular over the years:

- Gunpowder (late 1800's)
- Bump Keys (present)

Replay Attacks

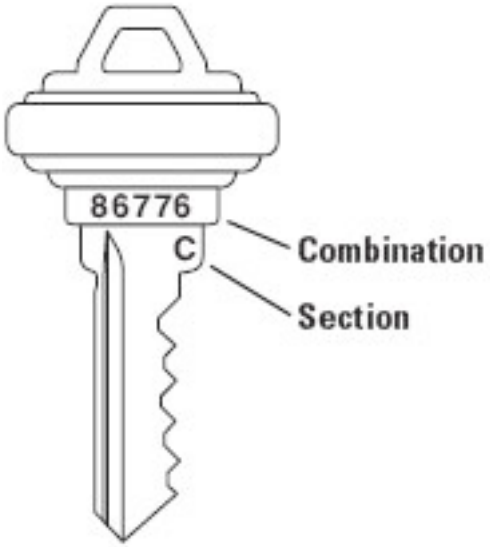
Physical keys are tokens that:

- Are unencrypted
- Have long validity periods (many years)
- Are protected by weak distribution channels (your pockets)

If someone can intercept and duplicate your key, this is effectively a replay attack

Key Blanks

Problem: key blanks are readily available, and manufacturers often stamp a **key code** (representing the cuts on your key) directly onto the key



Key Blanks

Traditional solution: patent the key blanks

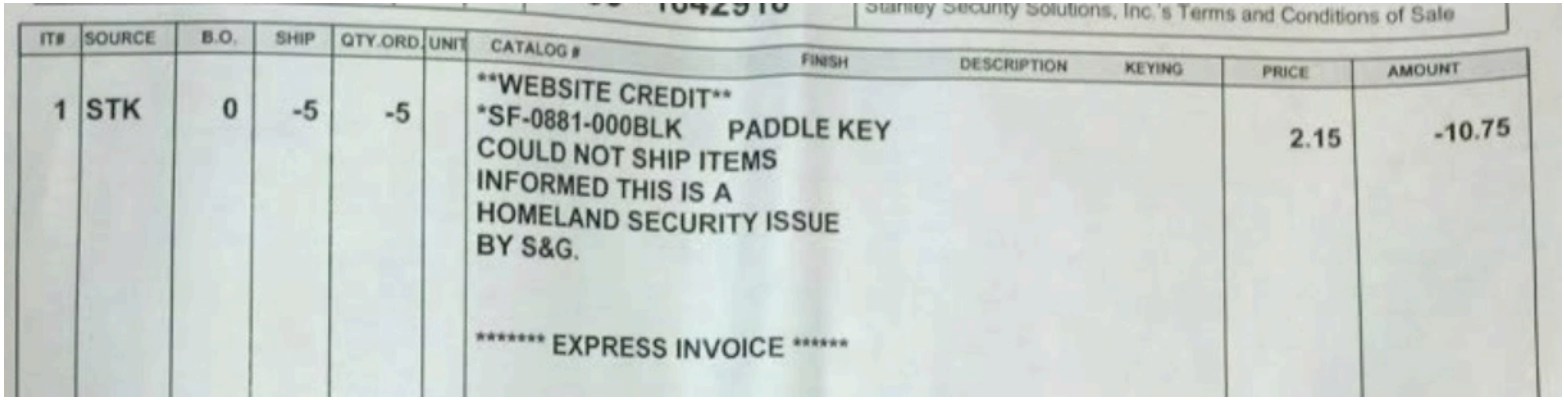
- Patent provides a window of between 14 and 20 years during which only the manufacturer can legally sell blanks
- Felony in the U.S. to duplicate Postal Service keys (up to 10 years in jail)

Equivalent of "secret encryption algorithm"

- Kerckhoff's Principle applied: the security of your system must not depend on the scarcity of your key blanks

Key Blanks

Most of US railway infrastructure is protected by 15 keys: copying is a **huge** vulnerability

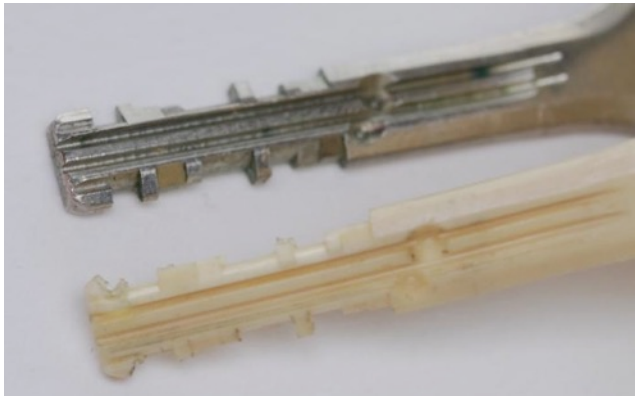


Stanley Security Solutions, Inc.'s Terms and Conditions of Sale

IT#	SOURCE	B.O.	SHIP	QTY.ORD.	UNIT	CATALOG #	FINISH	DESCRIPTION	KEYING	PRICE	AMOUNT
1	STK	0	-5	-5		**WEBSITE CREDIT** *SF-0881-000BLK COULD NOT SHIP ITEMS INFORMED THIS IS A HOMELAND SECURITY ISSUE BY S&G.		PADDLE KEY		2.15	-10.75

******* EXPRESS INVOICE ******

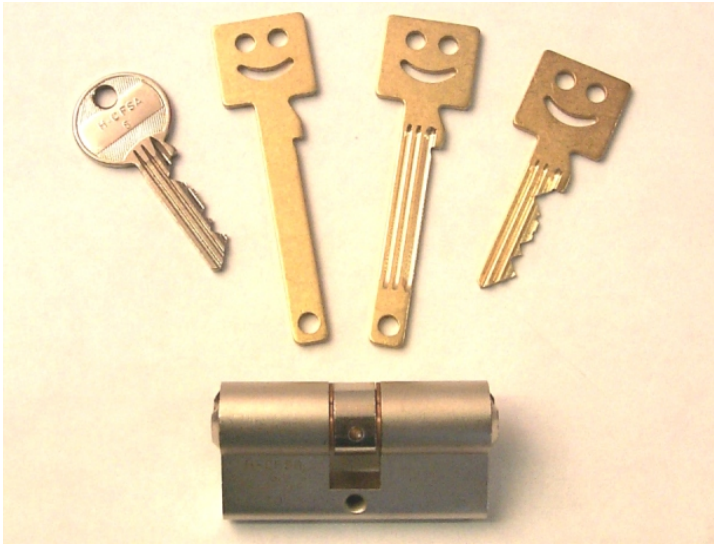
Epoxy-Based Key Casting



Source: LockWiki

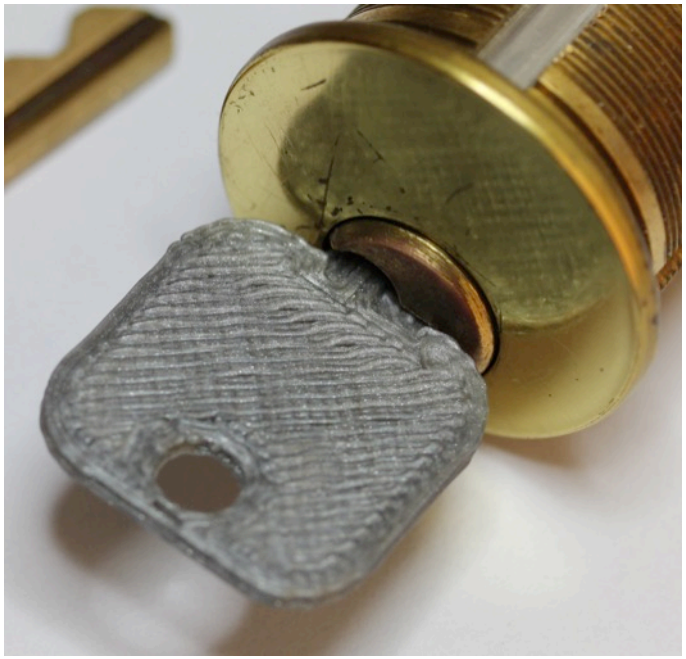
Key Blanks

Most common blanks can now be duplicated on a commercially-available milling machine (Easy Entrie)



Key Blanks

Hobbiest 3-D printers can now print with sufficient resolution to enable direct printing of polymer keys



Source: Nirav Patel

Key Blanks

Interesting engineering problem: how do you detect a non-original key?

- One recent trend is to introduce moveable elements into the key blank: parts of the key need to be able to move in certain ways
  - Hard to make unauthorized blanks
  - Similar to nonces (*e.g.*, Needham-Schroeder)
- New key designs are incorporating features that make them very hard to scan
  - Undercuts, folded blanks
  - Complex key cuts

Austral 904 TF-N "Chain Key" Padlock

Side-Channel Attacks

Example: Safe Locks

A problem was quickly noticed when ships started using safes with early combination locks to protect their valuables: the motion of the ships would often cause the safes to unlock themselves

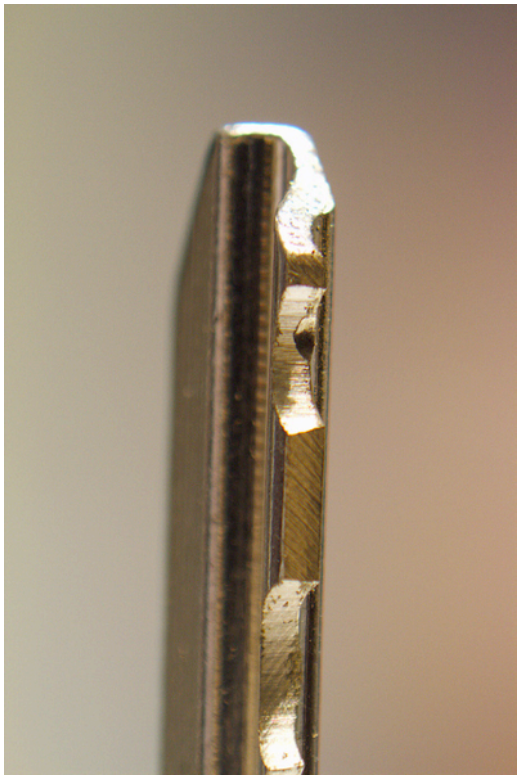
- Balanced wheels

Side-Channel Attacks

Example: Impressioning

By manipulating a properly prepared key blank in the lock, it's possible to read subtle marks that show the difference between correct and incorrect key cuts

- Filing away where the key is marked will eventually lead to a working key

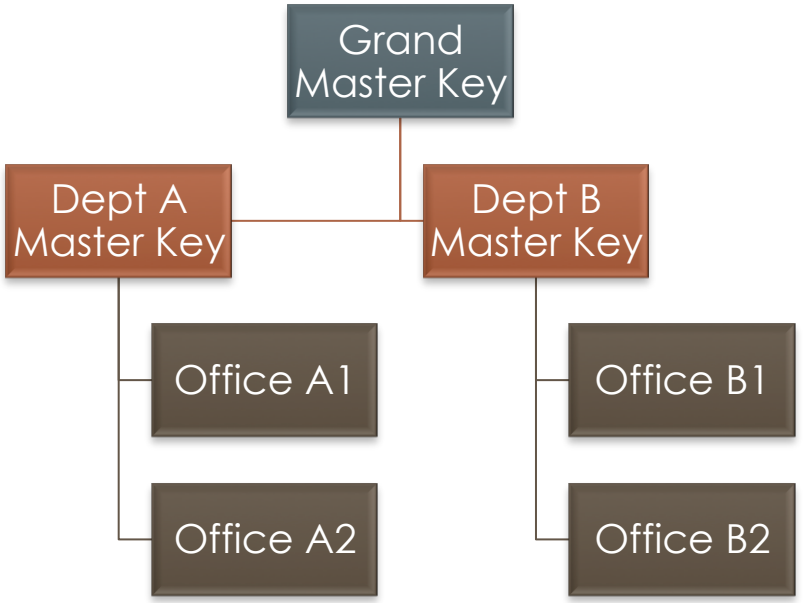


Source: dvanzuijlekom

Privilege Escalation

Most businesses have a **master key** system: provides for single keys that operate different groups of locks

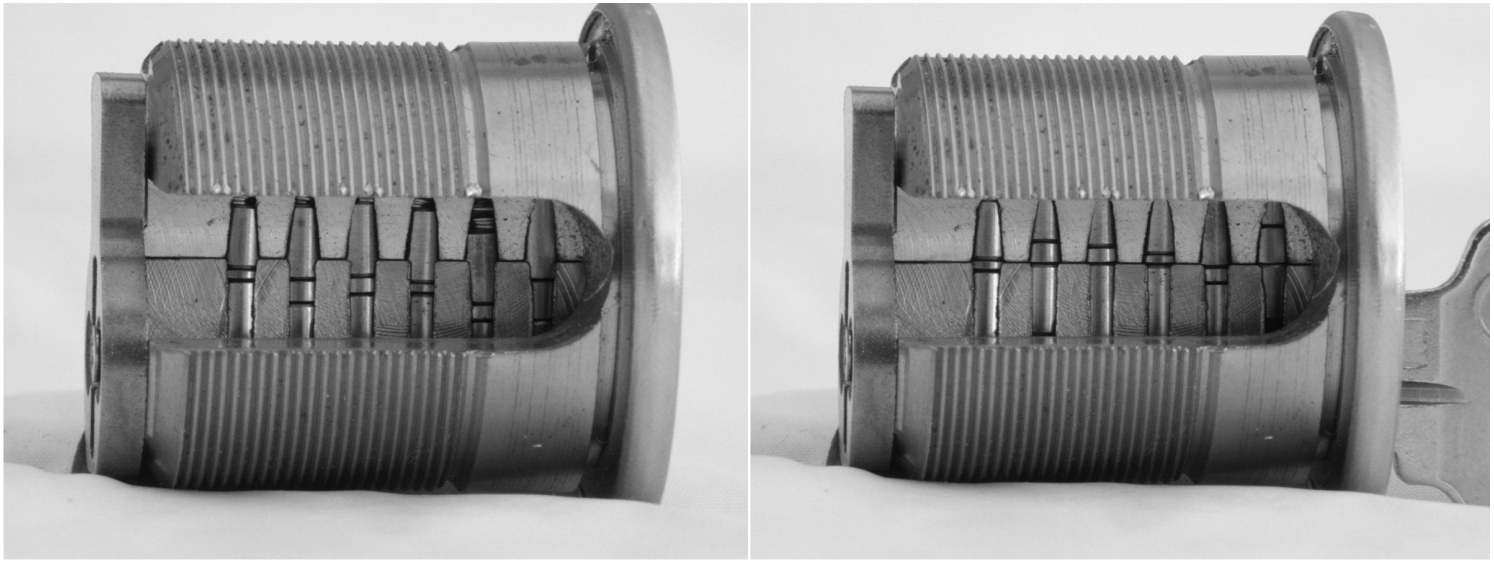
- A vulnerability in many systems makes it easy for someone with a lower-privilege key to create a higher-privilege key
- Rights Amplification in Master-Keyed Mechanical Locks (Blaze, 2002)



Master-keyed cylinders have secondary pins inserted; these create additional "breaks" in each pin stack

Problem: the pin stacks in most locks operate independently

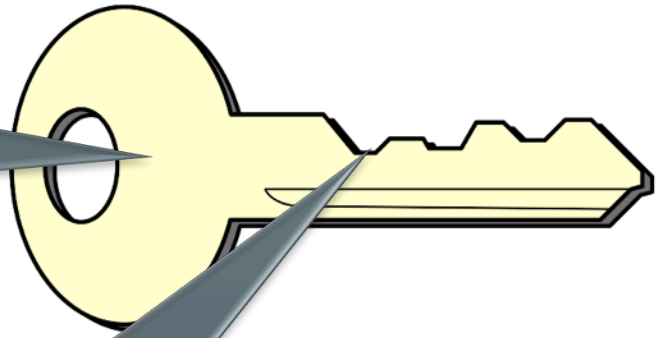
- The lock can be opened by the master key (M), the individual "change key" (C)… **or any combination of cuts from M and C**
- A lock with six master-key pins can be opened with $2^6 = 64$ different keys



Source: Matt Blaze

Privilege Escalation

Start with a low-level "change" key, and duplicate all but the first cut onto a fresh blank



Start filing down just the first position, identifying the cuts that will open the lock: from this you can determine the first cut in the master key

Repeat for the other positions

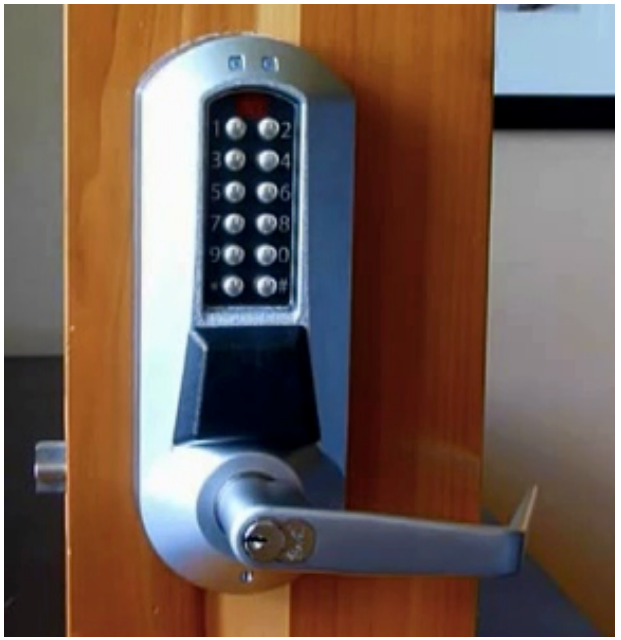
Thinking about System Design

System Design

Failure: Kaba E-Plex

High-end electronic lock; audit features record entry of staff

- Critical circuit traces pass directly under one of the status LEDs
- Shorting the traces opens the lock without any audit record



Source: InSecurity.org

System Design

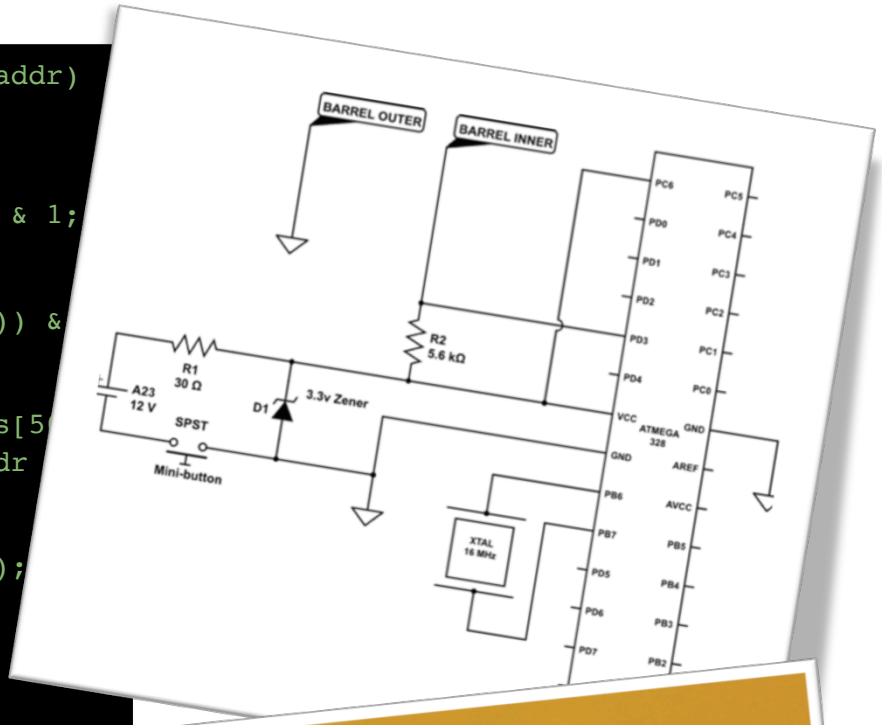
Failure: Onity HT

High-end electronic lock used in hotels; audit log records entry of staff/guests

- Interface on the bottom supports commands that allow reading the lock's memory (including passcodes) and opening the lock by providing a valid passcode

```
int readData(unsigned long int addr)
{

for(int i = 0; i < 8; ++i)
dbits[50 + 9 + i] = (addr >> i) & 1;

for(int i = 0; i < 8; ++i)
dbits[50 + i] = (addr >> (i + 8)) &
1;

for(int i = 0; i < 8; ++i) dbits[5
9 + 9 + i] = ((addr >> i) ^ (addr
(i + 8)) ^ (0x1D >> i)) & 1;

for(int i = 0; i < sizeof(dbits);
+i) {

   if(dbits[i] == 0) {
      pullLow();
      delayMicroseconds(16);
      pullHigh();
      delayMicros
   } else {
      pullLow();
      delayMicrose
      pullHigh();
      delayMicrose
      pullLow();
```

Source: Cody Brocious



Source: Matthew Jakubowski

Layered Security

Example: Drumm Geminy

Idea of a front-tier **firewall** applied to locking; designed for vandal-prone installations

- Moderate security lock
- Covers high-security lock
- Resistant to crazy glue, grinders, hacksaws, etc.

Thomas Slaight Paper Seal Padlock (19th-century, US Internal Revenue Service)

Paper Seals for Thomas Slaight Seal Padlock (US Internal Revenue Service)

Layered Security

Example: Safe Relockers

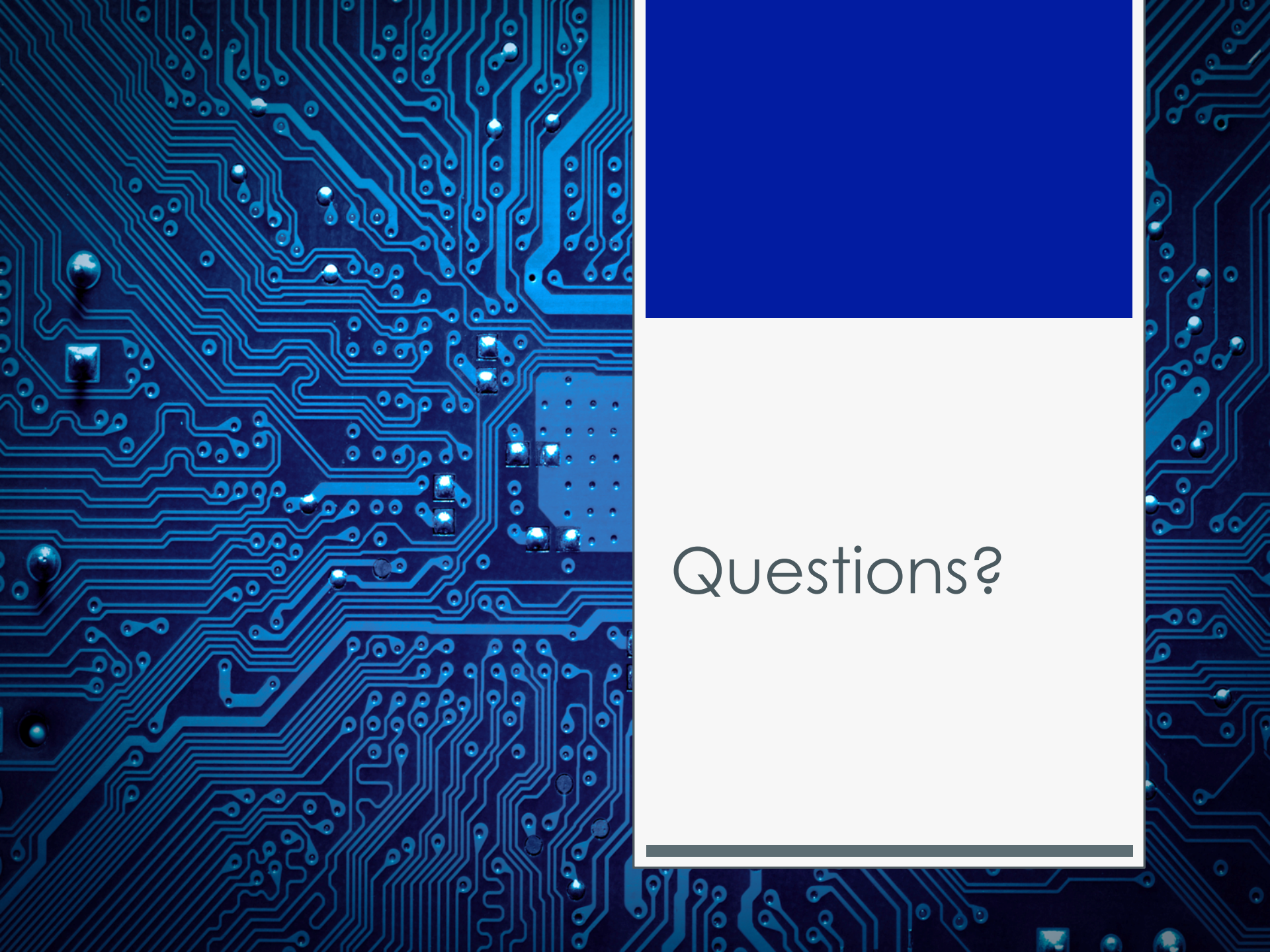
High-end safes have a web of "sensors" that detect attacks:

- Impact, cutting, high temperature, etc.
- Triggering any sensor releases a cable, firing a series of "relockers" that prevent the safe from opening

Layered Security

Future trend is towards "smart keys" to perform a cryptographic handshake, combined with a mechanical lock to resist physical attacks

- Ability to expire lost / stolen keys
- Easy to retrofit into existing systems
- Much harder to dissect and audit the electronic portion: unlikely manufacturers will open-source their code


Questions?