Threat modeling mechanical locking systems, by analyzing at puzzles?

Jan-Willem

May Contain Hackers 2022

Introduction

- Security awareness
- Misunderstood topic



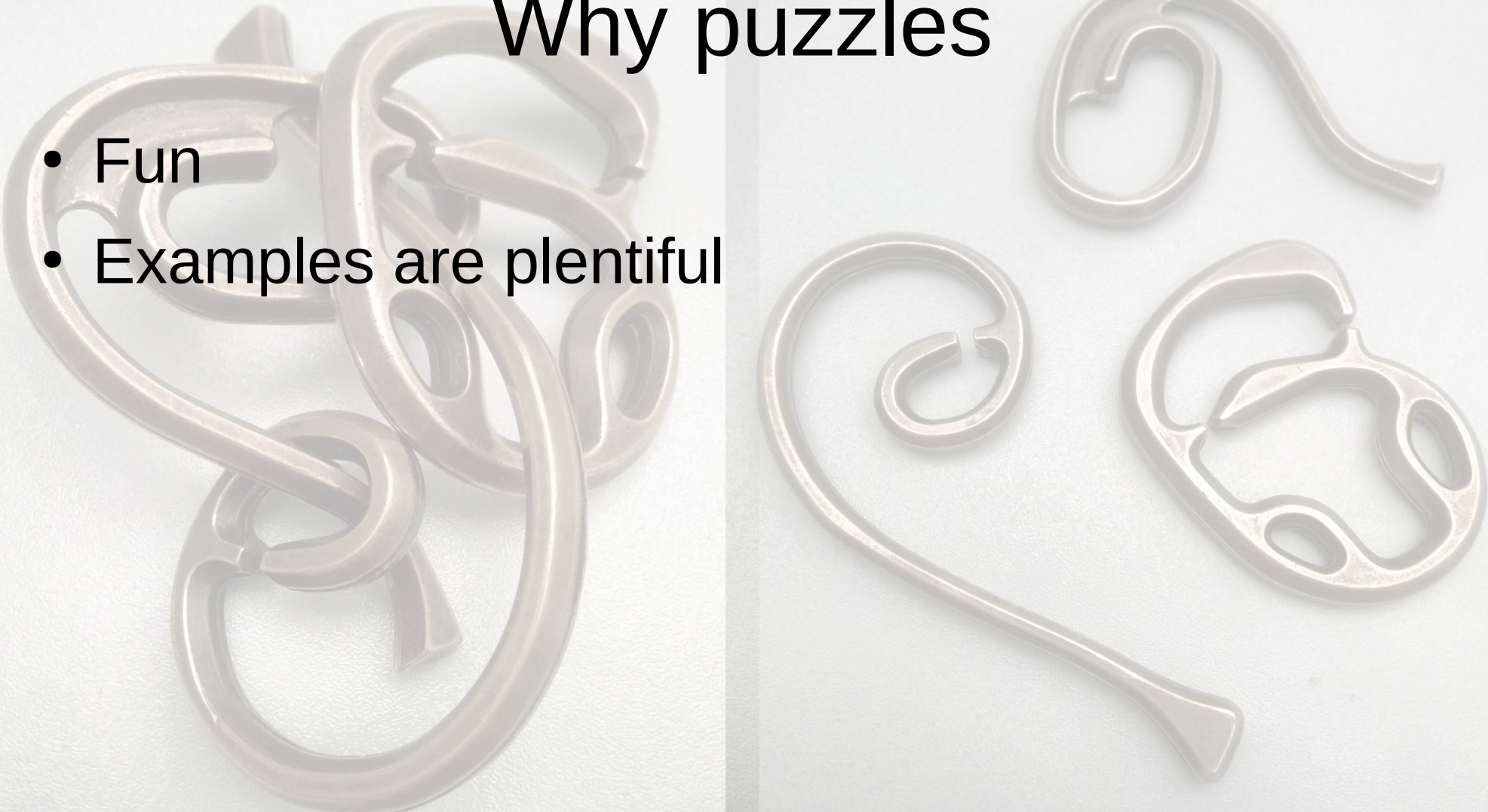
Introduction

- Security awareness
- Misunderstood topic
  - Prevent burglaries?
  - Bricks & Lions



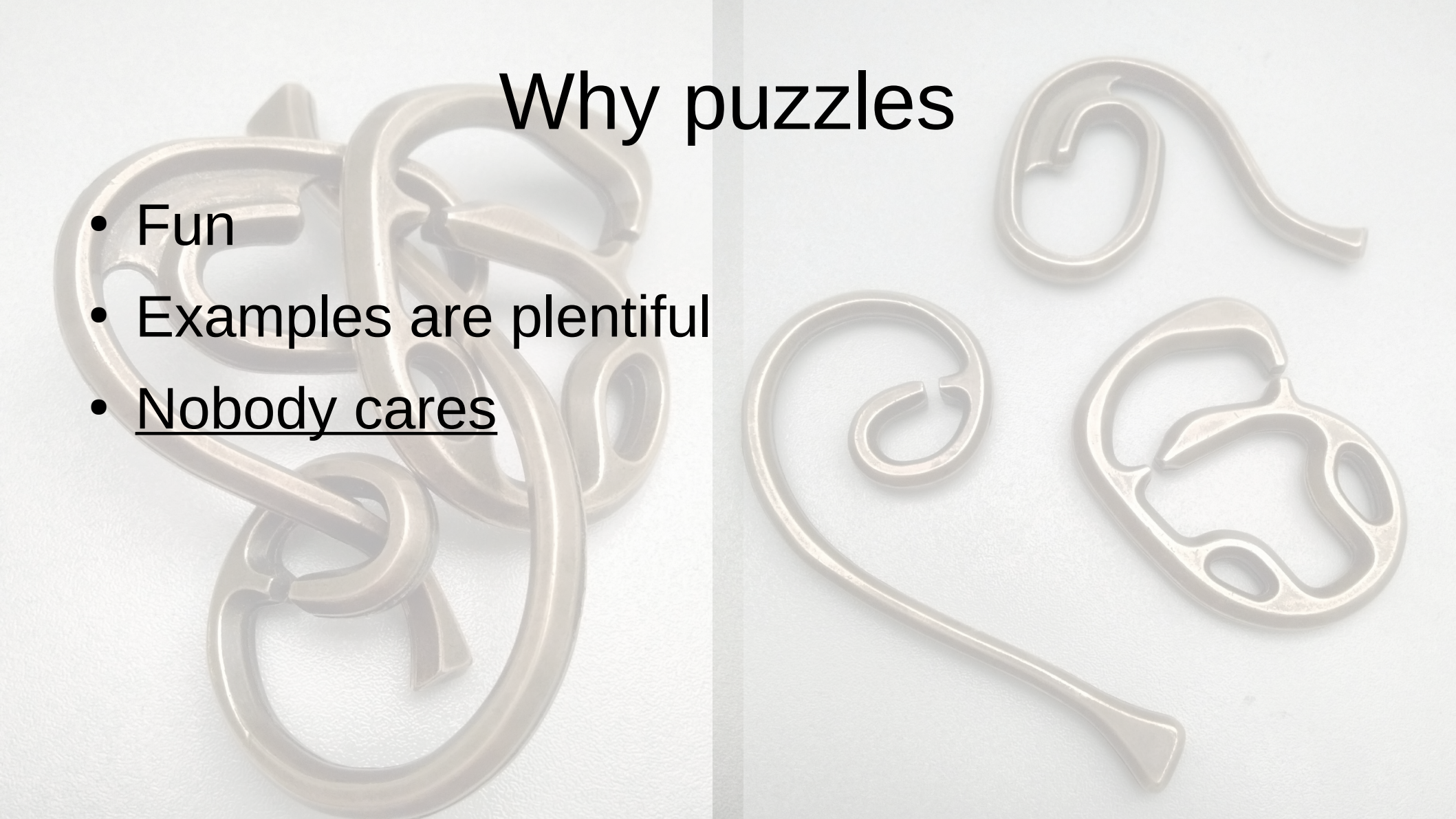
Why puzzles

- Fun
- Examples are plentiful



Why puzzles

- Fun
- Examples are plentiful
- Nobody cares





Follow

Jan-Willem CCX

@jwrm22

Nerd, Board member of TOOOL, Electrical engineer, Hardware Hacker #Cyber



The Open Organisation Of Lockpickers

- Started in 2002
- 50 members in the Netherlands
- Weekly lockpicking meetings
- Lockpicking village @ Clairvoyance

TOOL
The Open Organisation Of Lockpickers

Threat modeling

- Protect a system:
  - Find assets
  - Define attacker
  - Find vulnerabilities
  - Implement defense

Threat model

- Asset:
  - Valuable to the defender
- Can be:
  - Information
  - Money
  - IP
  - Etc.

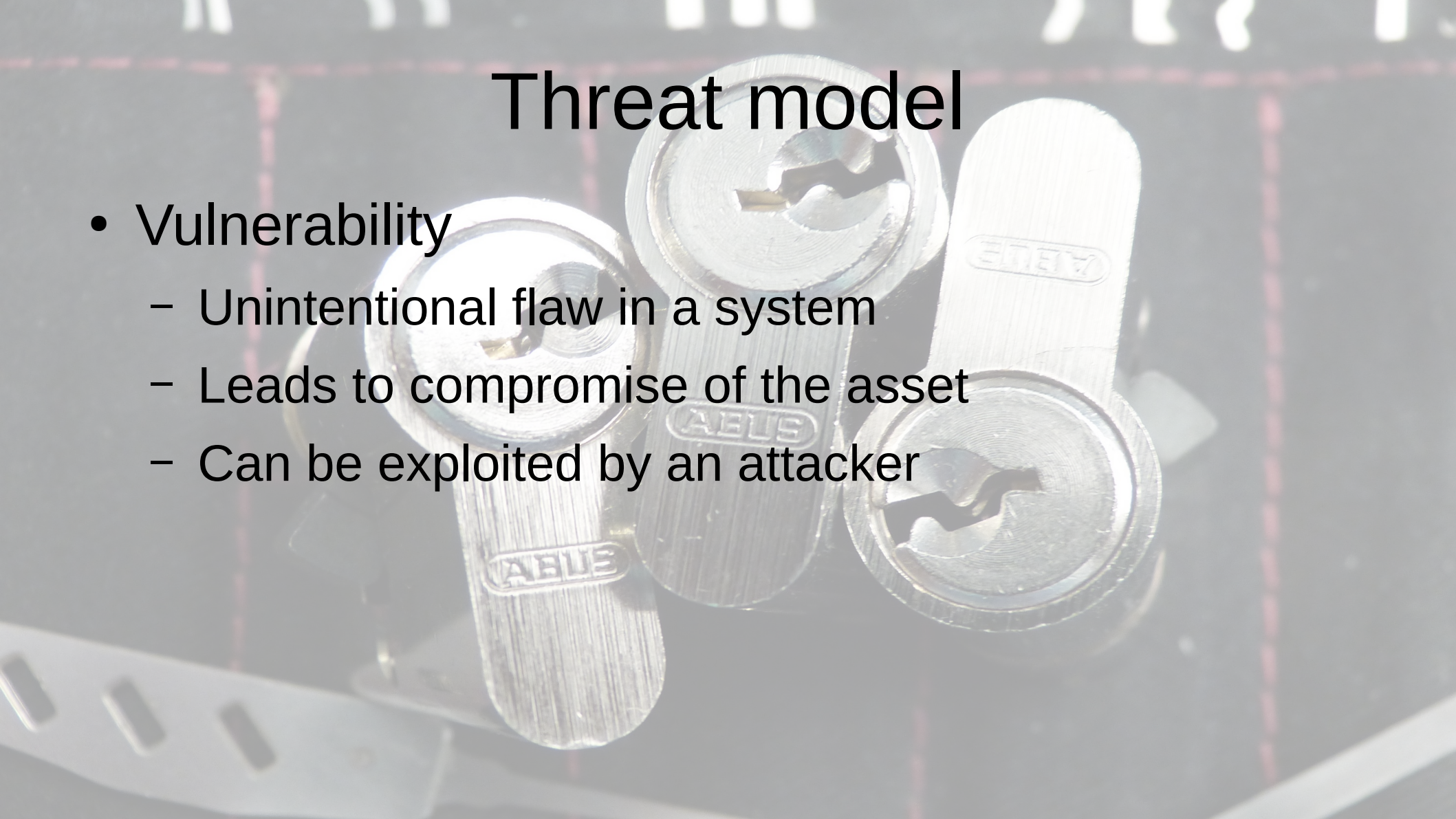
Threat model

- Attacker:
  - Entity
  - Skilled enough to gain access to asset
- Attackers need:
  - Motivation
  - Opportunity
  - Method

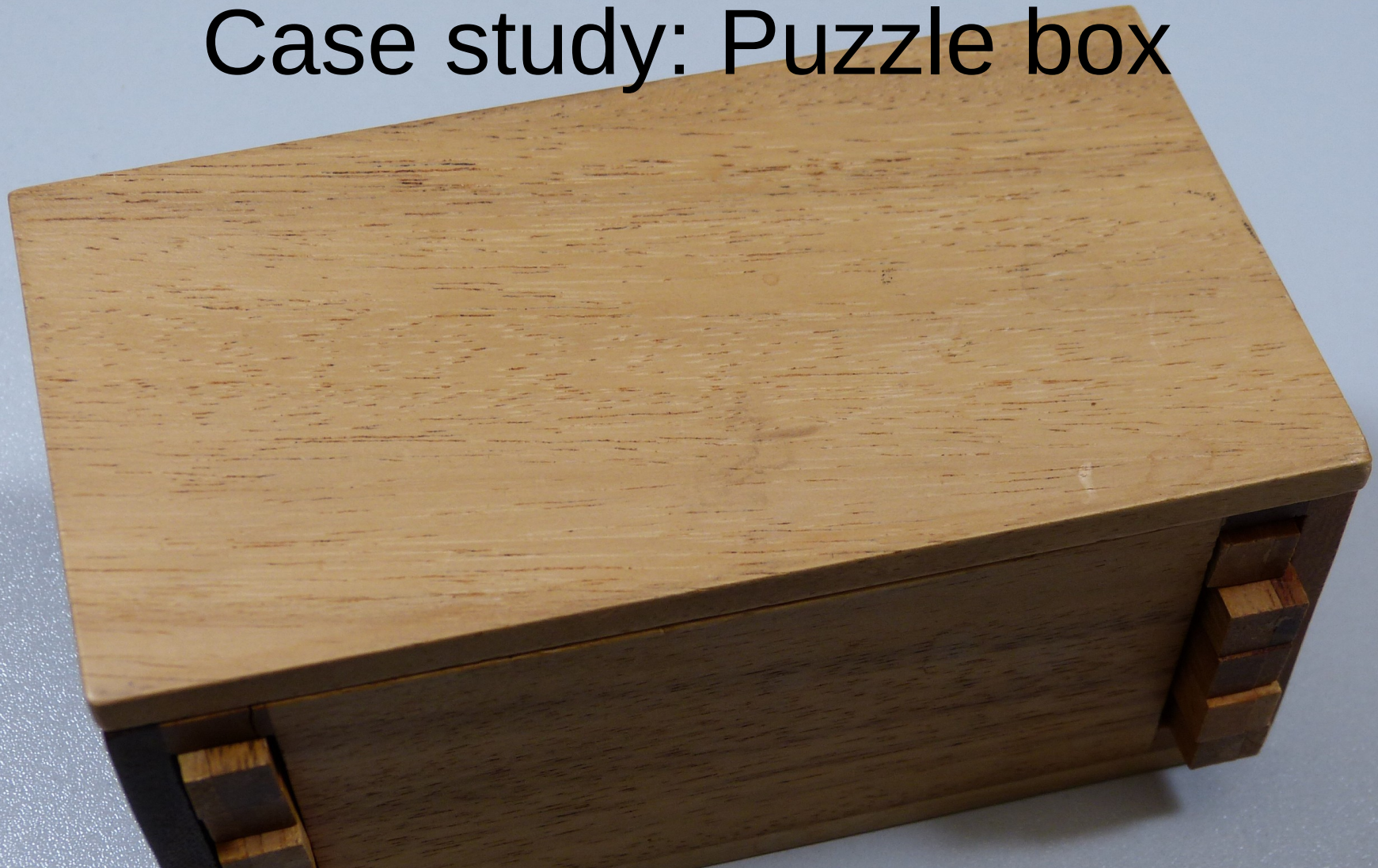


Threat model

- Vulnerability
  - Unintentional flaw in a system
  - Leads to compromise of the asset
  - Can be exploited by an attacker



Case study: Puzzle box





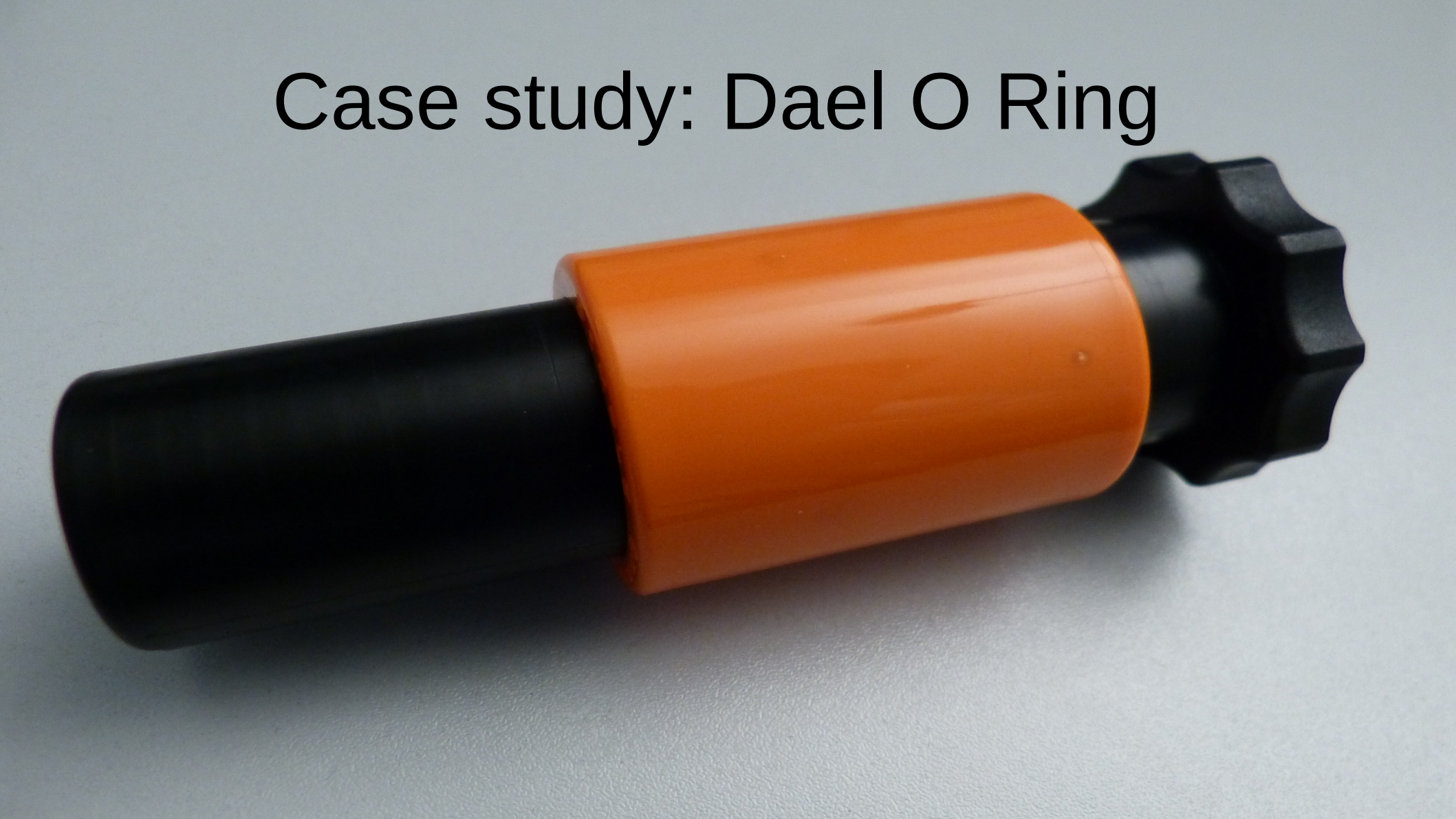
Case study: Puzzle box






CRYPTOGRAPHY™
RESEARCH
Congratulations! (assuming you didn't use a saw to open this)
We look forward to continuing to work with you.
Paul Kocher
www.cryptography.com

Case study: Dael O Ring



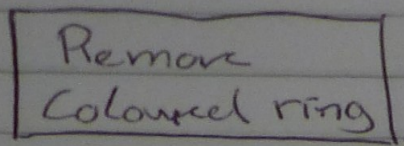



DAELING RING


DAELING RING
Collect them all!
EASY YELLOW
SIMPLE ORANGE
SILLY GREEN
COMPLEX BLUE
CRAZY RED
TERRIBLE BLACK


How to play DAELING RING?
1
2
3
"Start"
4
5
6
Click!
8 718274 770018
CE
0-3

Attack tree
DAEL O Rings



Puzzle makers
- Reputation
- Sales
- IP

Solve Maze
- Brute force
- Maze Solve algoritm
- Robot

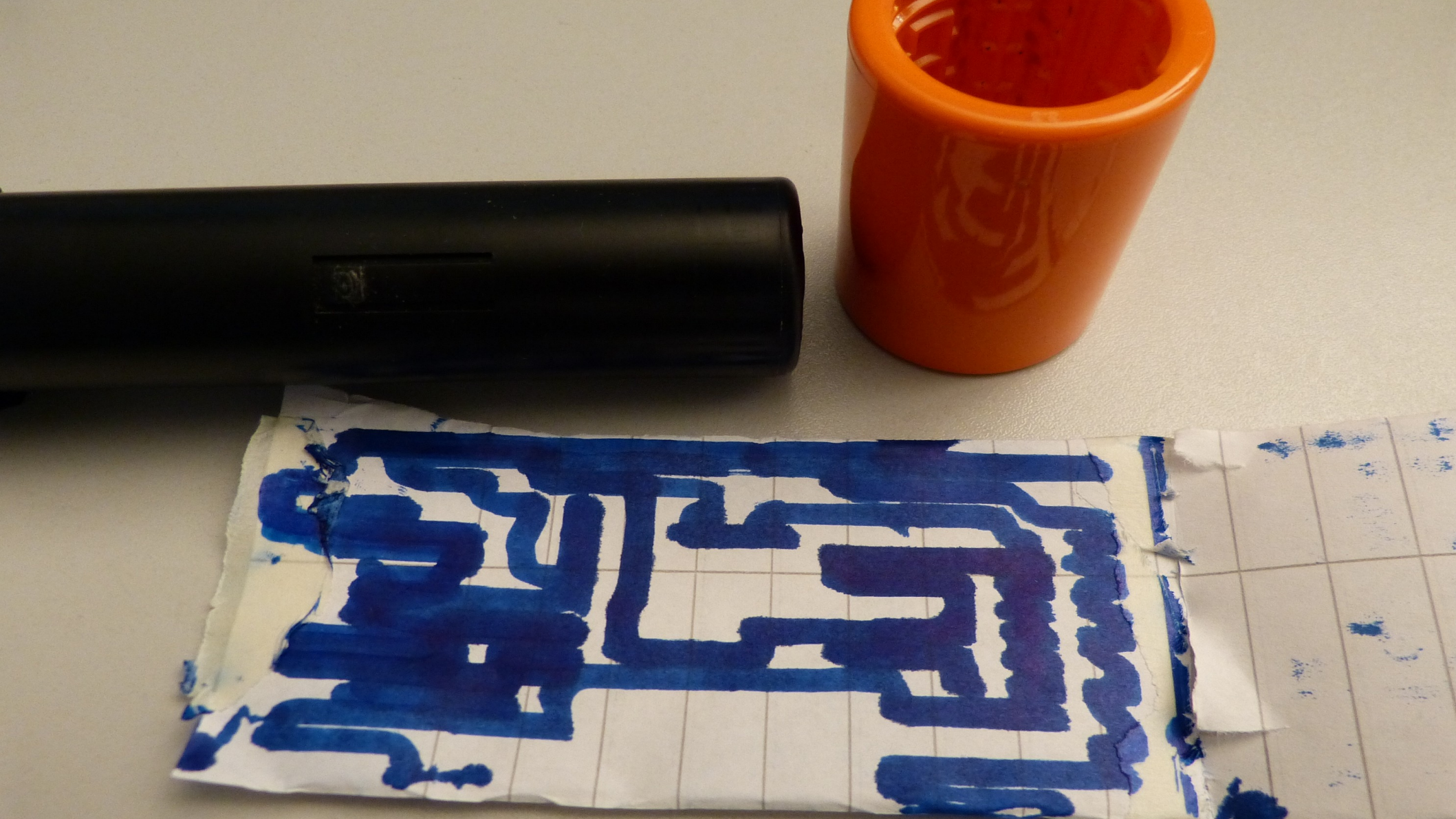
Learn Maze
- Internet search
  Find solution
- Ask Someone
- XRAY/echo
- Decoder tool
- Impressioning

Bypass Maze
- File knob
- Force maze
- Force reset mechanism

Mom
- Personal challenge







Locks are puzzles

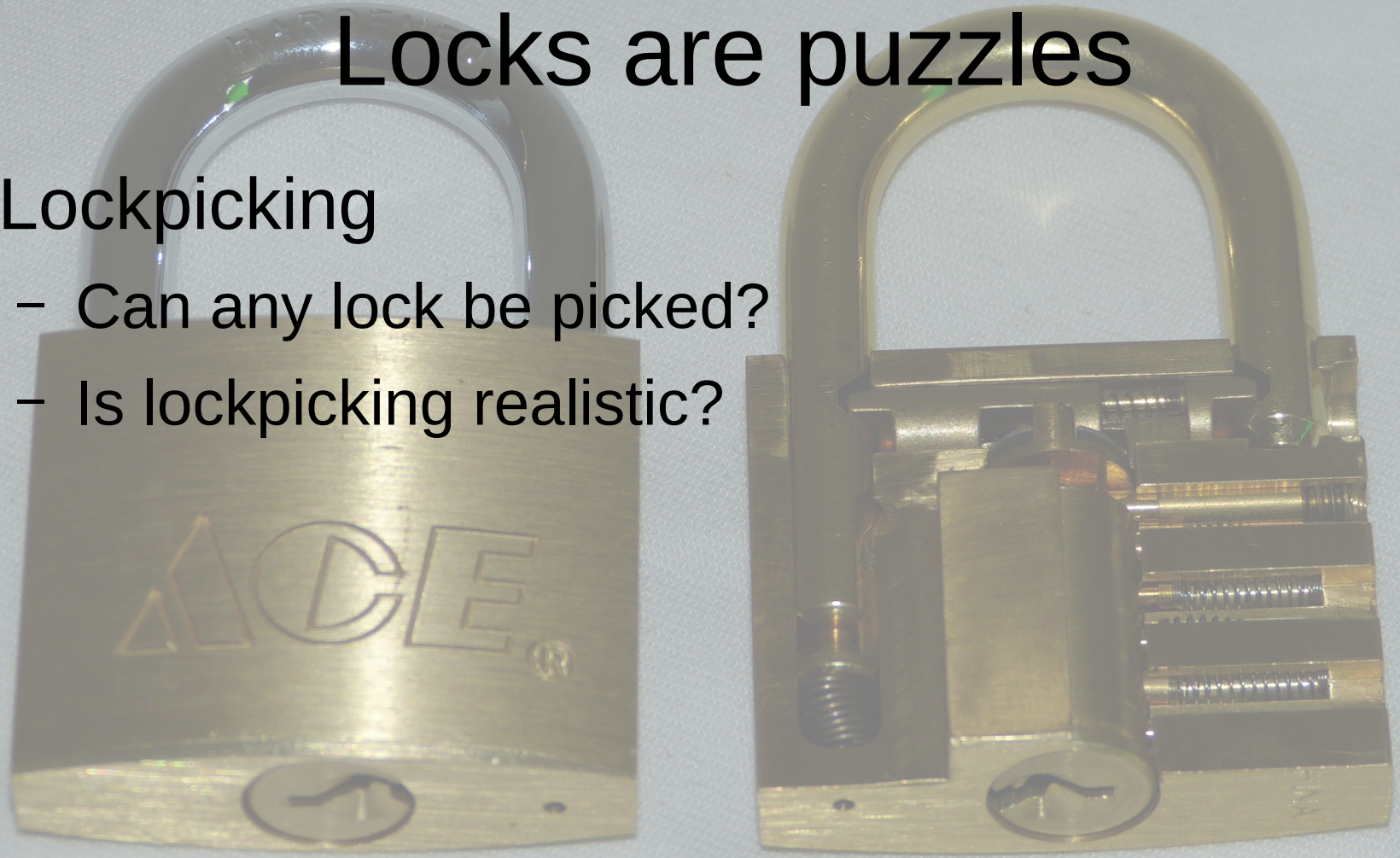
- Lockpicking
  - Challenge locks
  - Unpickable locks?





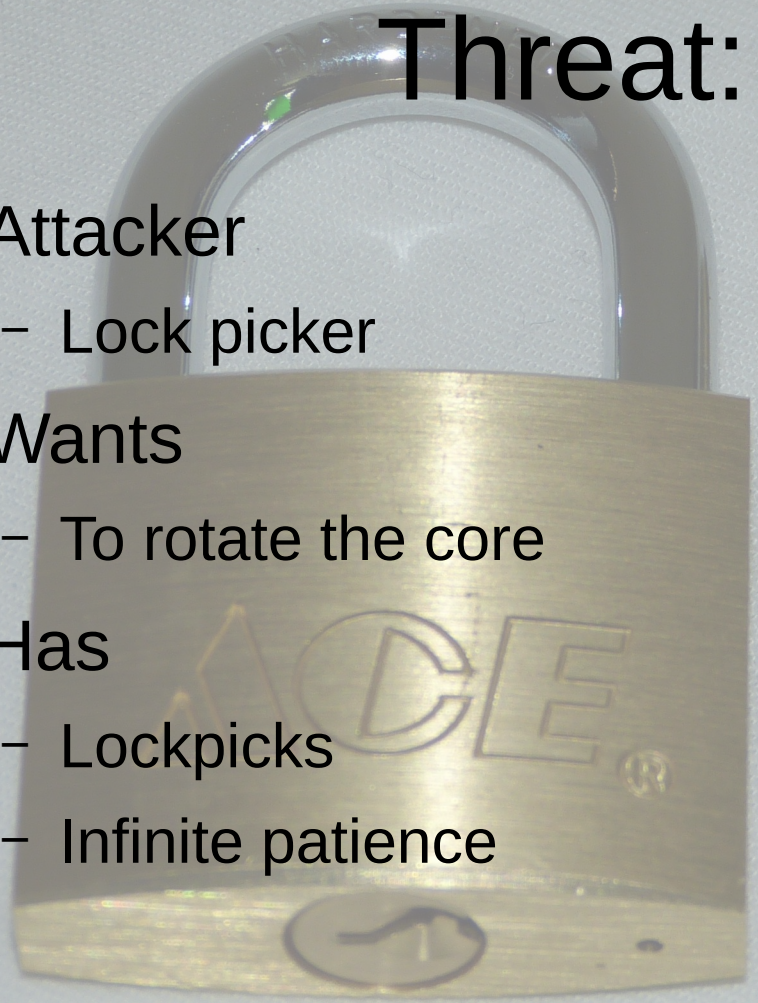
Locks are puzzles

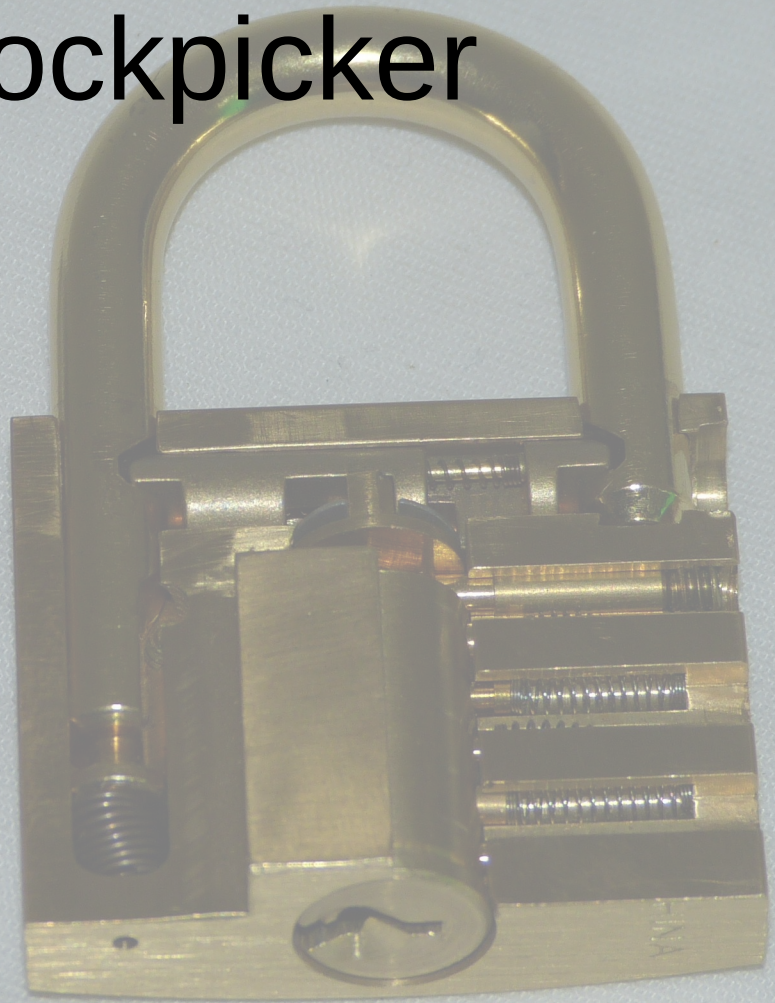
- Lockpicking
  - Can any lock be picked?
  - Is lockpicking realistic?



Threat: Lockpicker

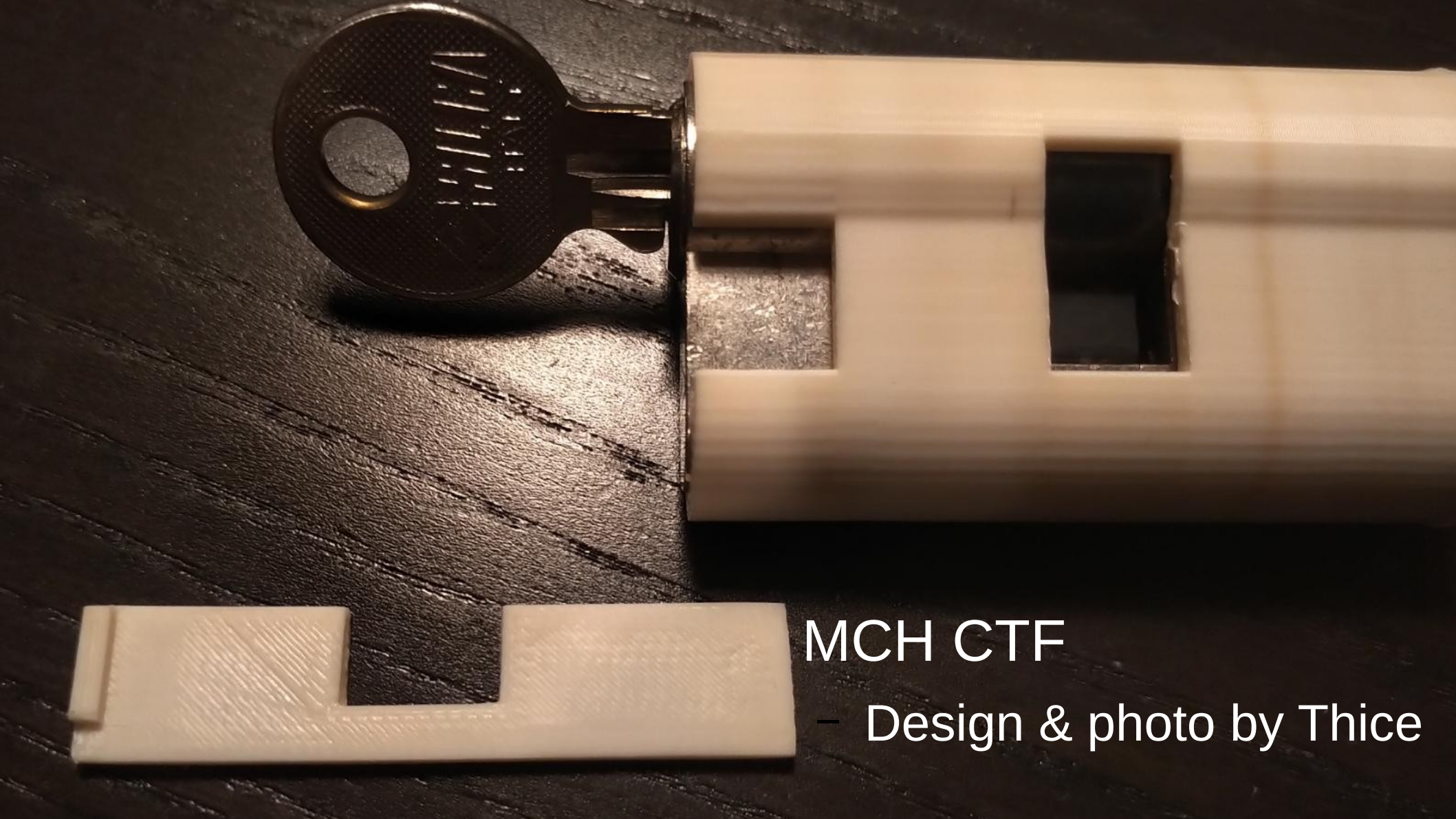
- Attacker
  - Lock picker
- Wants
  - To rotate the core
- Has
  - Lockpicks
  - Infinite patience



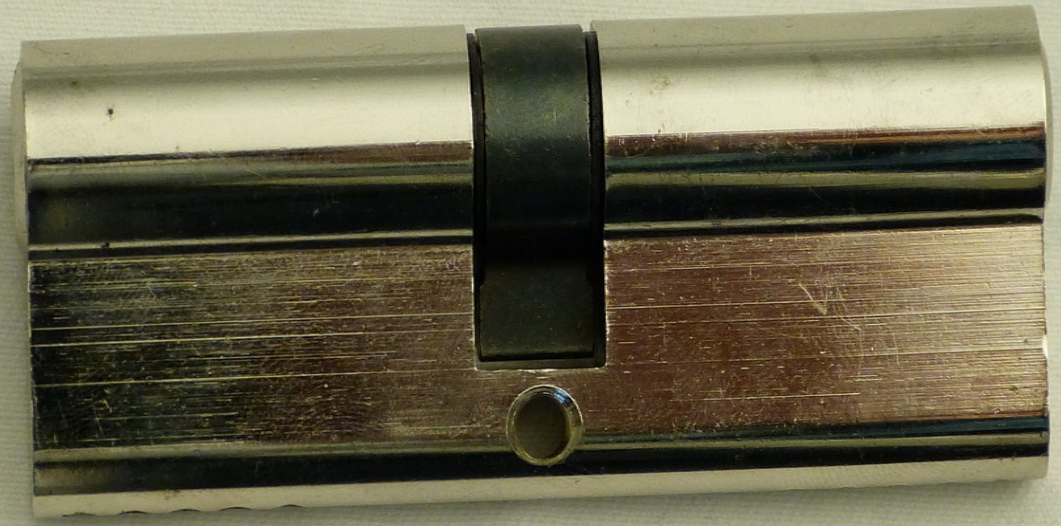


Rules of Lockpicking

- Pick your own locks.
- When locks are in use, find another to pick.

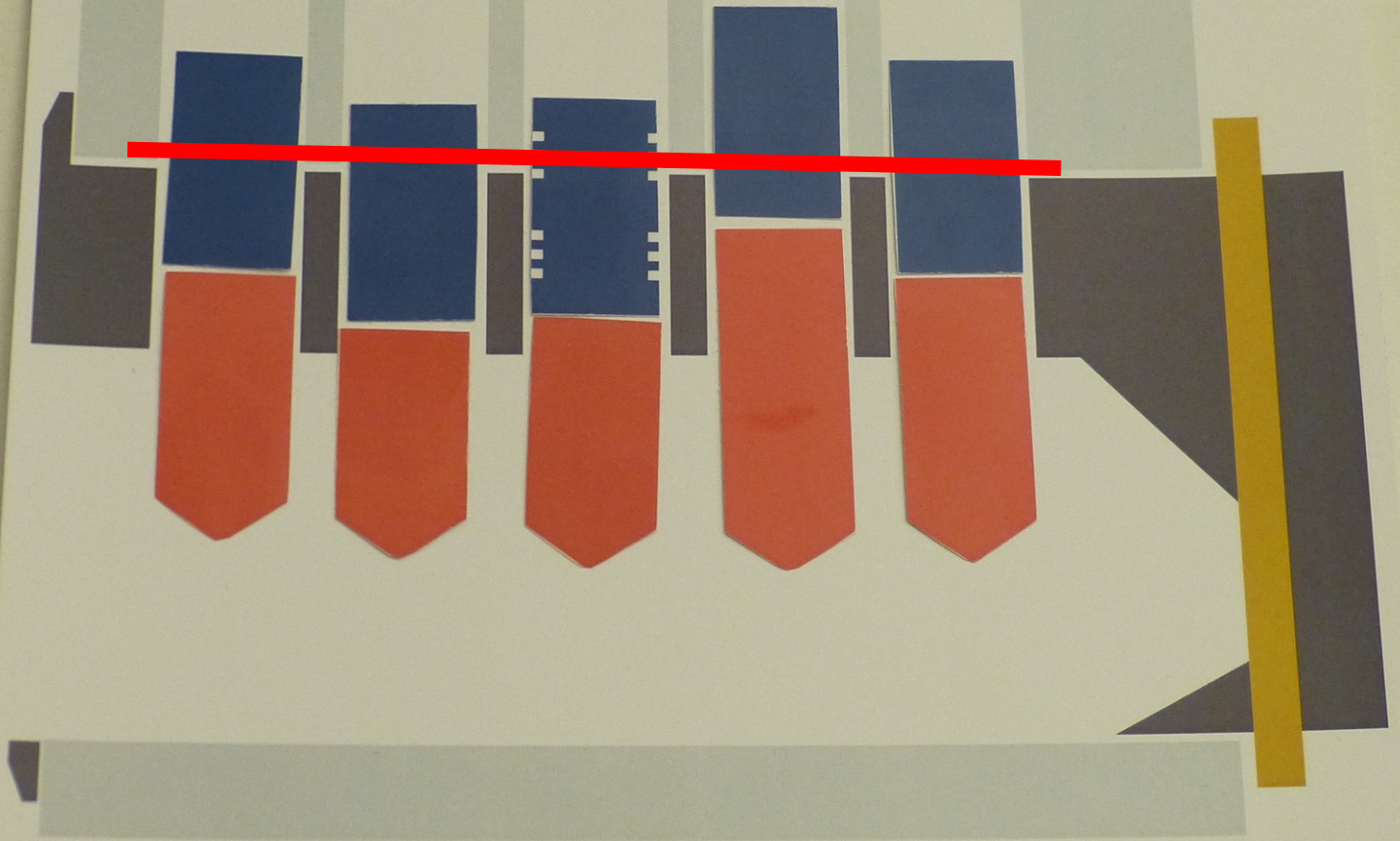

MCH CTF
– Design & photo by Thice

Locks

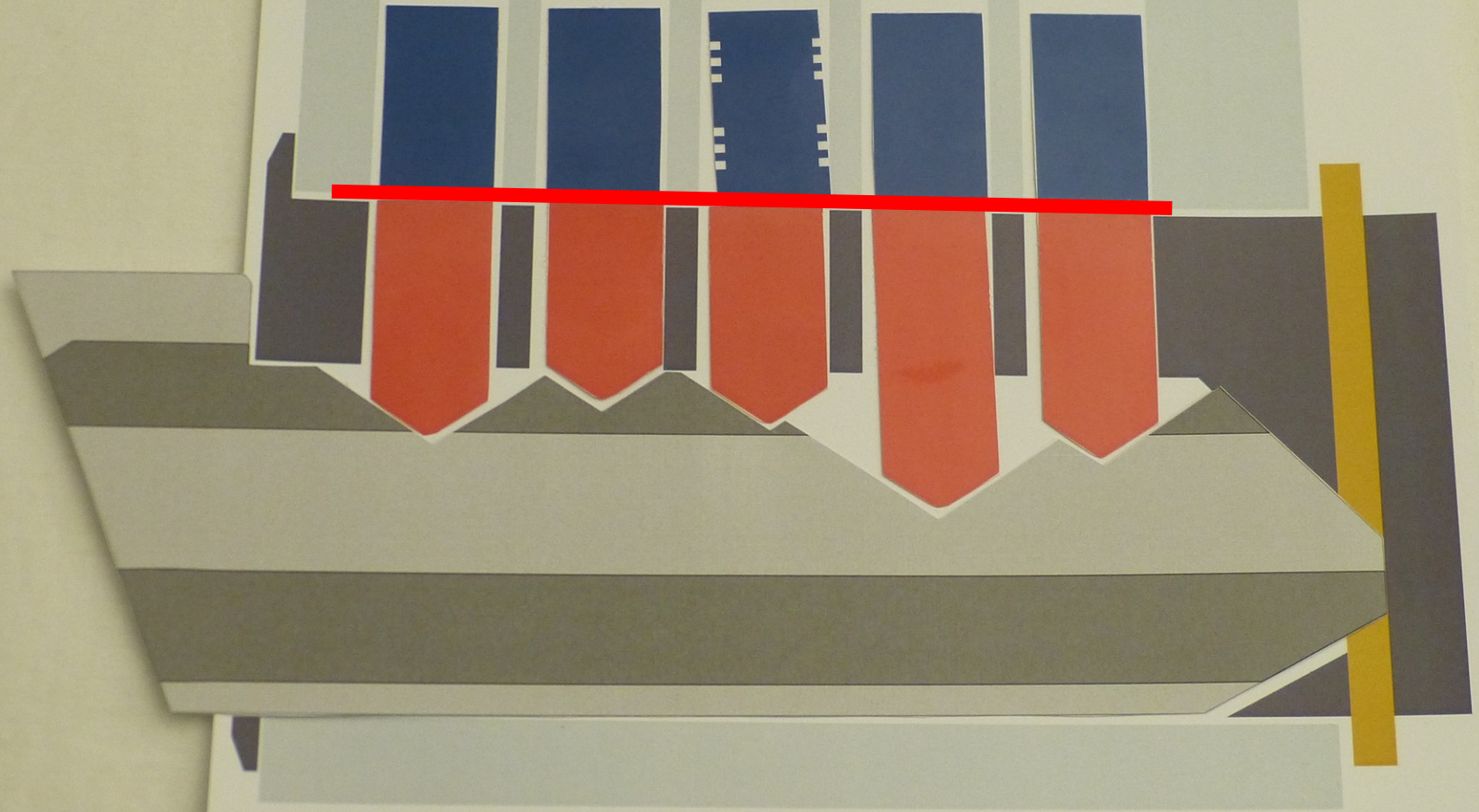




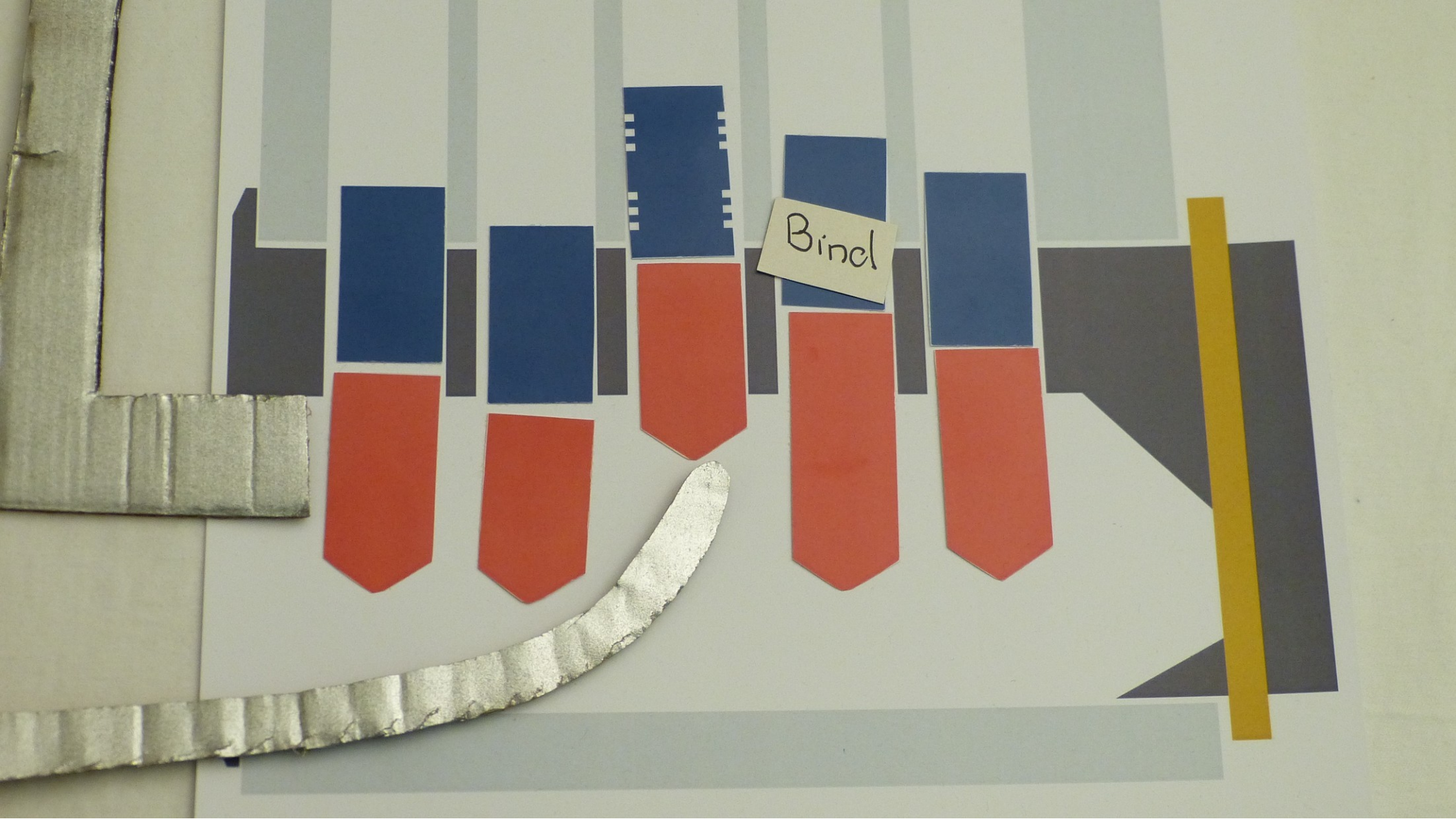
Without key



Correct key




PN08
PN09


Bind








UNION
ENGLAND
PARKES
UKLS
BUILDERS
UNION.
UNION
ENGLAND
PARKES

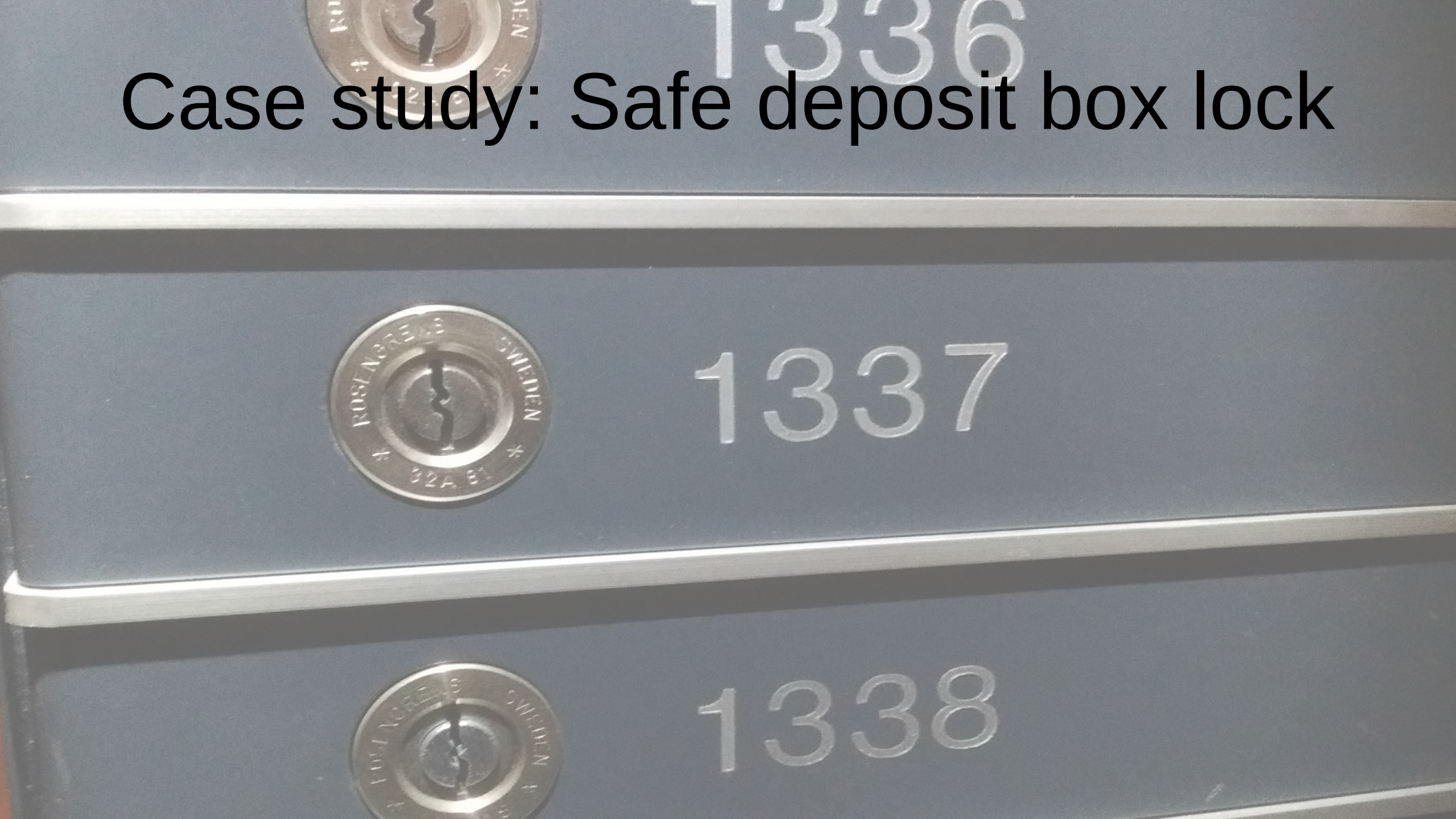
Case study: Unpickable locks

- Andy Pugh

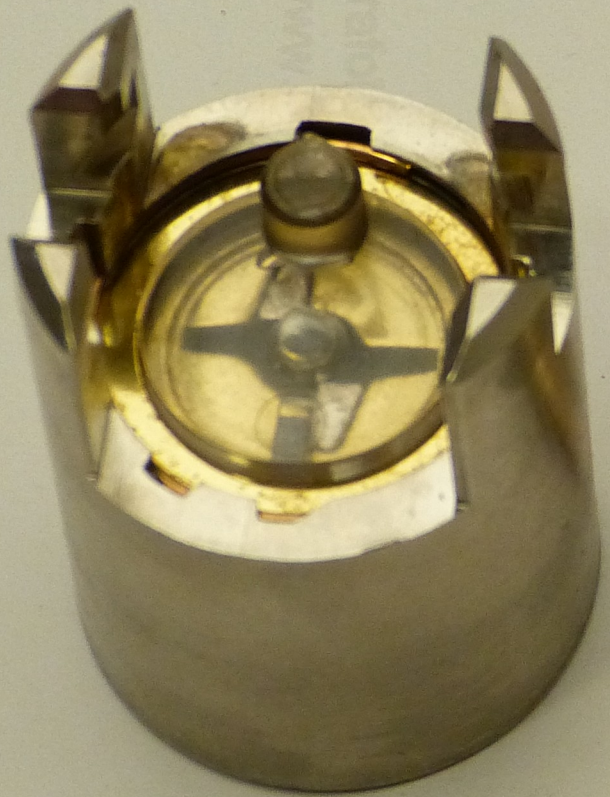




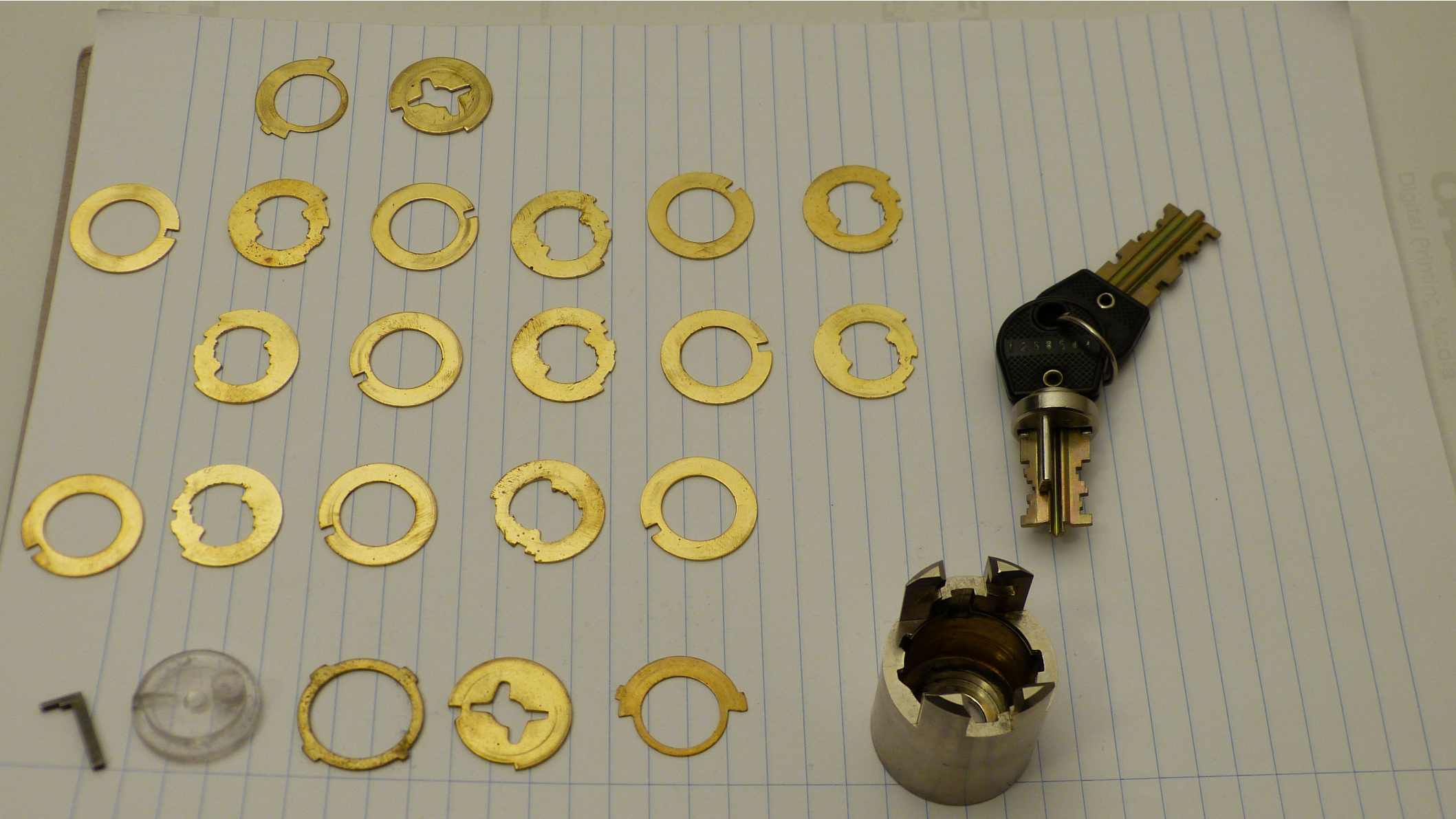
Case study: Safe deposit box lock




ROSENGRENS
SWEDEN
32A 81
ROSENGRENS SWEDEN
SK32A81SOS




ROSENBERGS
SWEDEN







SDB

- Many key combinations:
  - 6^8 > 1M
- Hard to duplicate key
- Anti pick features
- One surprise



SDB

- Many key combinations:
  - 6^8 > 1M
- Hard to duplicate key
- Anti pick features
- One surprise



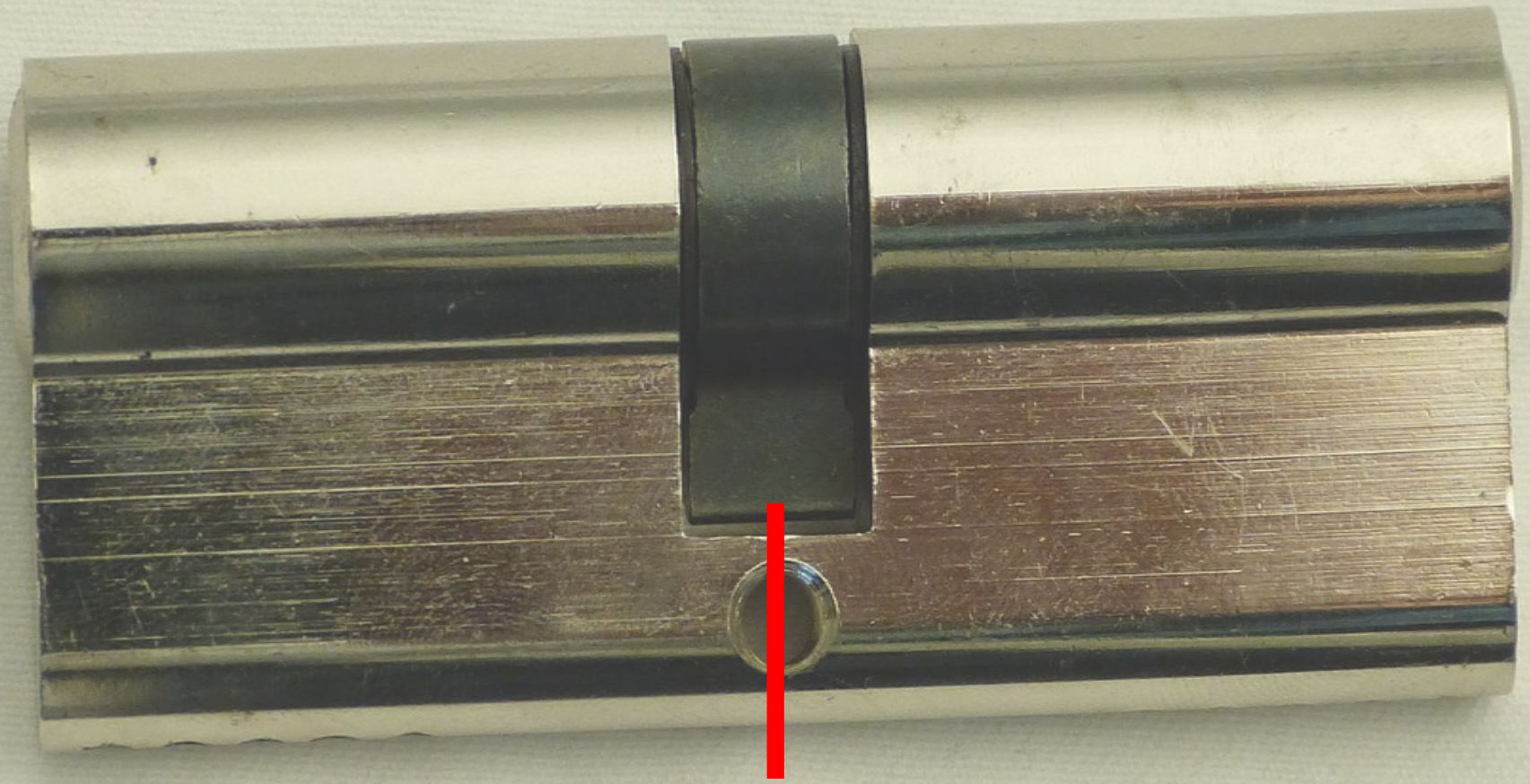
Threat: Burglar

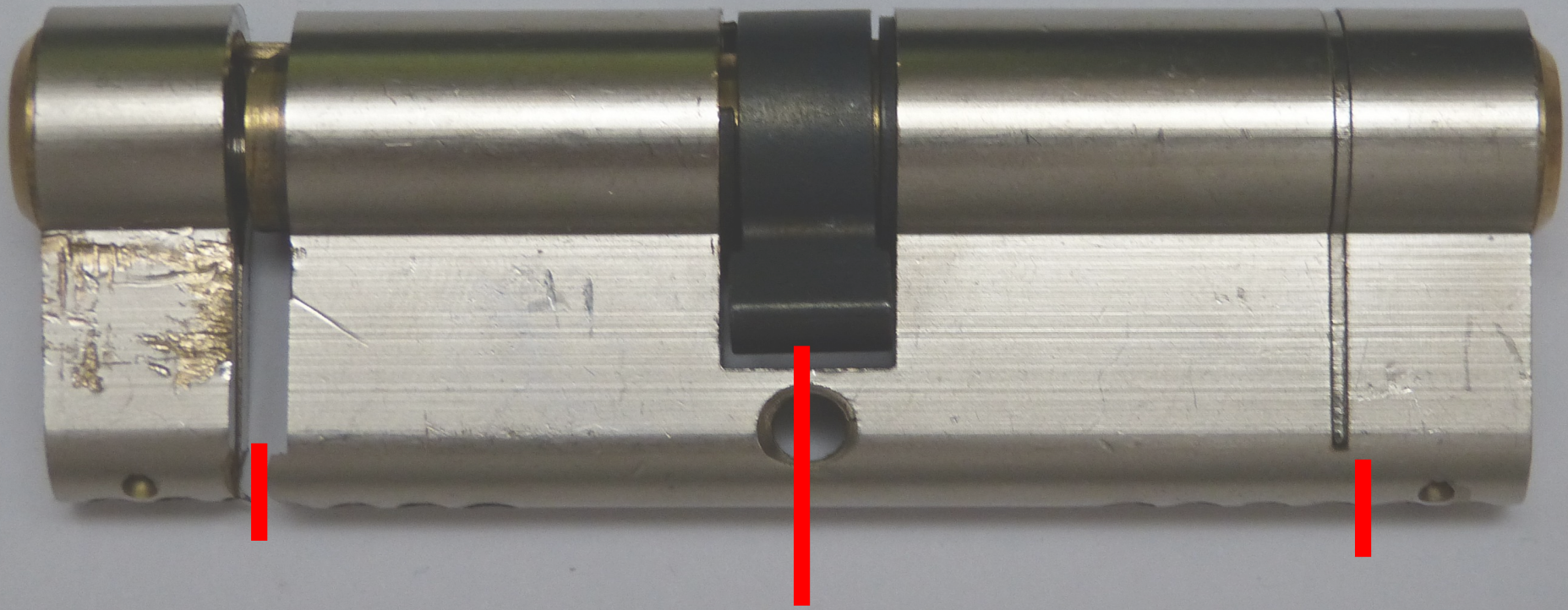
- Attacker
  - Burglar
- Wants
  - Access to the items the lock protects
- Has
  - Fast entry tools & methods
  - Little time; t < 120s

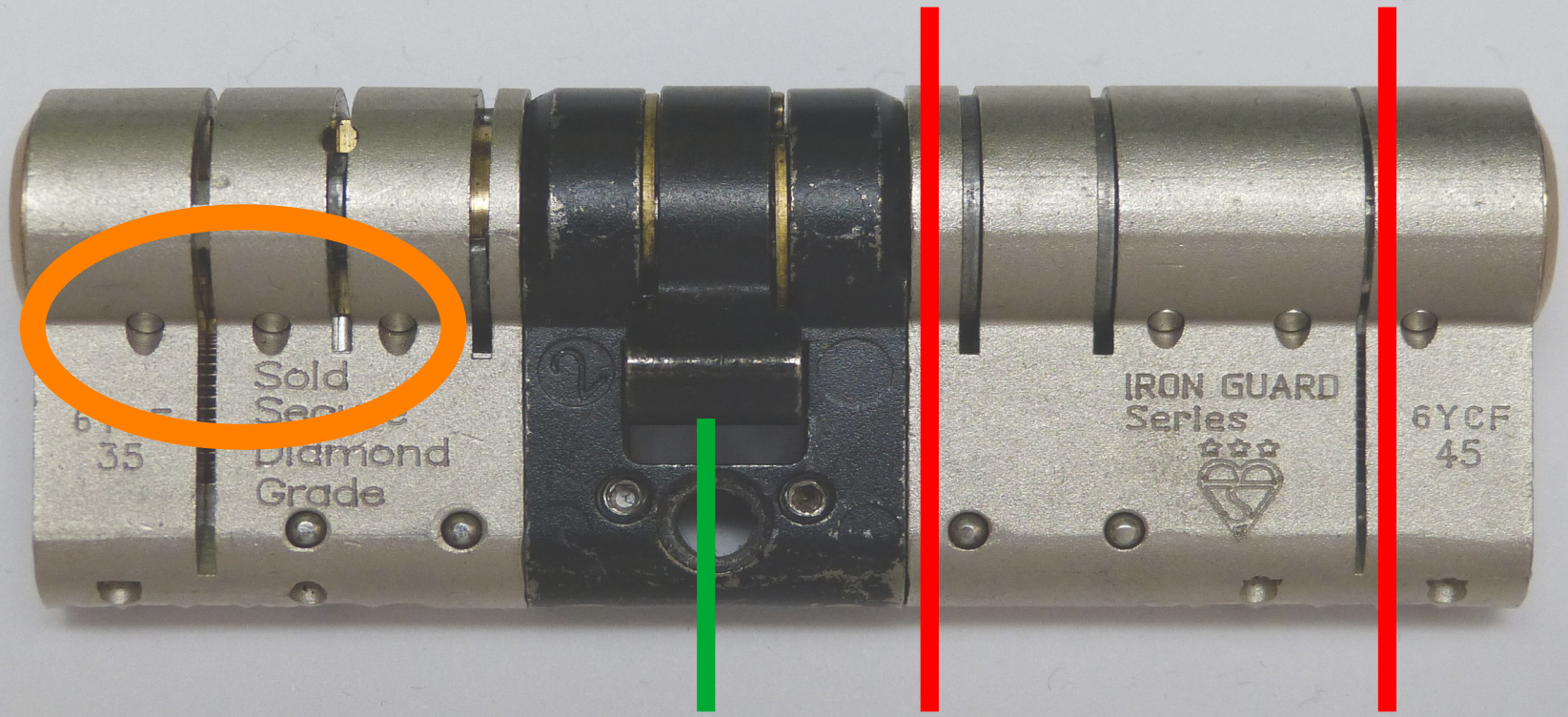


Euro profile cylinder








Sold
Diamond
Grade
IRON GUARD
Series
6YCF
45

(Better) Security advice

- Repeat: You can’t prevent burglaries
- You can make it harder to get in





(Better) Security advice

- Your threat model is not my threat model
- Consider the whole system
- Protect assets accordingly

(Better) Security advice

- Who has your keys?



(Better) Security advice

- Key control
  - Unauthorized Key duplication harder



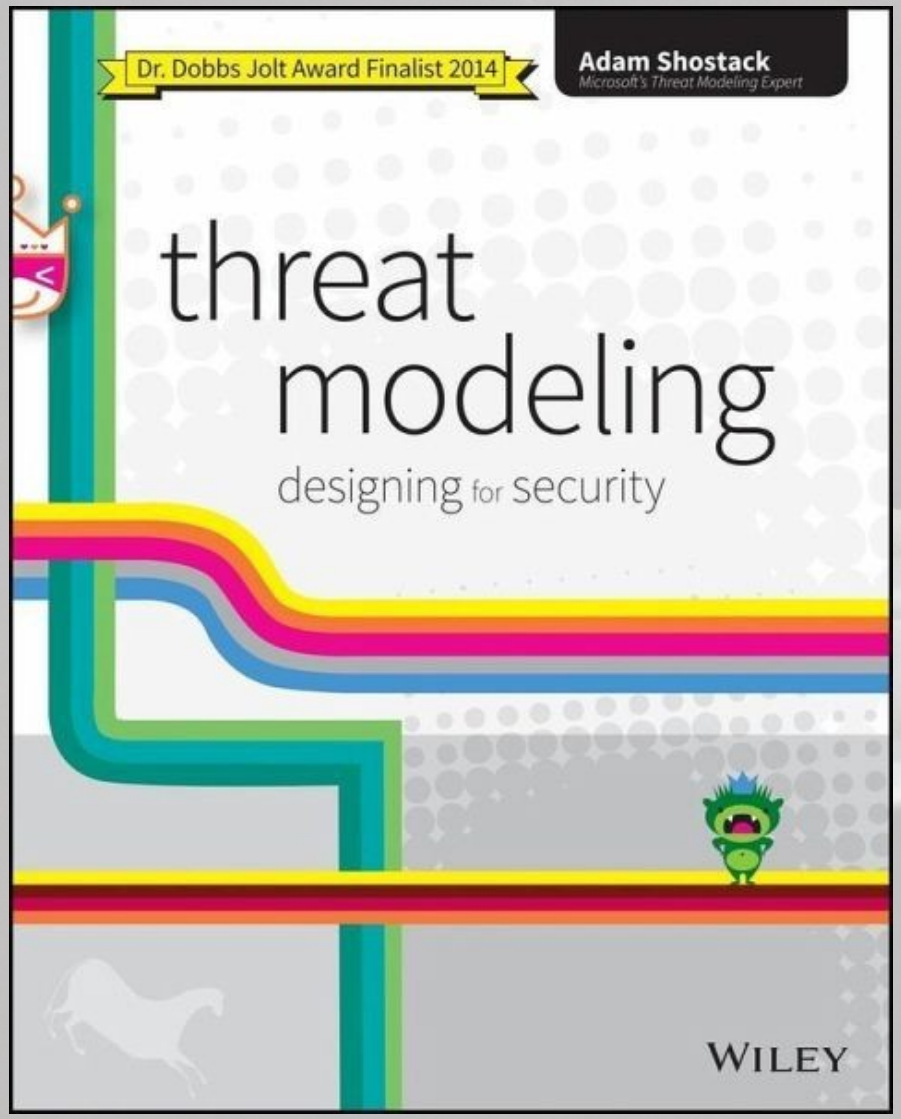
(Better) Security advice

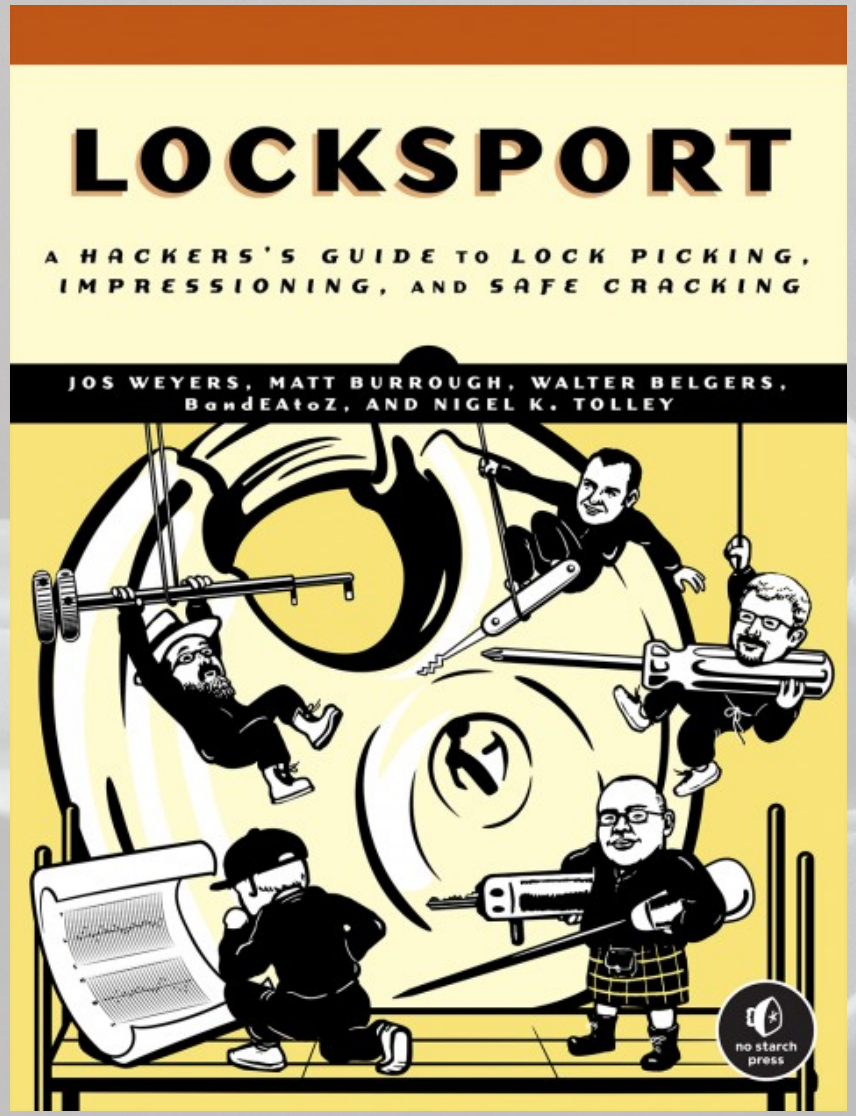
- Existing security schemes
  - SKG 3 = 5 minutes



Recap: Threat modeling

- For your system:
  - Find assets
  - Define attacker
  - Find vulnerabilities
  - Implement defense


Dr. Dobbs Jolt Award Finalist 2014
Adam Shostack
Microsoft's Threat Modeling Expert
threat modeling
designing for security
WILEY


LOCKSPORT
A HACKER'S GUIDE TO LOCK PICKING, IMPRESSIONING, AND SAFE CRACKING
JOS WEYERS, MATT BURROUGH, WALTER BELGERS, BandEAtoZ, AND NIGEL K. TOLLEY
no starch press

The end

- Question →
  - Lockpicking village next to Clairvoyance
- Contact:

  Jan-willem@Toool.nl

  @jwrm22