Exploiting Keypspace Vulnerabilities in Locks

Bill Graydon

@access_ctrl
b.graydon@ggrsecurity.com
github.com/bgraydon

GGR SECURITY CONSULTANTS
Take a look at your keyring...
Outline

- How locks & keys work
- Intro to the tools I’m releasing
- Brute forcing all possible keys
- Reading the pins in a lock
- Impressioning with extra information
- Keyed alike systems & lock disassembly in nonmastered systems
- Information theory and entropy
- How master keying works
- Deriving a master key from multiple low-level keys
- Rights amplification in mastered systems
- Special cases: construction keying, IC cores, Medeco, Mul-T-Lock
- Remediation
Software Analysis Tools

Try it yourself!

https://ggrsecurity.com/personal/~bgraydon/keyspace

Or:

https://tinyurl.com/key-space

Source:

https://github.com/bgraydon/lockview
https://github.com/bgraydon/keyspace
How Locks Work
What is a key?

Mechanically encoded information.
Background | Key Codes
<table>
<thead>
<tr>
<th>#</th>
<th>INCH</th>
<th>MM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.335</td>
<td>8.51</td>
</tr>
<tr>
<td>1</td>
<td>0.320</td>
<td>8.13</td>
</tr>
<tr>
<td>2</td>
<td>0.305</td>
<td>7.75</td>
</tr>
<tr>
<td>3</td>
<td>0.290</td>
<td>7.37</td>
</tr>
<tr>
<td>4</td>
<td>0.275</td>
<td>6.99</td>
</tr>
<tr>
<td>5</td>
<td>0.260</td>
<td>6.60</td>
</tr>
<tr>
<td>6</td>
<td>0.245</td>
<td>6.22</td>
</tr>
<tr>
<td>7</td>
<td>0.230</td>
<td>5.84</td>
</tr>
<tr>
<td>8</td>
<td>0.215</td>
<td>5.46</td>
</tr>
<tr>
<td>9</td>
<td>0.200</td>
<td>5.08</td>
</tr>
</tbody>
</table>
87527

52864
MACS - Maximum Adjacent Cut Specification

![Key Diagram]

- OK: 1 1 5 3 1
- No good - too steep: 1 1 9 3 1
MACS - Maximum Adjacent Cut Specification

[Diagram showing two keys: one marked 'OK' with adjacent cuts labeled 1, 1, 5, 3, 1, and another marked 'No good - too steep' with adjacent cuts labeled 1, 1, 9, 3, 1]
MACS = Maximum Adjacent Cut Specification

<table>
<thead>
<tr>
<th>Key Type</th>
<th>MACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schlage</td>
<td>7</td>
</tr>
<tr>
<td>Kwikset</td>
<td>4</td>
</tr>
<tr>
<td>Sargent</td>
<td>7</td>
</tr>
<tr>
<td>Yale</td>
<td>7</td>
</tr>
<tr>
<td>Weiser</td>
<td>7</td>
</tr>
<tr>
<td>Medeco</td>
<td>2,3,4</td>
</tr>
</tbody>
</table>
Keyspaces

In theory -

Number of depths to the power of the number of spaces

E.g. -

Schlage - 10 depths, to the power of 5 or 6 spaces - 100,000 or 1,000,000 possible combinations

Medeco - 6 depths, to the power of 5 or 6 spaces - 7000 or 46000 combinations

There are further limitations imposed by physical constraints!
### Keys vs. Passwords

<table>
<thead>
<tr>
<th>Trait</th>
<th>Password</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost to try one</td>
<td>$0.0000000000001</td>
<td>$0.30-$10.00</td>
</tr>
<tr>
<td>Detectability of brute force</td>
<td>Possible</td>
<td>Challenging</td>
</tr>
<tr>
<td>Length</td>
<td>Unlimited</td>
<td>Severely Limited</td>
</tr>
<tr>
<td>Complexity</td>
<td>Unlimited</td>
<td>Limited</td>
</tr>
<tr>
<td>Ease of changing</td>
<td>Easy</td>
<td>Costly and time-consuming</td>
</tr>
<tr>
<td>Privilege levels</td>
<td>Unlimited schemes</td>
<td>Limited to hierarchical*</td>
</tr>
</tbody>
</table>
The Economics of Brute-Force Attacks

Brute force = trying all possible keys

If we have n key codes to try, we need at most n blanks, possibly fewer

- Blanks cost between $0.13 and $3.00 - the common ones are cheap
- If you have access to a code cutting machine, the marginal cost of a new key cut is the blank + your time
- If you do not, locksmiths will cut keys to code for $3.00-$10.00 each

E.g. - if you can reduce the keyspace of a given lock to 1000 possible keys, the cost might be $450 (you own a code machine, blanks are $0.45 each) or $4000 (you need to use a locksmith, cost per cut key is $4.00)
Try-Out Key Set for "Smart" Type Locks that use the KW1 Key 256 Set
Try-Out Key Set for "Smart" Type Locks that use the KW1 Key 256 Set

Your Price: $394.90

This Tryout set has 256 keys in it, expect to have 98% success with all "smart key" type locks that use the KW1.
Lock Tolerances

Demo →
GM Try Out Key Set

Part Number: GMPK
Your Price: $85.95

Be the first to review this product

GM Try Out Key Set
62 key set

Try out keys are used in many cases as a first try. The success rate with this set is about 80%. (for GM's from 1967 - 1987 models) Set works on doors, trunks, and ignition for all single sided keyways A-K.
Decoding Locks
Re-Key A Lock
Re-Keying Set for Up to Six Locks

SCHLAGE
“C” TYPE LOCKS

All you’ll need is a screwdriver!

you’ll need is a screwdriver!

PRIME-LINE
<table>
<thead>
<tr>
<th>Depth of Cut</th>
<th>Bitting No.</th>
<th>Bottom Pin</th>
<th>Master Pin</th>
<th>Top Pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>.330</td>
<td>1</td>
<td>.171</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>.310</td>
<td>2</td>
<td>.189</td>
<td>.039</td>
<td>*.219</td>
</tr>
<tr>
<td>.290</td>
<td>3</td>
<td>.210</td>
<td>.060</td>
<td></td>
</tr>
<tr>
<td>.270</td>
<td>4</td>
<td>.231</td>
<td>.081</td>
<td></td>
</tr>
<tr>
<td>.250</td>
<td>5</td>
<td>.249</td>
<td>.099</td>
<td>.180</td>
</tr>
<tr>
<td>.230</td>
<td>6</td>
<td>.270</td>
<td>.120</td>
<td></td>
</tr>
<tr>
<td>.210</td>
<td>7</td>
<td>.291</td>
<td>.141</td>
<td></td>
</tr>
<tr>
<td>.190</td>
<td>8</td>
<td>.309</td>
<td>.160</td>
<td>.145</td>
</tr>
<tr>
<td>.170</td>
<td>9</td>
<td>.330</td>
<td>.180</td>
<td></td>
</tr>
<tr>
<td>.150</td>
<td>0</td>
<td>.351</td>
<td>—</td>
<td></td>
</tr>
</tbody>
</table>

EPD = .498  TFC = .216  BCC = .156  MACS = 7
* INVERT .219 BOTTOM PIN USE AS TOP PIN
Password Re-Use

- Is bad

Key Re-Use

- Is called “keyed alike” and is a common and accepted arrangement

In a keyed-alike system, the key space is 1!
Keyed Alike - When Your Keyspace is 1

- Elevators
- Most alarms (i.e. Detex)
- Enterphone systems
- Most controller boxes
- Golf carts
- Heavy equipment
- Police cars
- Traffic light controllers
- Telecom boxes
- Almost all other utilities
- New York City
- HVAC / Building automation systems
- Many city’s fire safety boxes
- Many regional Knox boxes
- Vending machines
- Postal keys
- Luggage - TSA keys
- Handcuffs

HOPE XI: Howard Payne & Deviant Ollam, This Key is Your Key, This Key is My Key
Lock Disassembly
DEF CON 26 - m010ch - Please Do Not Duplicate Attacking the Knox Box
Information Theory
Shannon Entropy

**Information** = stuff we know.

**Entropy** = stuff we don’t know.

We know whether a stop light is red or green. The colour of a stop light is **information**.

We don’t know the outcome of a random variable, such as a coin flip or a dice roll. A coin flip and or dice roll has **entropy**. A key or password has entropy.
Measuring Entropy

Once we \textit{do know} the information, how many bits on a hard drive will it take to write it down (on average)?

A coin flip → \textbf{one bit}

A random number 0..255 → \textbf{8 bits}

A random number 1..10 → \textbf{3.32 bits}

3 random numbers 1..10 can be encoded in a number 0..10^3.
We can use 10 bits to encode 0..1023. So 10 bits will encode 0..999.
10 bits / 3 random numbers 1..10 ≈ 3.33 ≈ \textbf{3.32 bits / random number}
Measuring Entropy

Number of bits it takes to write down a number $0..x$
→ $\log_2(x)$

Number of bits of entropy ($H$) for a random variable with $n$ outcomes:
→ $H = \log_2(n)$

E.g:

A fair coin flip, 2 outcomes: $\log_2(2) = 2$ bits
A random number $0..255$: $\log_2(256) = 8$ bits
A random number $1..10$: $\log_2(10) = 3.322$ bits
Key Entropy Examples

Number of bits in a piece of information (e.g. key, password) -

- 8-character ASCII password - 8*8=256 bits of entropy
- 10-digit passcode, 3 characters long - 1000 combinations or 9.97 bits
- EVVA MCS key, 4 rotors with 8 positions each - 8^4=4096 or 12.00 bits of entropy
- Schlage 5-pin system - 5^10 or 100000 combinations (16.6 bits)

If there are N possibilities, and all possibilities are equiprobable, then entropy (H) is given by:

\[ H = \log_2(n) \]

If some possibilities are more likely than others, entropy goes down. E.g., dictionary-based passwords; avoidance of deep cut keys; key coding to deter picking
Entropy: 2 Possibilities, Unequal Probability

Master key decoded to 14767 or 94767…

When 50/50 chance…

\[ H = -p_1 \log_2(p_1) - p_2 \log_2(p_2) \]

\[ H = -0.5 \log_2(0.5) - 0.5 \log_2(0.5) = -\log_2(0.5) = \log_2(2) = 1 \text{ bit.} \]

Are these equiprobable?

\[ H = 0.95 \log_2(0.95) + 0.05 \log_2(0.05) = 0.286 \text{ bits} \]

In the extreme, if one option is certain, that’s 0 bits!

In general… \( H = -\sum p \log_2(p) \)
Joint+Conditional Entropy, Mutual Information
Master Keying
<table>
<thead>
<tr>
<th>Depth of Cut</th>
<th>Bitting No.</th>
<th>Bottom Pin</th>
<th>Master Pin</th>
<th>Top Pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>.330</td>
<td>1</td>
<td>.171</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>.310</td>
<td>2</td>
<td>.189</td>
<td>.039</td>
<td>.219</td>
</tr>
<tr>
<td>.290</td>
<td>3</td>
<td>.210</td>
<td>.060</td>
<td></td>
</tr>
<tr>
<td>.270</td>
<td>4</td>
<td>.231</td>
<td>.081</td>
<td></td>
</tr>
<tr>
<td>.250</td>
<td>5</td>
<td>.249</td>
<td>.099</td>
<td>.180</td>
</tr>
<tr>
<td>.230</td>
<td>6</td>
<td>.270</td>
<td>.120</td>
<td></td>
</tr>
<tr>
<td>.210</td>
<td>7</td>
<td>.291</td>
<td>.141</td>
<td></td>
</tr>
<tr>
<td>.190</td>
<td>8</td>
<td>.309</td>
<td>.160</td>
<td>.145</td>
</tr>
<tr>
<td>.170</td>
<td>9</td>
<td>.330</td>
<td>.180</td>
<td></td>
</tr>
<tr>
<td>.150</td>
<td>0</td>
<td>.351</td>
<td>—</td>
<td></td>
</tr>
</tbody>
</table>

EPD = .498  TFC = .216  BCC = .156  MACS = 7
* INVERT .219 BOTTOM PIN USE AS TOP PIN
<table>
<thead>
<tr>
<th>Depth of Cut</th>
<th>Bitting No.</th>
<th>Bottom Pin</th>
<th>Master Pin</th>
<th>Top Pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>.330</td>
<td>1</td>
<td>.171</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>.310</td>
<td>2</td>
<td>.189</td>
<td>.039</td>
<td>* .219</td>
</tr>
<tr>
<td>.290</td>
<td>3</td>
<td>.210</td>
<td>.060</td>
<td></td>
</tr>
<tr>
<td>.270</td>
<td>4</td>
<td>.231</td>
<td>.081</td>
<td></td>
</tr>
<tr>
<td>.250</td>
<td>5</td>
<td>.249</td>
<td>.099</td>
<td>.180</td>
</tr>
<tr>
<td>.230</td>
<td>6</td>
<td>.270</td>
<td>.120</td>
<td></td>
</tr>
<tr>
<td>.210</td>
<td>7</td>
<td>.291</td>
<td>.141</td>
<td></td>
</tr>
<tr>
<td>.190</td>
<td>8</td>
<td>.309</td>
<td>.160</td>
<td>.145</td>
</tr>
<tr>
<td>.170</td>
<td>9</td>
<td>.330</td>
<td>.180</td>
<td></td>
</tr>
<tr>
<td>.150</td>
<td>0</td>
<td>.351</td>
<td>—</td>
<td></td>
</tr>
</tbody>
</table>

EPD = .498  TFC = .216  BCC = .156  MACS = 7

* INVERT .219 BOTTOM PIN USE AS TOP PIN
Master Keyed Lock Disassembly
Deducing the Master from Multiple Change Keys

Demo →
Rights Amplification

Demo →
Construction Core Systems
Interchangeable Core Systems
159 Possible Medeco TMKs If…

Intelligence: large facility

Intelligence: IC System

Reduce further with change keys and other information.

Demo ➔
Medeco Biaxial
Nonmastered Medeco Locks
Physical Creation of Keys
Getting a Key Cut

1. Identify the blank
2. Determine the bitting code you want
3. Go to a locksmith (not a hardware store or 7/11)
4. Ask if they can cut you a key by code
5. Give them the blank and code: e.g. “A Schlage SC1 with bitting code 0-4-2-8-5”
6. If they say “that key is restricted, I can’t cut you that”... check out our DEF CON 27 talk on Duplicating Restricted Mechanical Keys or wait a year for our (tentative) DEF CON 29 part II of that talk.
Defenses

- Avoid very large mastering systems
- Don’t master high-security and low-security facilities on one system
  - Very high risk locations should be off-master (current requirement for USA nuclear arsenals)
- A missing lock is as bad as a missing GMK!
- Consider alternatives to the 2-step system
  - Other specific defenses
  - If this is in your threat model
- Use a restricted keying system - it won’t stop a determined attacker, but it can slow them down and drive their costs up
- Your facility should be secure even if an attacker has the GMK
  - All a lock does is keep honest people honest. Add alarms, guards, etc.
- Use IC or electronic components to make rekeying easier
Master keys for O'Hare Airport security access were lost, costing city in ‘five figures’

A set of keys that provides almost total access to O'Hare Airport were lost and never recovered. But there were rare consequences for the employee involved, a Sun-Times investigation found.

By Robert Herguth | Jun 21, 2018, 5:00am CDT

Lost, stolen campus master keys too expensive to replace

The master keys at UCA have recently been brought into the light due to an investigation involving a lost key.

The investigation began in June after a theft was reported in Assistant Director of Financial Aid for Scholarships Andrew Linn's office in McCastlain Hall, Jeff Pitchford, vice president of university and government relations, said.

A thief reportedly broke in and stole four pills out of Linn's office. The key used was a grand...
Questions?

b.graydon@ggrsecurity.com
@access_ctrl

Go try it!
https://ggrsecurity.com/personal/~bgraydon/keyspace

Or: https://tinyurl.com/key-space

Source:
https://github.com/bgraydon/lockview
https://github.com/bgraydon/keyspace

A huge thank you to Josh Robichaud, Karen Ng and Jenny & Bobby Graydon for their help in preparing this talk.