Cryptology and Physical Security

Matt “Fingers” Blaze
AT&T Labs – Research
mab@research.att.com

What this talk will be about

- Why we as computer security / cryptology researchers should think about locks
- How mechanical locks work
- How to bypass locks
- A “new” attack against master key systems
- Lessons learned

Physical Security

- Mechanical locks are used to protect the physical world from attackers
  - Ubiquitous: residential, commercial, industrial, schools, government, etc.
- To control access to locking mechanism:
  - Combination locks aim to require demonstration of a secret procedure
  - Keyed locks aim to require possession of a secret physical token, a “key”

What can locksmiths teach us about computer security?

- Our language
  - "keys," "intruders," "breaking" systems, etc.
- More importantly, much of our philosophy
  - depending on keys as the only secret
  - the folly of security by obscurity
- Perhaps we can also learn something by studying the systems from which we took this language and philosophy

What can we teach locksmiths?

- Much of physical security design and practice is informal, based on folklore
- They've lately embraced security by obscurity!
  - probably more for the security of the trade than for that of the users…
- Many of the analysis techniques of computer security and cryptology can be applied to locks
- How secure are locks?
  - Can they be made more secure?

C. Tomlinson, 1853

- A commercial, and in some respects a social doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery.

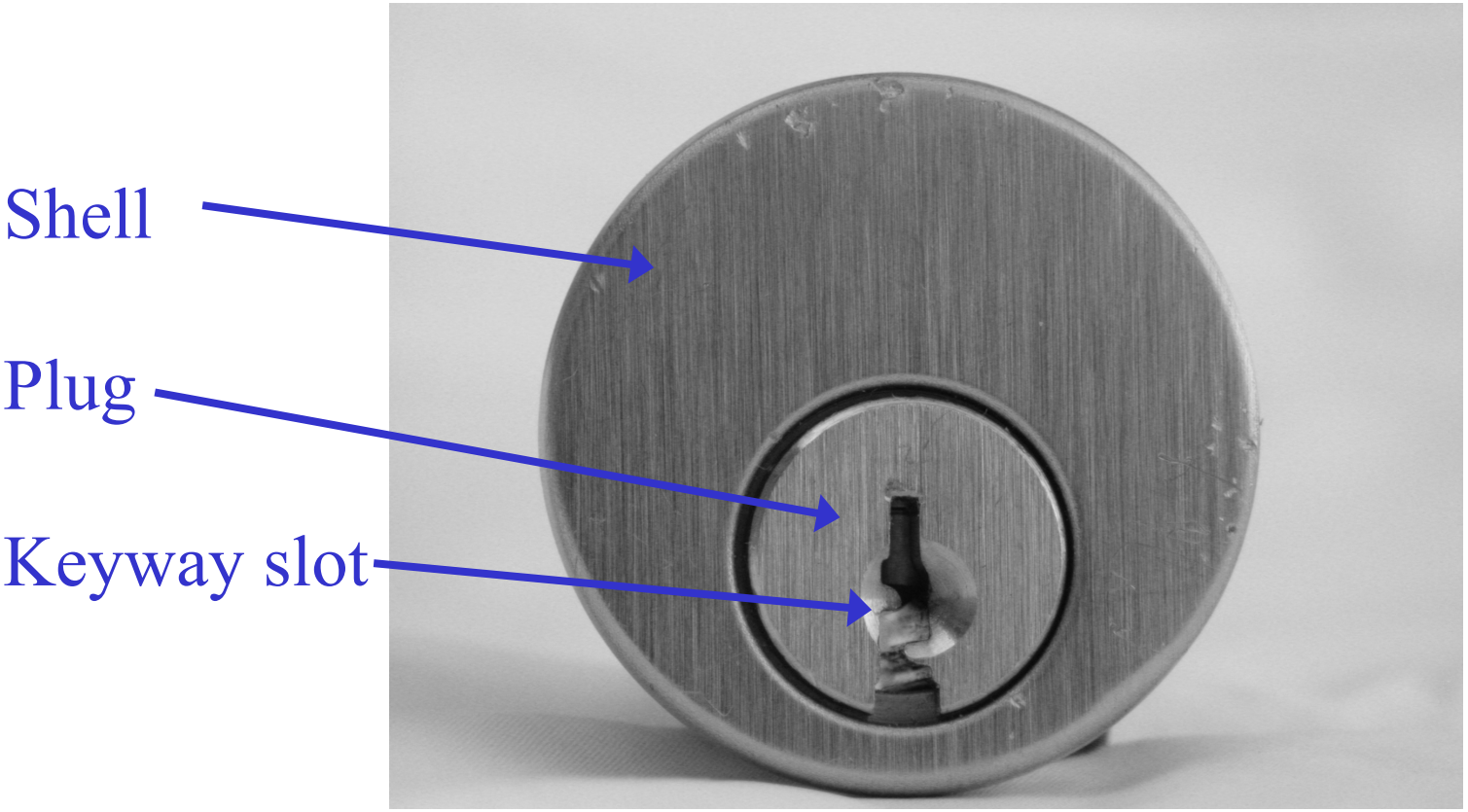
- Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done. If a lock, let it have been made in whatever country, or by whatever maker, is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance.

- It cannot be too earnestly urged that an acquaintance with real facts will, in the end, be better for all parties. Some time ago, when the reading public was alarmed at being told how London milk is adulterated, timid persons deprecated the exposure, on the plea that it would give instructions in the art of adulterating milk; a vain fear, milkmen knew all about it before, whether they practiced it or not; and the exposure only taught purchasers the necessity of a little scrutiny and caution, leaving them to obey this necessity or not, as they pleased.

The Pin Tumbler Lock

- Ubiquitous in most parts of the world
  - at least one protects your home and office
- A *shell*, mounted on the door (or whatever)
- A *plug*, which can rotate freely within the shell and which is linked to the locking mechanism
- A *keyway* slot, cut into the front of the plug

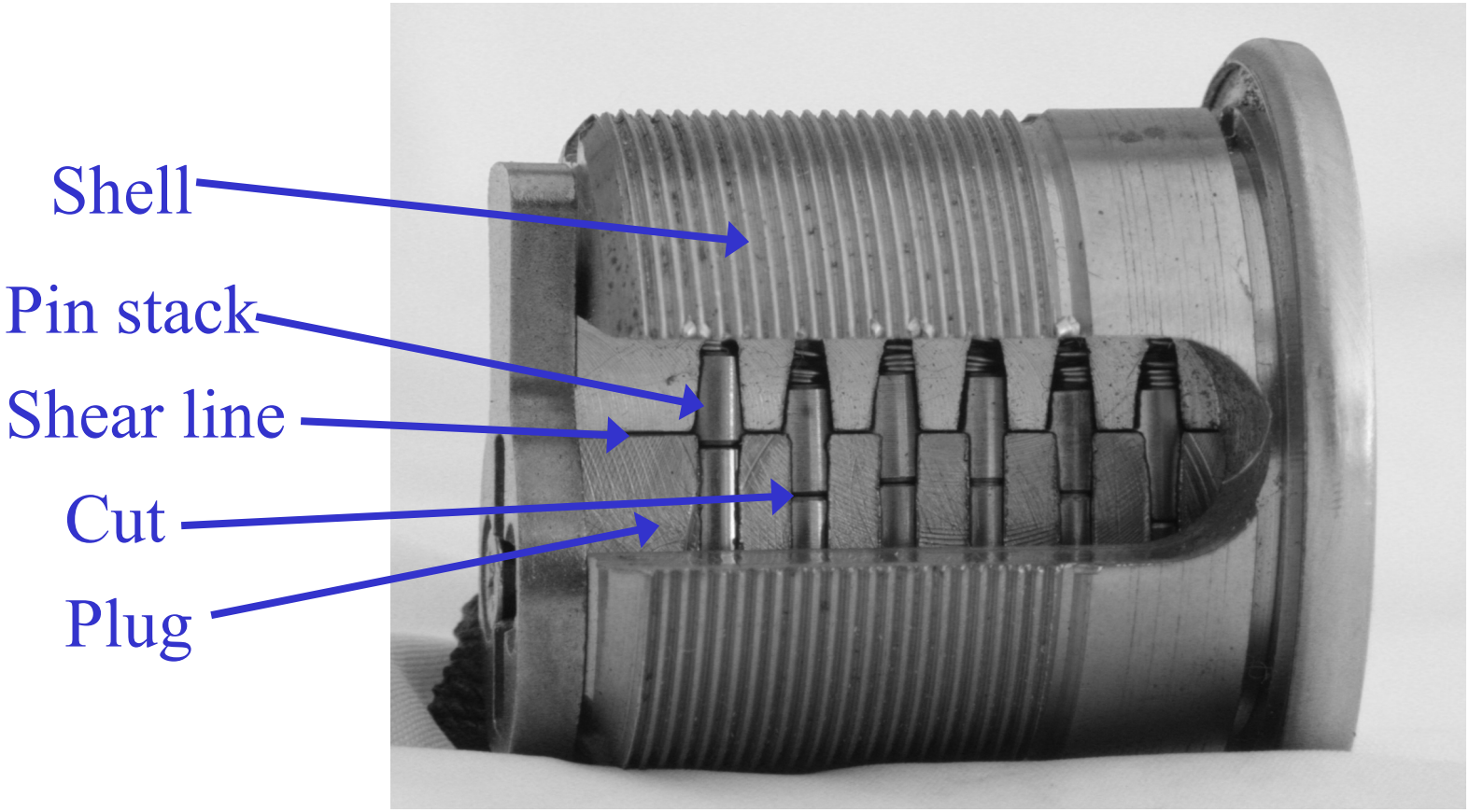
Pin tumbler lock



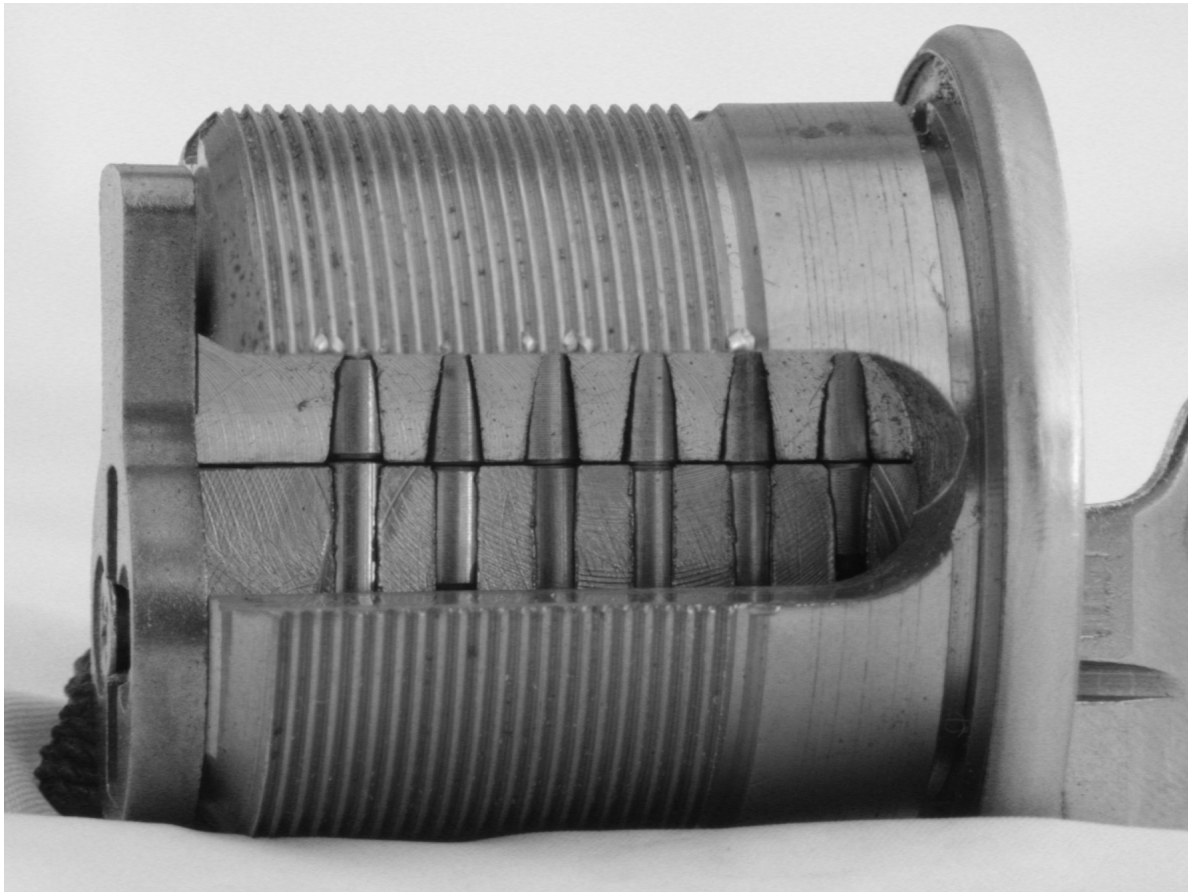
Inside a pin tumbler lock

- The *shear line* is the plug/shell boundary
- A set of *pin stacks* protrude from holes in the shell into holes in the plug
  - prevents the plug from rotating
  - typically held down by springs
- Each pin stack has a *cut*
  - height corresponds to the correct key
  - with no key in lock, all cuts sit within the plug
  - when all cuts line up at the shear line, plug can rotate

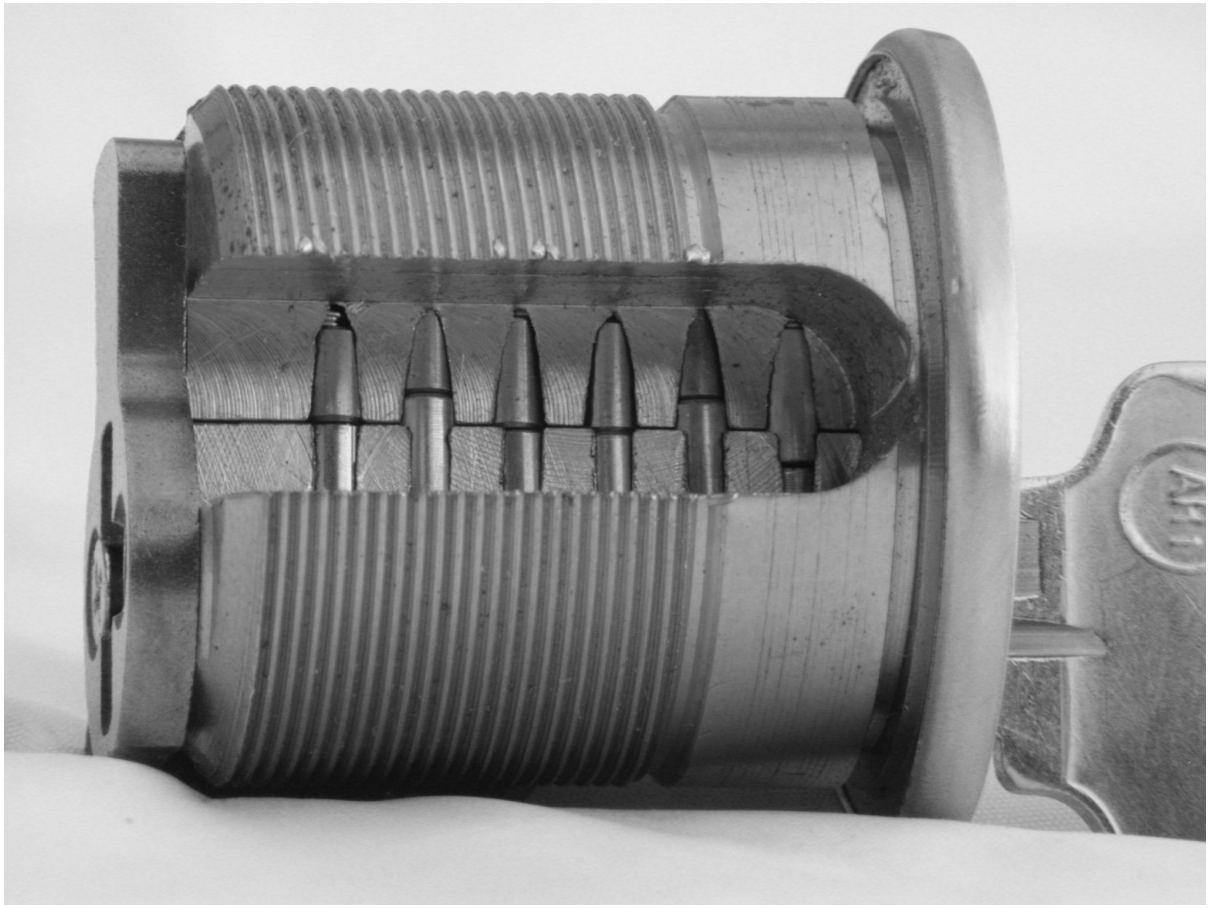
Inside a pin tumbler lock



Correct Key
(all cuts at shear line)



Incorrect Key
(some cuts not at shear line)



Threats against locks

- Exhaustive search of keyspace
- Brute force
- Manipulation (picking)
- Decoding
- Bypass

How secure are locks…
…against exhaustive search?

- Two parameters
  - *P*, the number of pin stacks
    - typically between 4 and 7
  - *H*, the number of different heights used for cuts
    - typically between 4 and 10
- Number of keys is therefore at most H^P
  - Sometimes can't have a high cut right next to low cut
    - "Maximum Adjacent Cut Specification" (MACS)
  - Typical lock has between 240 and 10^7 distinct keys

Only 240 to 10^7 different keys??! You've got to be kidding!

- Yes, this is tiny by computer standards
  - but locks exist on a human scale
- Testing a key is an online, serial operation
  - takes a few seconds to do each test
  - trying all would take between 12 minutes and a year
  - risk of discovery (especially when it's not your lock)
- Keys typically cost between $0.15 and $1.00 each
  - full set costs between $35 and $$10^7$ (wholesale)
- Sometimes exhaustive search is practical
  - but 240 keys still won't fit in your pocket

How secure are locks…
…against brute force?

- In physical security, brute force does not refer to exhaustive search of the keyspace…
- Usually, even a really cheap lock will be one of the strongest parts of the system
  - doors are made of wood, sheet metal, etc
  - windows are made of glass
  - walls are made of drywall
- Disadvantage: leaves evidence and is noisy
  - some criminals don't mind this

How secure are locks…
…against manipulation?

- Maybe you don't really need a key
- Several techniques:
  - Lock picking
    - pin-by-pin, impact guns, bump keys
  - Decoding
    - impressioning and other techniques
  - Direct bypass of locking mechanism
    - …and more

Lock Picking

- In a perfect lock, all of the pin holes in the shell line up exactly with holes in the plug
  - so when you turn the plug with no key inserted, all of the pins block rotation exactly equally
- But real locks aren't perfect
  - in reality, the pin stacks are slightly misaligned
  - one of the pins stacks is the *most* misaligned
  - .001 inches or so of misalignment, typically

How to pick locks

- Put slight torque on the plug
  - just enough to *bind* the most misaligned pin
- Gently push up each of the pins until you find the one that resists (that's the most misaligned one)
- Push that pin up until the cut reaches the shear line
  - plug will turn slightly – you can feel it
  - top pin will be trapped above the shear line as long as torque is applied
- Repeat with the new most misaligned pin
- There are special tools for this

Countermeasures to lock picking

- Try to minimize misalignment
  - this is difficult and expensive
- Use more pin stacks
  - better locks have 6 or 7; typical locks have just 5
- Use a narrow keyway with many wards
  - makes it difficult to insert picking tools
- Use pick-resistant pins
  - funny shapes that give a false indication of reaching the shear line
- Special lock designs (sidebars, rotating pins, etc)

Decoding: “reading” the lock to make a key

- Disassemble lock and measure the pin cut heights
  - but if you can do this, you don’t *need* a key
- Use a special tool that fits in keyway and probes each pin stack to measure the cut height
- Impressioning: exploit the fact that pins at the wrong height tend to leave marks on key
  - keep filing at each pin position until marks disappear
  - common technique used by locksmiths

How secure are locks…
…against bypass?

- Sometimes the lock isn't the only way to operate the locking mechanism
  - Credit card or knife can push latch open
  - Tools inserted through keyway can manipulate lock
  - Prying doorframe past deadbolt strike can open door
  - Bent wire pushed under door can turn interior knob
  - Padlock "shims" can retract latch
  - Car "slim-jims" can manipulate lock linkage
- These techniques work surprisingly often!

Good news and bad news

- Good news: most burglars don’t pick locks
  - picking locks is hard – requires skill and tools
  - brute force or getting a copy of the key are the main attacks used by real criminals
- Bad news
  - getting a key is often surprisingly easy
  - NYC has above-average burglars

Déjà vu all over again?

- Small keyspaces
  - remind you of wireless security?
  - or 40 bit exportable cryptography?
- Brute force
  - remind you of buffer overruns?
- Lock picking and decoding
  - remind you of the TENEX paging password attack?
- Lock mechanism manipulation
  - remind you of virtually all Microsoft products?

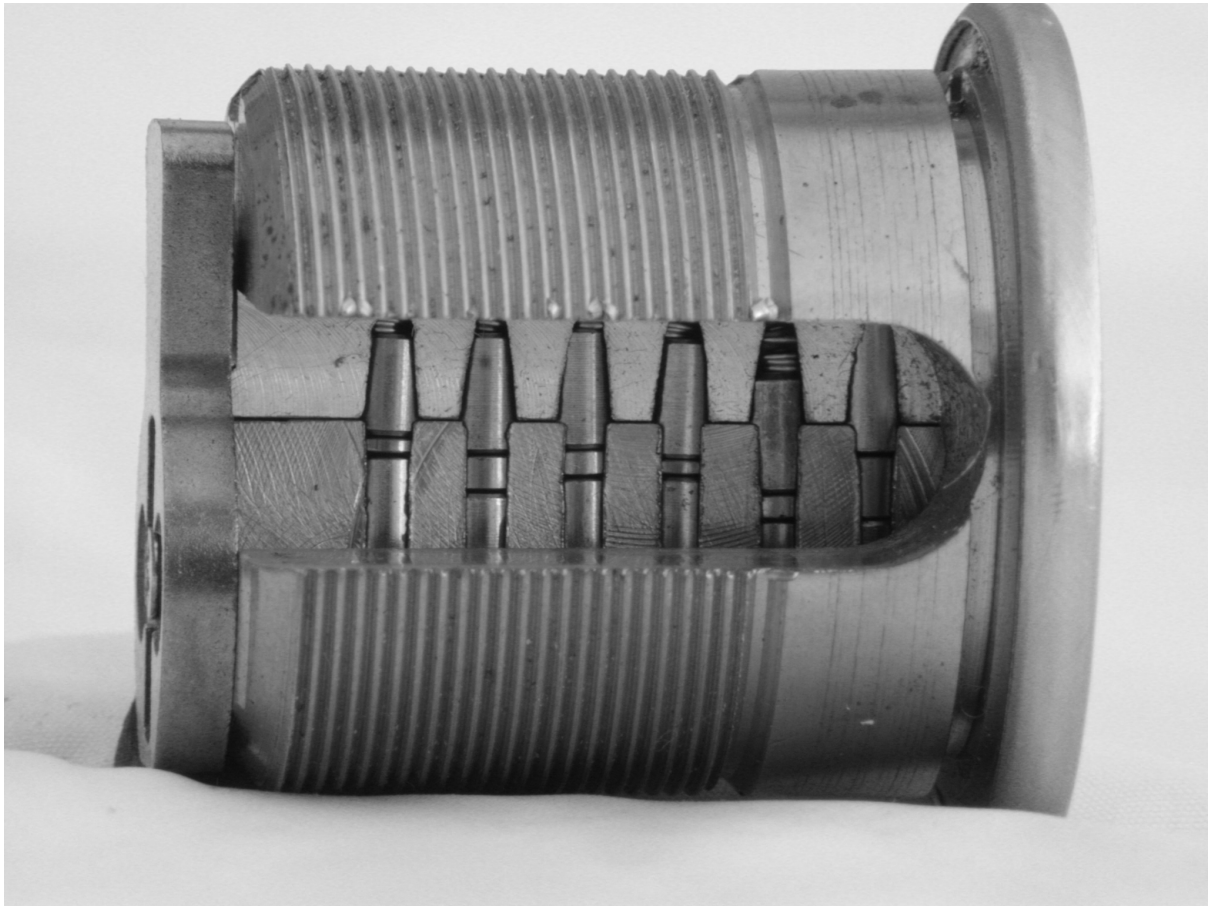
Master Keying

- Sometimes more than one key can operate a lock
- Institutions like to have *master keys* that open entire groups of locks
  - for managers, security guards, janitors, etc
- *Change Keys* operate just one lock
- The *Top Master Key (TMK)* operates all locks
- There may be more than one level of mastering
  - sub-master, grand-master, great-grand-master, etc.
  - may overlap (3rd floor master, electrical closet master)

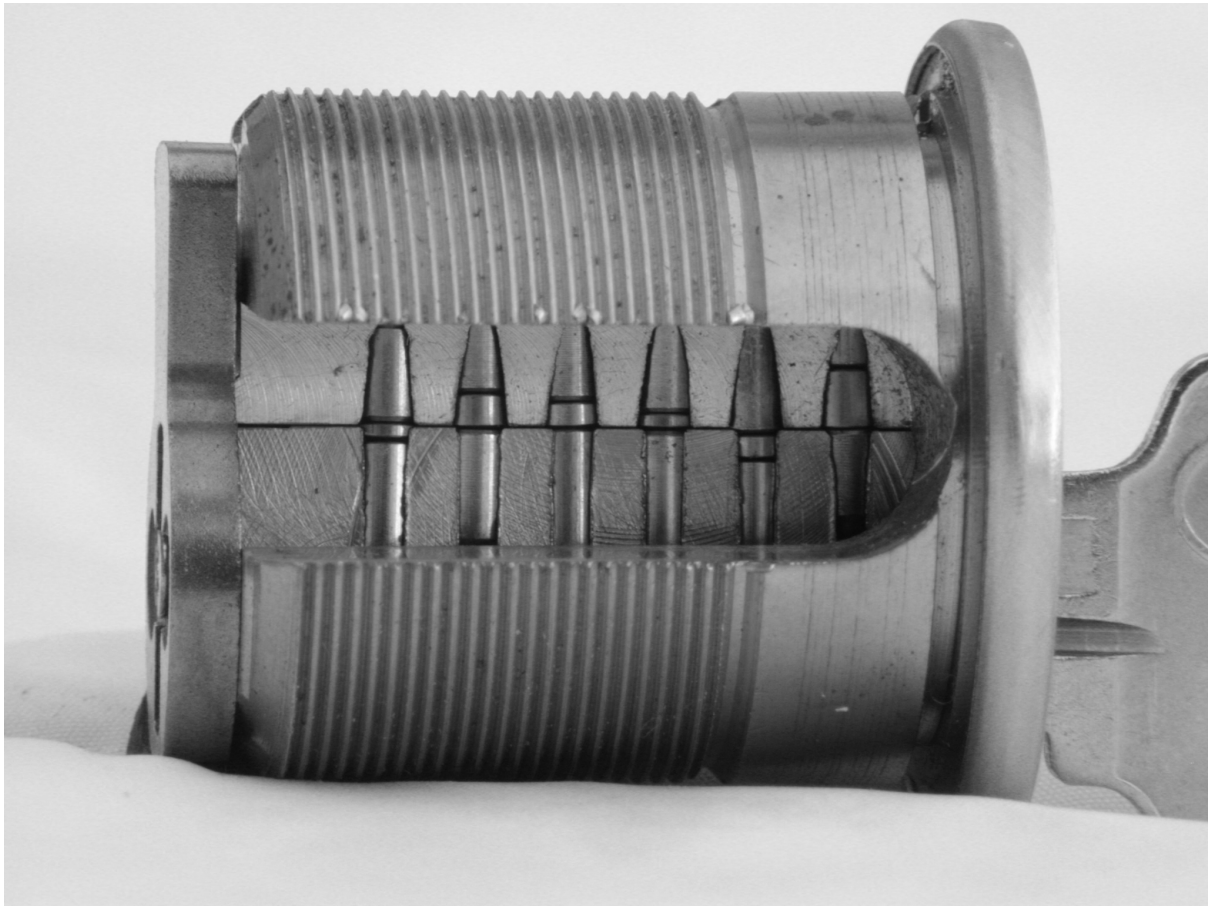
Some ways to master key locks

- Install 2 or more cylinders, linked together
  - one keyed to change key, others to master(s)
- Special lock design – “master rings”
  - requires special lock (expensive)
- Use only a subset of pins for change keys
  - grossly reduces security
- Add extra “master” cuts to pin stacks
  - most common technique, subject of this talk

Mastered pin-tumbler lock
2 cuts on each pin stack



Key raises one cut to shear line (other cut can be above or below)



An example

- Lock *A* has pins 1-5 cut at heights 1 and 2
- Lock *B* has pins 1-5 cut at heights 2 and 4
- Key 11111 is a change key for *A*
- Key 44444 is a change key for *B*
- Key 22222 is a master key for both
- Actually, 2^5 keys operate each lock
  - 12121 opens lock *A* (but not lock *B)*

Master keying standard practices

- Total Position Progression (TPP)
  - every pin stack has two cuts
  - no change key uses a master cut in any position
- Rotating Constant (RC)
  - every change key uses the master cuts in the same number of positions (C)
  - C pin stacks in each lock have only the master cut; the rest have two cuts
  - the particular positions vary (“rotate”) from lock to lock

Master keying security issues

- Exposure to lost keys
  - compromise of the master key is really bad
- Reduced pick resistance
  - two cuts on pins means more chances to pick
- Unwanted cross keying
  - keys from the same or other systems may open more locks than intended
- Unauthorized rights amplification
  - turn a change key into a master

Rights amplification

- If you can turn a change key into a master, there's little point in having change keys
  - might as well have all locks keyed alike
- A primary security objective of locks is to control insider access
  - give access to some places but not others

Some rights amplification attacks

- Take a lock apart and measure cut heights
  - the cut that doesn't correspond to change cut at each position is the master
  - conspicuous, risk of improper reassembly
- TPP systems: conspire with friends
  - get a bunch of change keys and measure them
  - the "unused" height at each position is the master
  - works only against TPP systems and also requires that attacker have friends

A new, improved attack: Locks as oracles

- Requires access to a single lock and its key
  - plus a few blank keys
- No disassembly or skill required
- Simple idea
  - a lock is an oracle that accepts or rejects keys
  - lock behaves the same way whether pins are at master or change height
  - learn the master height one pin at a time

The attack

- *P* is number of pins, *H* is number of heights
- For each pin *p* from *1* to *P*
  - for each height *h* from *1* to *H*
    - prepare a test key cut as the change key at every position except *p*
    - at position *p*, cut height *h*
    - try the key (ask the oracle)
- Each working test key corresponds to master key height at the position under test

A simple optimization

- Consumes *P(H-1)* blank keys as described
- Only need *P* blanks
  - re-use blanks at each position
  - start by cutting position *p* to tallest height
  - cut it down by one height after testing
- Still requires *P(H-1)* probes of lock

Some practical considerations

- Total cost of attack: $2.00 or less
- Blanks can be cut with a file or a machine
- Blanks are readily available for most locks
- Some systems don't follow standard mastering practices (TPP, RC)
  - usually this makes the attack even easier
- Yes, it really works

Countermeasures

- Don’t do master keying
- Use a lock design that resists this attack
  - e.g., master rings (requires special locks)
- Add “false” cuts to pin stacks
  - increases susceptibility to cross keying
  - but makes it more difficult to learn true TMK

Lessons learned

- Cryptology can be applied to locks
  - locks as oracles
  - related key attacks
  - bit-by-bit key discovery
- Master keying sounds familiar…
  - key escrow
  - smartcard systems with global secrets

References

- M. Blaze. “Rights Amplification in Master-Keyed Mechanical Locks.” t*o appear.* 2002.
  `http://www.crypto.com/mk.pdf`
- M. W. Tobias. *Locks, Safes and Security (2/e).* 2001.
- B. B. Edwards. *Master Keying by the Numbers (2/e).* 1997.