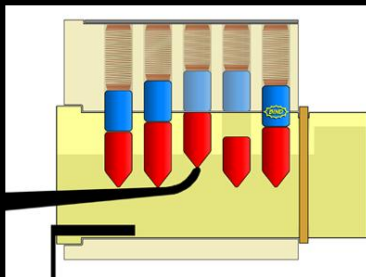
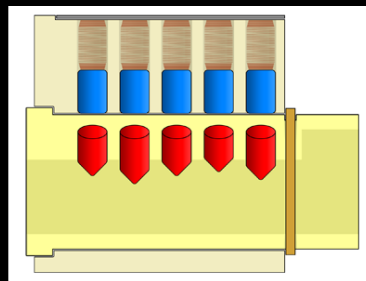


New

Ten Things You Should Know About Lockpicking



by Deviant Ollam
Event Name
XXXX-XX-XX

Who am i ?



Who am i ?



Who am i ?



**THE
CORE
GROUP**

auditing
assessments
research
trainings



Who am i ?



**THE
CORE
GROUP**

auditing
assessments
research
trainings



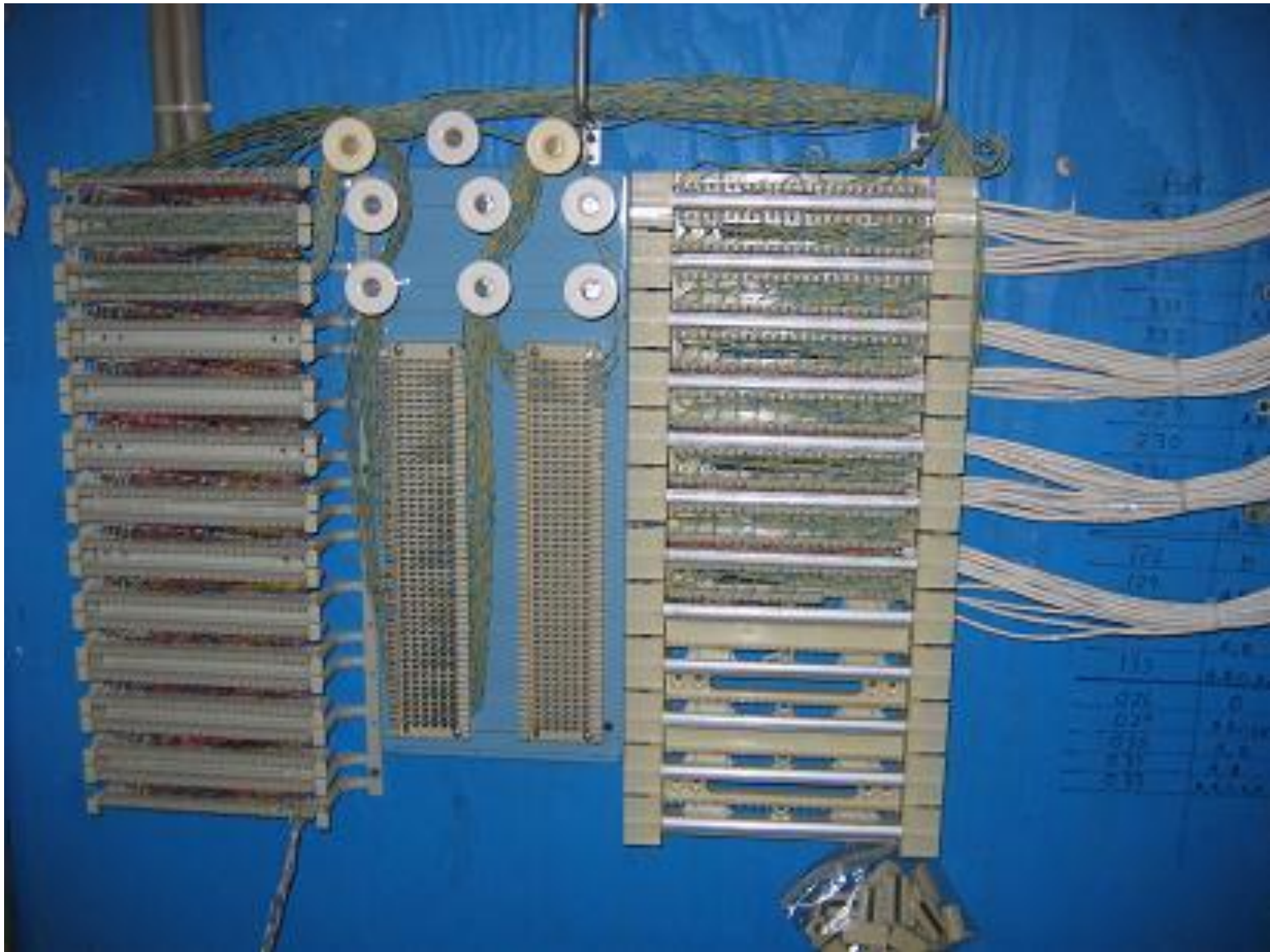
workshops
public lectures
lockpick village
contests & games

Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals







111	
112	
113	
114	
115	
116	
117	
118	
119	
120	
121	
122	
123	
124	
125	
126	
127	
128	
129	
130	
131	
132	
133	
134	
135	
136	
137	
138	
139	
140	
141	
142	
143	
144	
145	
146	
147	
148	
149	
150	



All your hard work here...



All your hard work here... gets undermined here



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
- 2. Pin tumblers are universal**

Pin Tumbler Locks



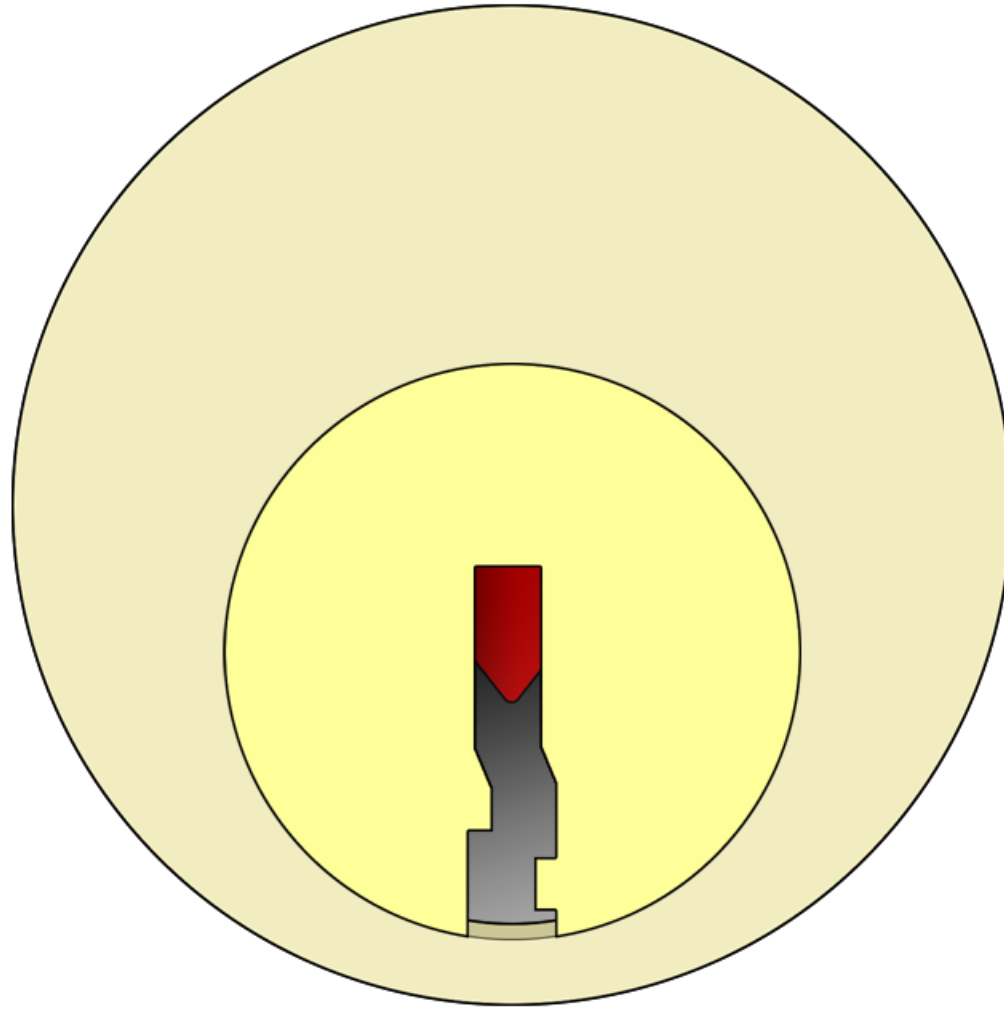
Pin Tumbler Locks



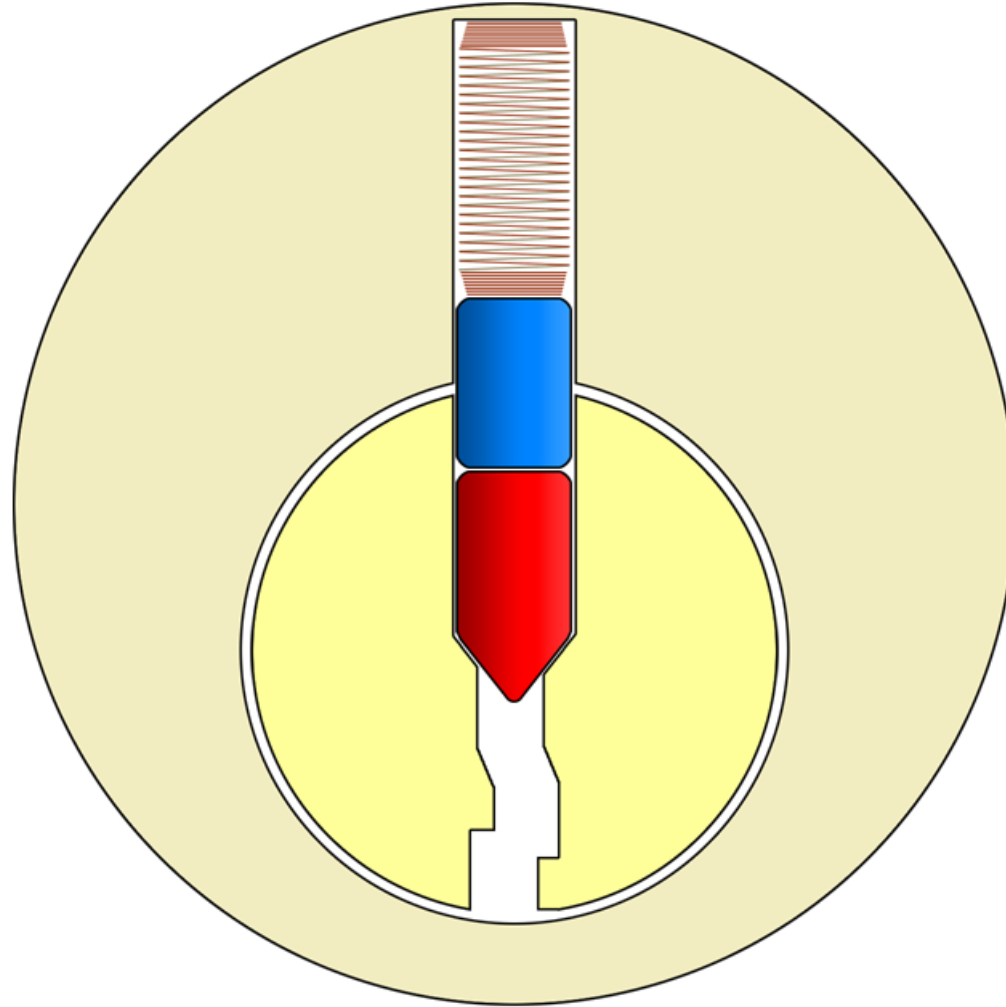
Pin Tumbler Locks



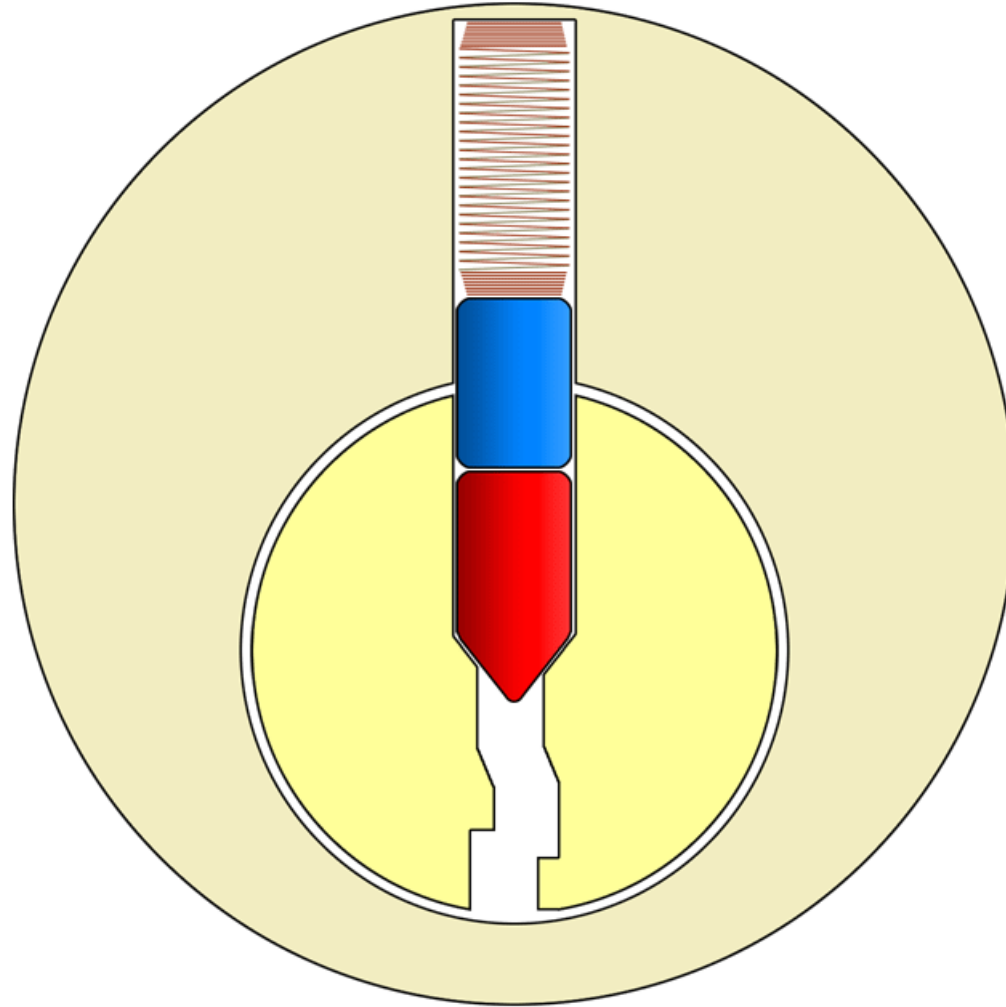
The View From Outside



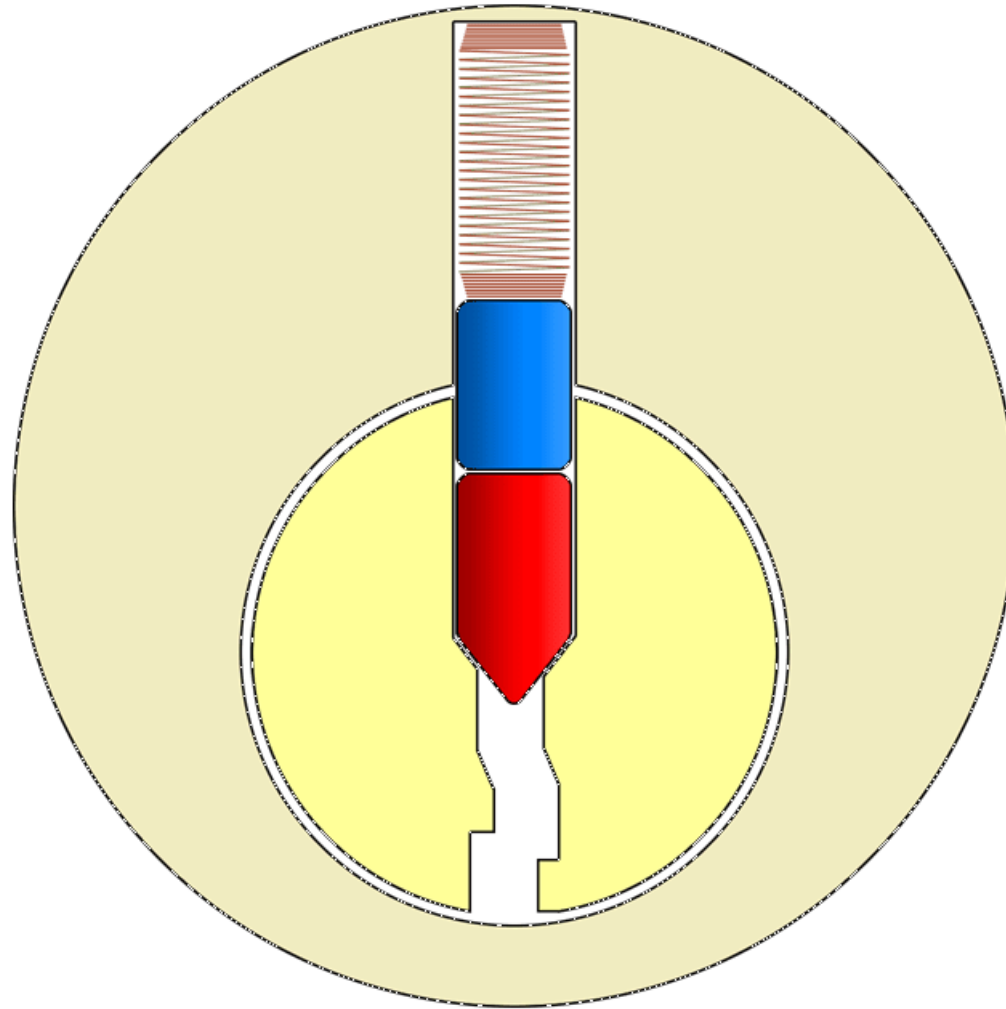
What's On The Inside



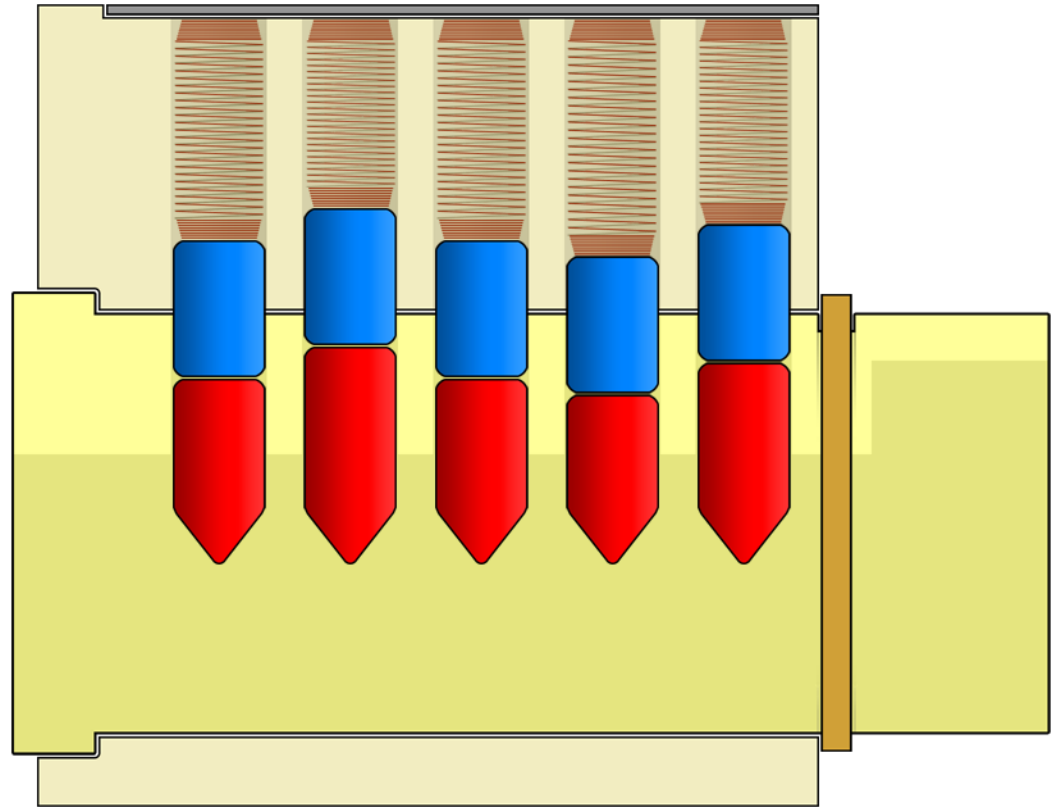
What's On The Inside



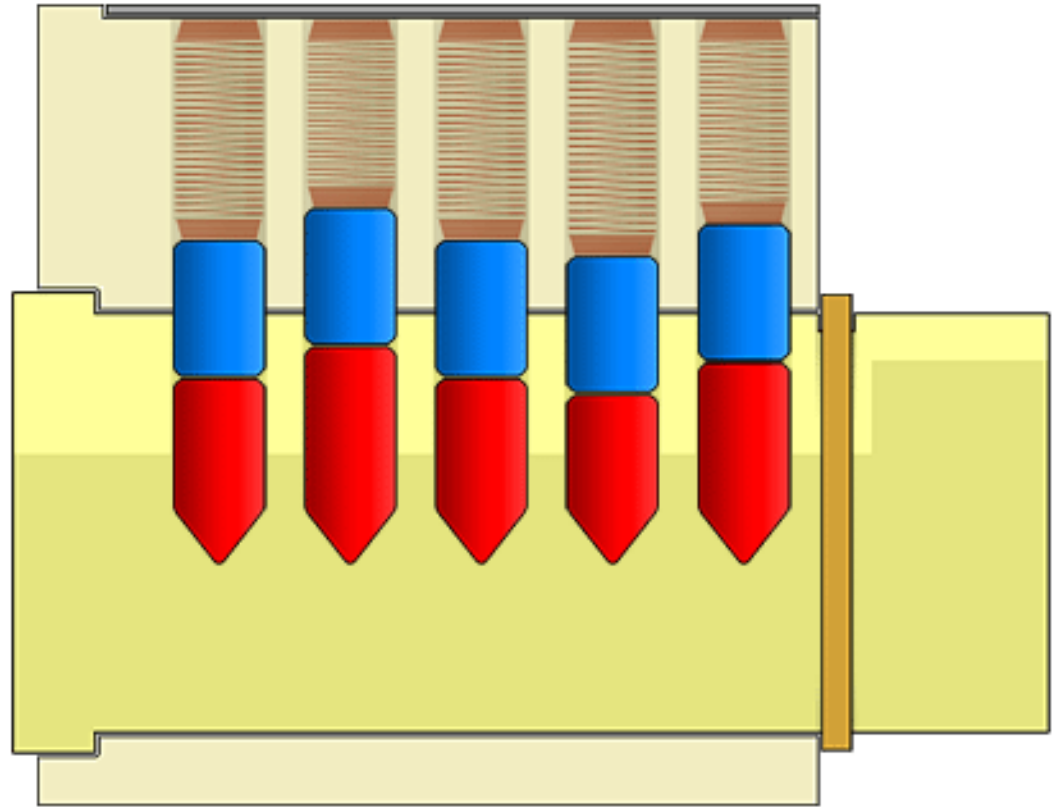
What's On The Inside



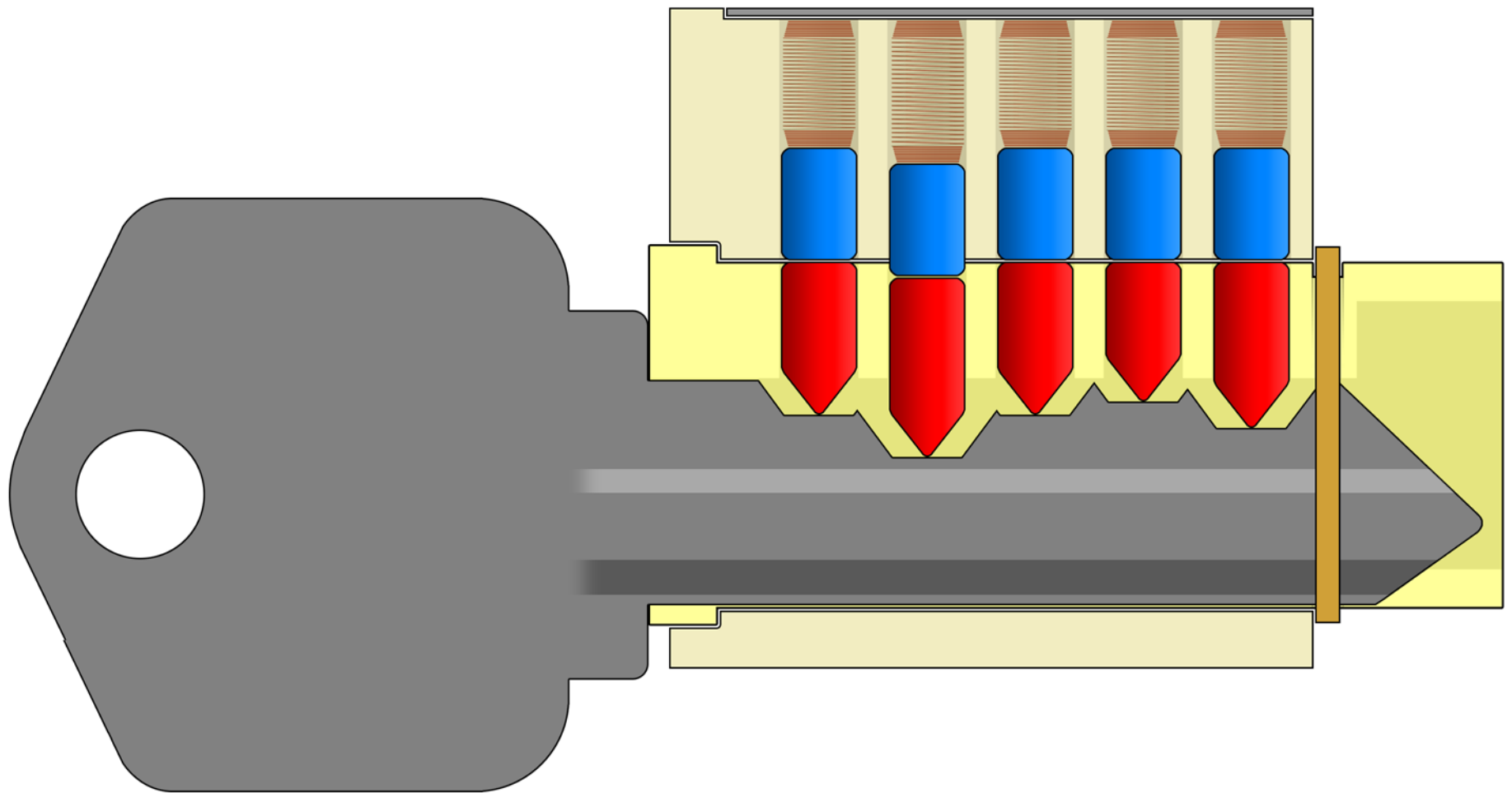
It's Not Just a Single Pin Stack



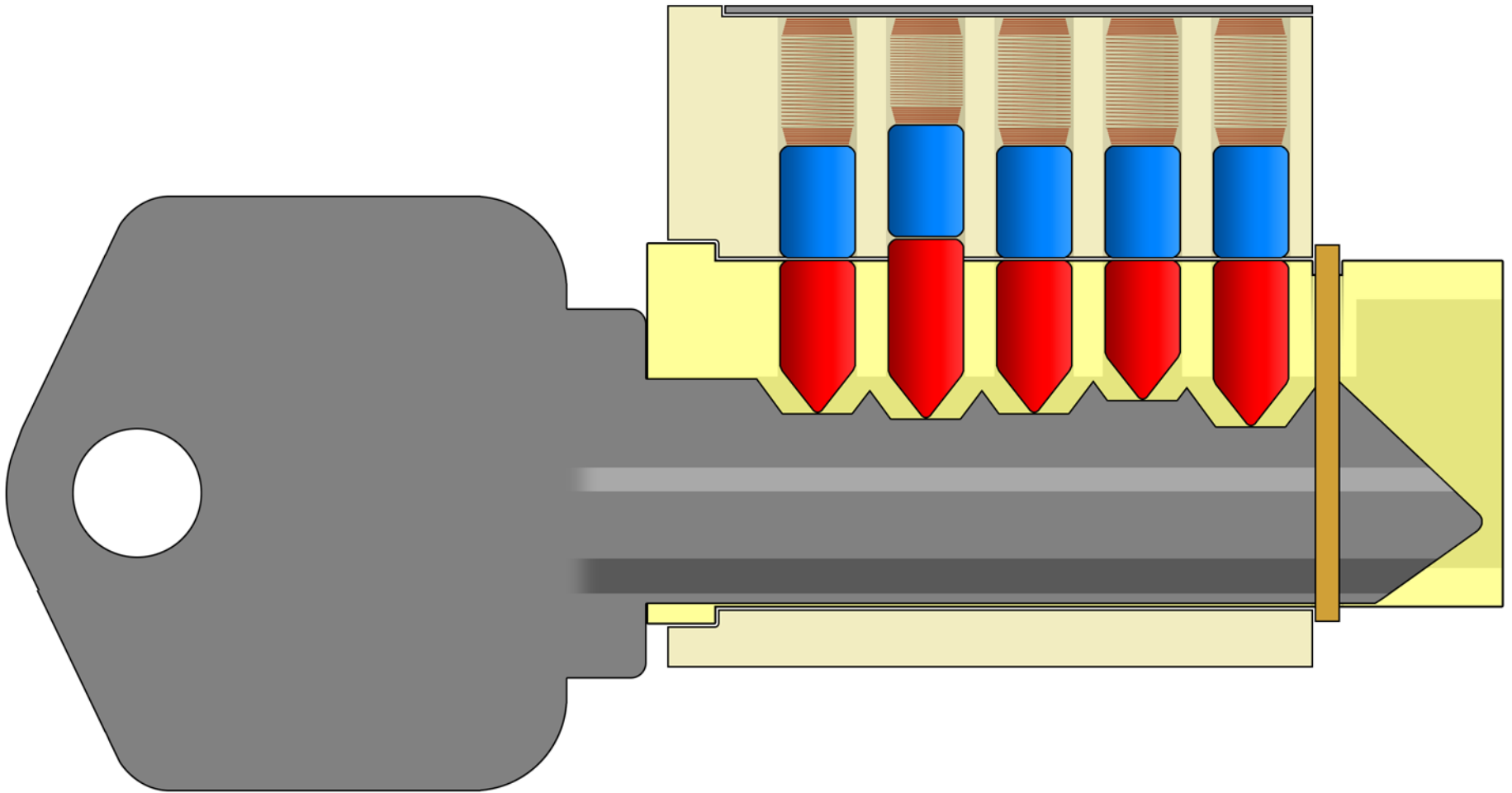
It's Not Just a Single Pin Stack



The Key Has To Be Just Right



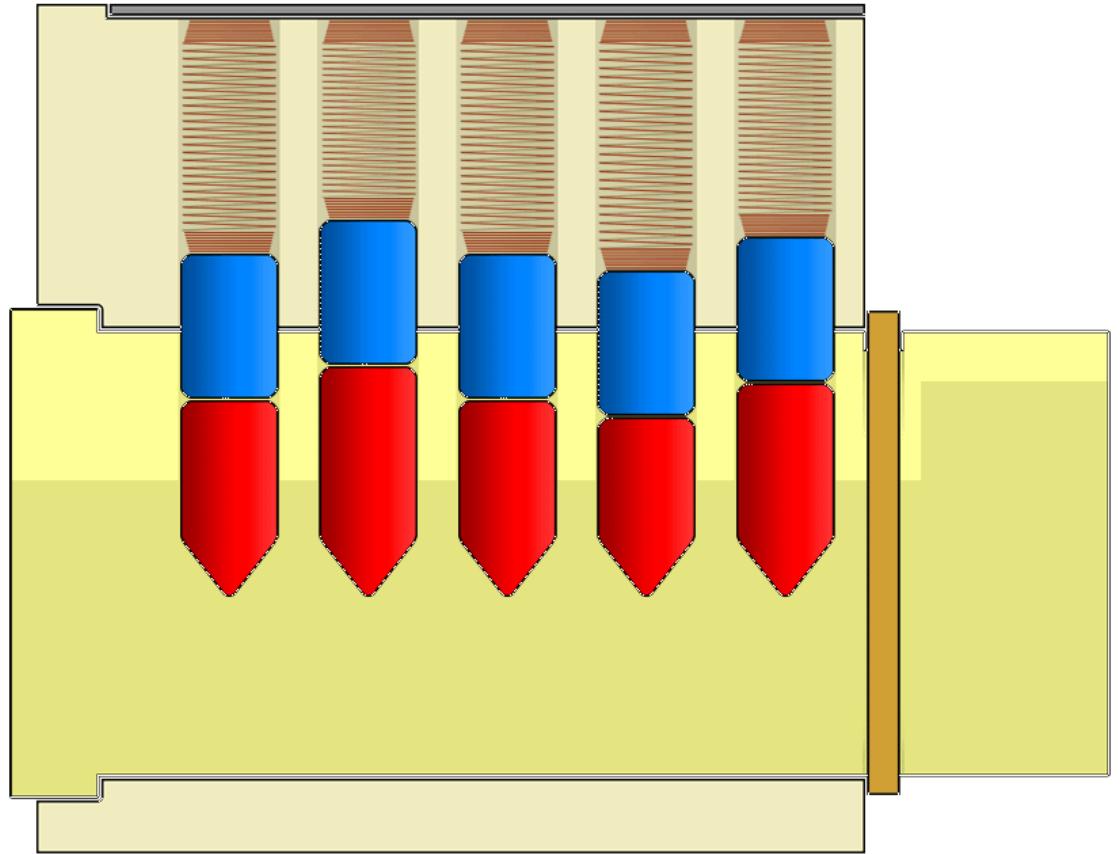
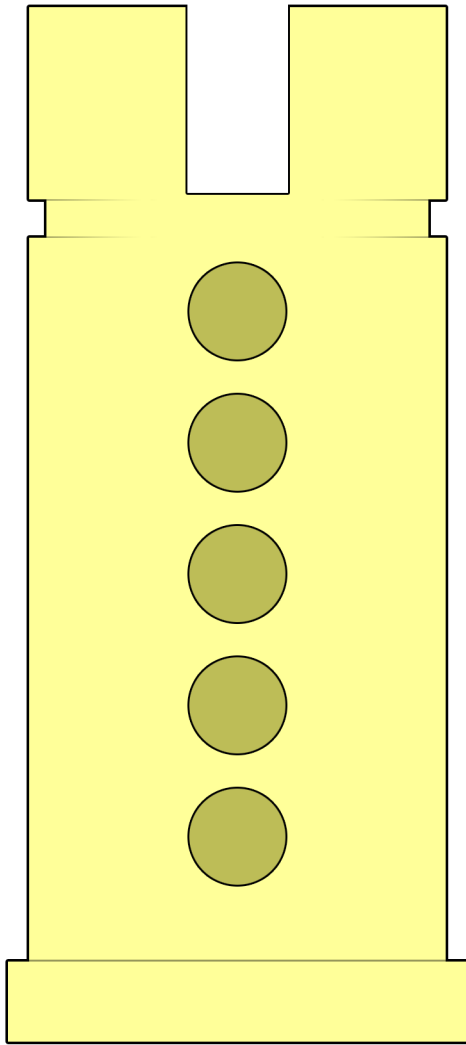
The Key Has To Be Just Right



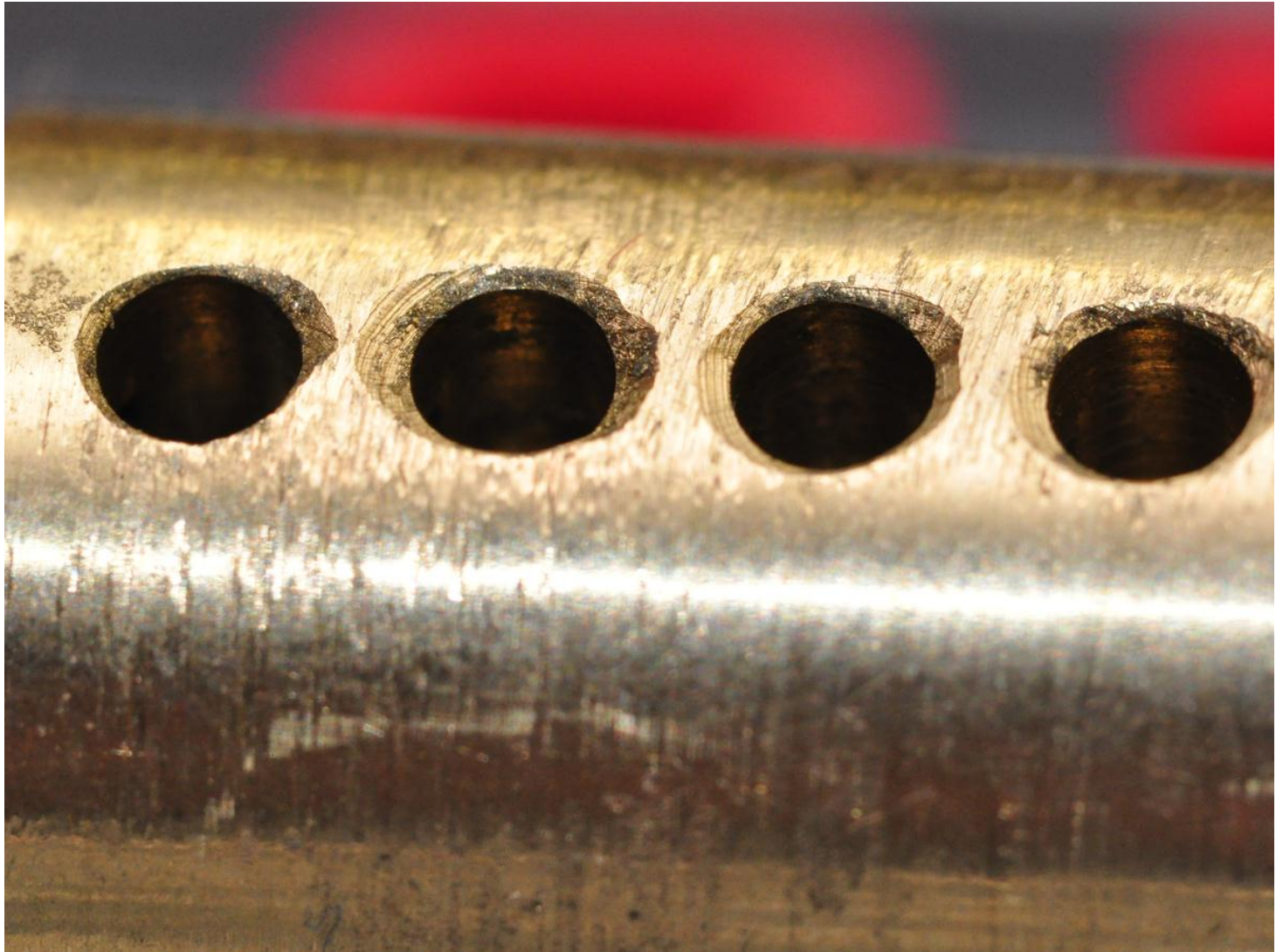
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
- 3. Picking is simple and fun**

In An Ideal World ...



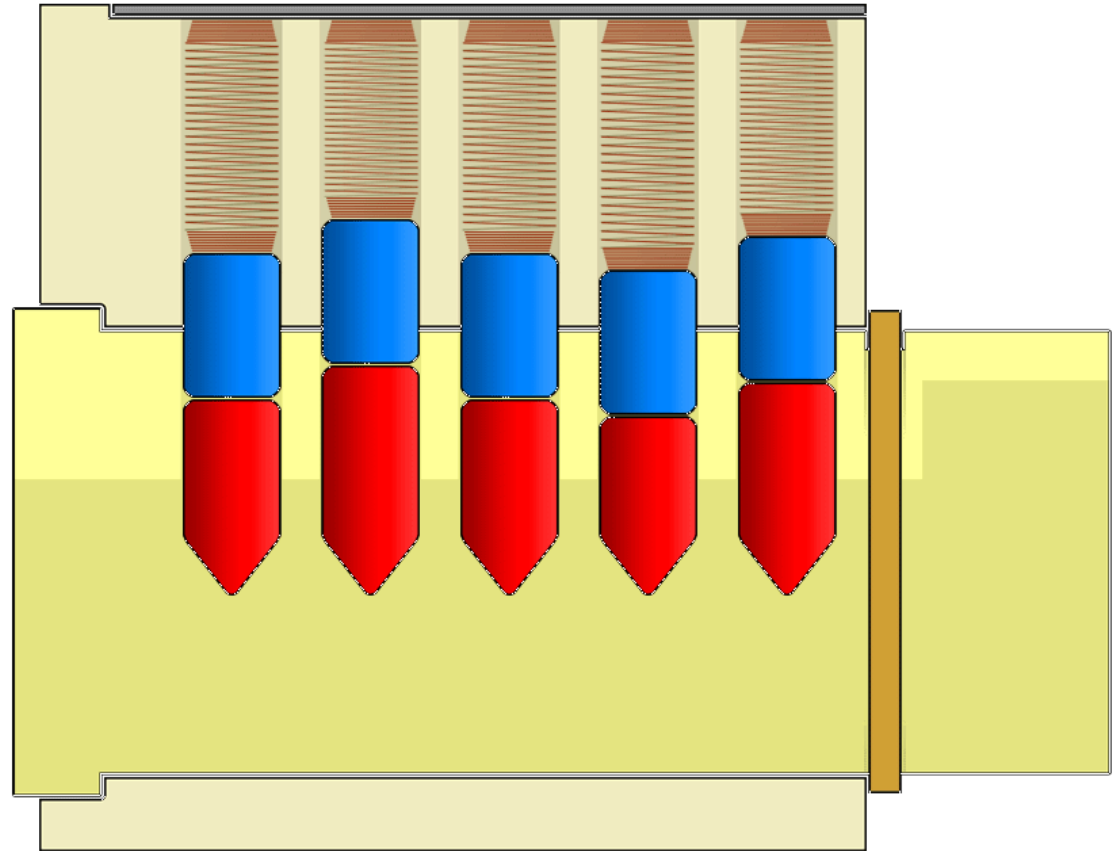
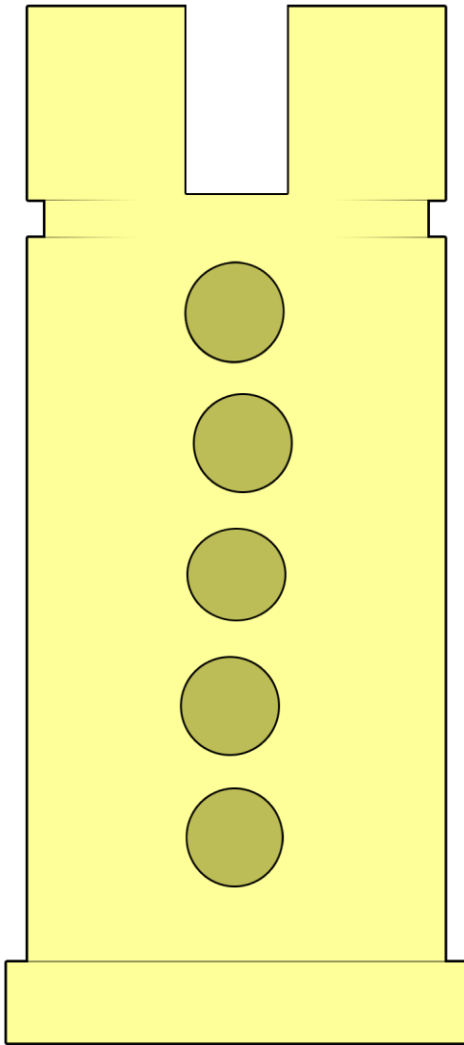
In The Real World ...



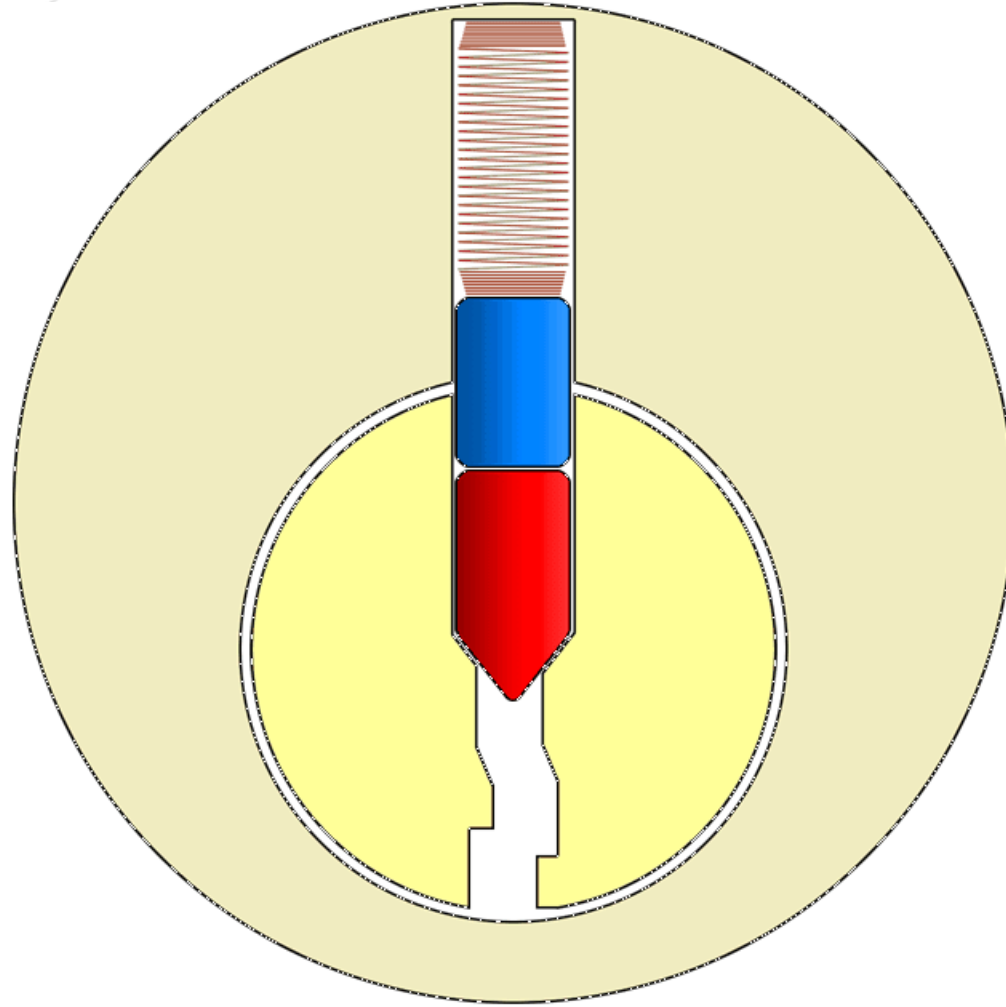
In The Real World ...



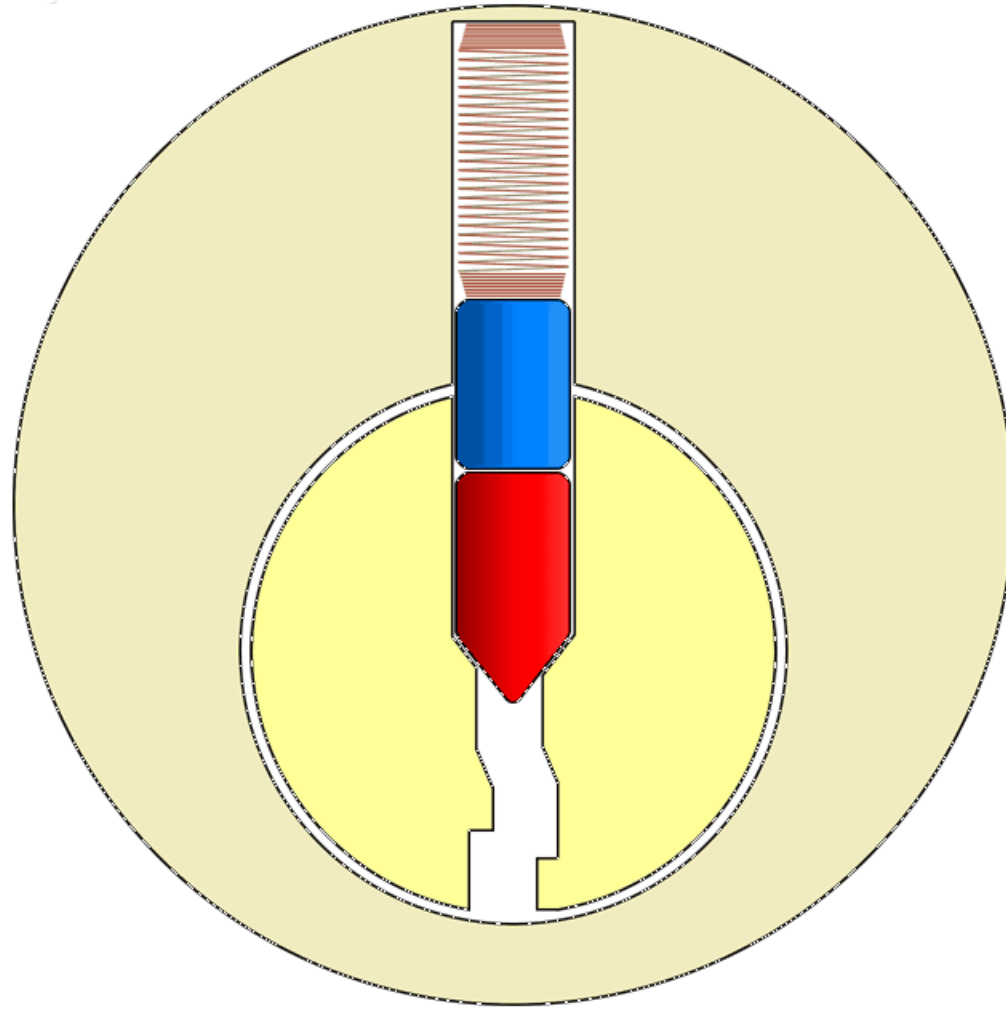
In The Real World ...



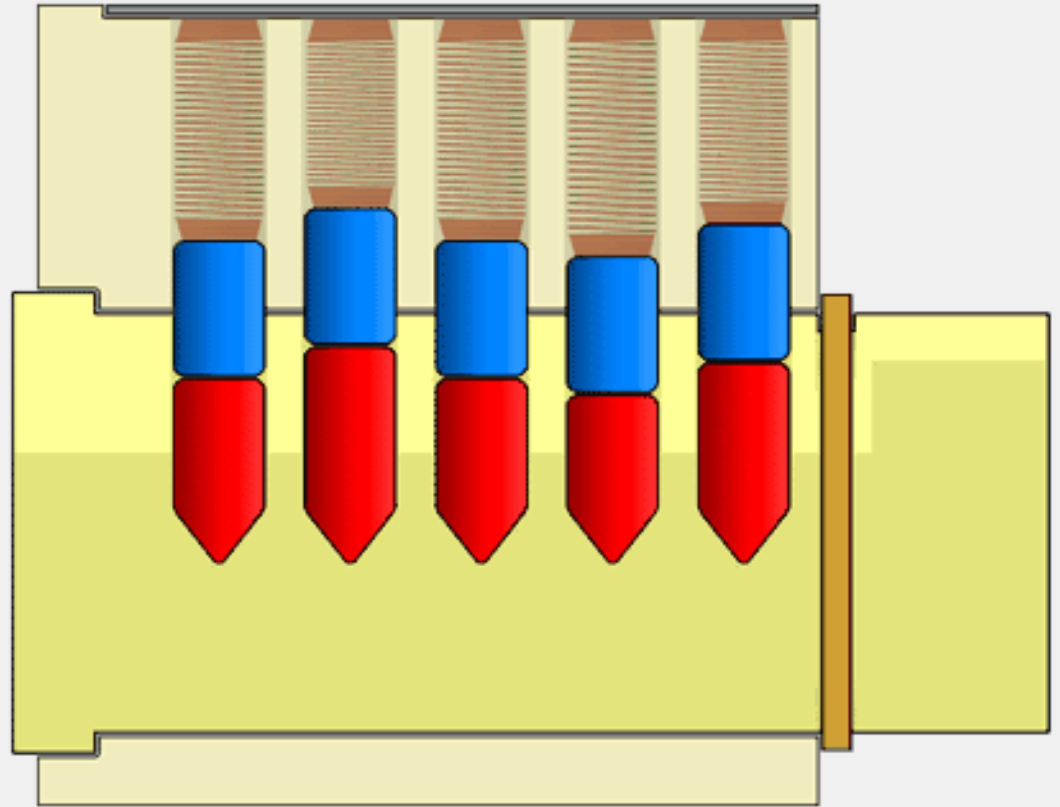
Setting a Pin



Setting a Pin



Setting the Pins



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement

Other Ways of Arranging the Pins



Other Ways of Attacking the Pins



A Fun Tubular Lock Story



A Fun Tubular Lock Story



A Fun Tubular Lock Story



A Fun Tubular Lock Story



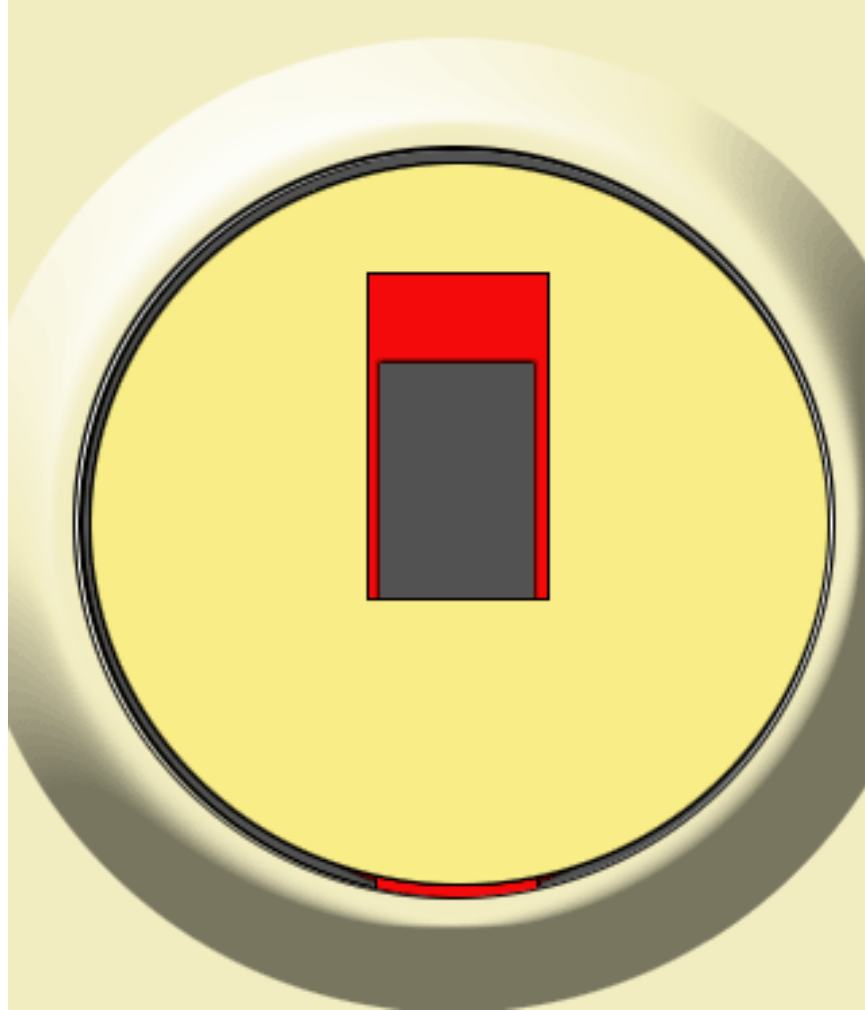
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. **Other everyday designs are often weak, too**

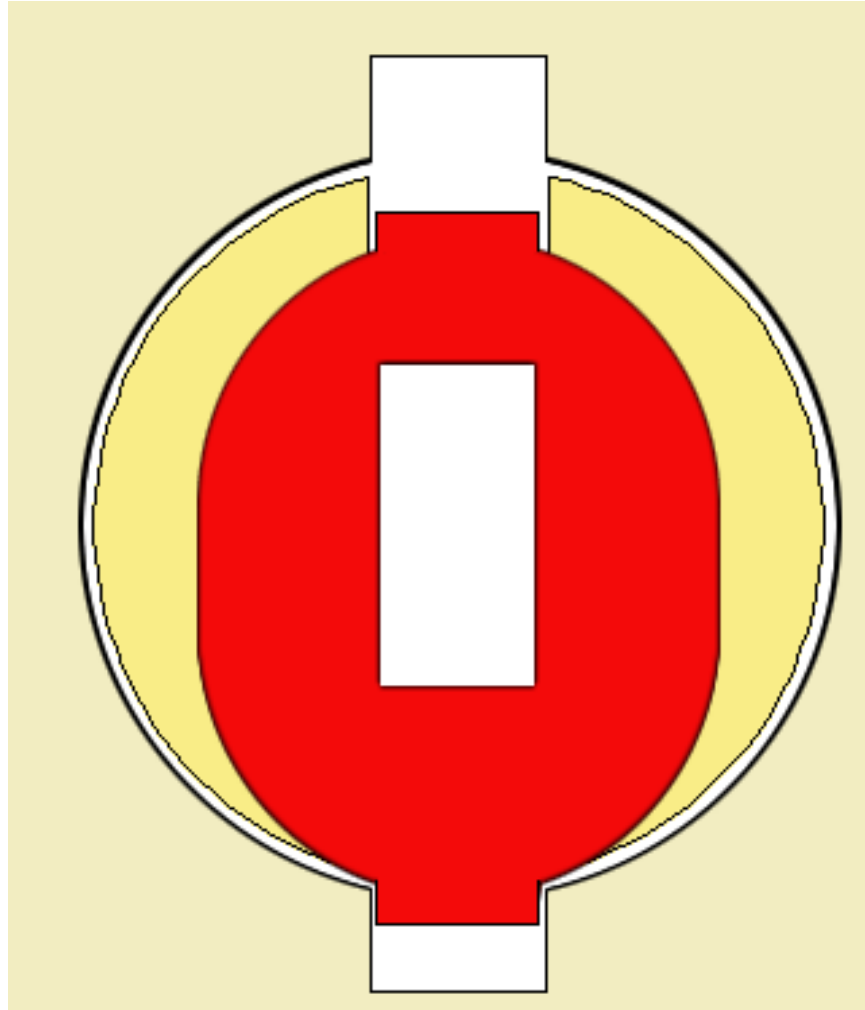
Wafer Locks



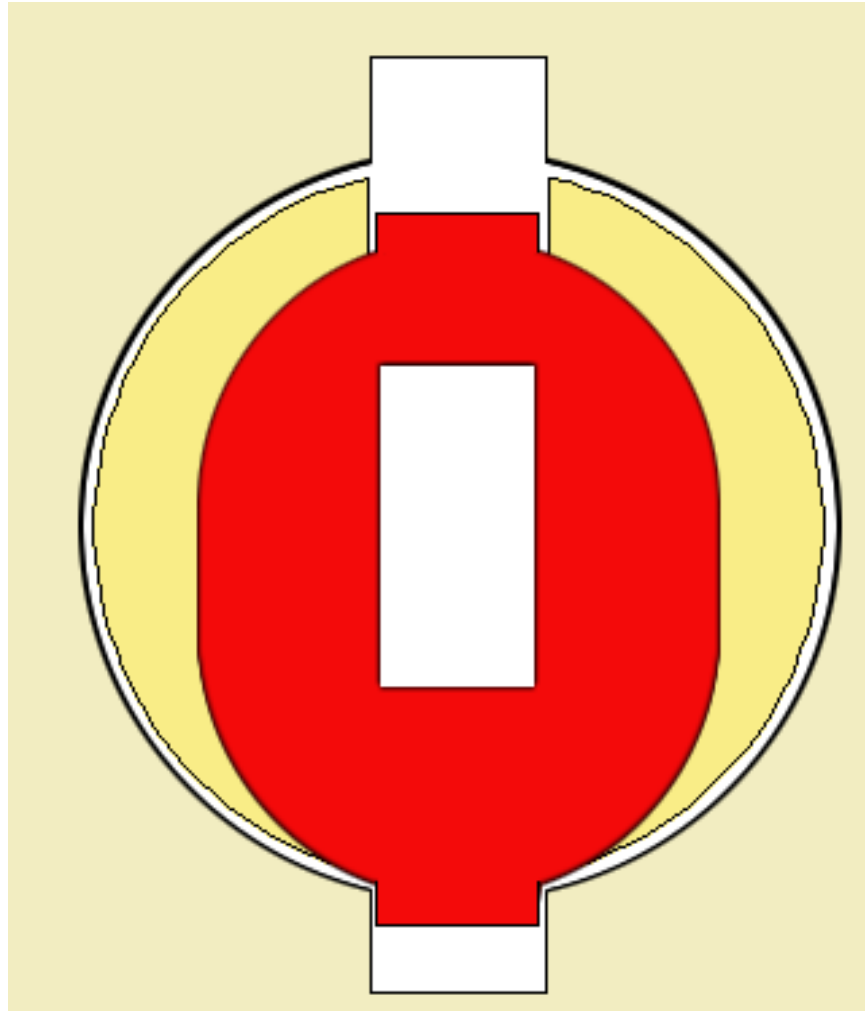
Wafer Locks



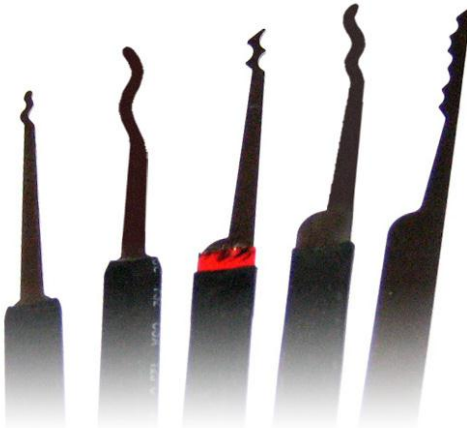
Wafer Locks



Wafer Locks



Raking & Jiggling



Wafer Lock Usage



Wafer Lock Usage



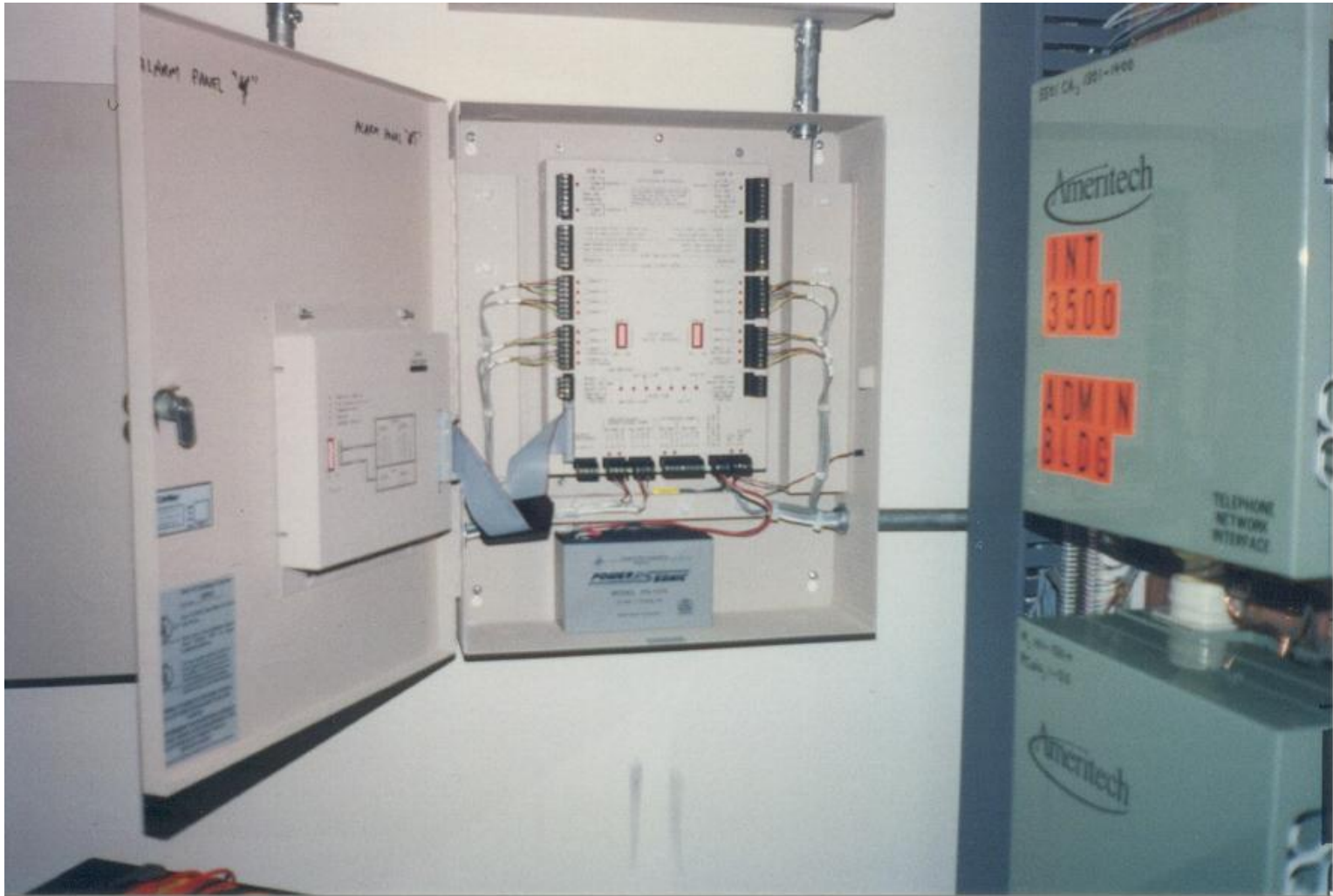
Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



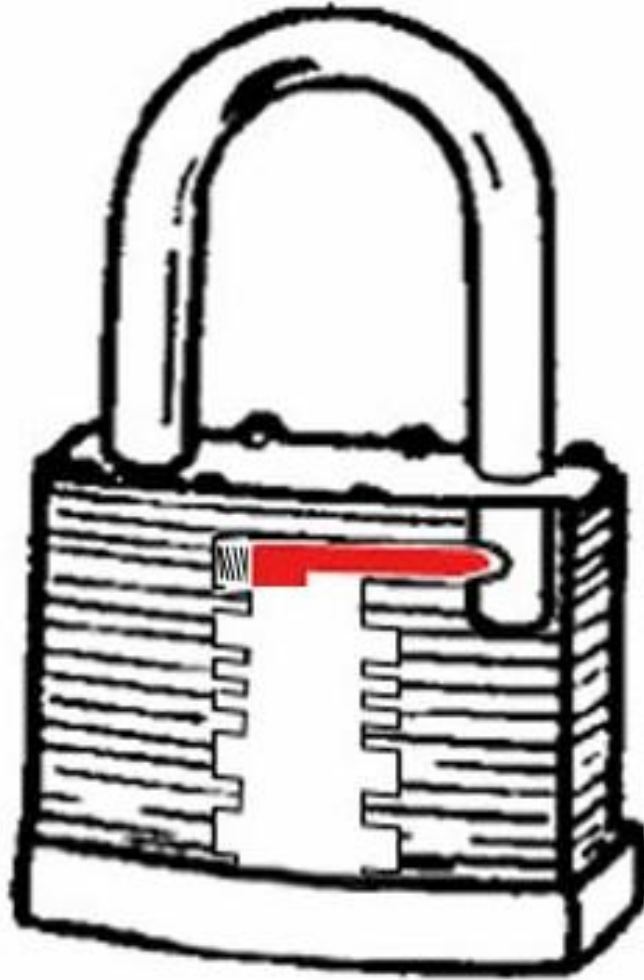
Wafer Lock Usage



Warded Locks



Warded Locks



Warded Locks



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Warded Lock Usage



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings

Popular Padlocks



Terrible Padlocks



Padlock Shims



Padlock Shims... From a Catalog



Padlock Shims... From a Beer Can



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shims



Padlock Shim Prevention

Double Ball Mechanism



Padlock Shim Prevention

Which Padlocks are Protected?



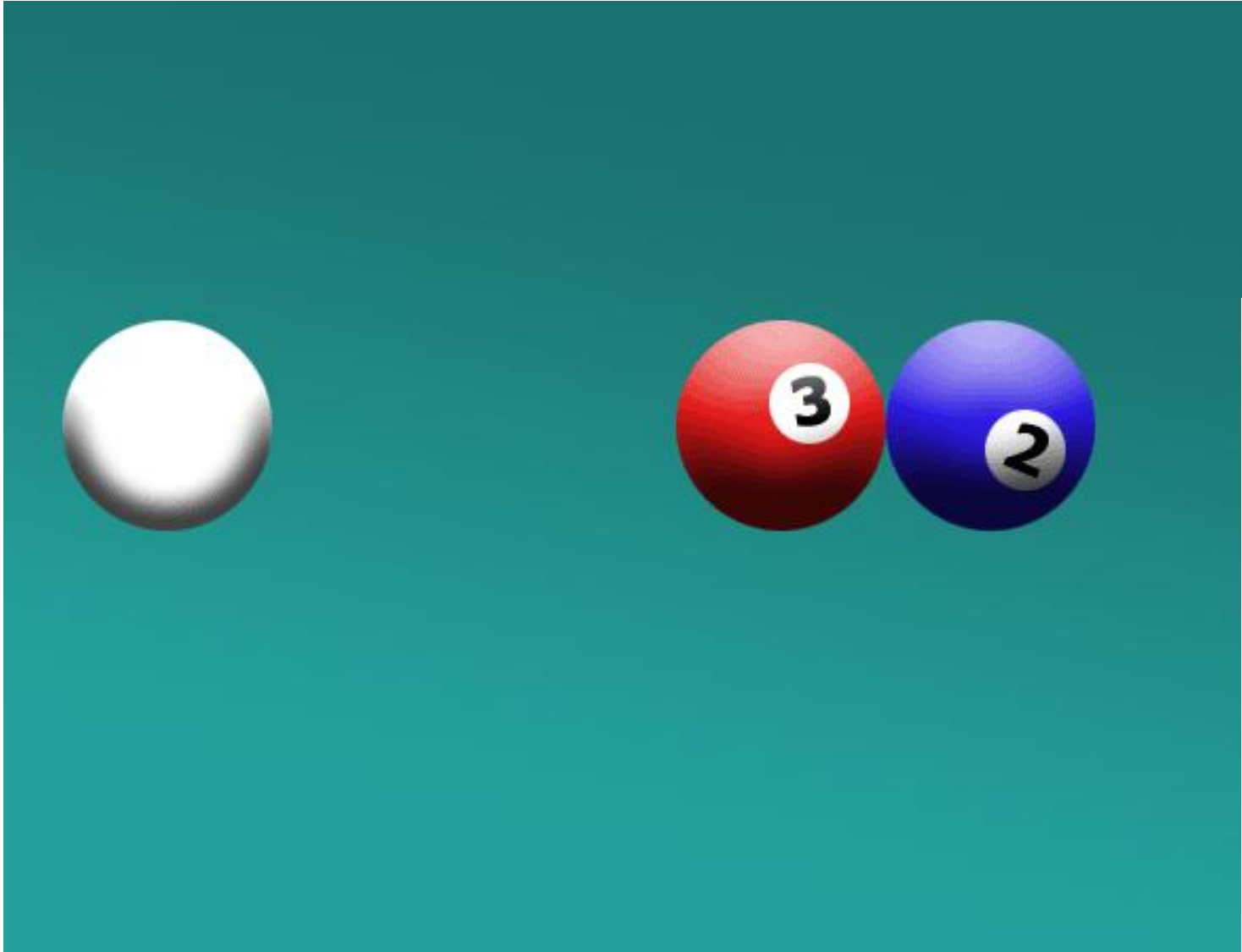
Padlock Shim Prevention



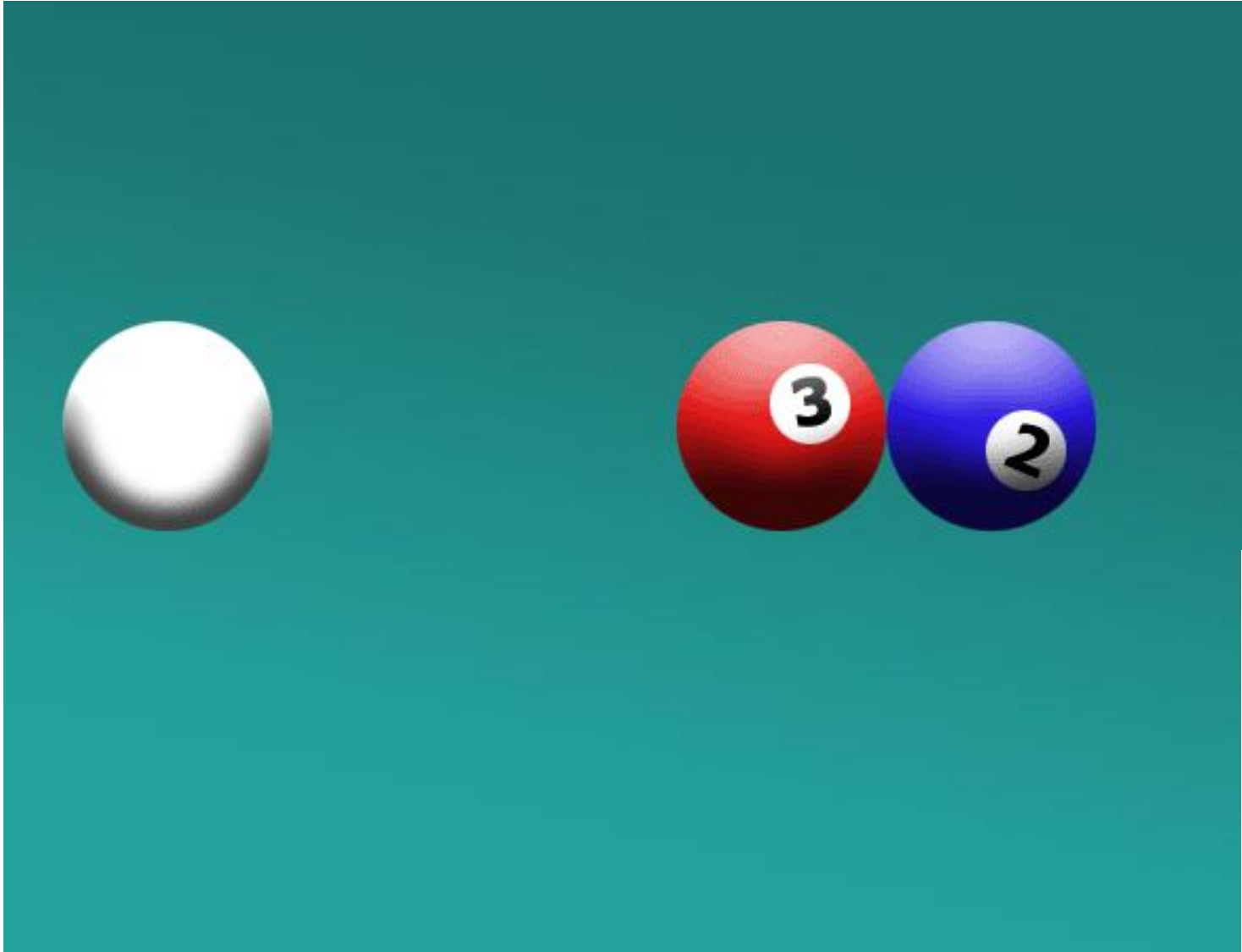
Padlock Shim Prevention



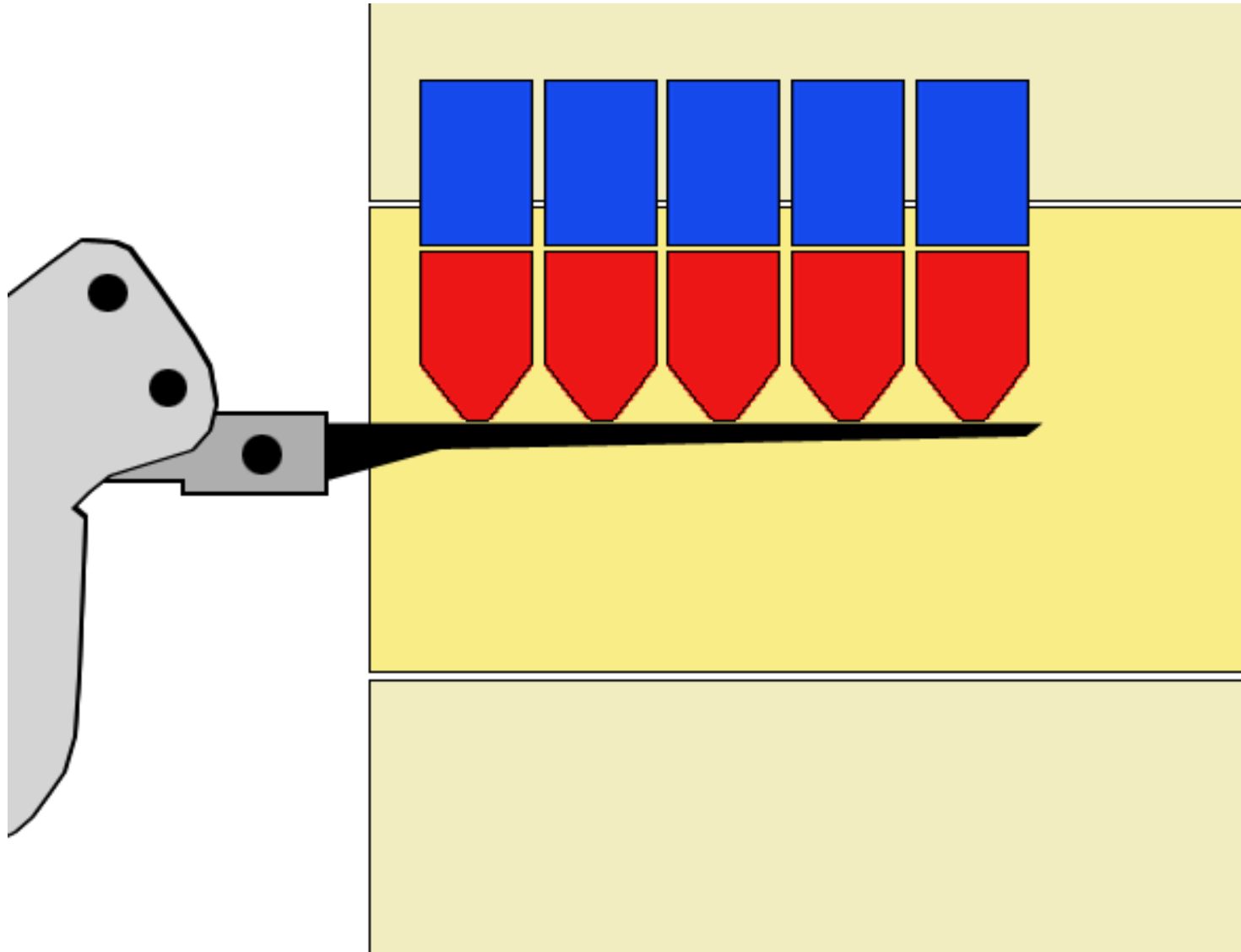
Bumping



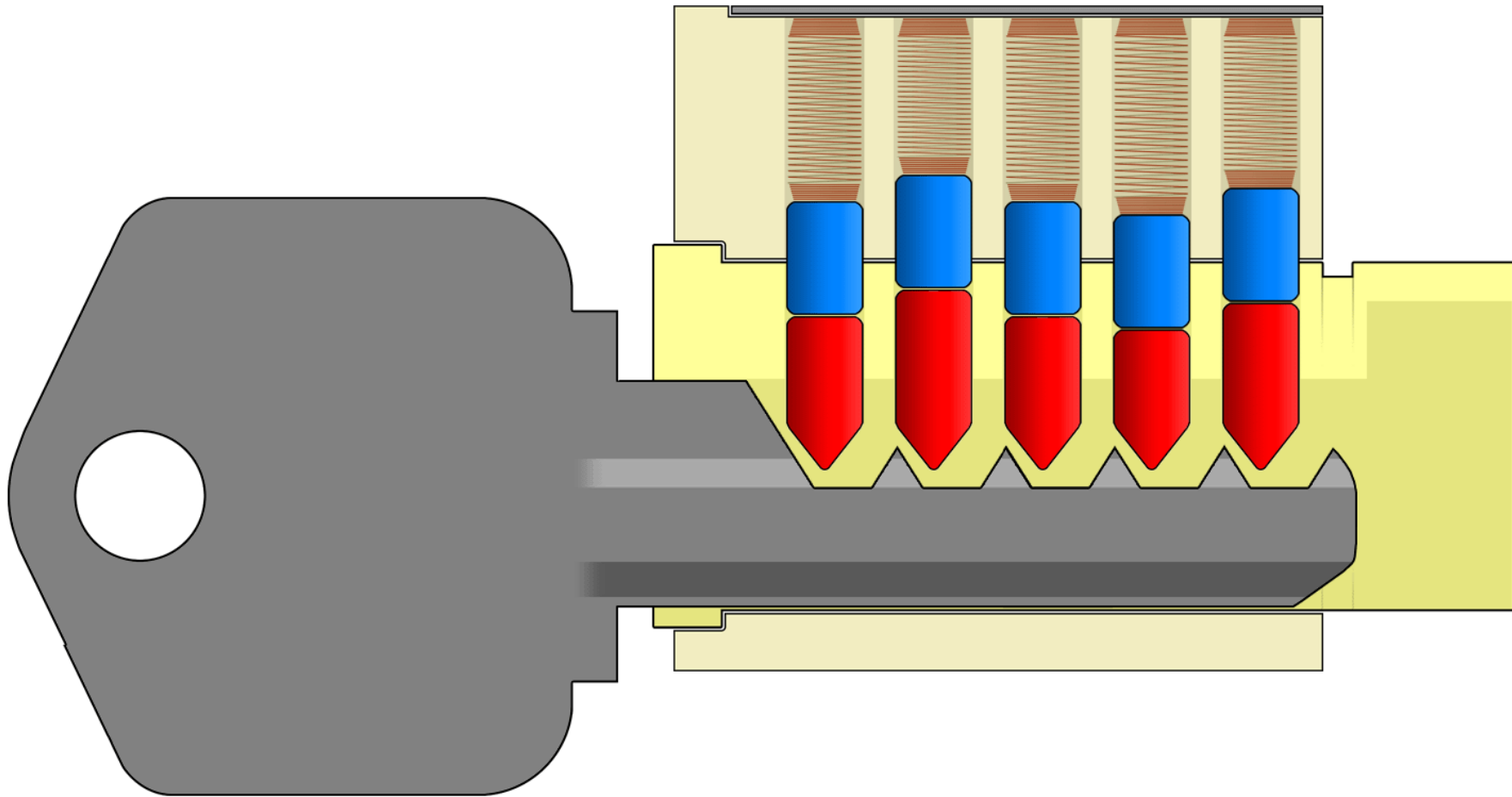
Bumping



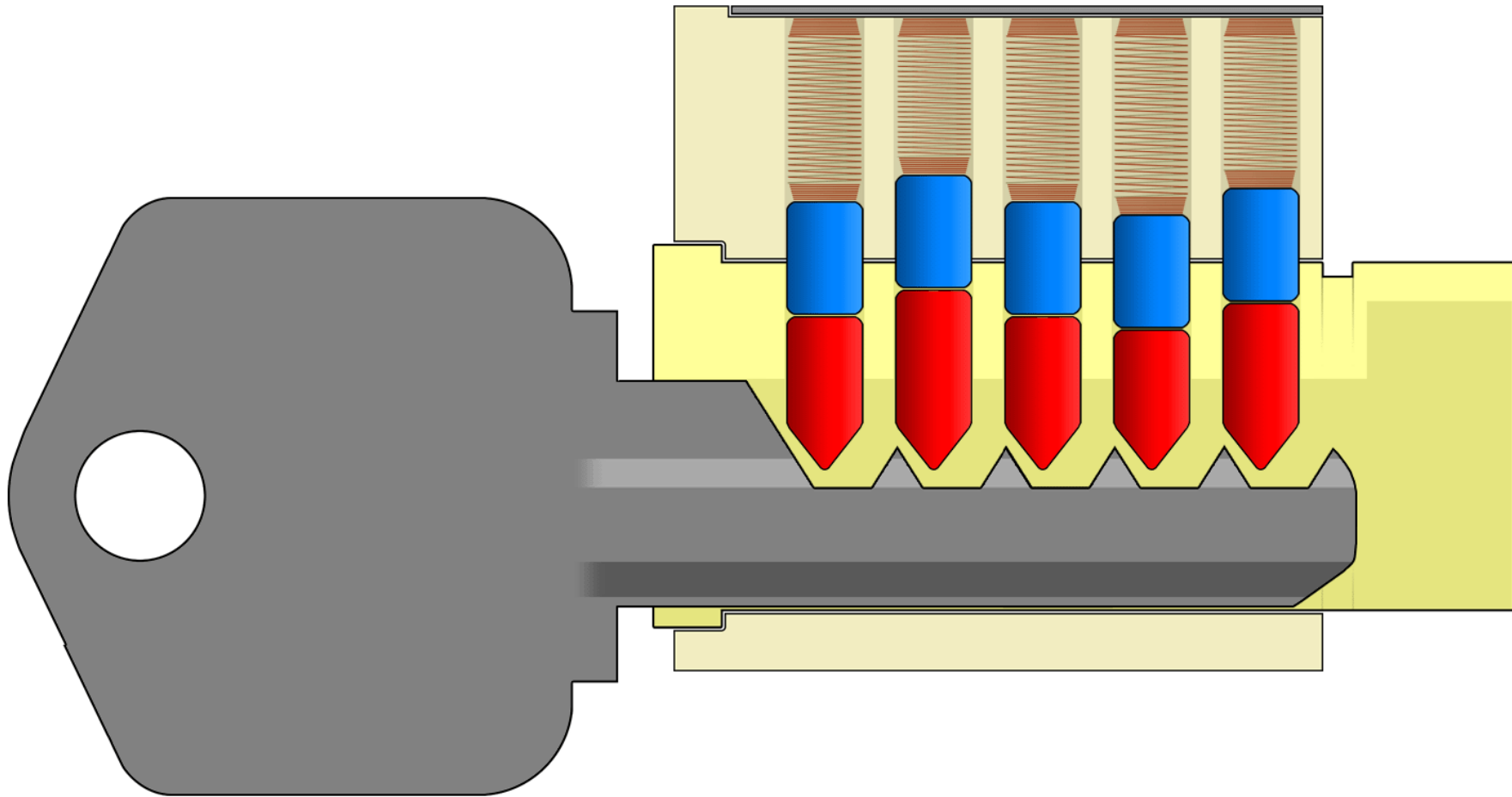
Bumping



Bumping



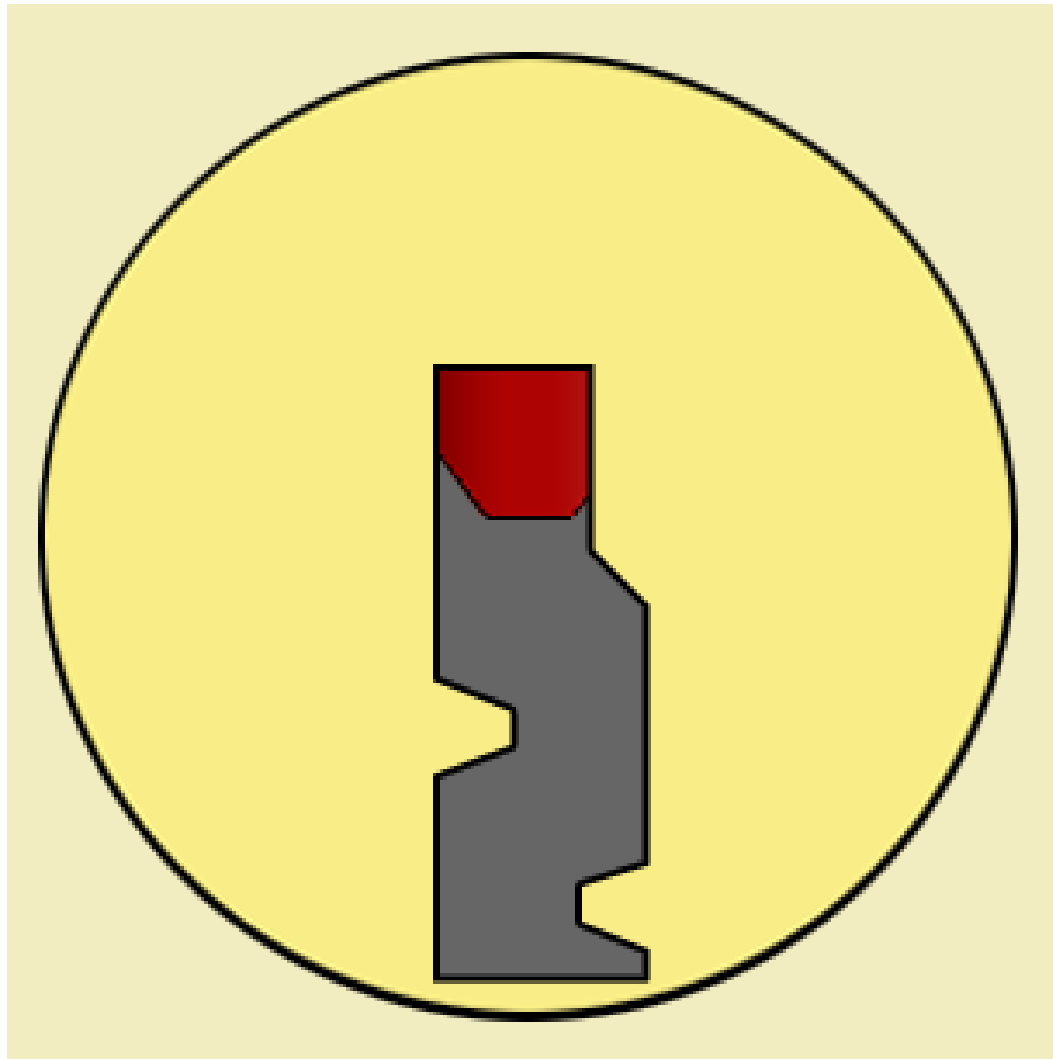
Bumping



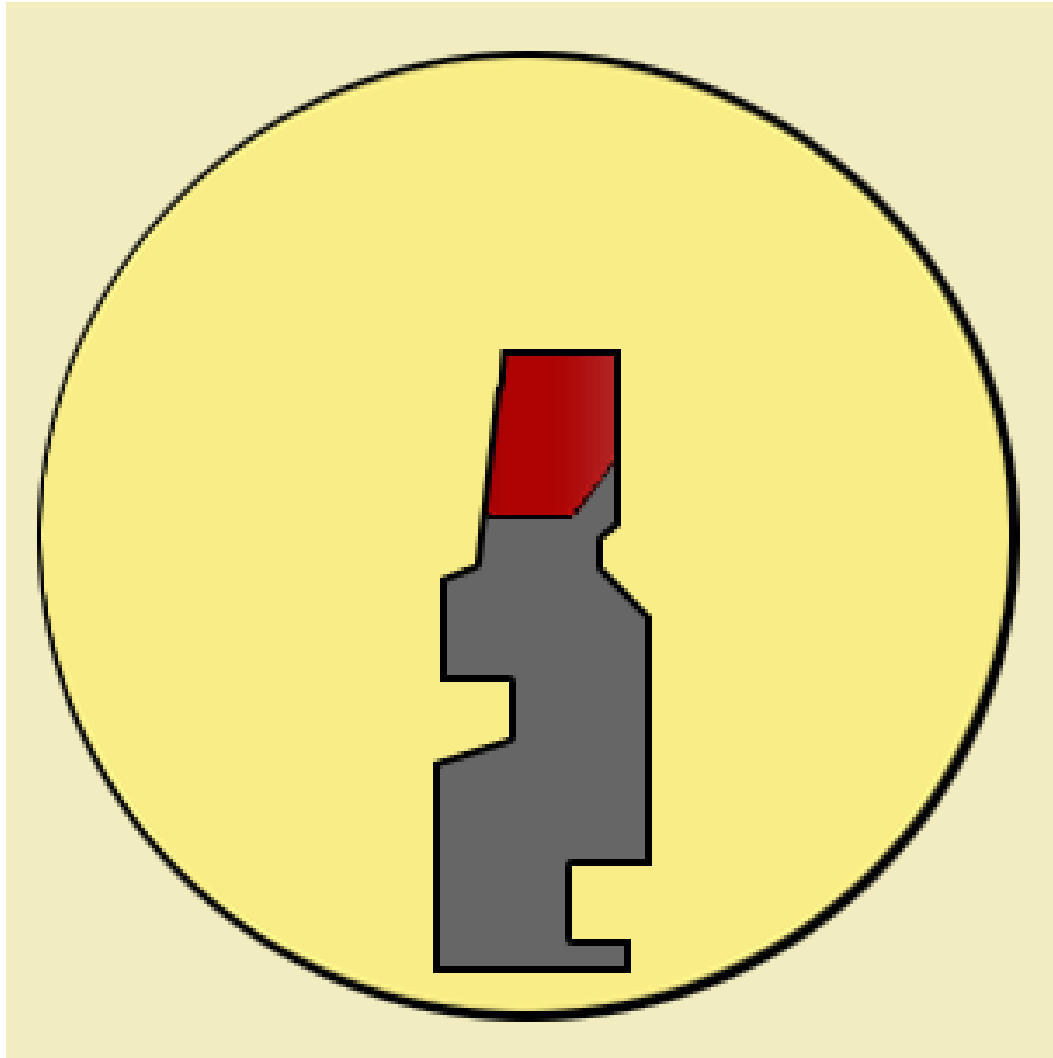
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
- 7. Many locks are pick resistant**

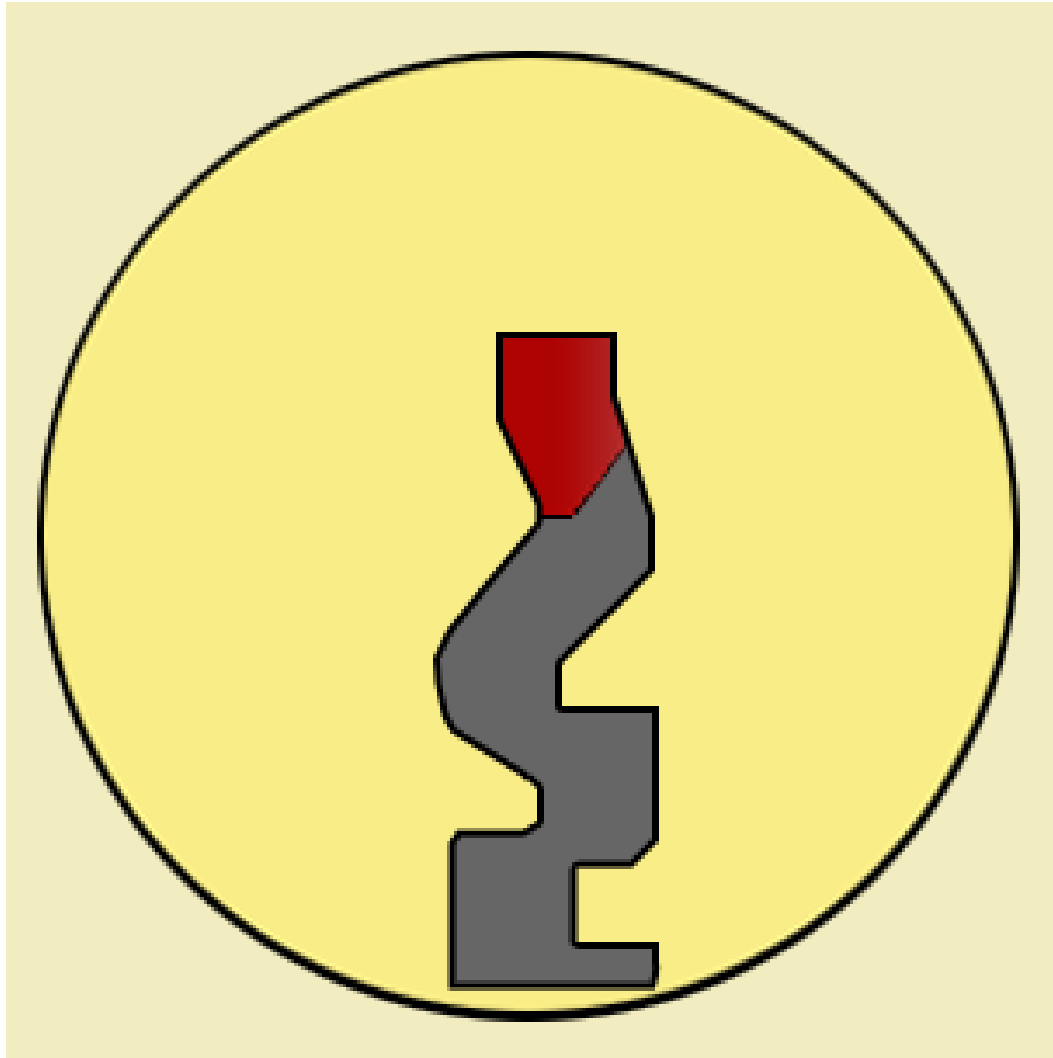
Pick-Resistant Keyways



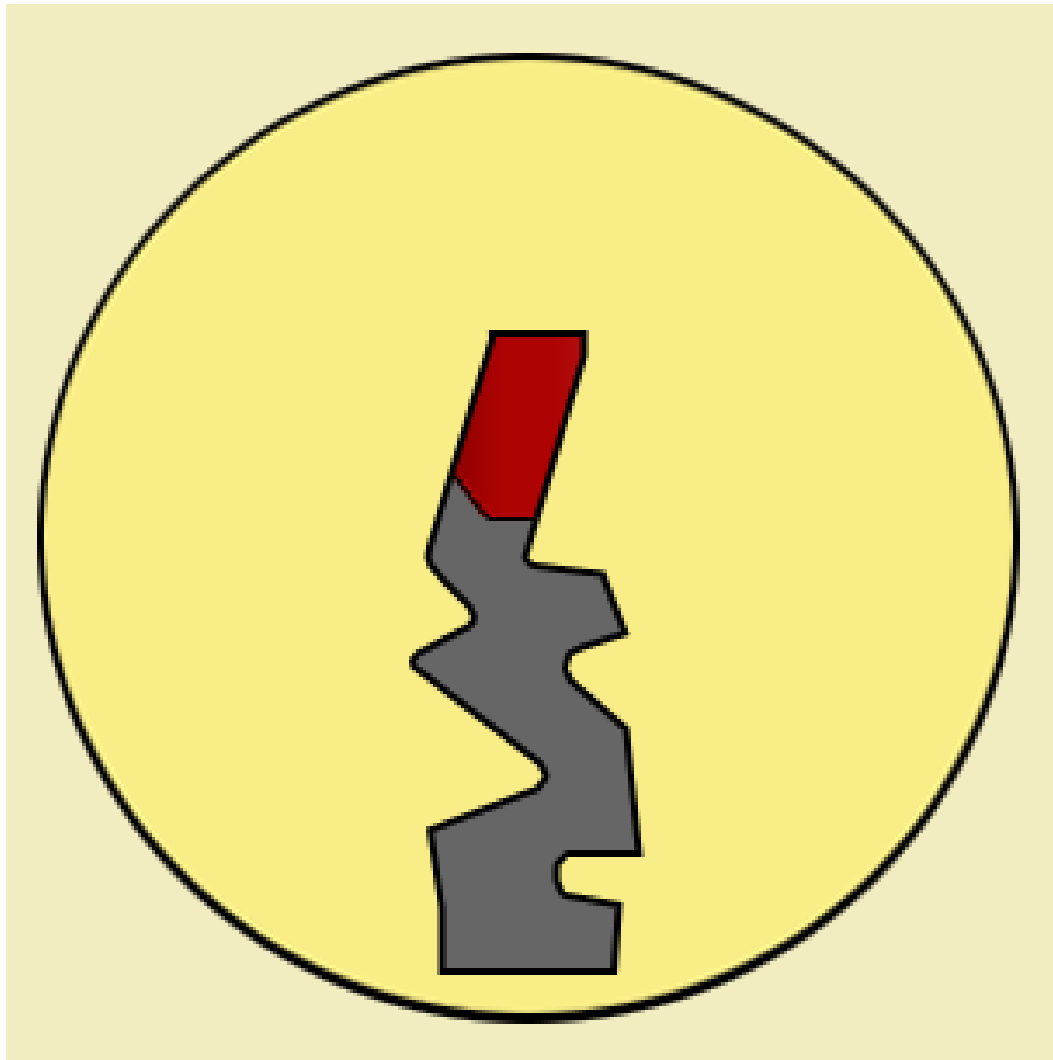
Pick-Resistant Keyways



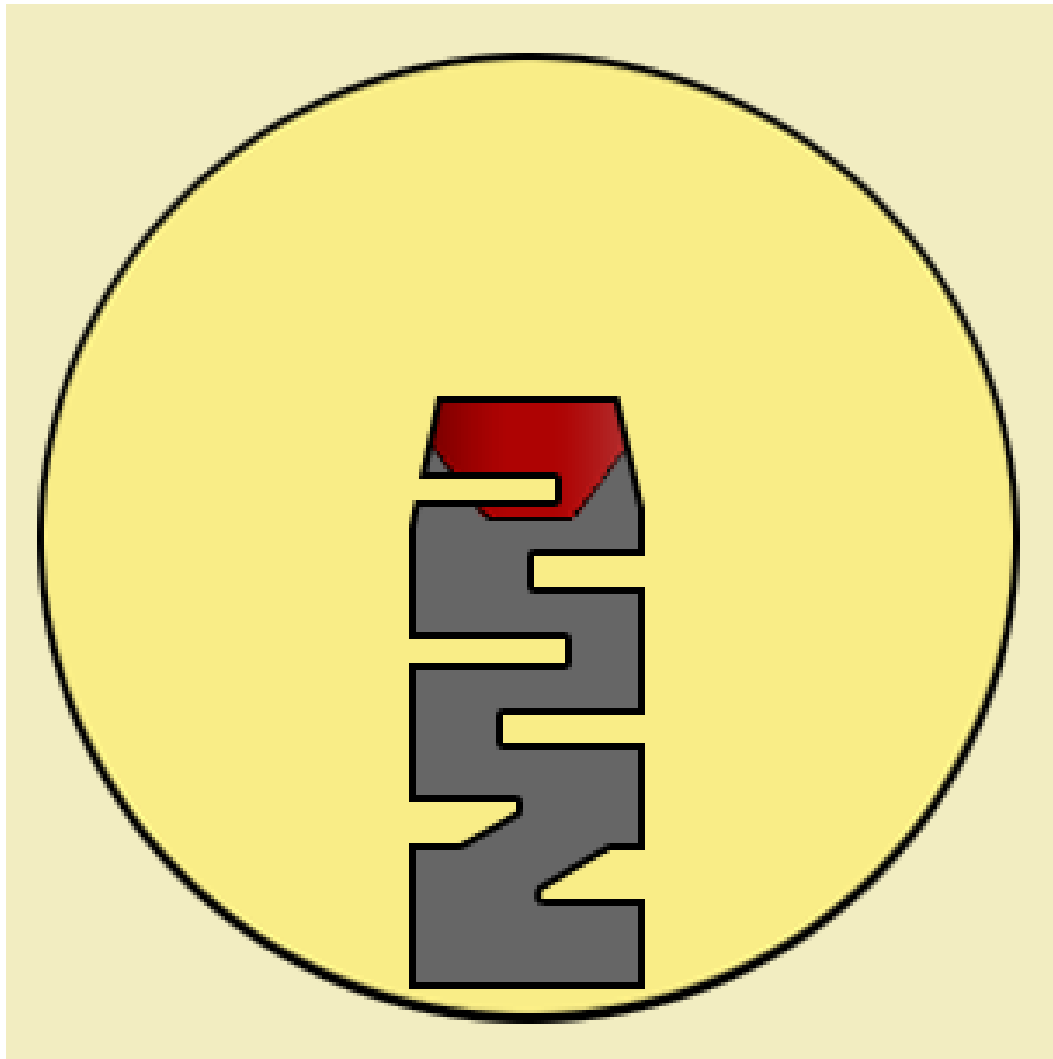
Pick-Resistant Keyways



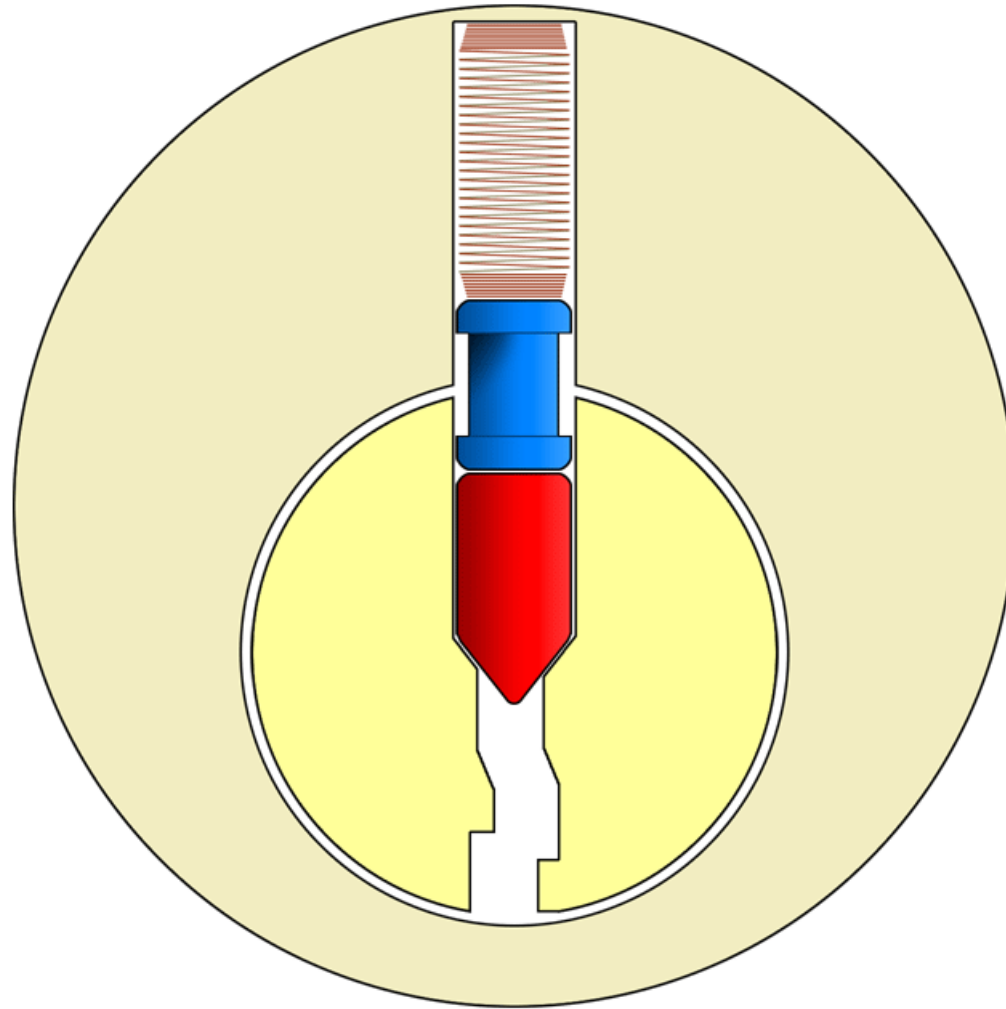
Pick-Resistant Keyways



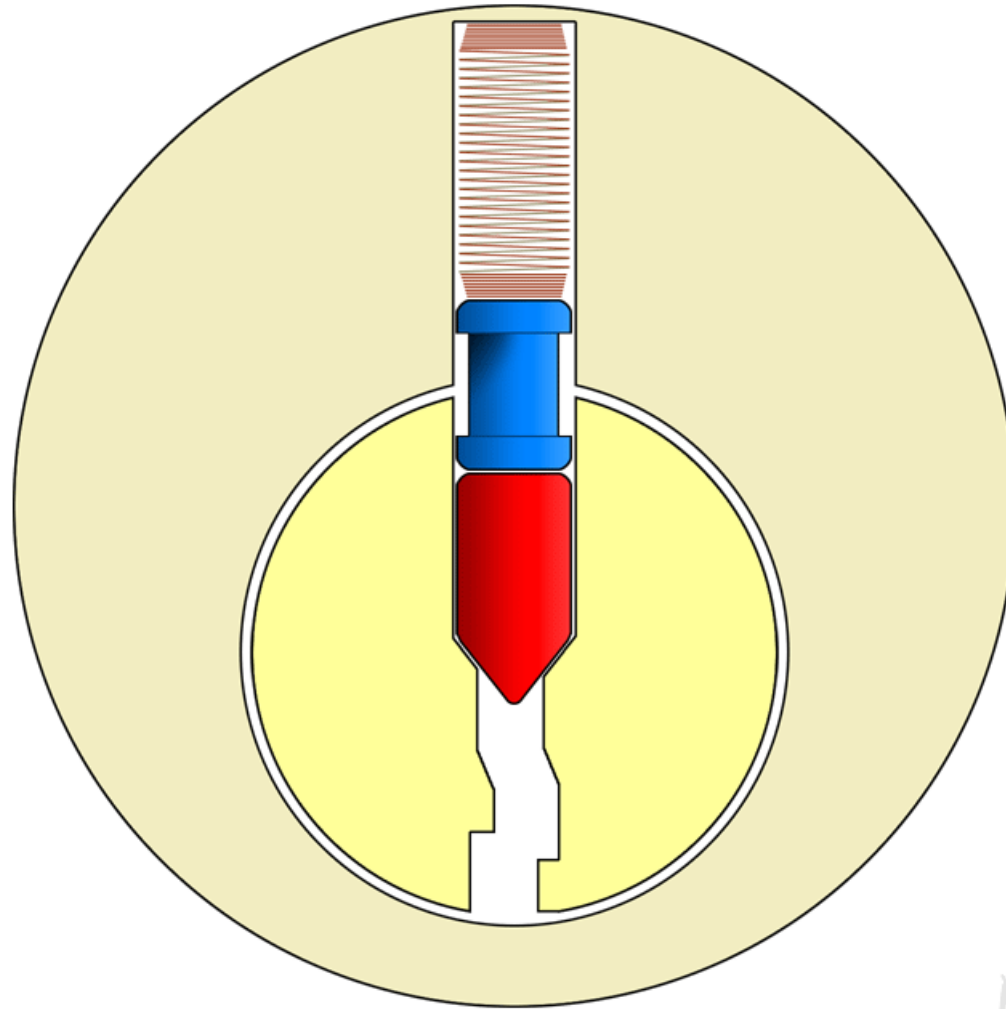
Pick-Resistant Keyways



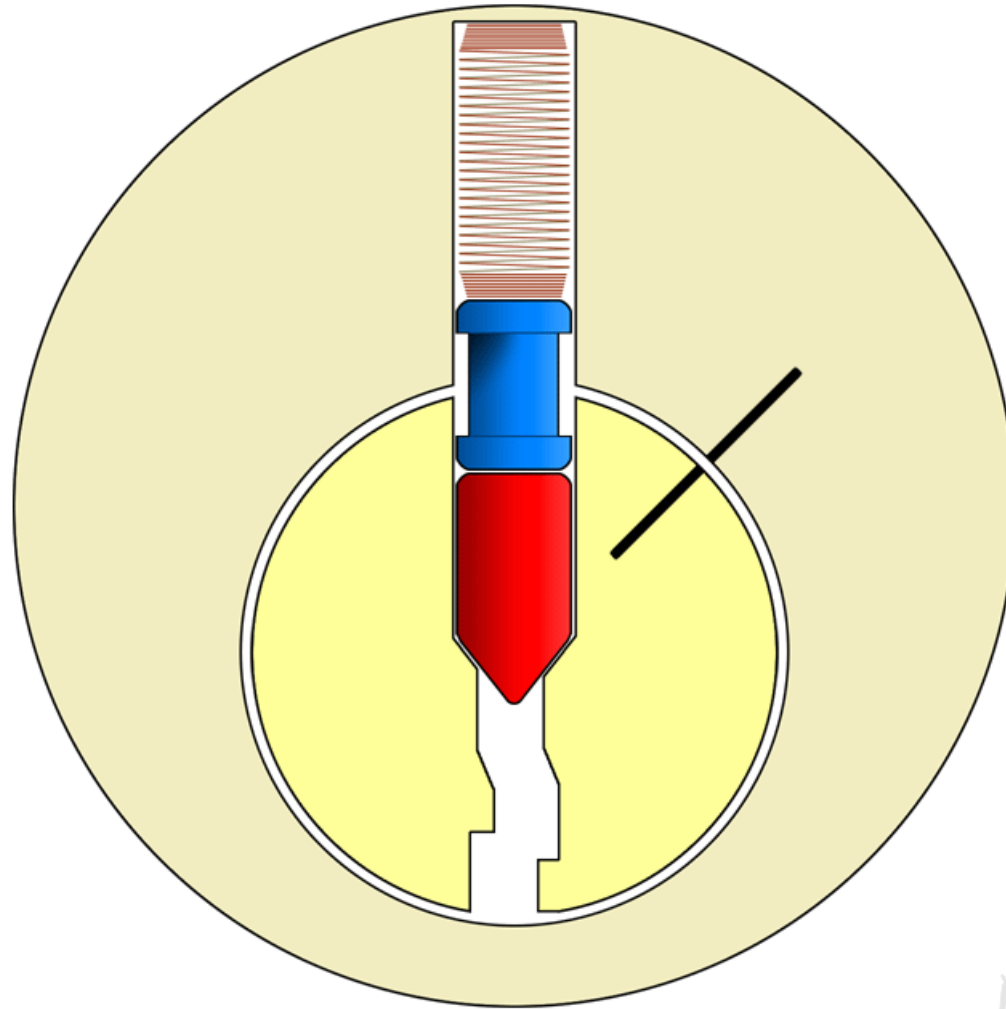
Pick-Resistant Pins



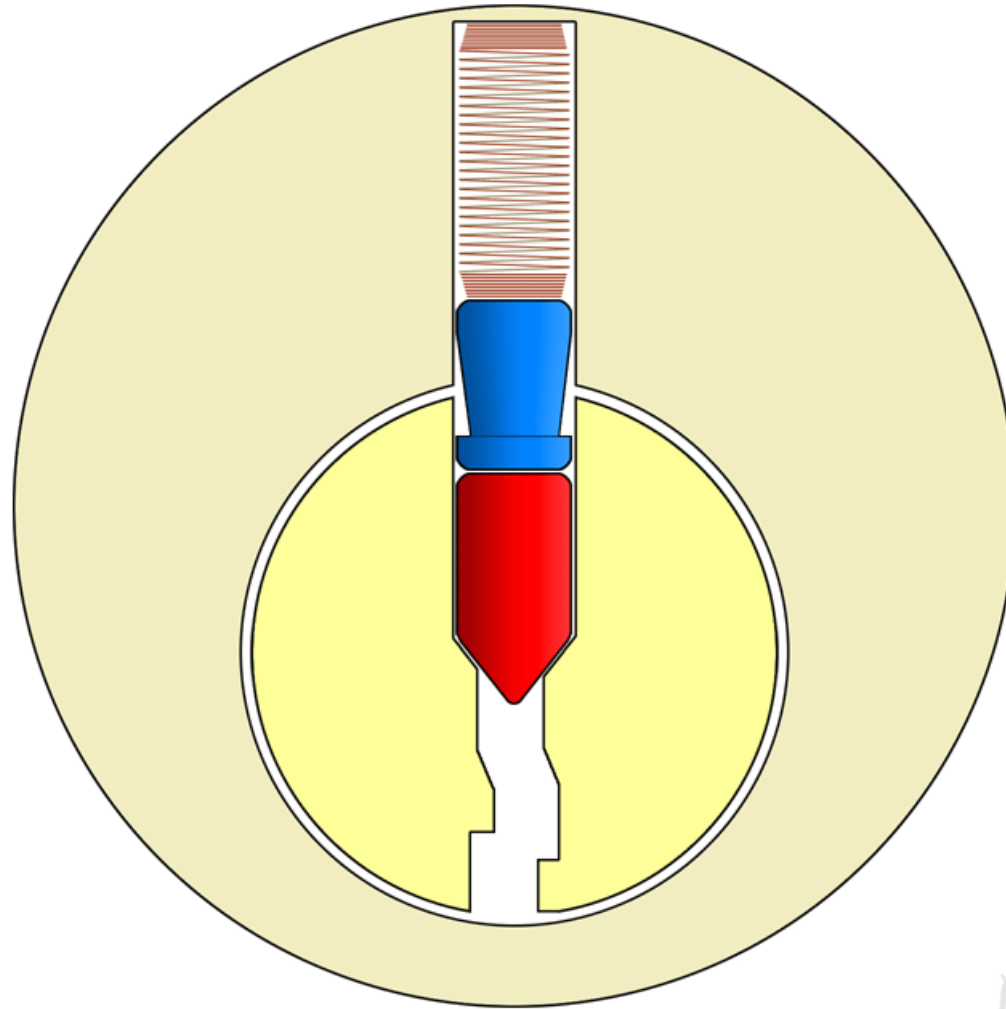
Pick-Resistant Pins



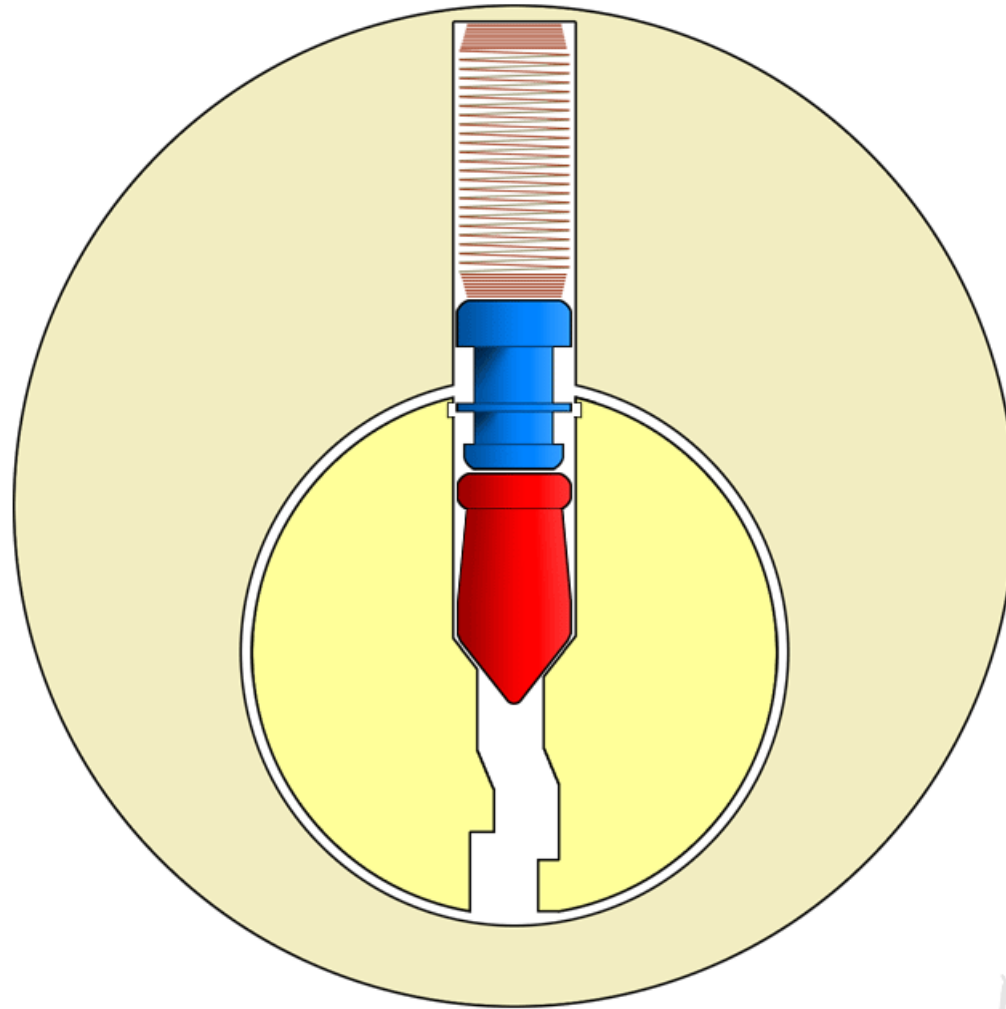
Pick-Resistant Pins



Pick-Resistant Pins



Pick-Resistant Pins

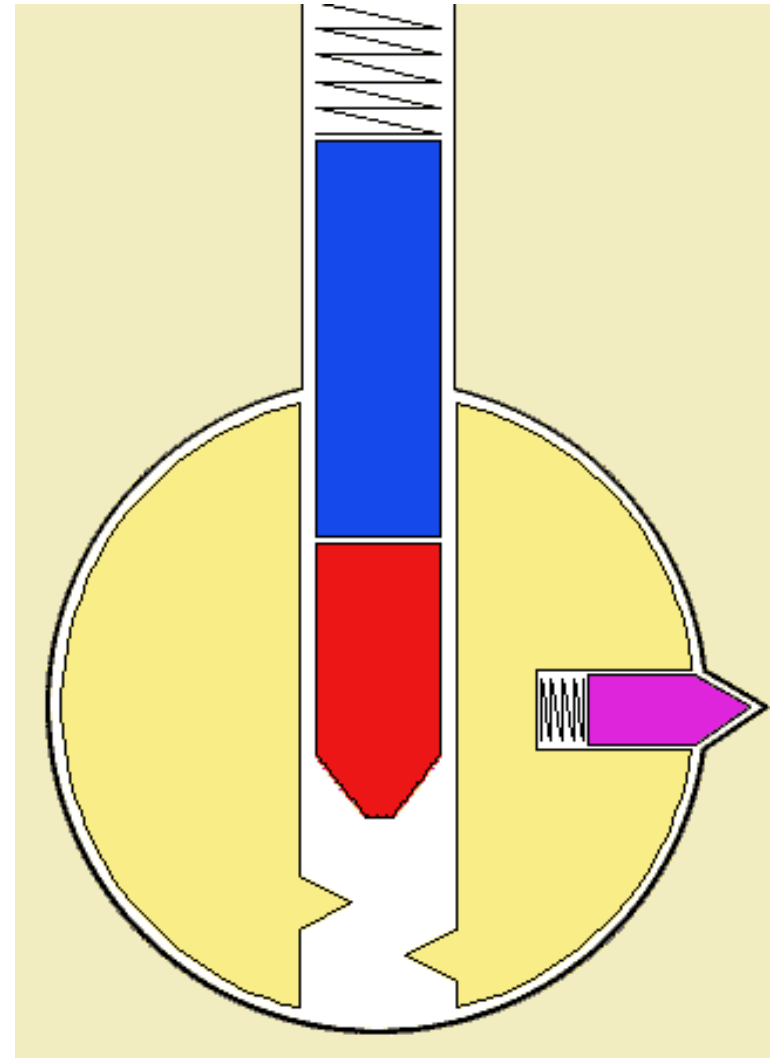


Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
- 8. Some locks are wickedly secure**

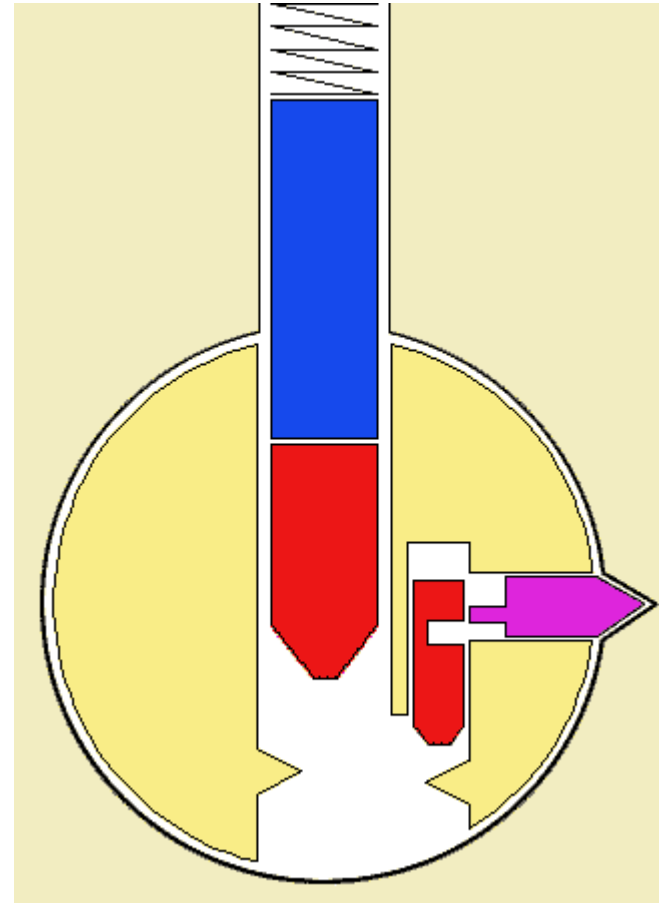
Side Bars

- Similar to side pins
- Restrict plug movement
- Harder to pick than pin stacks



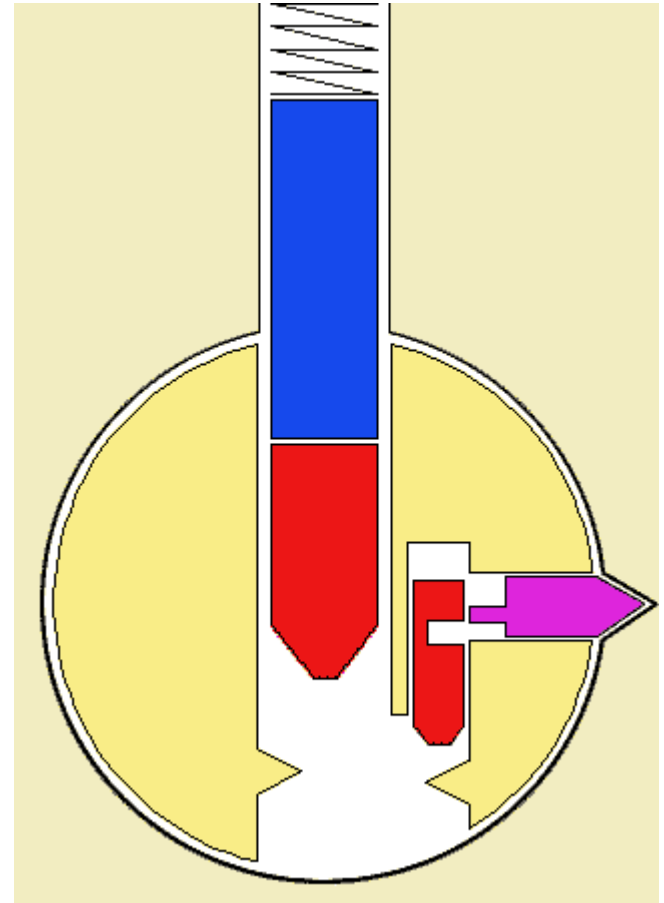
Side Bars

Finger Pins



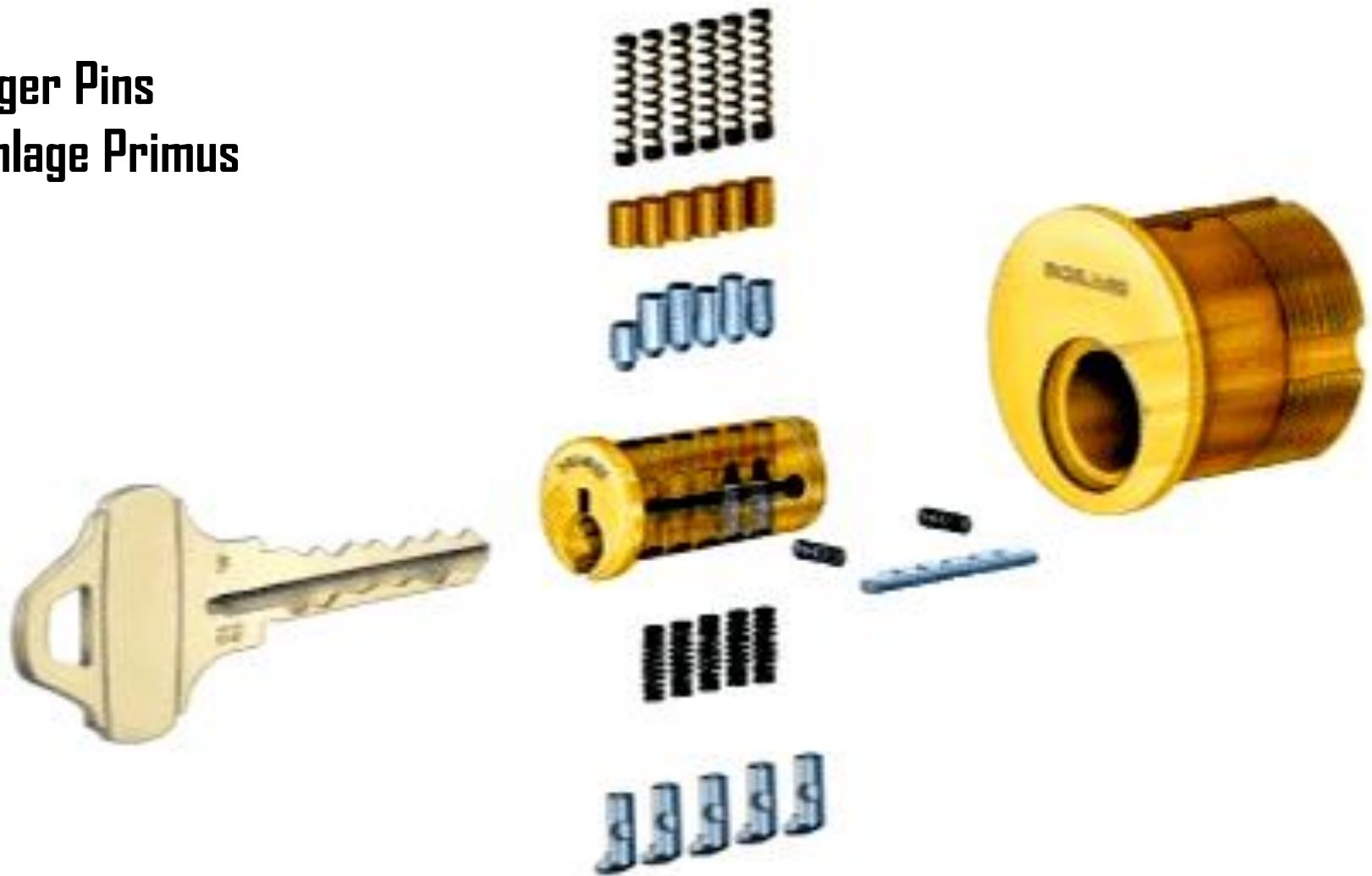
Side Bars

Finger Pins



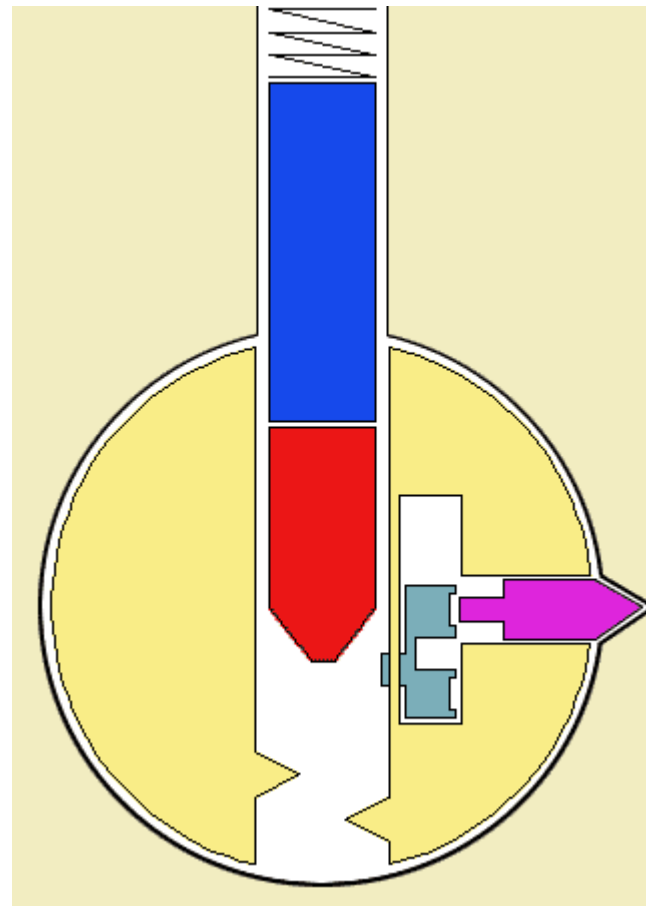
Side Bars

Finger Pins
Schlage Primus



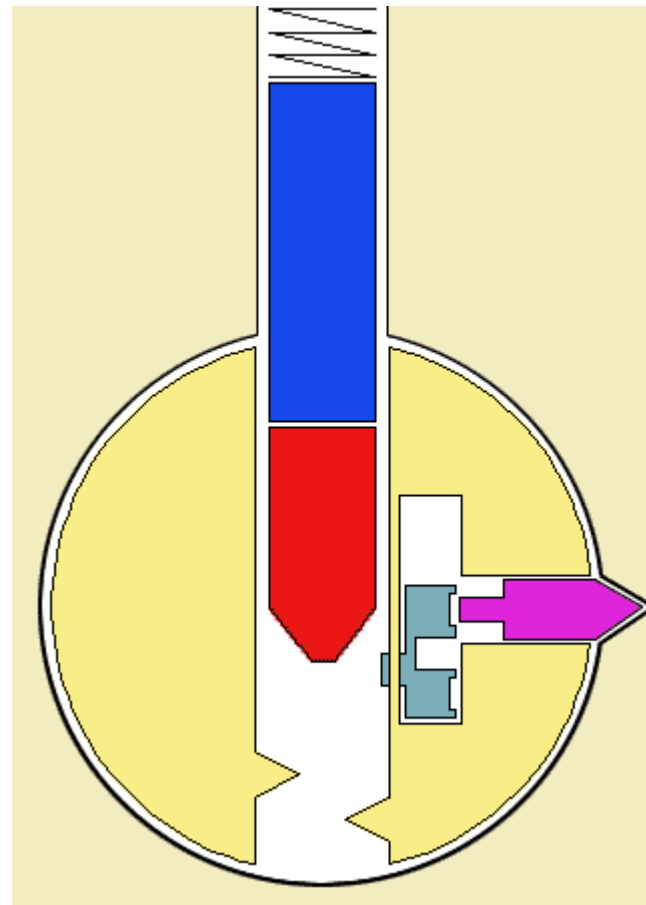
Side Bars

Sliders



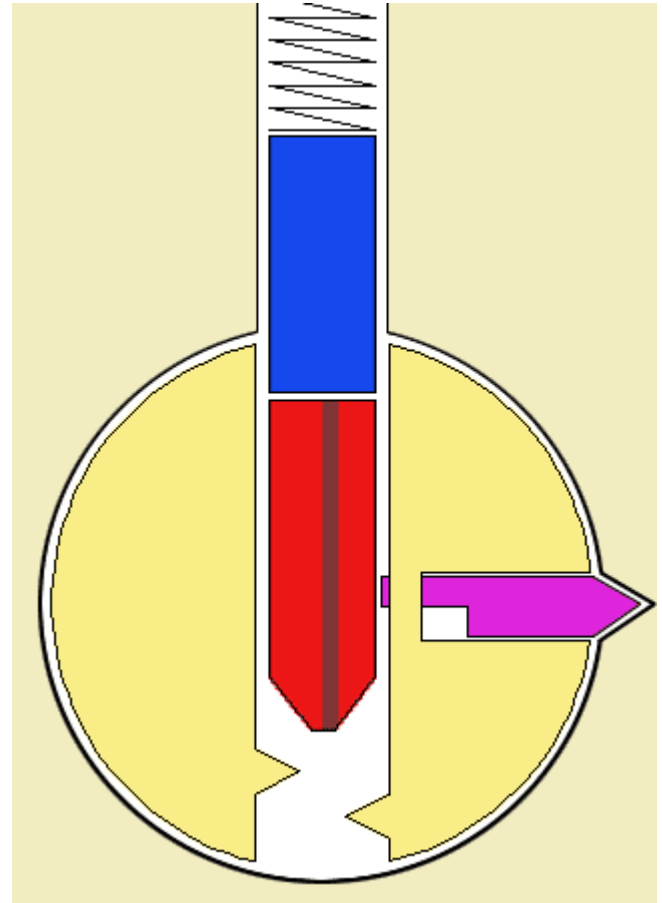
Side Bars

Sliders



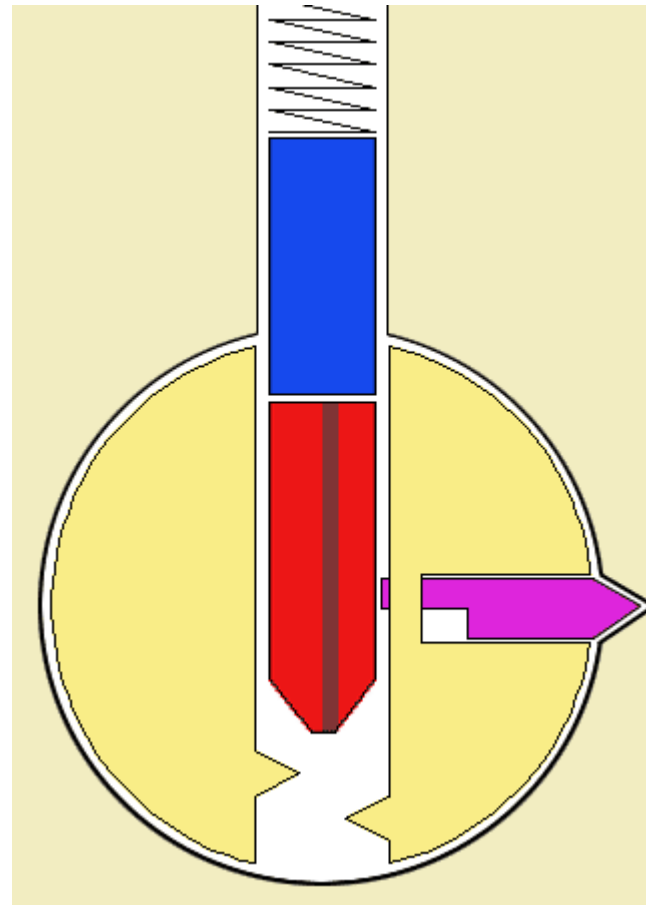
Side Bars

Rotating Pins



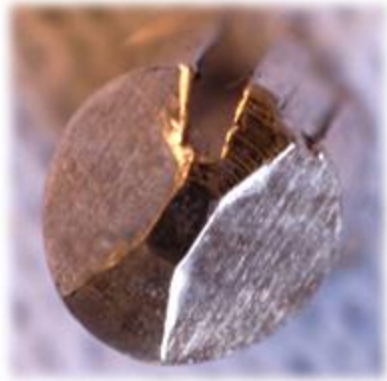
Side Bars

Rotating Pins



Rotating Pins

Medeco Locks



Medeco plug exposed, key pins rotating to align sidebar cuts



Top View

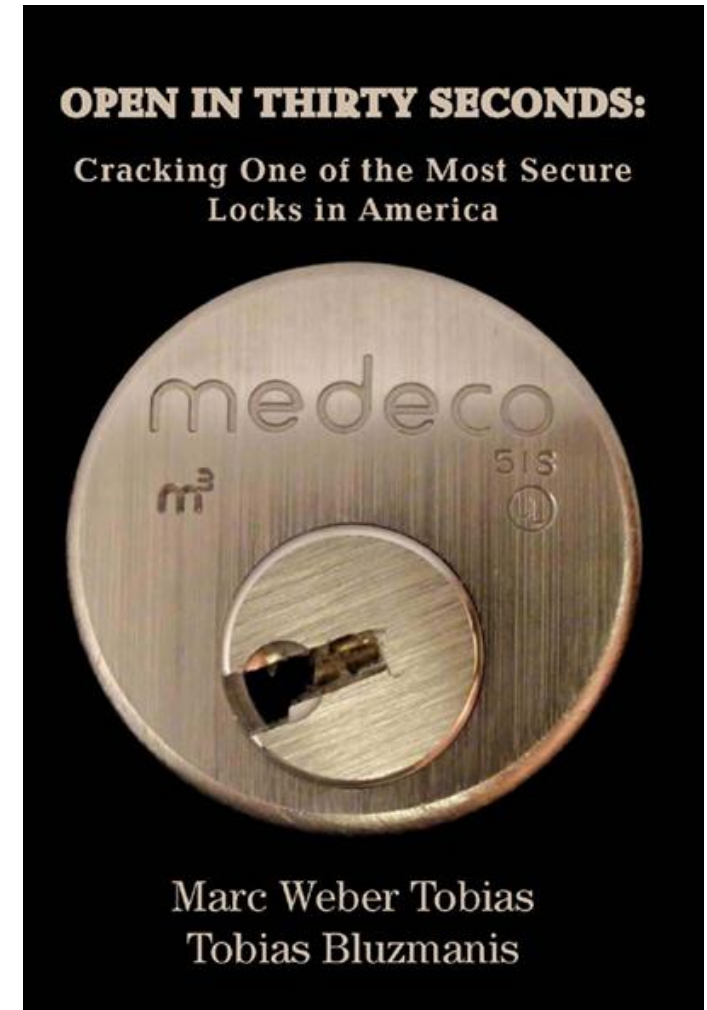


Side View

Rotating Pins

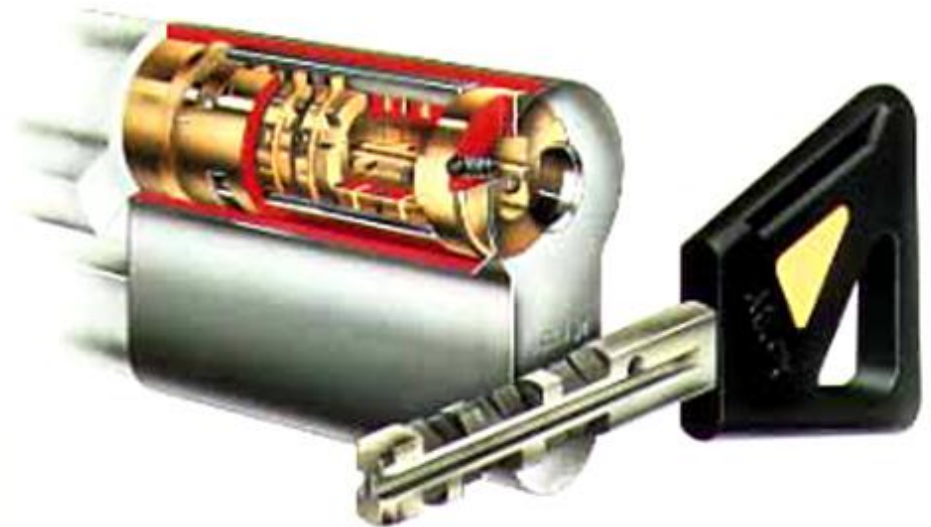
Medeco Locks Totally shot now

- Can be picked
- Can be bumped
- Numerous weaknesses
- **"Open in 30 Seconds"**
 - Marc Tobias
 - Tobias Bluzmanis



Rotating Disks

- **Tremendous Security**
 - Mimics a safe lock
- **Very Difficult To Pick**
 - Takes much time and great skill
 - Specialized tools required



Rotating Disks

- **Tremendous Security**
 - Mimics a safe lock
- **Very Difficult To Pick**
 - Takes much time and great skill
 - Specialized tools required
- **Two-in-One Tool**
 - Manipulates disks individually
 - Decodes cut positions



Barry Wels picking a rotating disk lock with Mike Glasser

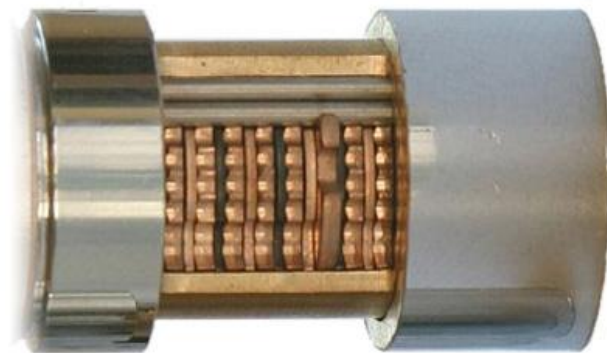
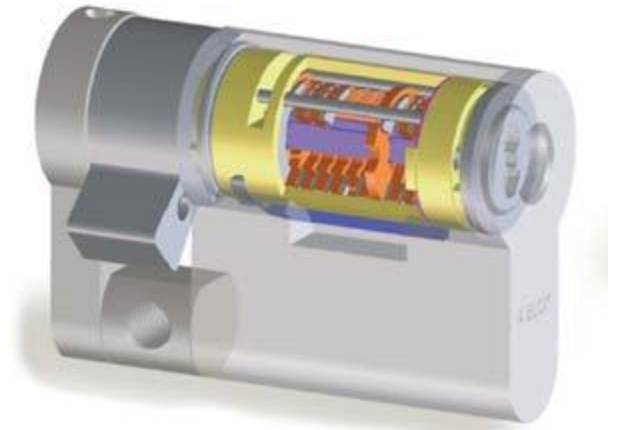
Specialized Rotating Disks

- **Abloy Protec**

- Not just rotating disks
- Disk blocking mechanism
- False cuts everywhere

- **“Unpickable?”**

- Closest I ever come to using that word
- Two-in-one tools cannot be used



Magnetic Locks

- **Miwa**

- Japanese company
- Array of magnetic pins
- Simple North / South

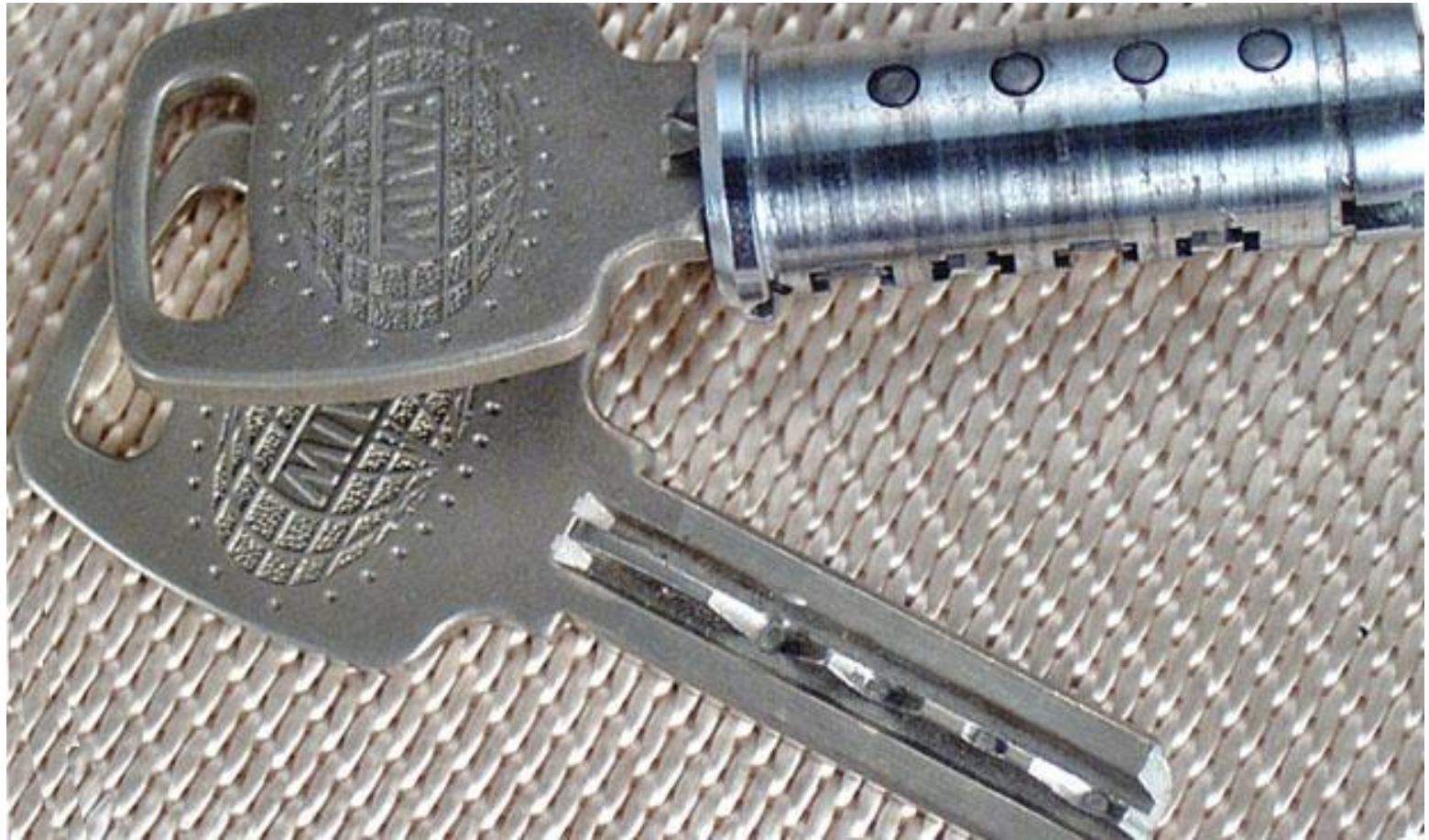


- **Evva MCS**

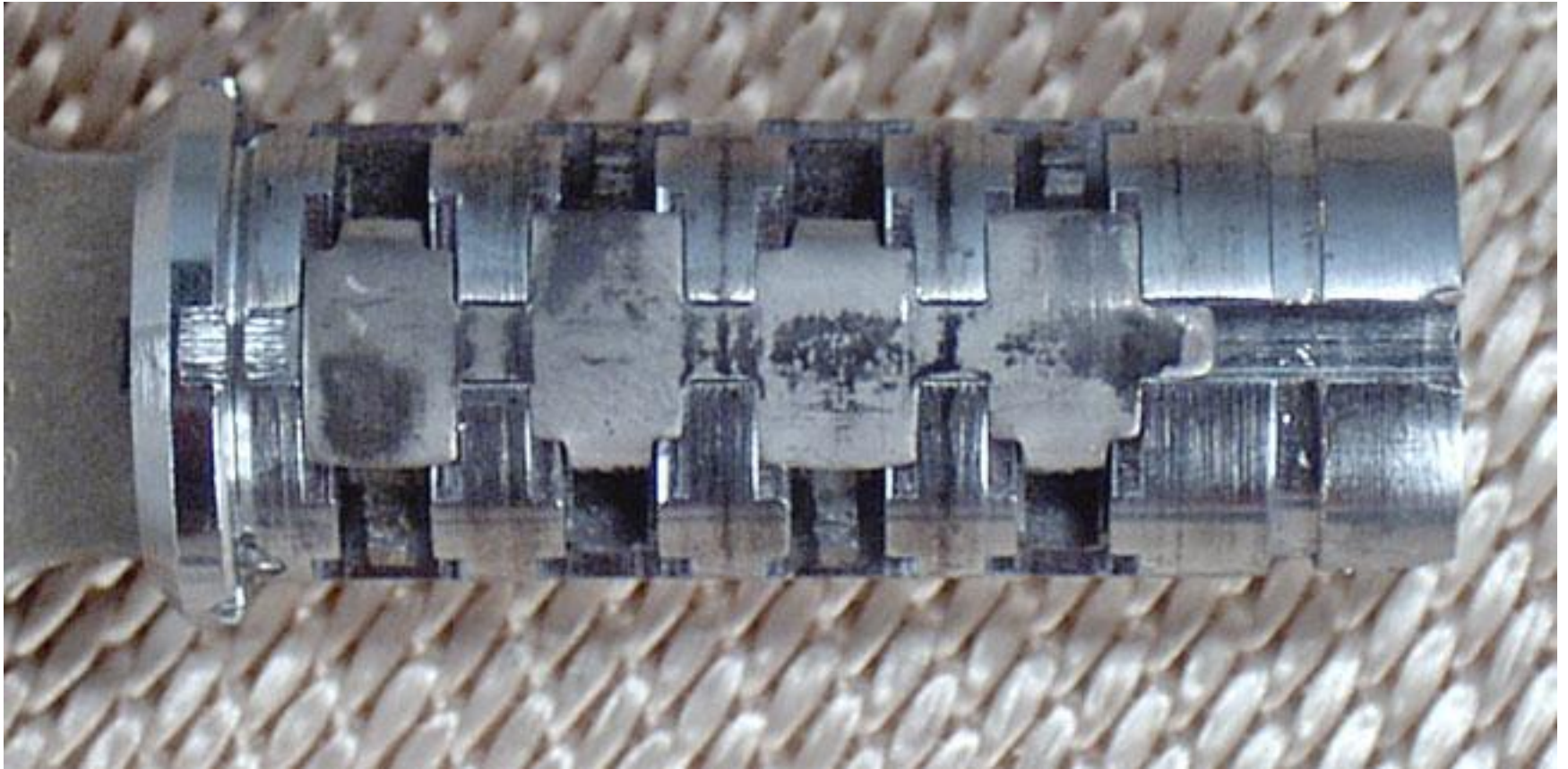
- Austrian company
- Axial-rotated magnets
- Interaction with sidebar



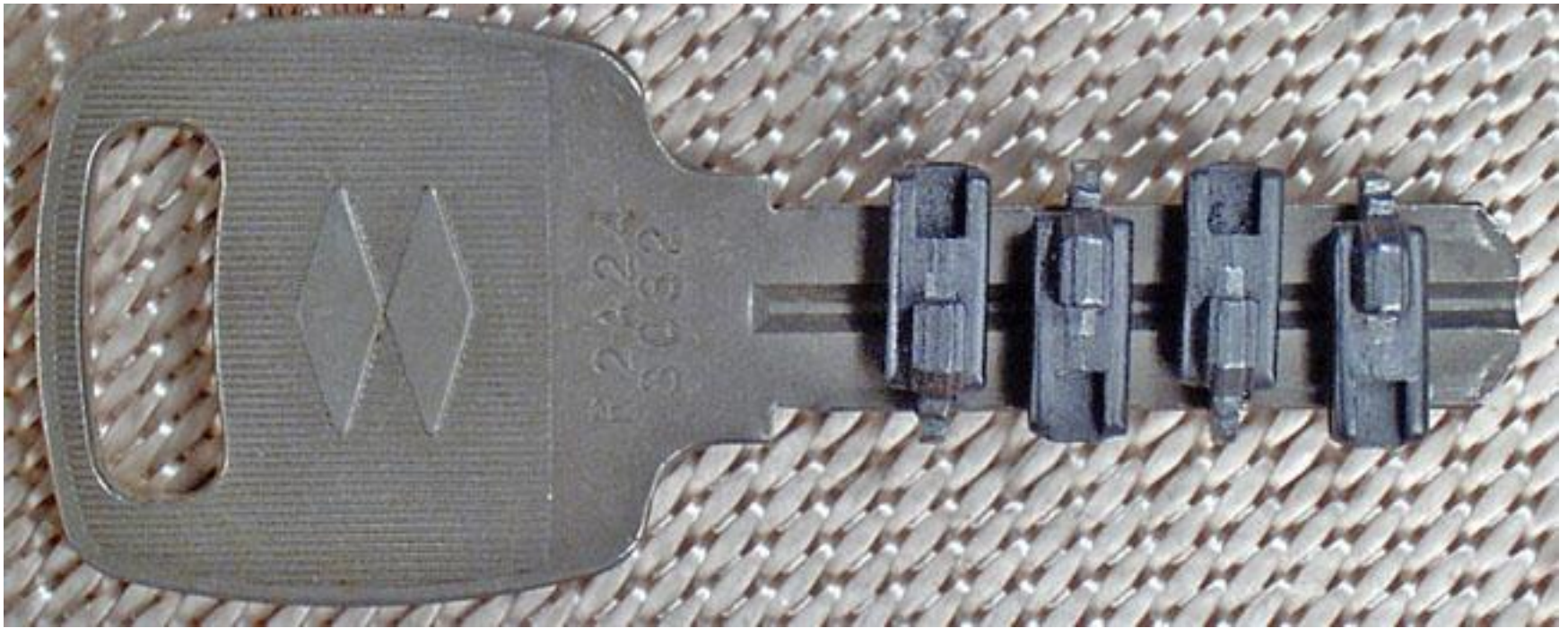
Miwa Magnetic Locks



Miwa Magnetic Locks

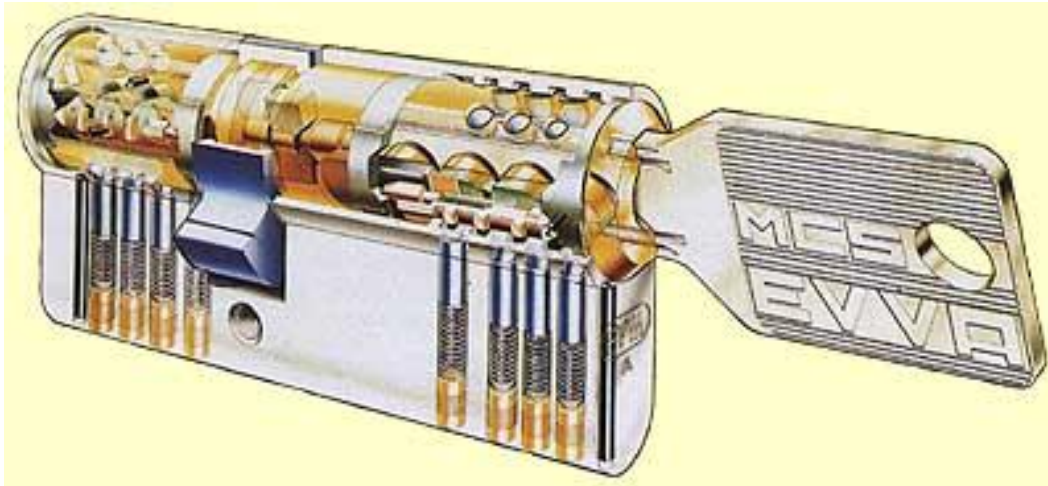


Miwa Magnetic Locks



Evva Magnetic Code System

- Possibly most duplication-resistant lock out there



Mul-T-Lock



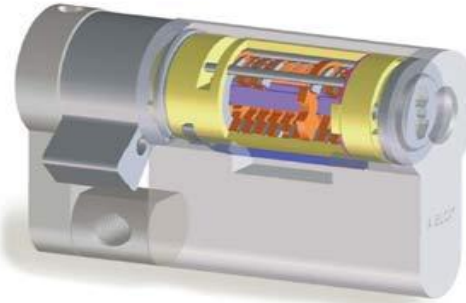
Mul-T-Lock



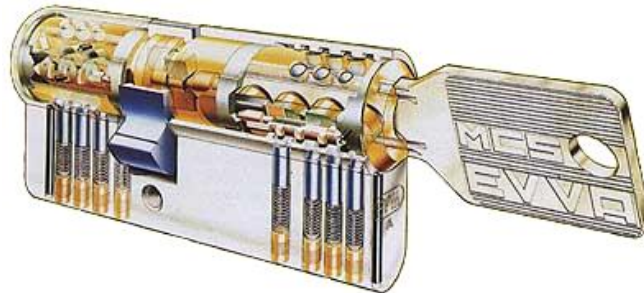
Mul-T-Lock



No Known Attack or Bypass



 **ABLOY**
Protec




MCS



 **MTS**
MULT-LOCK

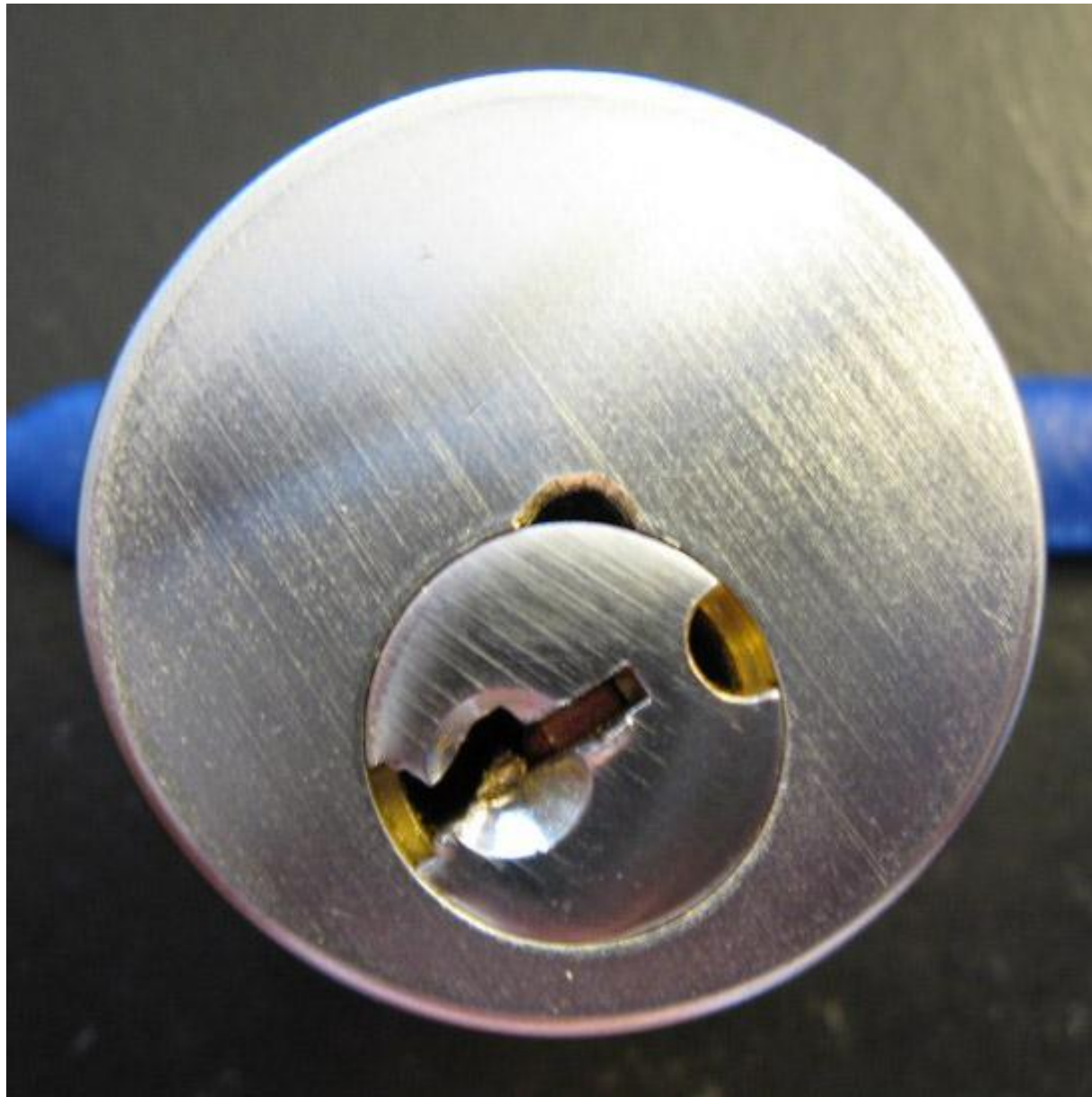
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
8. Some locks are wickedly secure
9. **It comes down to your attackers and defenders**













Most Attacks are Brute Force



Social Engineering



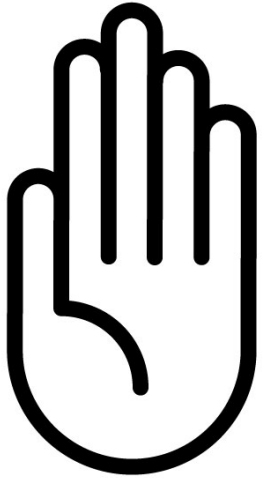
Social Engineering



Social Engineering

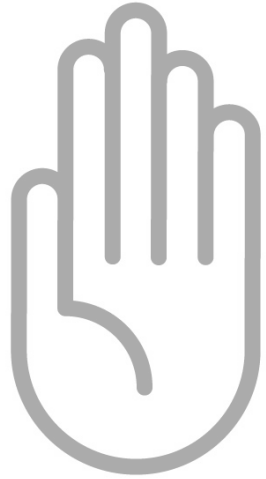


Social Engineering Preparedness

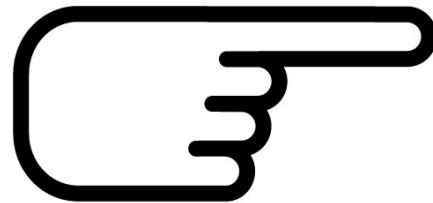


Stop

Social Engineering Preparedness

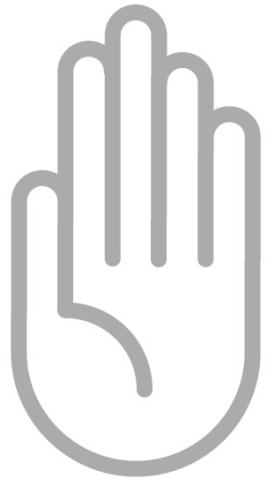


Stop



Challenge

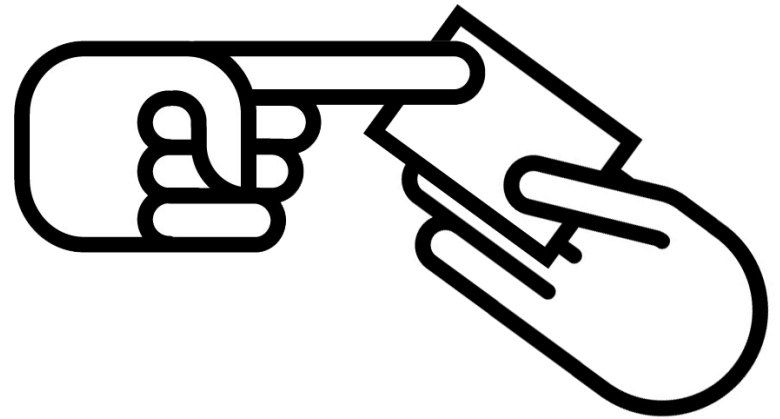
Social Engineering Preparedness



Stop

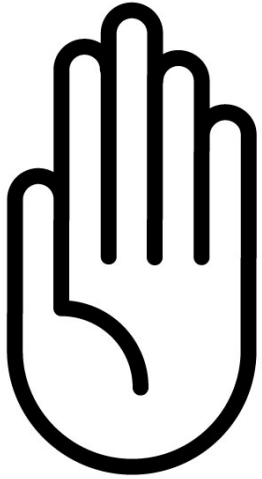


Challenge

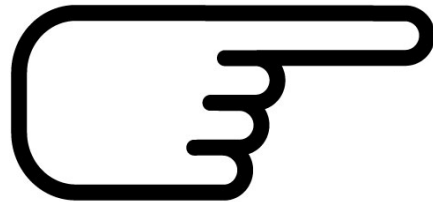


Authenticate

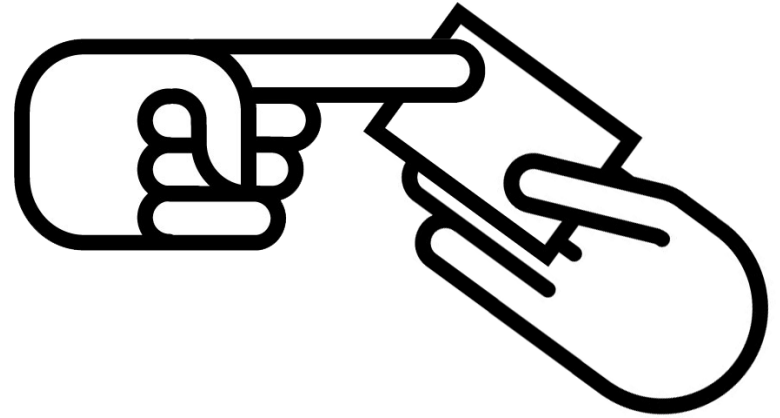
Social Engineering Preparedness



Stop

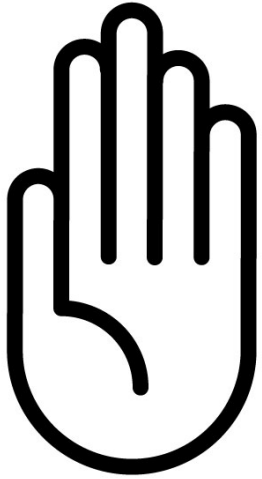


Challenge

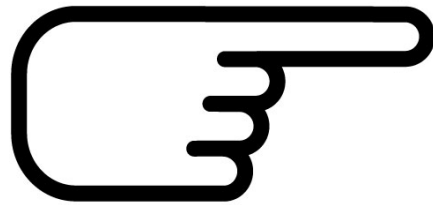


Authenticate

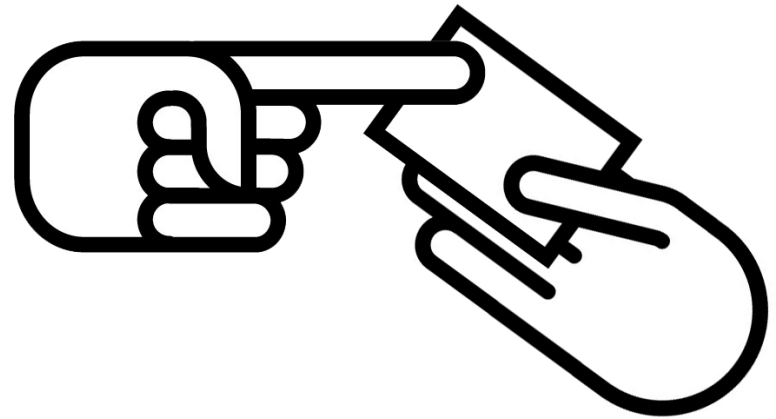
Social Engineering Preparedness



Stop



Challenge



Authenticate

... then you follow this with "Reward"

Social Engineering



Social Engineering



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
8. Some locks are wickedly secure
9. It comes down to your attackers and defenders
10. The truth is out there... or, rather, *in* there

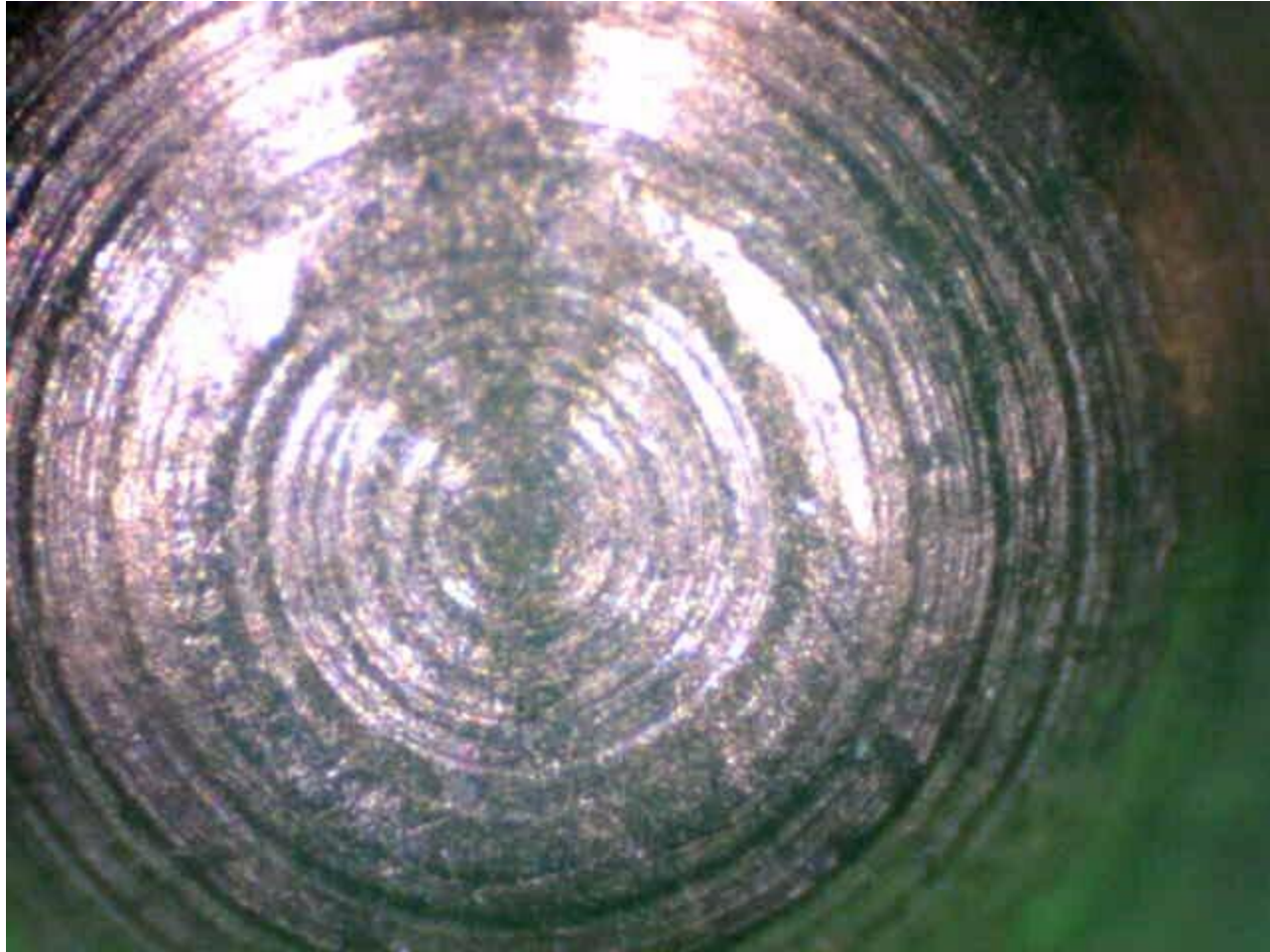
Forensic Evidence



Forensic Evidence



Forensic Evidence



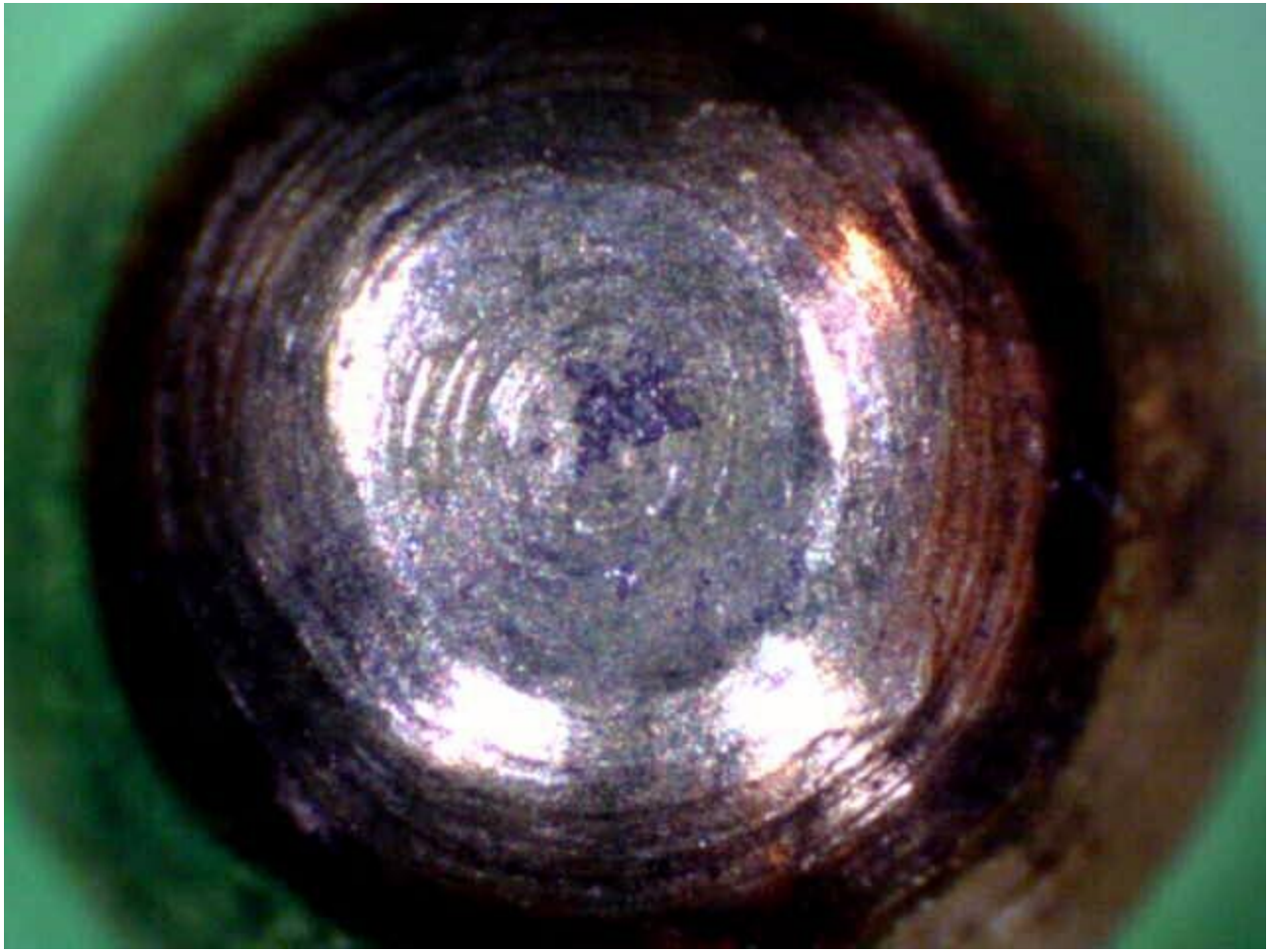
Forensic Evidence - 250 uses



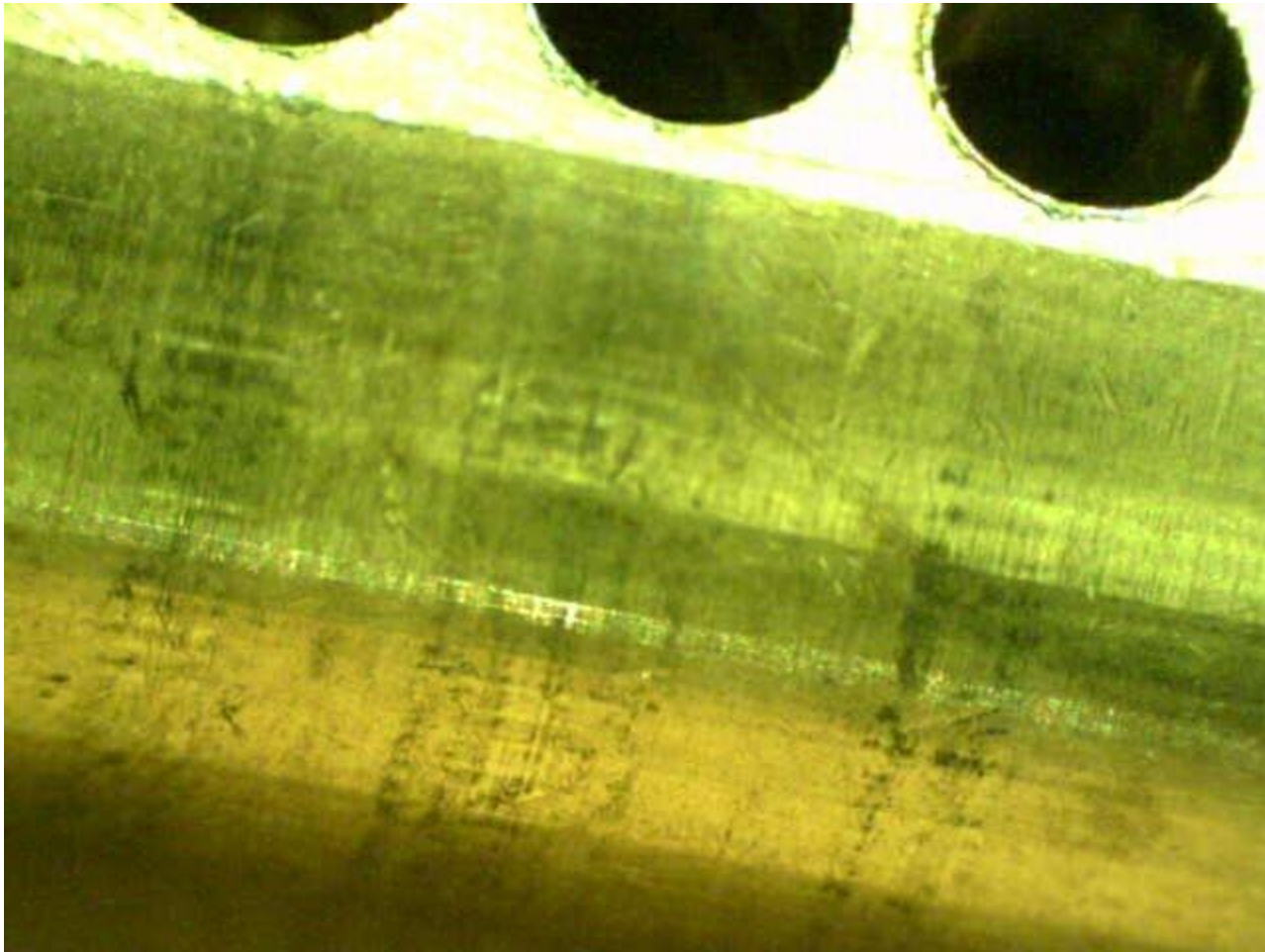
Forensic Evidence - 1,500 uses



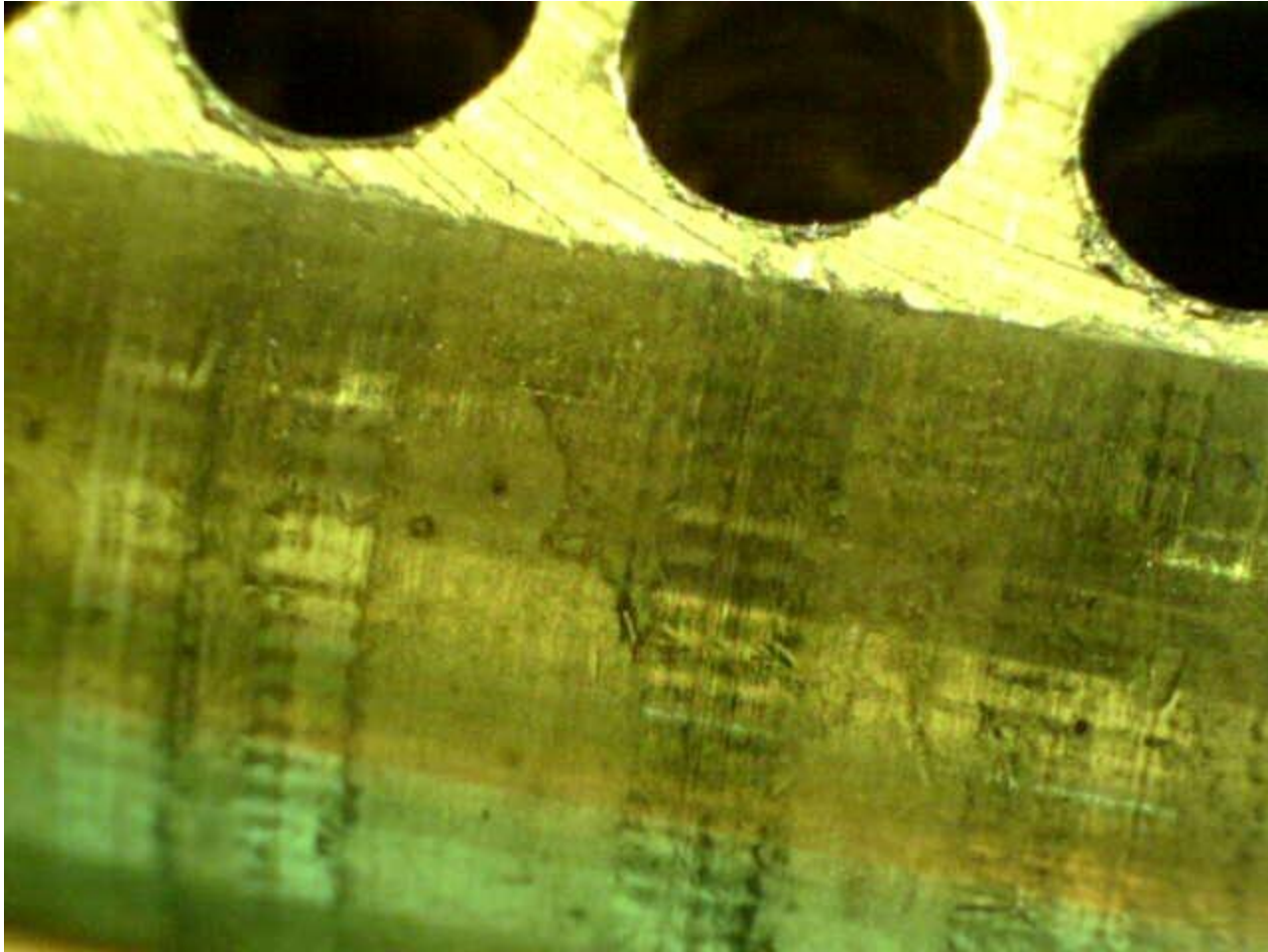
Forensic Evidence - 5,000 uses



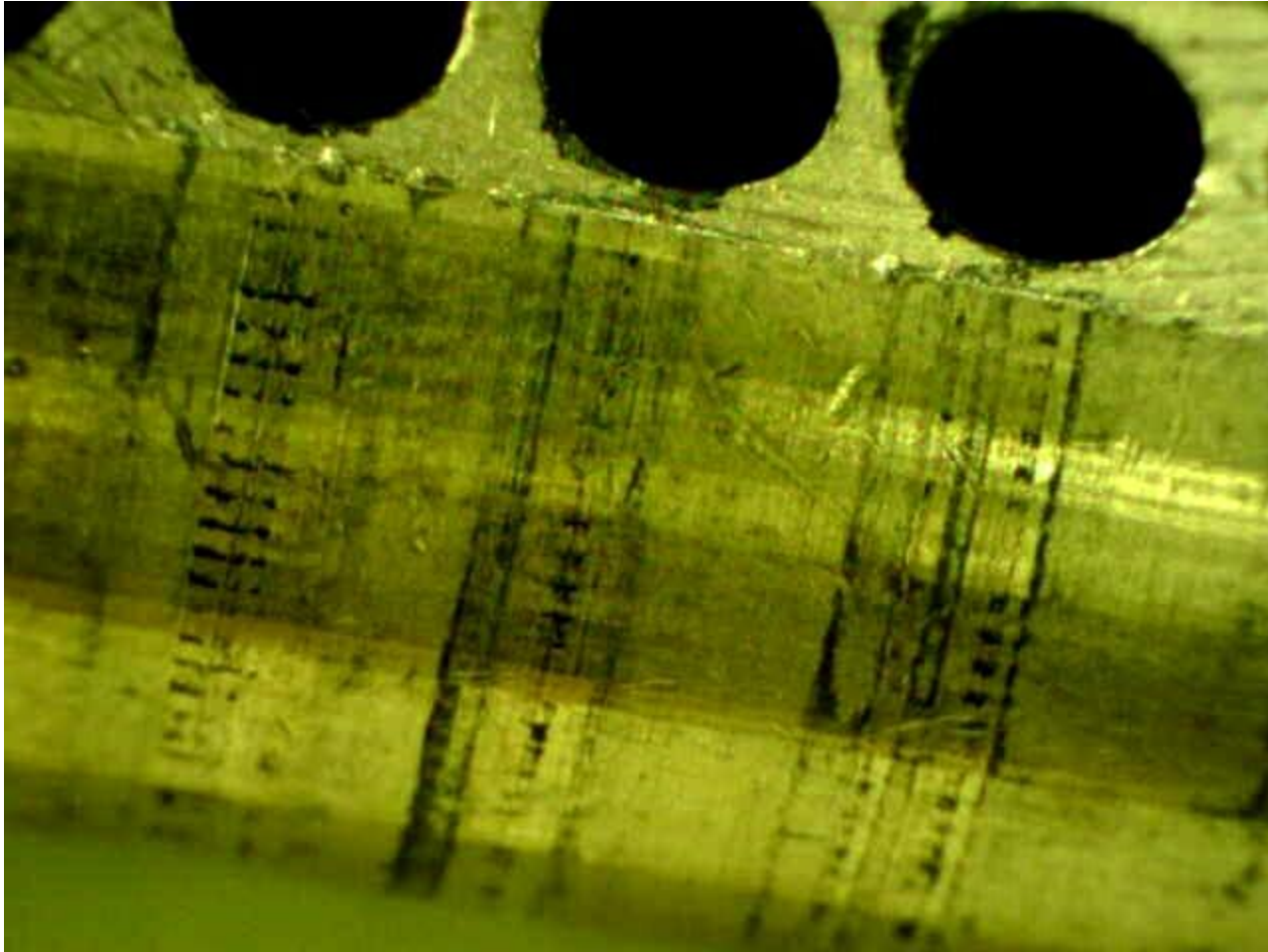
Forensic Evidence - 250 uses



Forensic Evidence - 1,500 uses



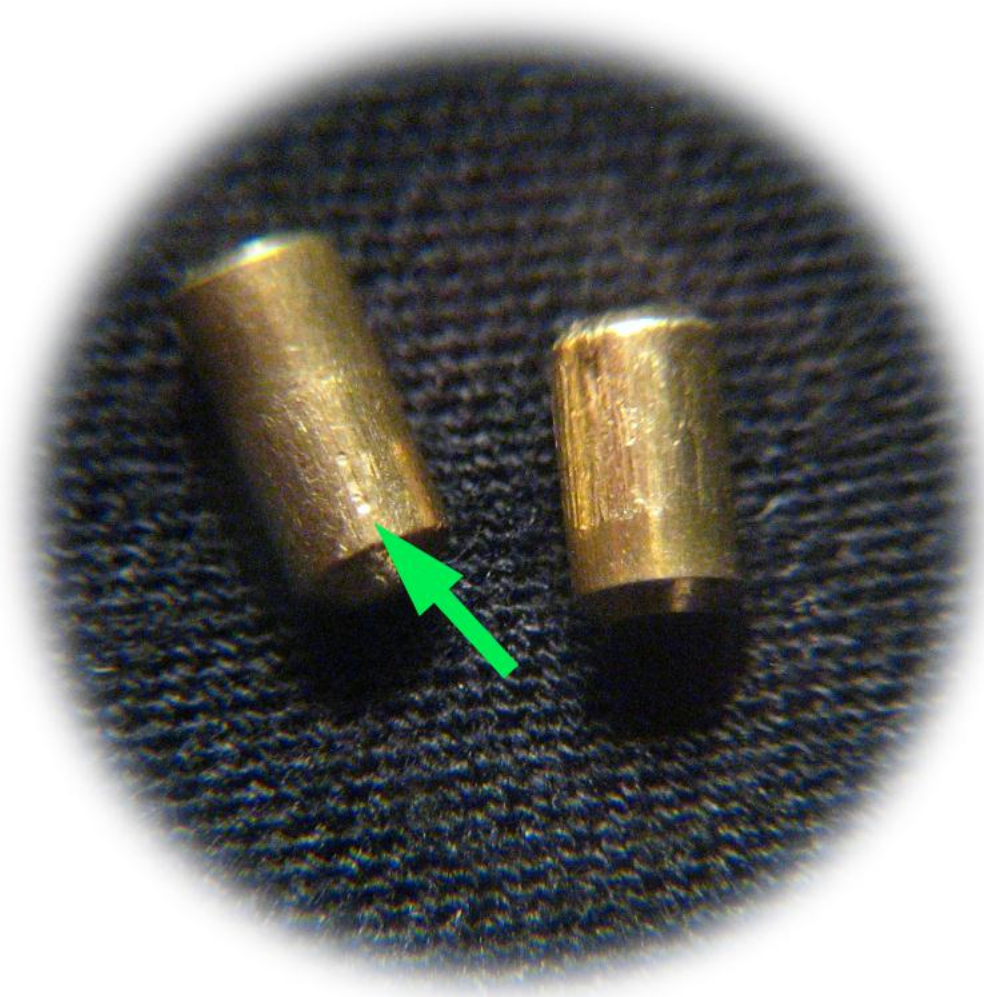
Forensic Evidence - 5,000 uses



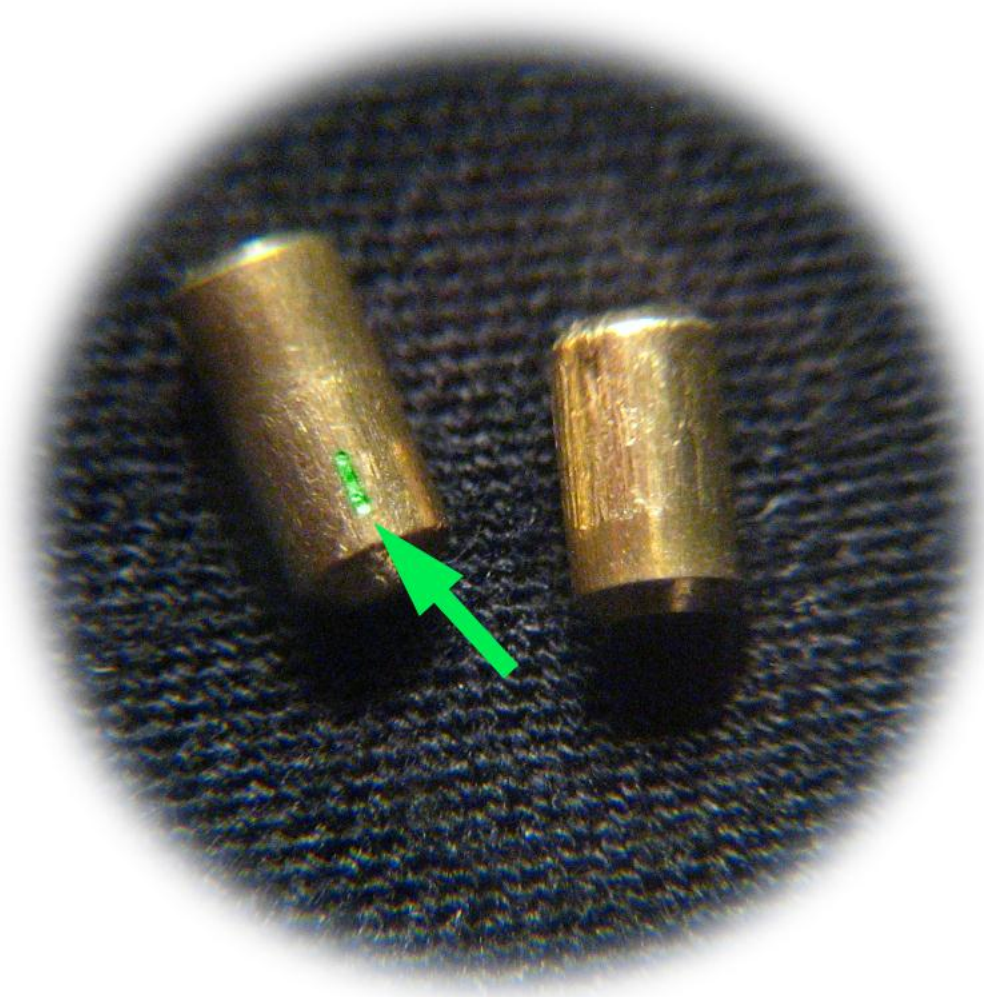
Forensic Evidence



Forensic Evidence



Forensic Evidence



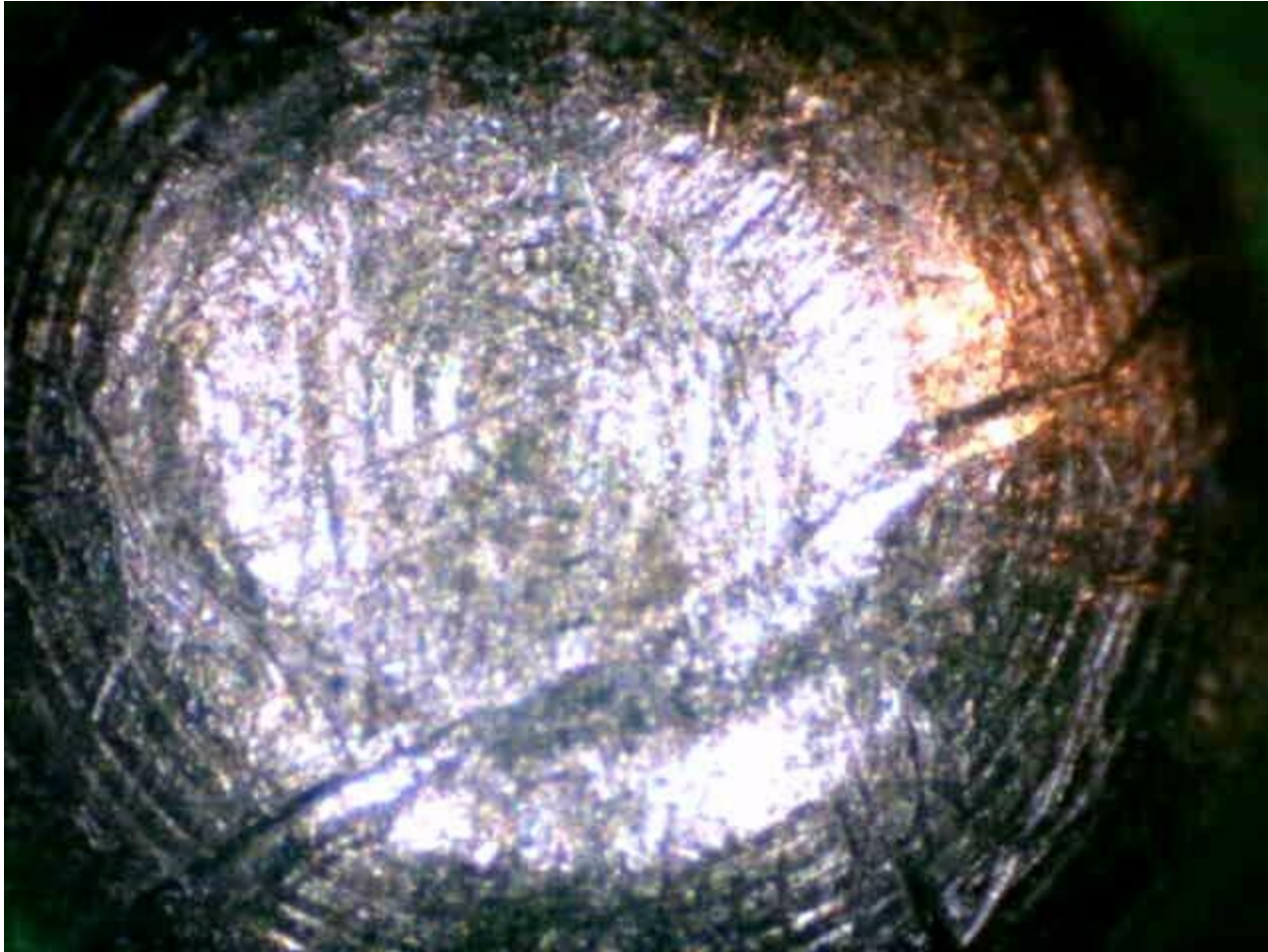
Forensic Evidence



Forensic Evidence - picking



Forensic Evidence - raking



Forensic Evidence - both



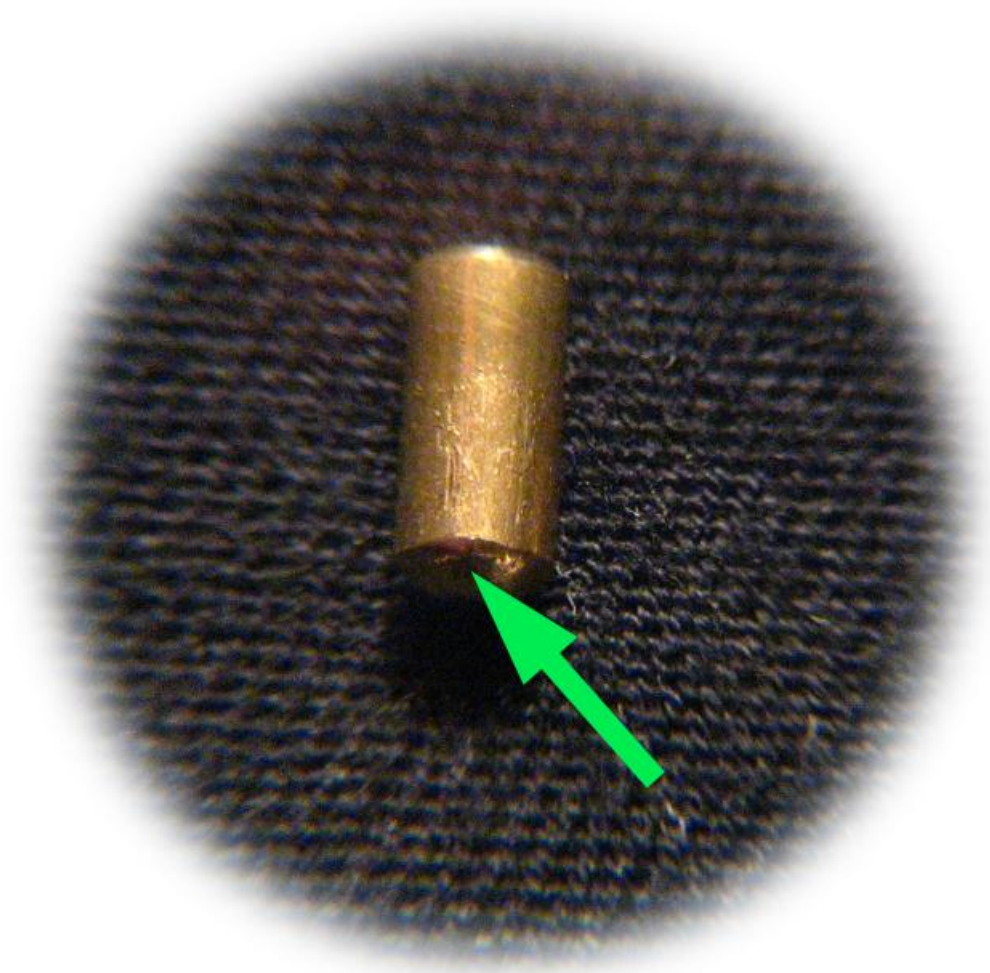
Forensic Evidence - ugh



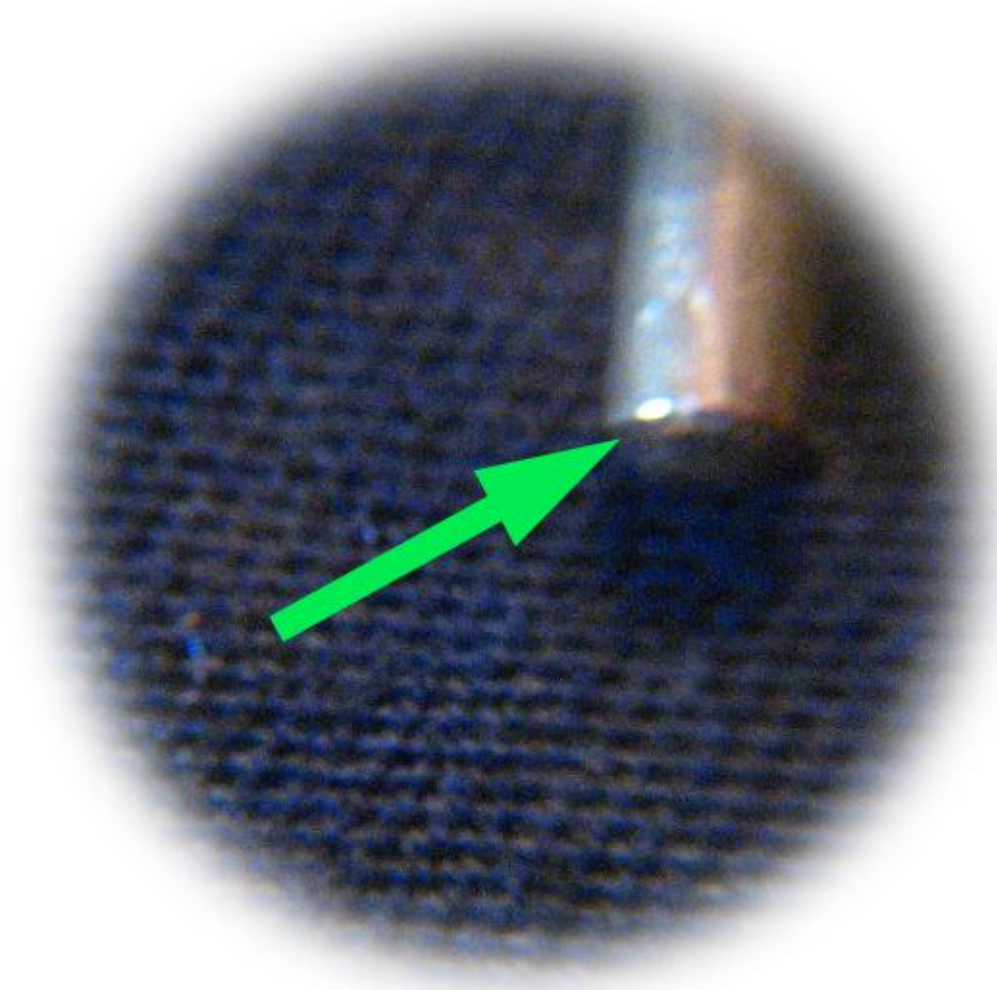
Forensic Evidence - wow



Forensic Evidence



Forensic Evidence



Forensic Evidence - bumping



Forensic Evidence - bumping



Security is only as effective



... as the people behind it

Thank you very much.



Special thanks to TOOOL, Babak, and Daisy

<http://deviating.net>

<http://enterthecore.net>

<http://tool.us>

this presentation is CopyLeft by Deviant Ollam. you are free to reuse any or all of this material as long as it is attributed and freedom for other s to do the same is maintained

