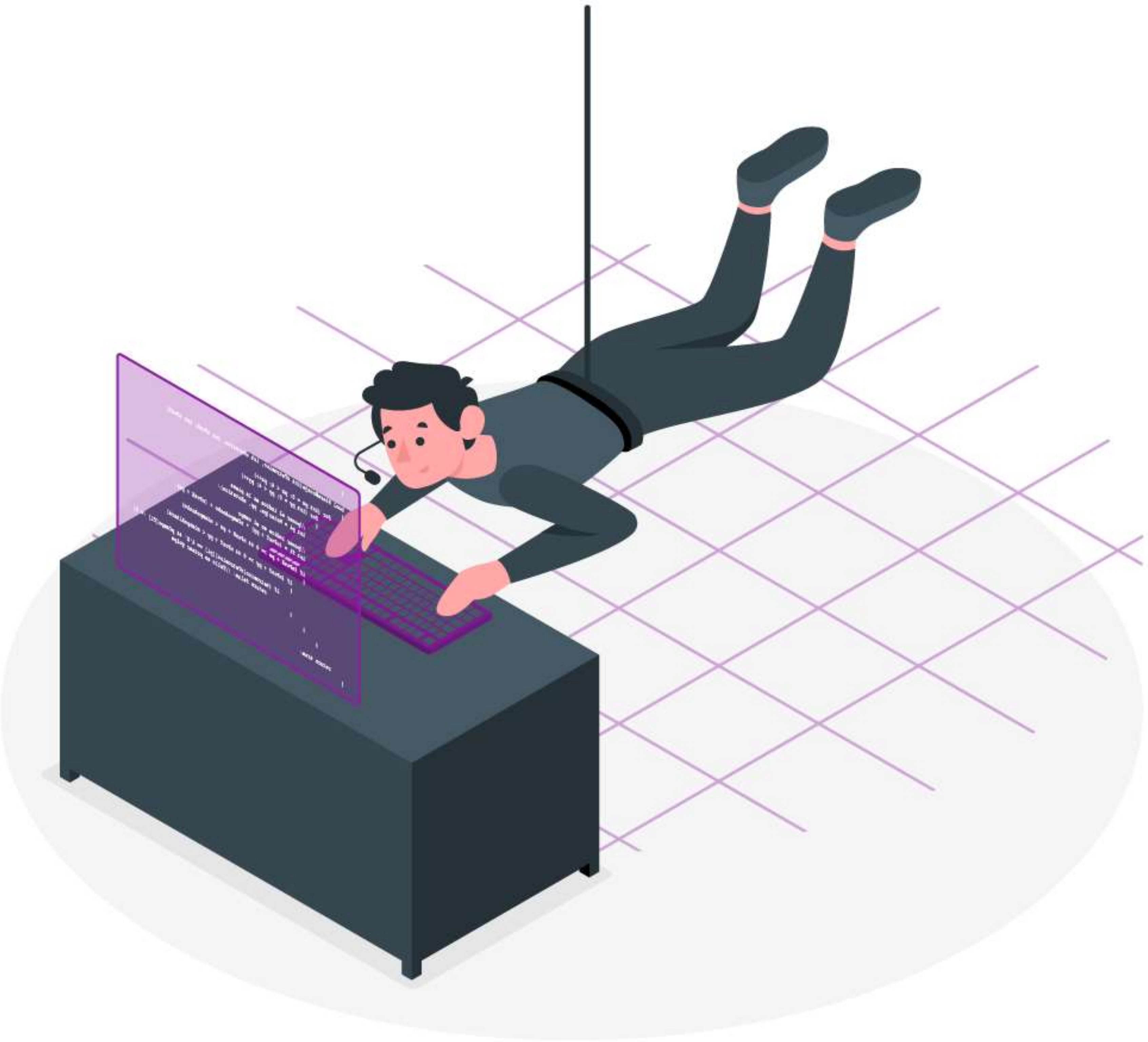
axelum

The Forgotten Attack Vector



Chris Cowling

11.10.2023

# whoami

Red Team Operator/Penetration Tester

1 of ±20 people with RTA Covert Entry Certification

Alphabet soup after my name

20+ years' experience

Primarily Blue-chip companies & Formula 1

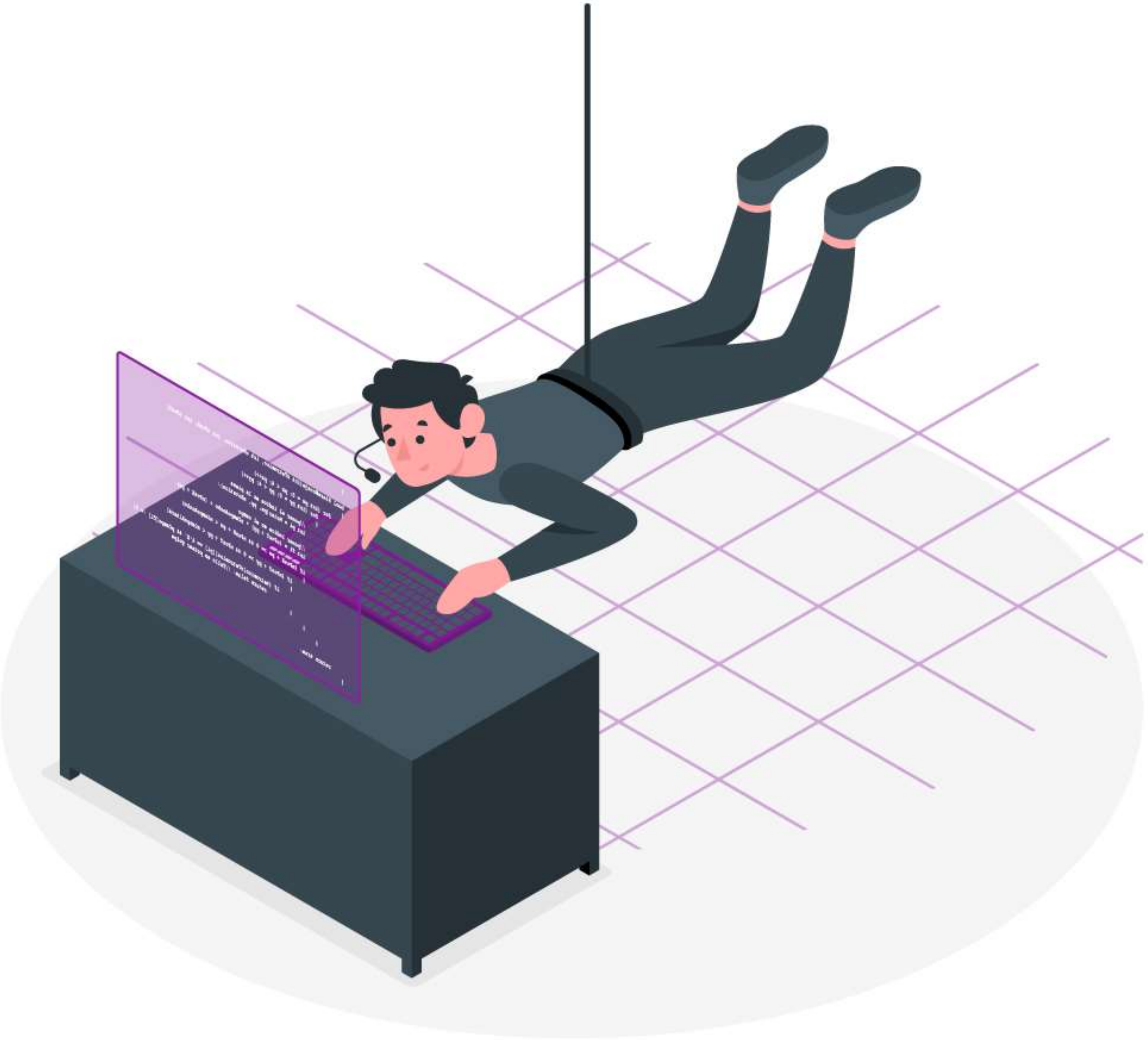
Cyber is getting harder

…in some ways

- Phishing is getting harder as users get trained
- Options such as macros being removed mean more complicated attack chains
- Constant penetration tests and SSDL are making it harder to get in from the web
- EDRs or XDR products are making the cat & mouse game of executing your payload more fun
- The evolution of AI is becoming an unknown factor

What if I told you that you didn‘t need to do initial access?

- The same vulns exist in the real world!



Physical Access

Making a comeback

"Given physical access to an office, the knowledgeable attacker will quickly be able to find the information needed to gain access to the organisation's computer systems and network." - Gregory White, 2003

Larger Attack Surface

- WiFi
- Physical Documents
- Photographs

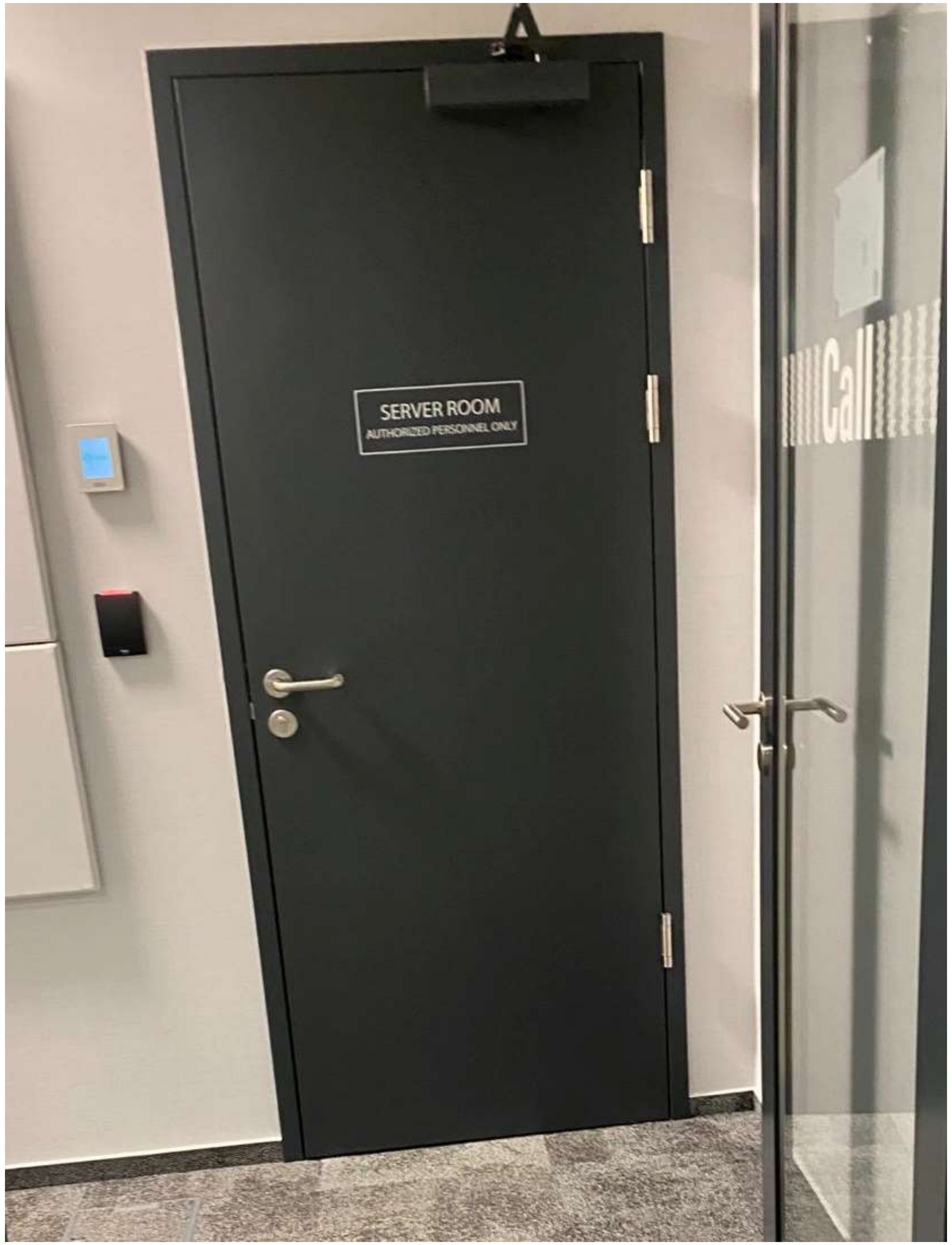
Direct Network Access

- Placing a network implant
- Direct access to the network
- Typically slurps documents sent to printers

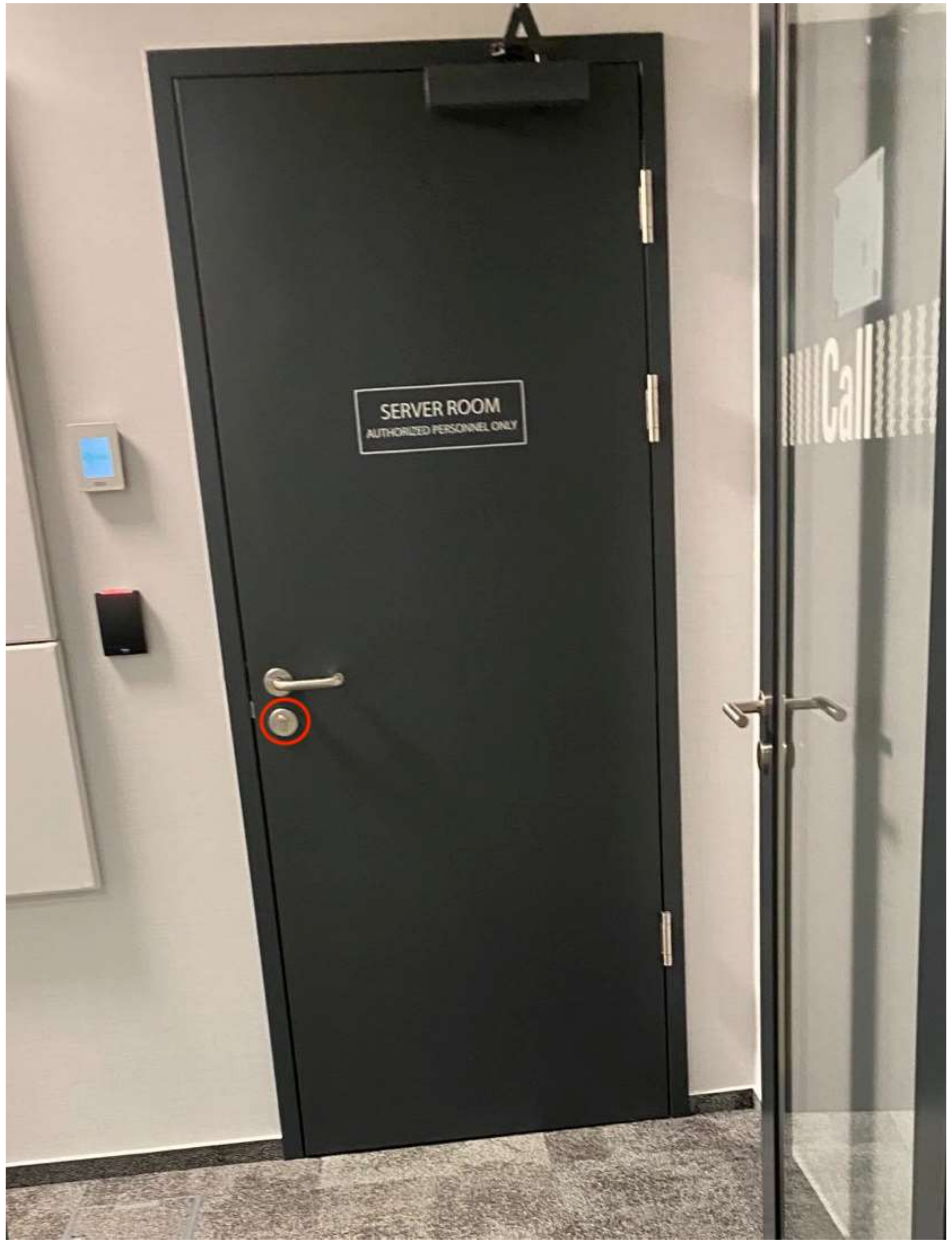
Personal Attacks

- Hardware Keyloggers
- Video Recording Devices
- Listening Devices

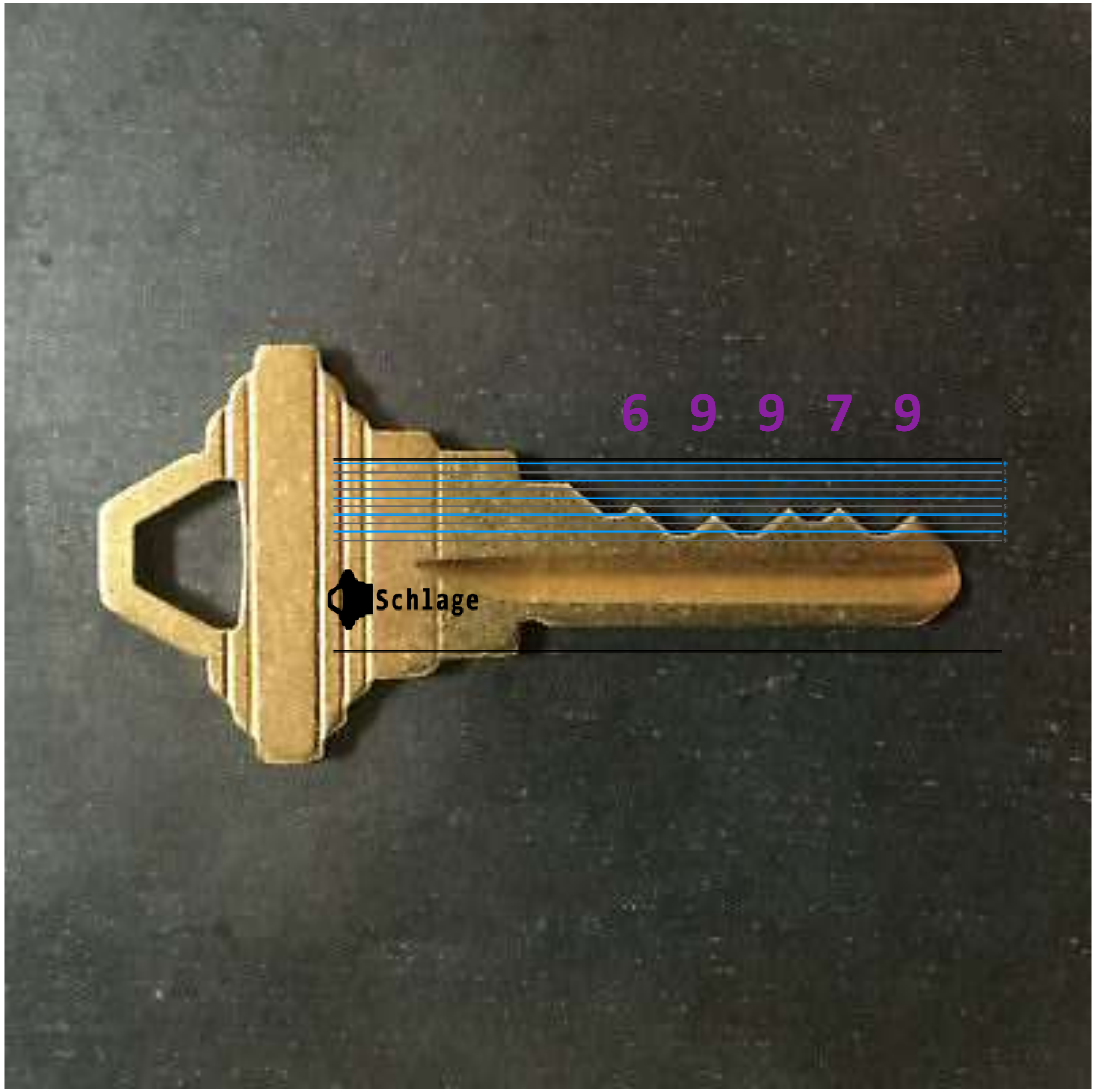
Introducing our door



Method 1: Use the Key Luke !

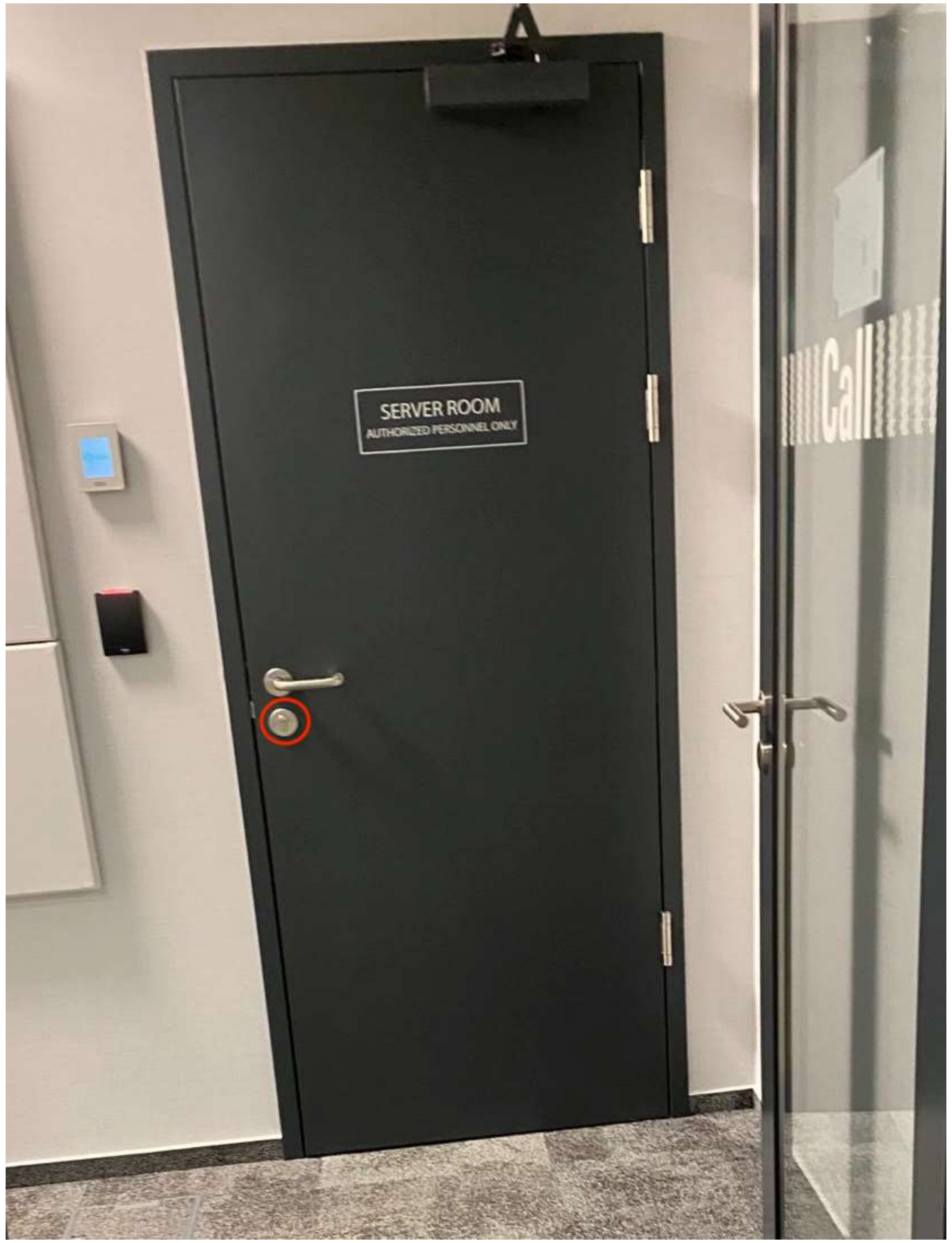


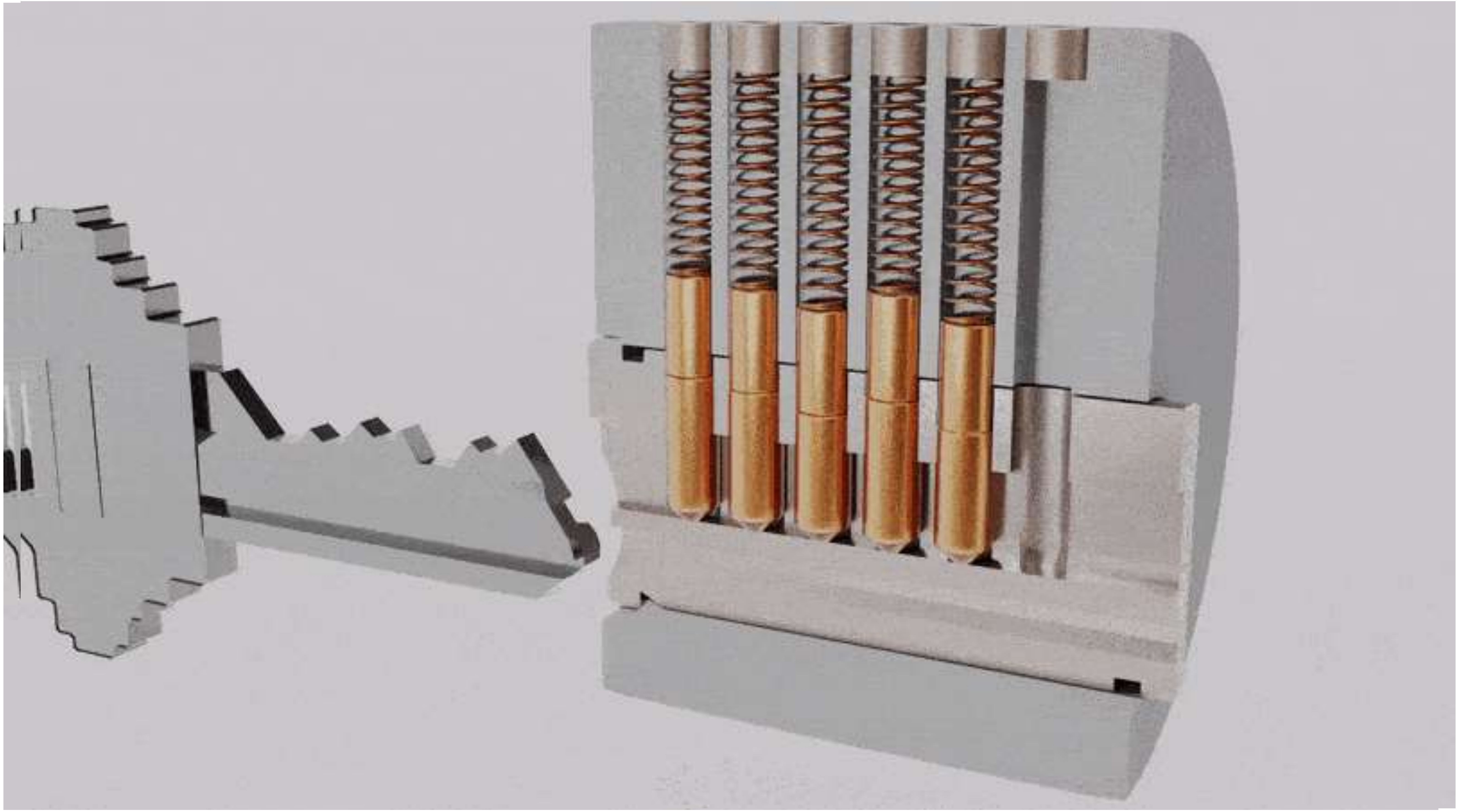
Photograph a key

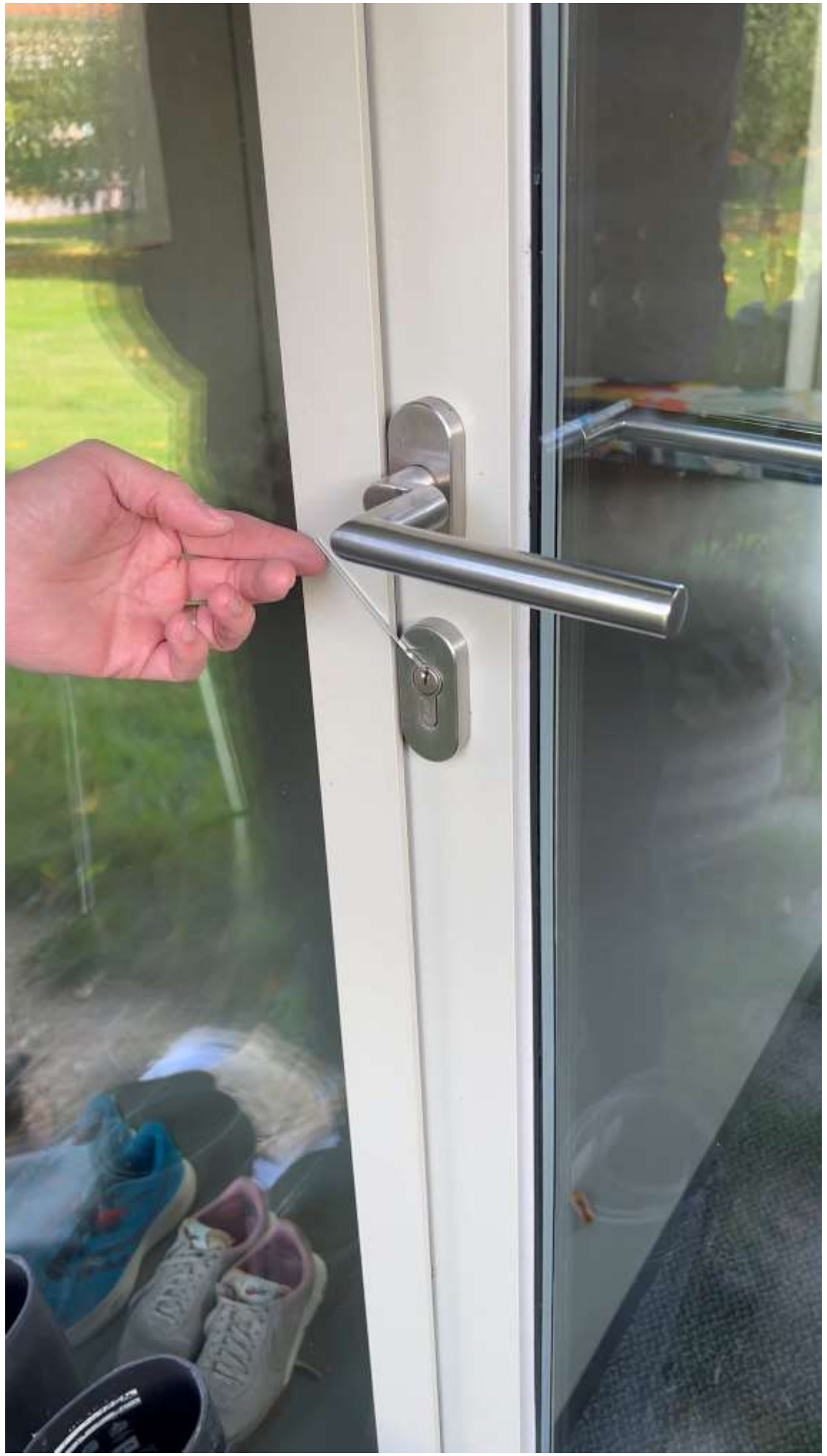


[redacted]

Method 2: Pick the Lock!

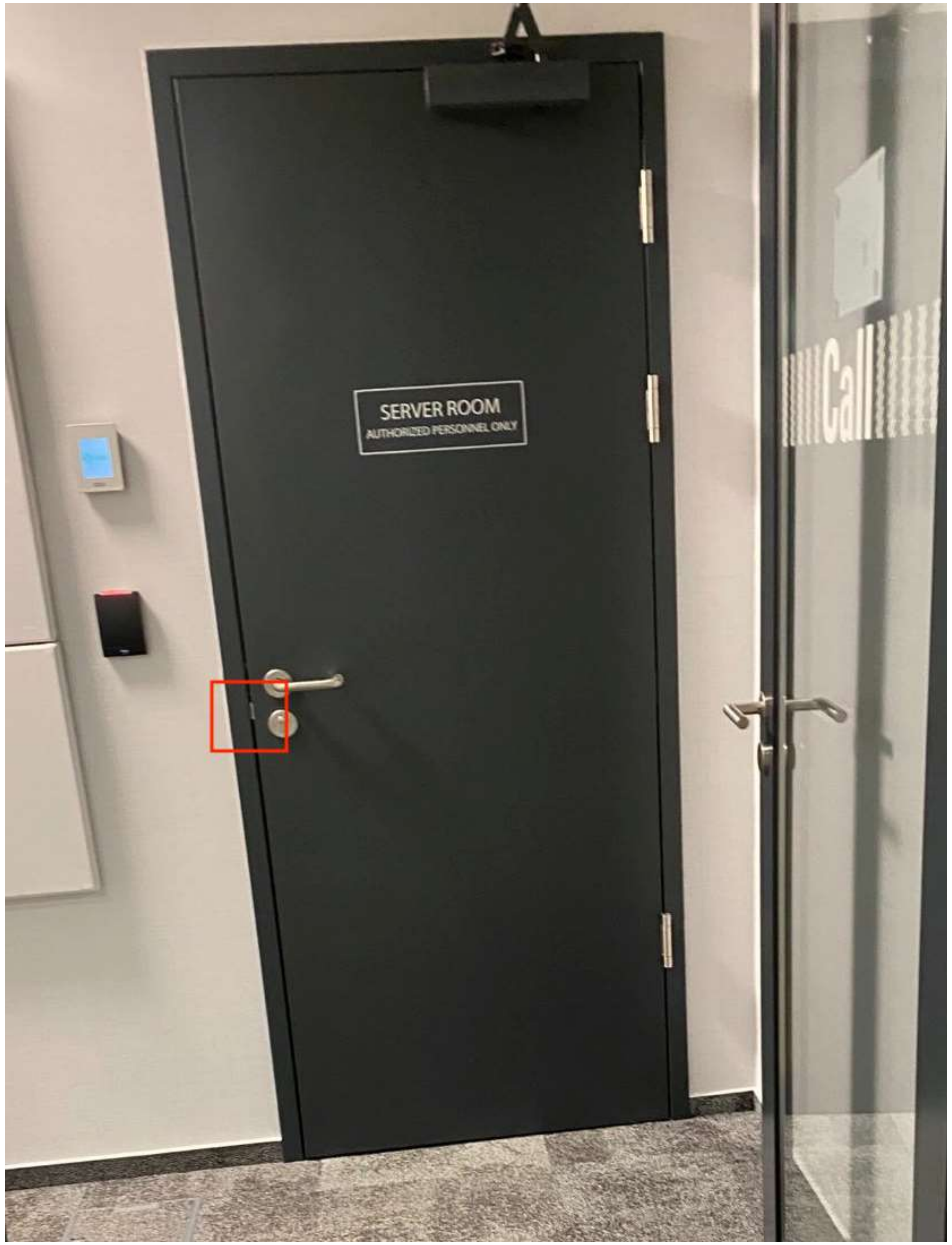






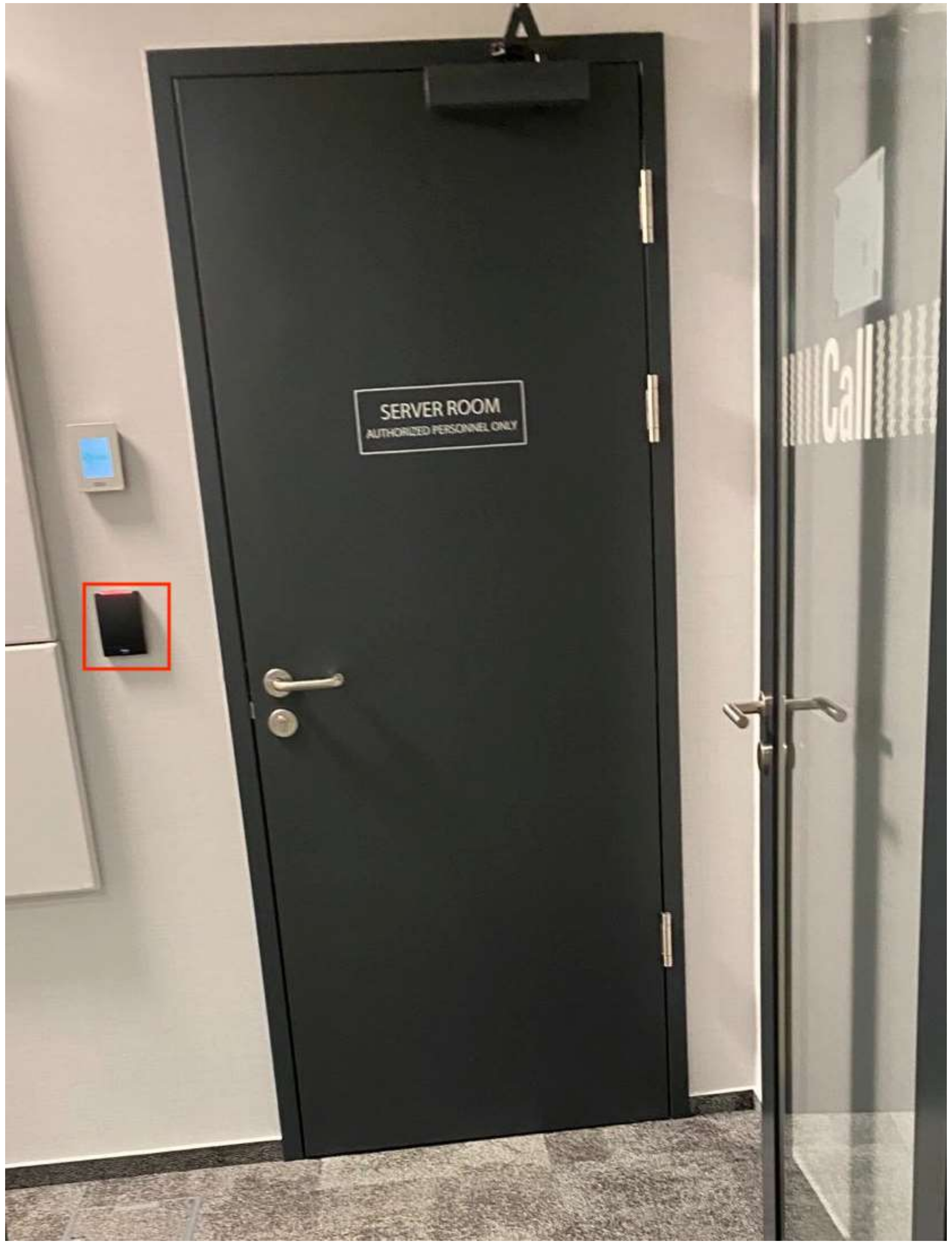
axelum

Method 3: Slip the latch!



axelum

Method 4: PACS

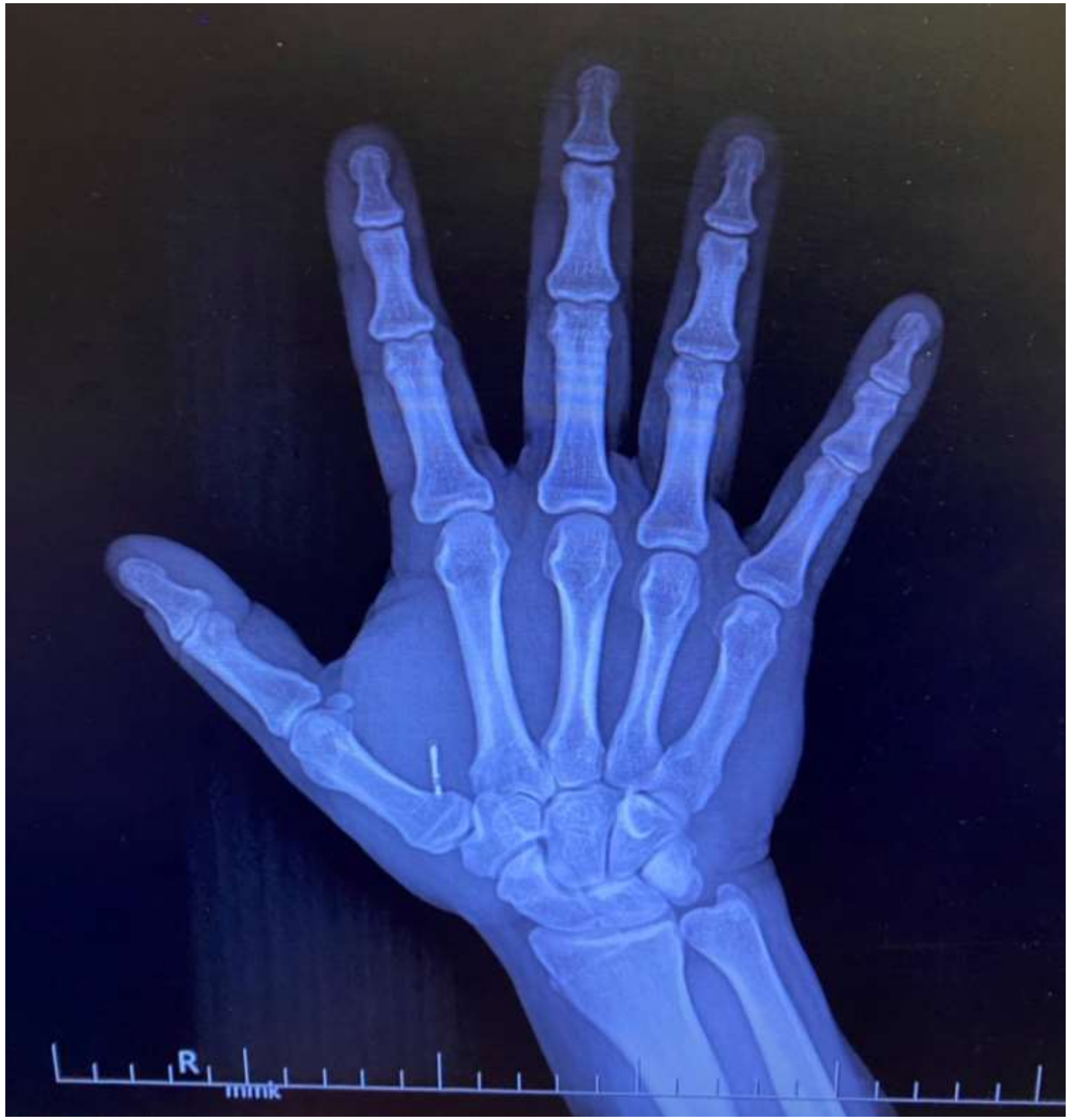


RFID Tools

A
B
PROXGRIND
ChameleonTiny
Professional

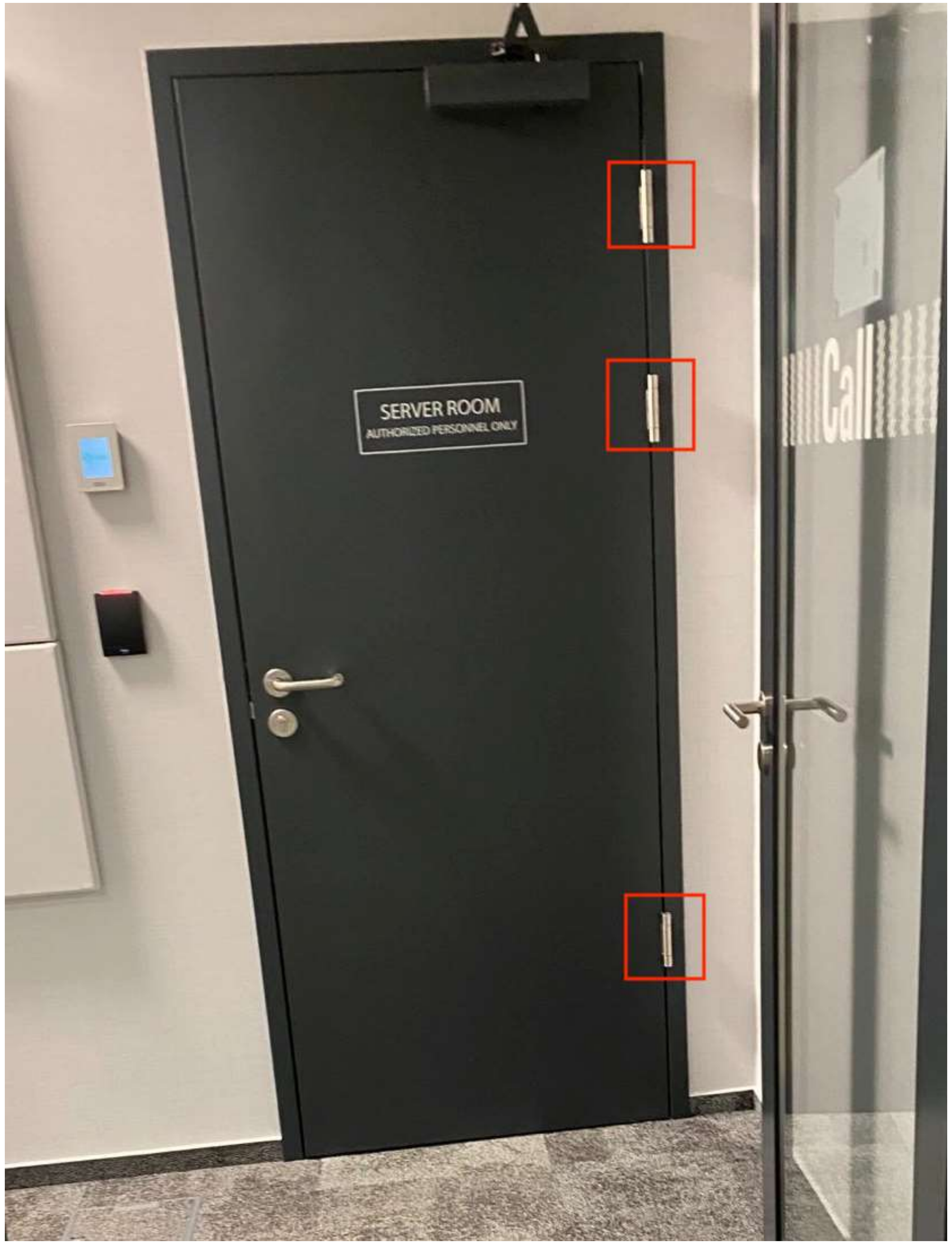
FLIPPER ZERO
Now Available!
FLIPPER

What do you copy them to ?

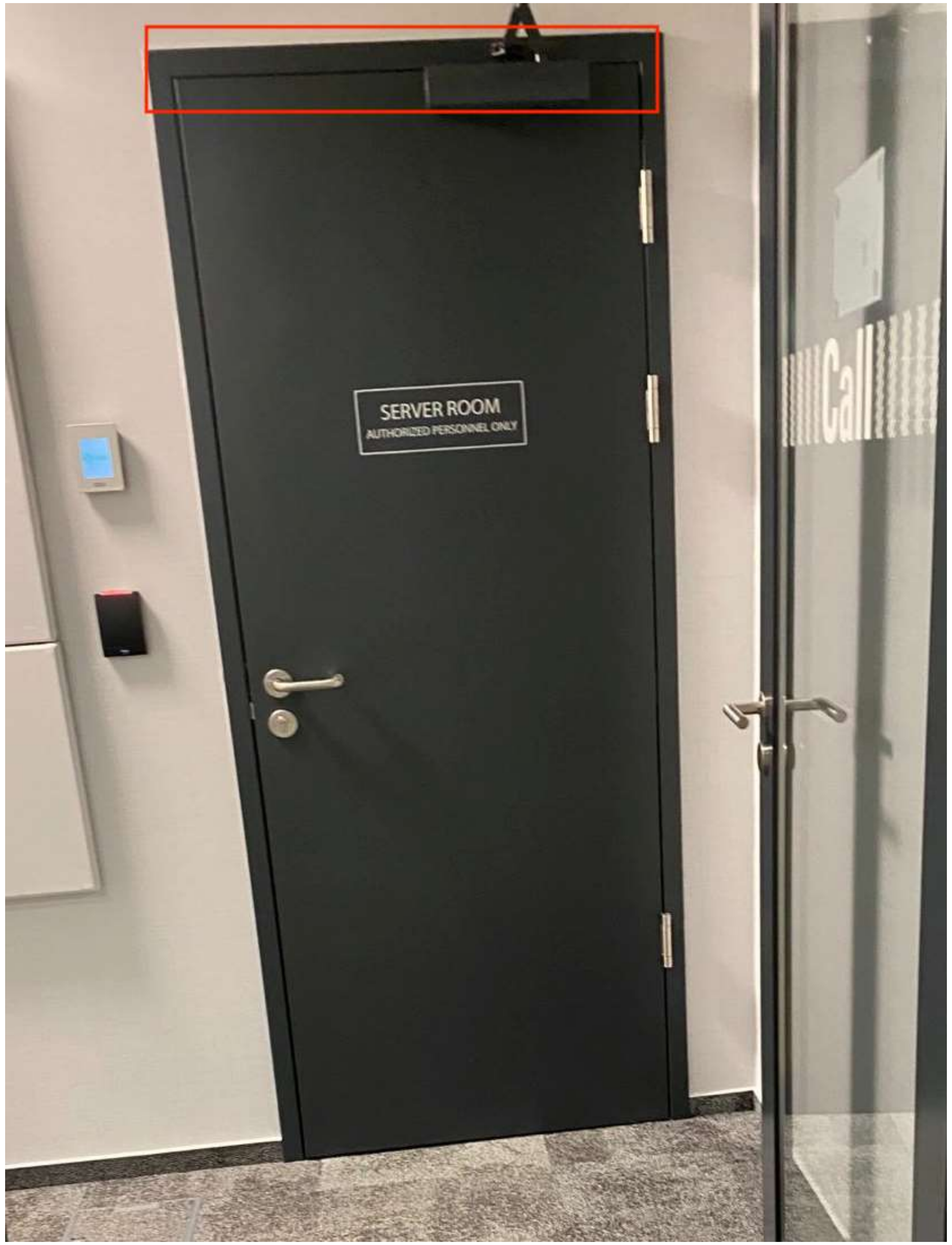


ESPKey

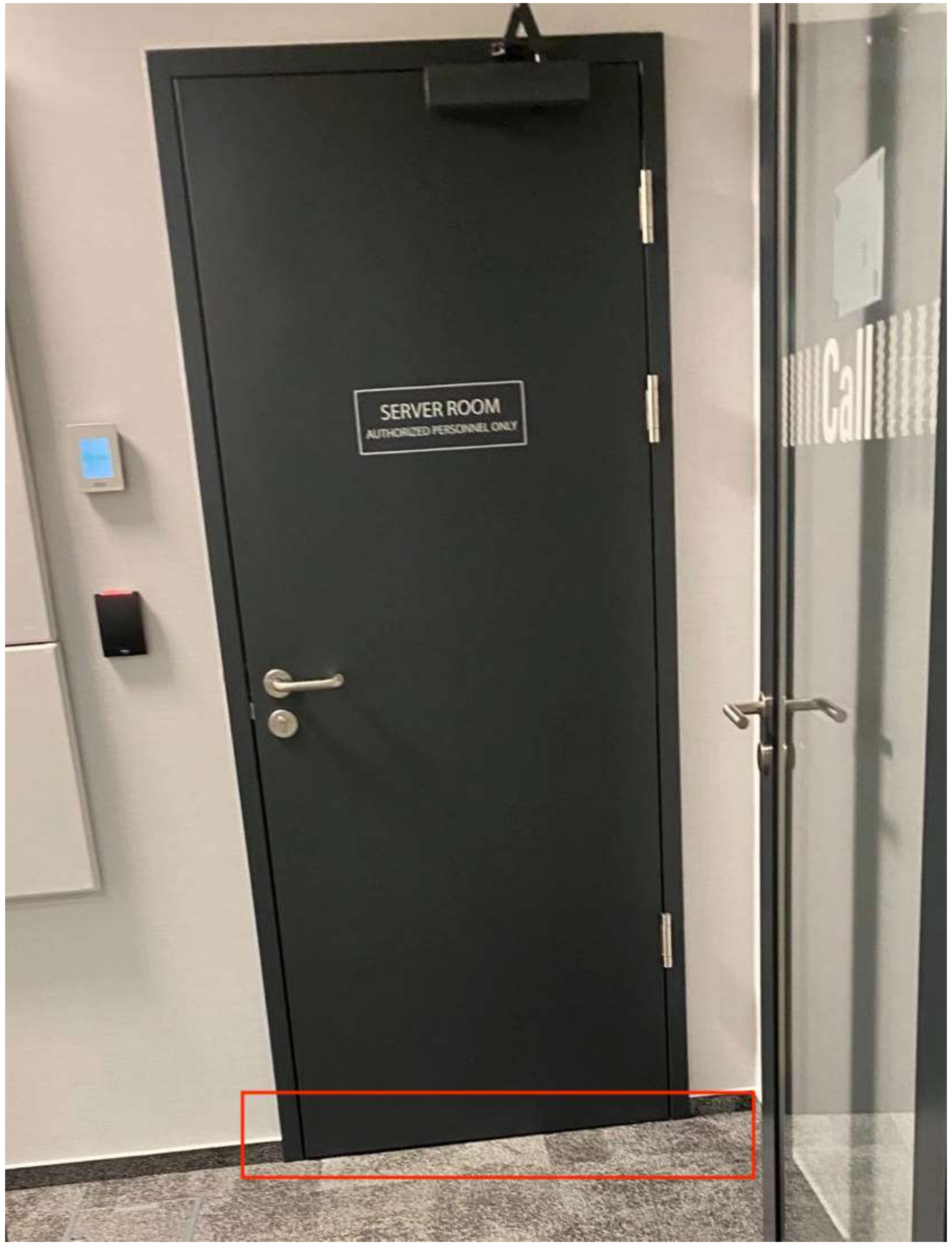
Method 5: Hinges



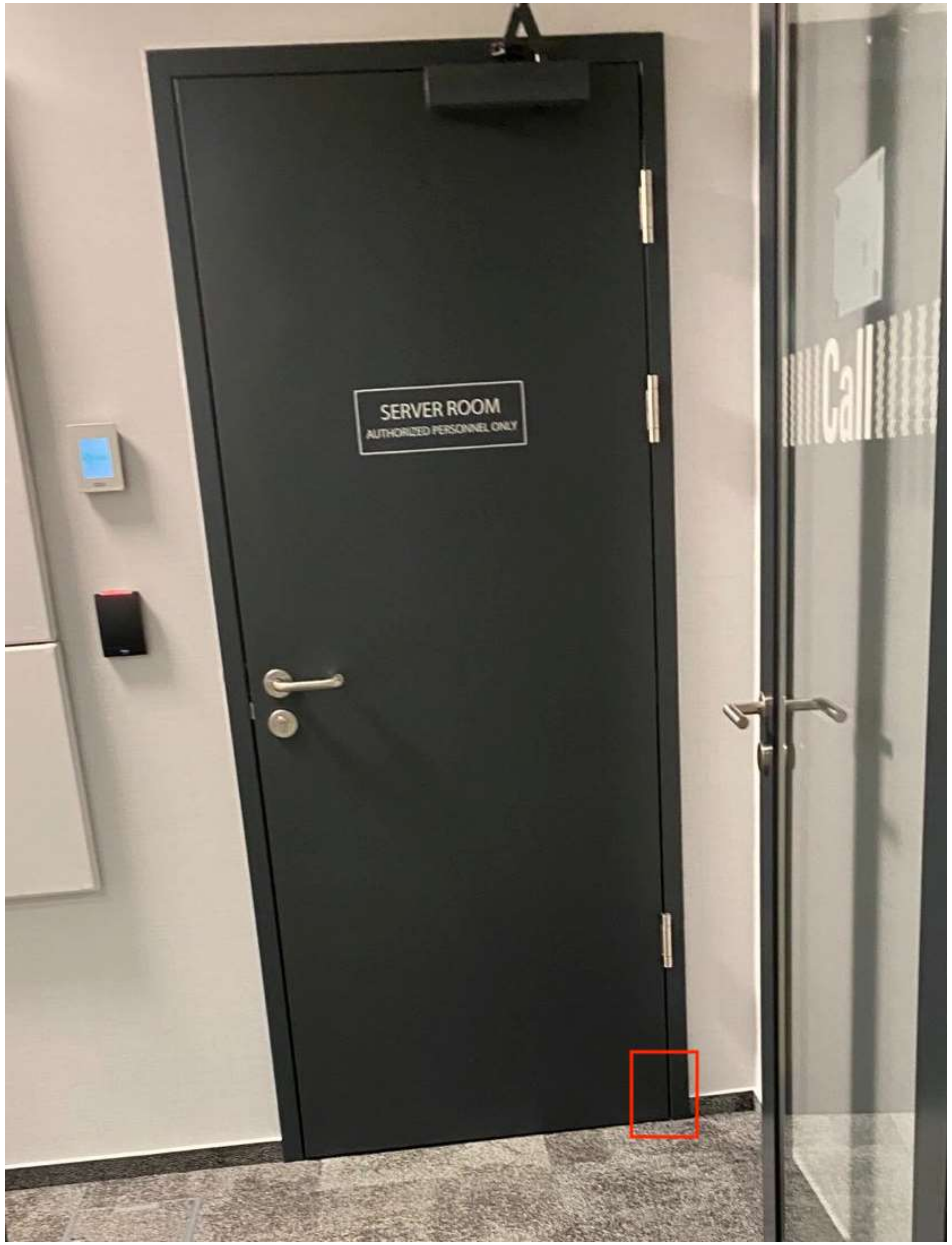
Method 6:
Over-the-door



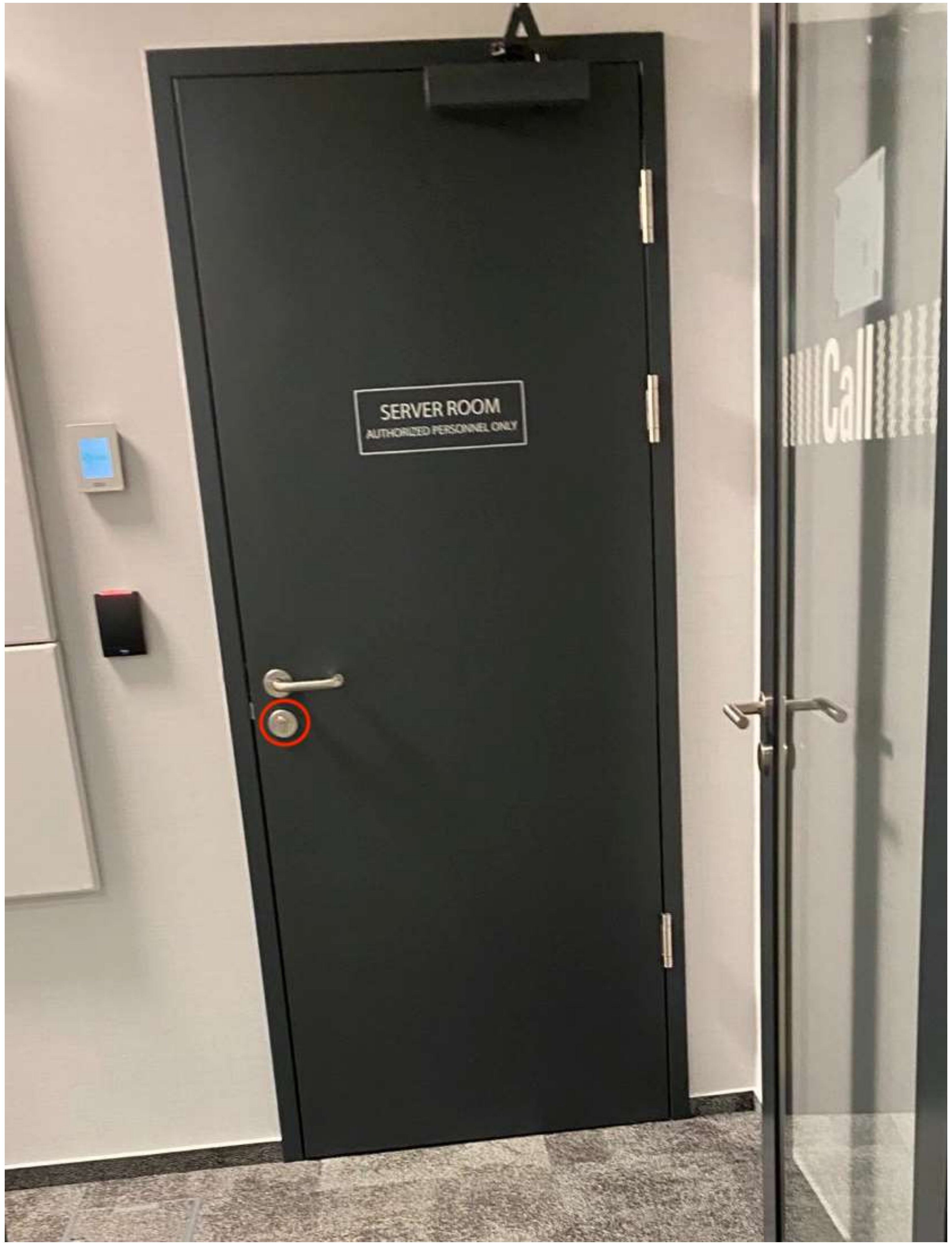
Method 7:
Under-the-door



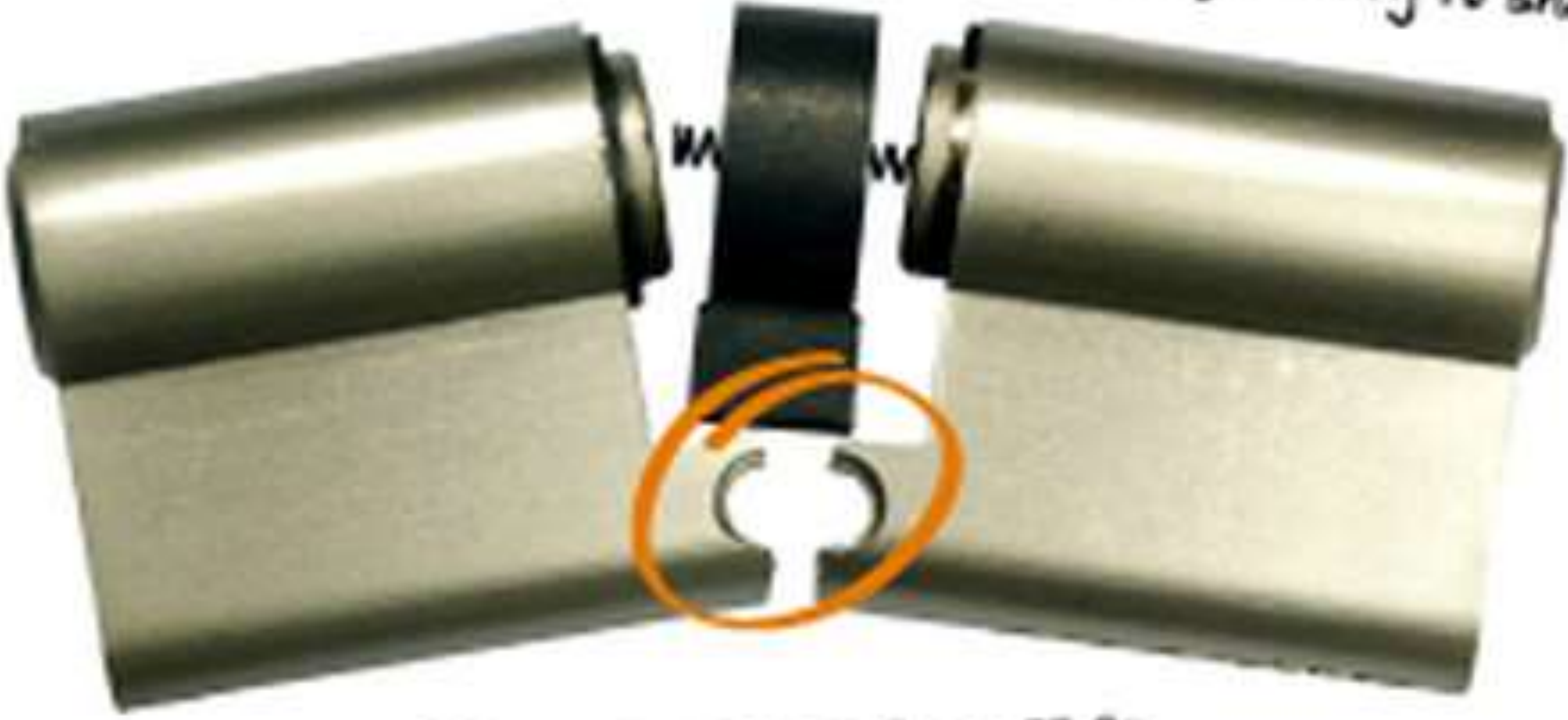
Method 8: The Pencil



Method 9: Destructive ?



[redacted]



The lock construction creates a weak point making it easy to snap!

13 seconds is all it takes to break-in!

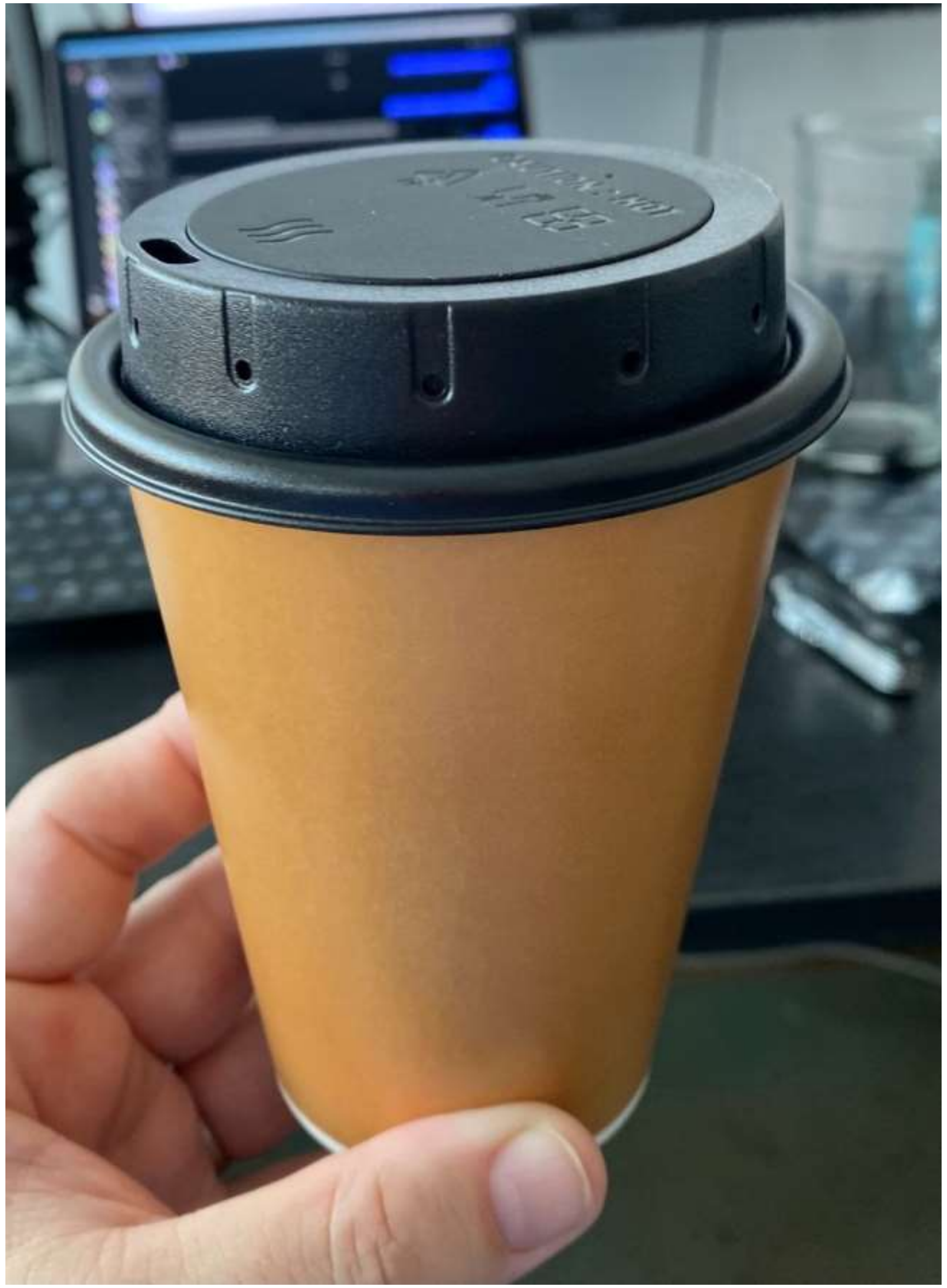
All before discuss

- Building segregation
- Cameras
- Alarms & Reed switches
- PIR Sensors
- Keypads
- Push Bars
- Glass Doors
- Thumbturns
- Garage Doors
- SDR
- REX Sensors
- REX button
- Disabled Access
- Door telephony
- Elevators
- Windows

EXIT
AUTOMATIC
CAUTION
DOOR
AUTOMATIC
CAUTION
DOOR

Or even mention Social Engineering

But you'd notice someone spying on you, right ?



axelum

www.axelum.eu

axelum

axelum