Physical Security

Let’s think like a defender …


Computer Science and
Engineering Building

Let’s think like an attacker…

Mystery hot tub: Who installed the 'bubbler' on the roof of a University of Michigan building?

By KELLIE WOODHOUSE Higher education reporter

39 Comments

Posted on Fri, Feb 24, 2012 : 11:34 a.m.


CHASE
NO ENVELOPES OR DEPOSIT SLIPS NEEDED.
NEW! DepositFriendly ATM
GET YOUR CASH. TWICE AS FAST.

(voting machine)

What Is Physical Security?

- Any physical object that creates a barrier to unauthorized access
- This includes: locks, latches, safes, alarms, guards, guard dogs, doors, windows, walls, ceilings, floors, fences, door strikes, door frames and door closers

Destructive vs. Nondestructive Entry

- Destructive entry
  - Involves using force to defeat physical security
  - Methods involve crowbars, bolt cutters and sledge hammers
  - Negative impact on IT resources is apparent
  - Remediation steps also obvious
- Nondestructive entry
  - Compromises security without leaving signs of a breach
  - Defeats intrusion detection
  - Greater and long-term threat

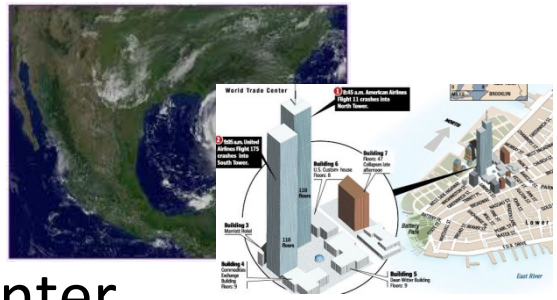
Is Physical Security An IT Concern?

- You have been working hard to secure your network from cyber attacks
  - Redundant layers of authentication, firewalls, and intrusion detection systems should protect against electronic methods of entry
- But what if an attacker gains access to the server room or network wiring closet ...
  - Is you network still safe?

Type of Threats to Physical Environment

- Natural / Environmental
  - Earthquakes, floods, storms, hurricanes, fires, snow/ice
  - Consequence of natural phenomena
- Man made / Political Events
  - Explosives, disgruntled employees, unauthorized access, employee errors, espionage, arson/fires, sabotage, hazardous/toxic spills, chemical contamination, malicious code, vandalism and theft
  - Acts of commission or omission

Lessons-Learned for U.S.



- Major Domestic Events:
  - 2005 Hurricane Katrina (1,836)
  - 2001 9/11 Attack: World Trade Center, Pentagon, and Shanksville, PA (2,982)
  - 1995 Federal Office Building, Oklahoma City (168)

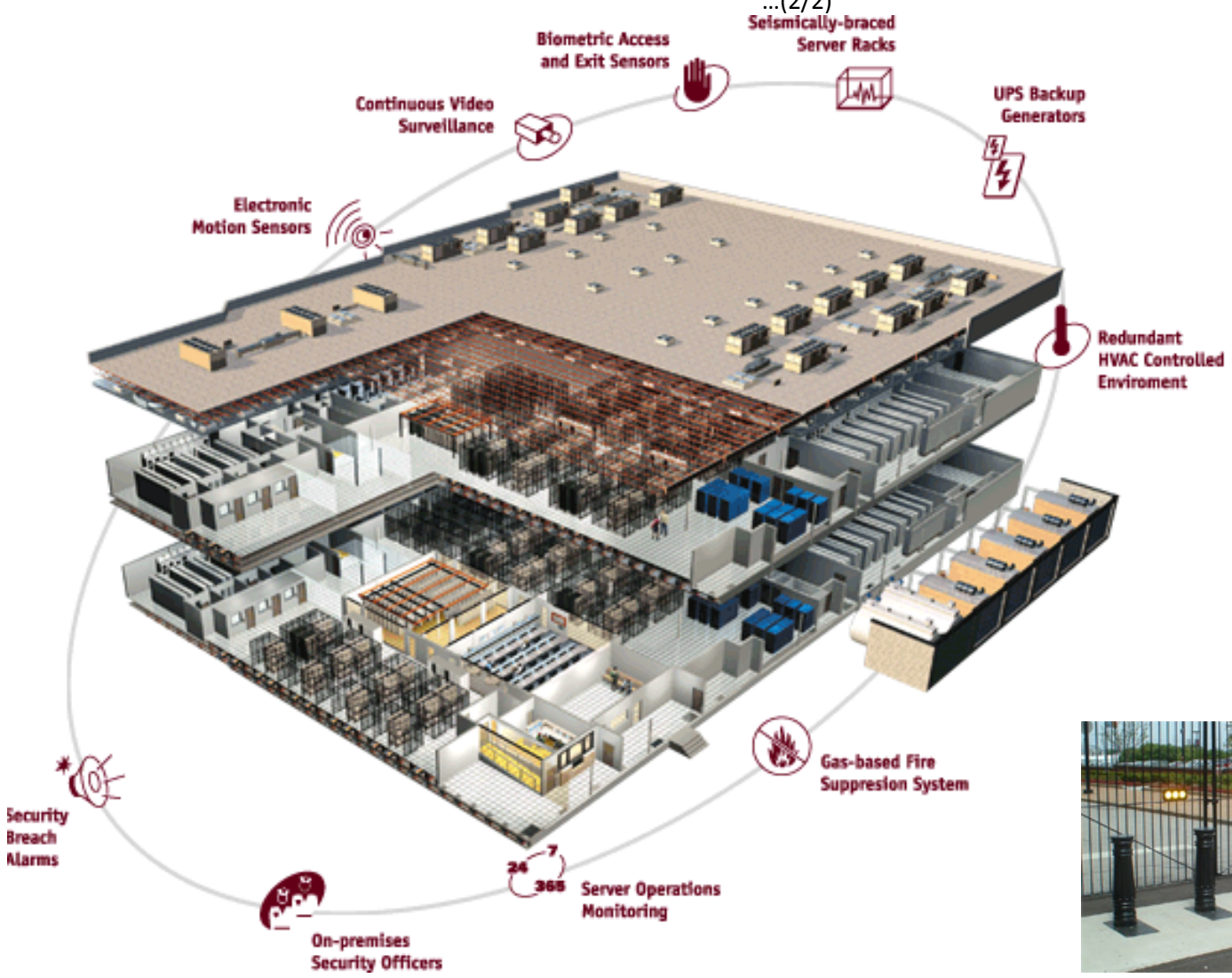
- Major International Events:
  - 1998 U.S. Embassy, Kenya (237)
  - 1983 Beirut Barracks, Lebanon (309)

Categories of Security Controls

- Management (Administrative) Controls
  - Policies, Standards, Processes, Procedures, & Guidelines
    - Administrative Entities: Executive-Level, Mid.-Level Management
- Physical Controls
  - Physical Security (Facility or Infrastructure Protection)
    - Locks, Doors, Walls, Fence, Curtain, etc.
    - Service Providers: FSO, Security Guards, Dogs
- Technical (Logical) Controls
  - Access Controls , Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - CCTV & Camera, IDS, Moisture detection system, Fire/Smoke detection system, Fire suppression, Environmental control system, UPS, etc.
    - Service Providers: Building Architect, Critical Infrastructure Protection (CIP) Engineer, Operations Center.

Strategic Approach to Physical Security

...(2/2)



Source: Global Crossing website

Physical Controls – Facility Construction

- Structured barriers: Perimeter structure
- Walls & Fencing
  - Specific gauge and fabrication specifications (e.g. No. 11 gauge galvanized chain-link fencing material.)
  - Specify height, or need for "top guard" (e.g. 8-ft in height, 6-in. under ground with top guard.)

Height	Protection
1 meter / 3 – 4 ft	Deters casual trespassers
2 meter / 6 – 7 ft	Too high to climb easily
2.4 meter / 8 ft with top guard	Deters determined intruder

Source: *Official (ISC)² Guide to The CISSP Exam*

Physical Controls – Facility Construction

- Structured barriers: Entry points
  - Gates, bollards, roadways.
  - Doors, windows, ventilation airways, manhole covers, etc.
  - Department of State and DoD Anti-Ram Vehicle Barrier Certification Criteria (SD-STD-02.01):

Vehicle Weight: 15,000 lb.	
Speed Rating	**Speed at Impact**
K4	30 mph
K8	40 mph
K12	50 mph

Vehicle Weight: 15,000 lb.	
Penetration Rating	**Penetration Distance**
L3	< 3 ft
L2	3 – 20 ft
L1	20 – 50 ft

Reference: http://www.probarrier.com/faq/certify.asp

Technical Controls – Entrance Protection

Entry access control systems

- Turnstiles
  - Revolving doors that can be activated to “lock” and not allow unauthorized individuals to enter or leave facility
  - To prevent “piggybacking”.
- Mantraps
  - Routing people through two stationary doorways
- Fail-safe
  - Door defaults to being unlocked.
- Fail-secure
  - Door defaults to being locked.

Technical Controls

Entry access control systems –

- Mechanical locks:
  - Key
  - Combination locks
  - Magnetic locks

- Electronic locks:
  - Combination lock
  - Proximity / RFID badge
  - Bio-metric

How does one evade these controls?

Social Engineering

Scenario

- You have conducted pen tests of your web site
- You have a sophisticated ASA firewall sitting on the border which can use adaptive rule sets to detect potential attacks
- You have security officers monitoring the inbound packet streams using SNORT to look for attacks
- Your website is bulletproof…

Scenario

- But…and this really happened
- At 3 am a guy walks up to the front lobby door and holds up a sign to the cleaning crew that says in English and Spanish “Perdi, mis llaves!”
- The guy has an ID card that says “Marriott Elite Silver”. The crew lets him into the building.
- Guy walks around and finds a locked door marked “Server Room”. Unfortunately, it’s a crypto lock.

Scenario

- Three guesses and no luck.
- Guess what, the Armstrong ceiling tiles!
- Turn over a trashcan, pop the tile, the wall the doesn’t go all the way up.
- The guy climbs over the wall and is in the server room safe and sound.
- Now, the guy walks over to your web server, pops Knoppix into the DVD drive and reboots the server.

Scenario

- With knoppix running, mount the hard drive, locate the windows passwords take a quick picture, reboot the server, remove the disk, exit the building.
- The adminstrator password is “ScoobyDoo!”
- Later that night, attempt to connect to the linux server which is available via ssh, login as root with password, well, you guessed it.
- Dump all employee data with SS numbers, etc. from the database.

The Social Engineering Threat

- Spear Phishing, et. al
  - This is the art of getting you to compromise your own systems
  - “Click this link to reset your bank password”
- True Social Engineering
  - If I can talk my way past your guards, your security system, your fence, your locks, your guns and tasers, etc. You have already lost.
  - Beware the human with the clipboard and laminated id card.

Avoiding Social Engineering

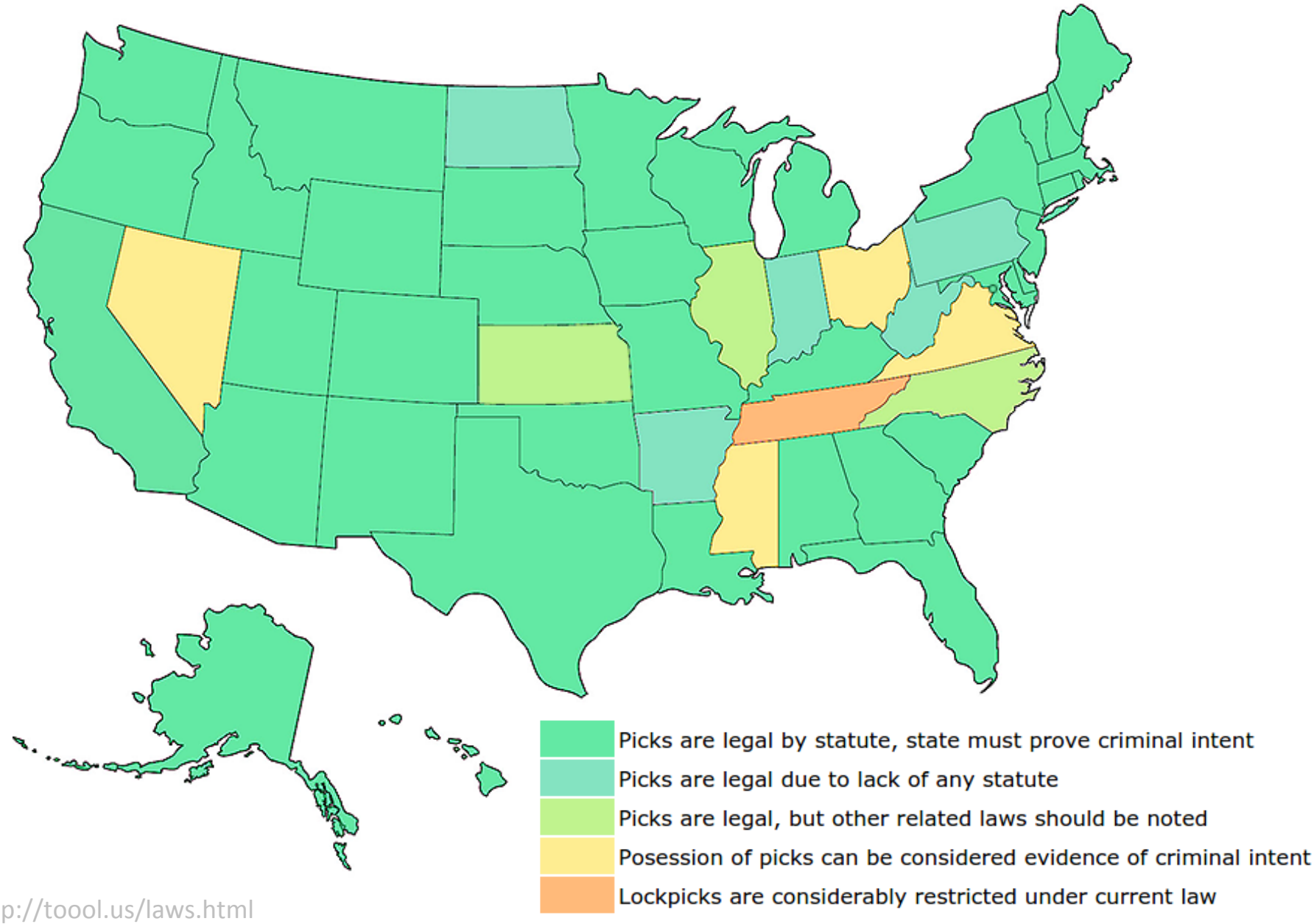
- Training, Training, Training
  - Your individuals with access must be trained properly!
    - EVERYONE must have their ID checked and be escorted
  - Your staff must also be trained properly.
    - Anyone without ID should be approached, politely.
    - “Hi, may I help you find somone?”
  - You must eliminate phishing attacks via regular and repeated training. You must test this on a regular basis.

Locks and Keys

Legal Notice

- Laws regarding lock picking vary significantly state-by-state
- In most states purchase and possession of dedicated lock picking tools is legal
  - Penalties are raised significantly if you get caught using them in the commission of a crime

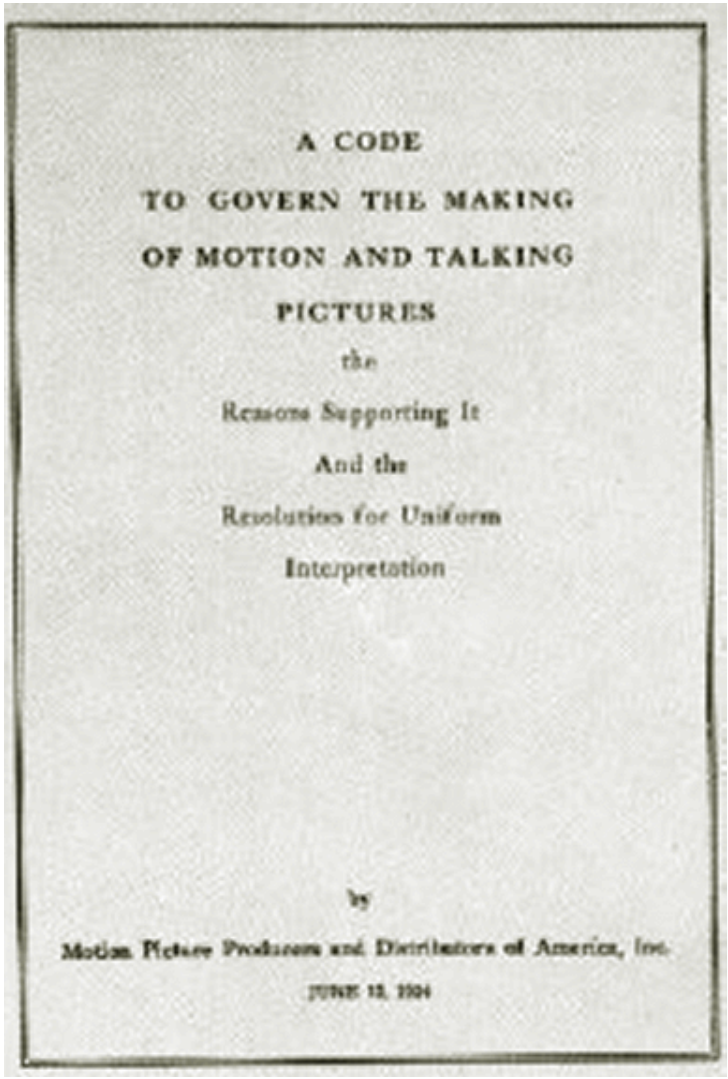
Public domain image from http://commons.wikimedia.org/wiki/File:Madame_Restell_in_jail.jpg



http://toool.us/laws.html

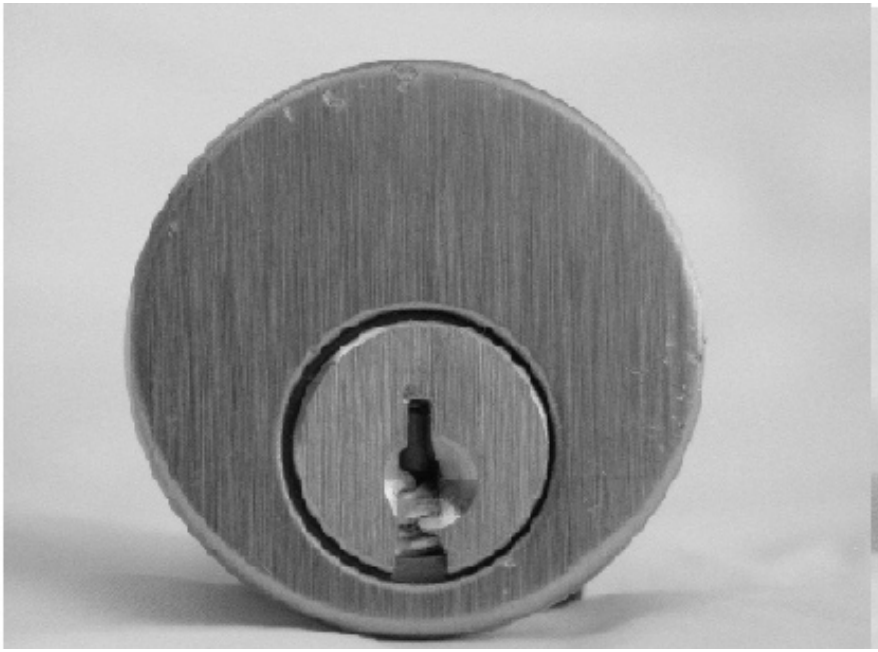
Lock Picking in Movies

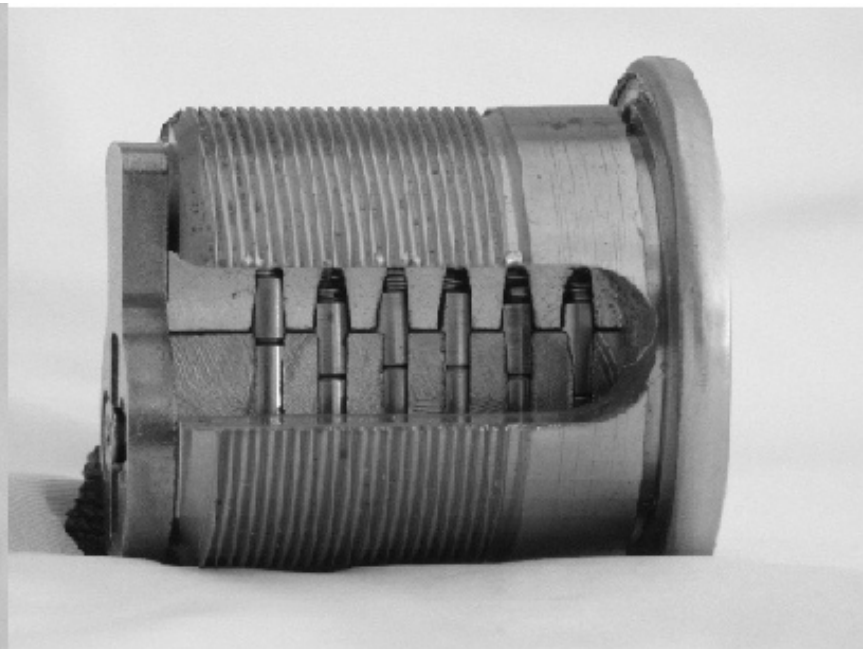
- Genuine lock picking in movies used to be prohibited
- Before 1967, the Hays code (Motion Picture Production Code) required censorship of Hollywood movies
  - "All detailed (that is, imitable) depiction of crime must be removed, such as lock picking or mixing of chemicals to make explosives"

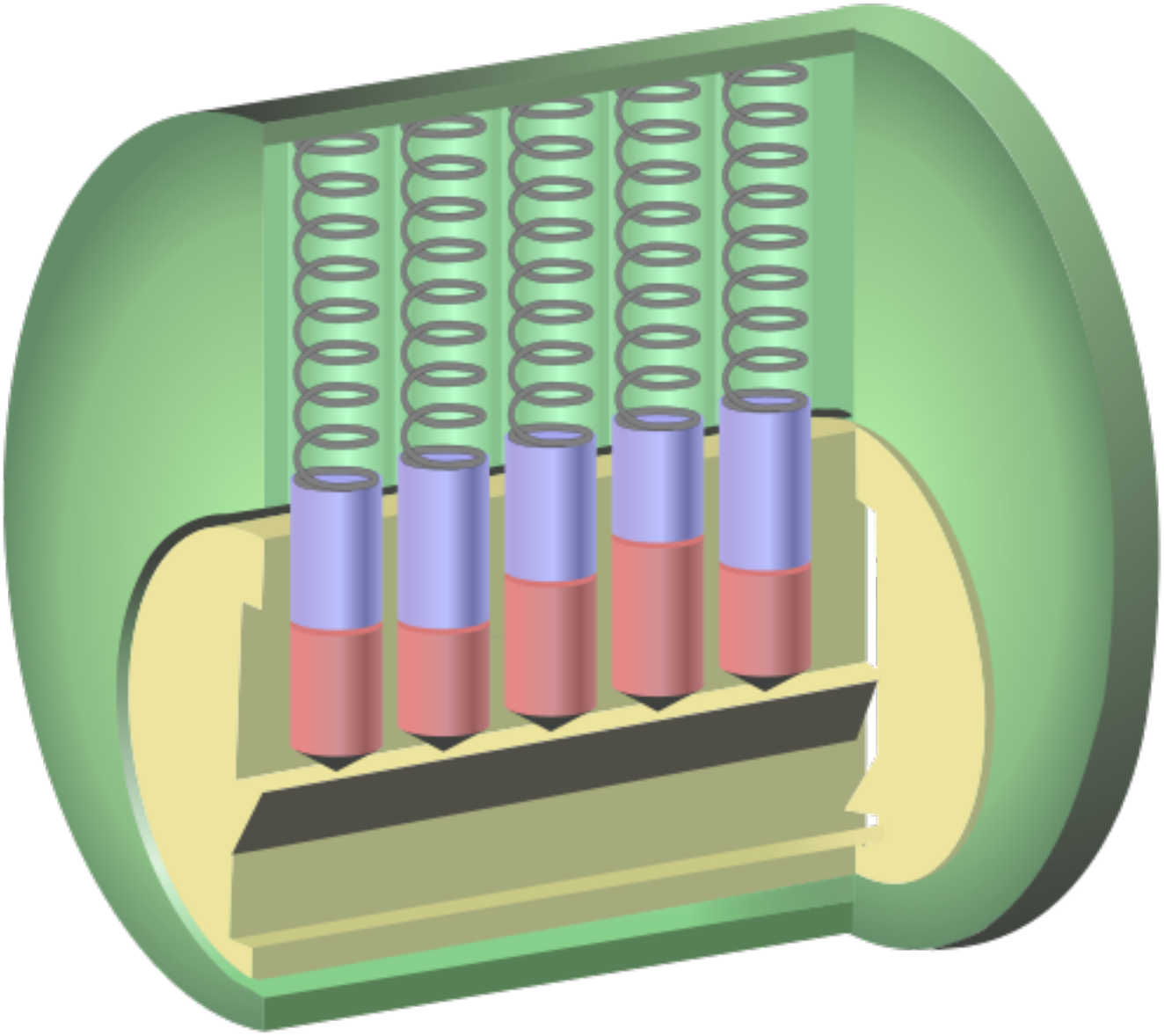

A CODE
TO GOVERN THE MAKING
OF MOTION AND TALKING
PICTURES
the
Reasons Supporting It
And the
Resolutions for Uniform
Interpretation
by
Motion Picture Producers and Distributors of America, Inc.
JUNE 13, 1934

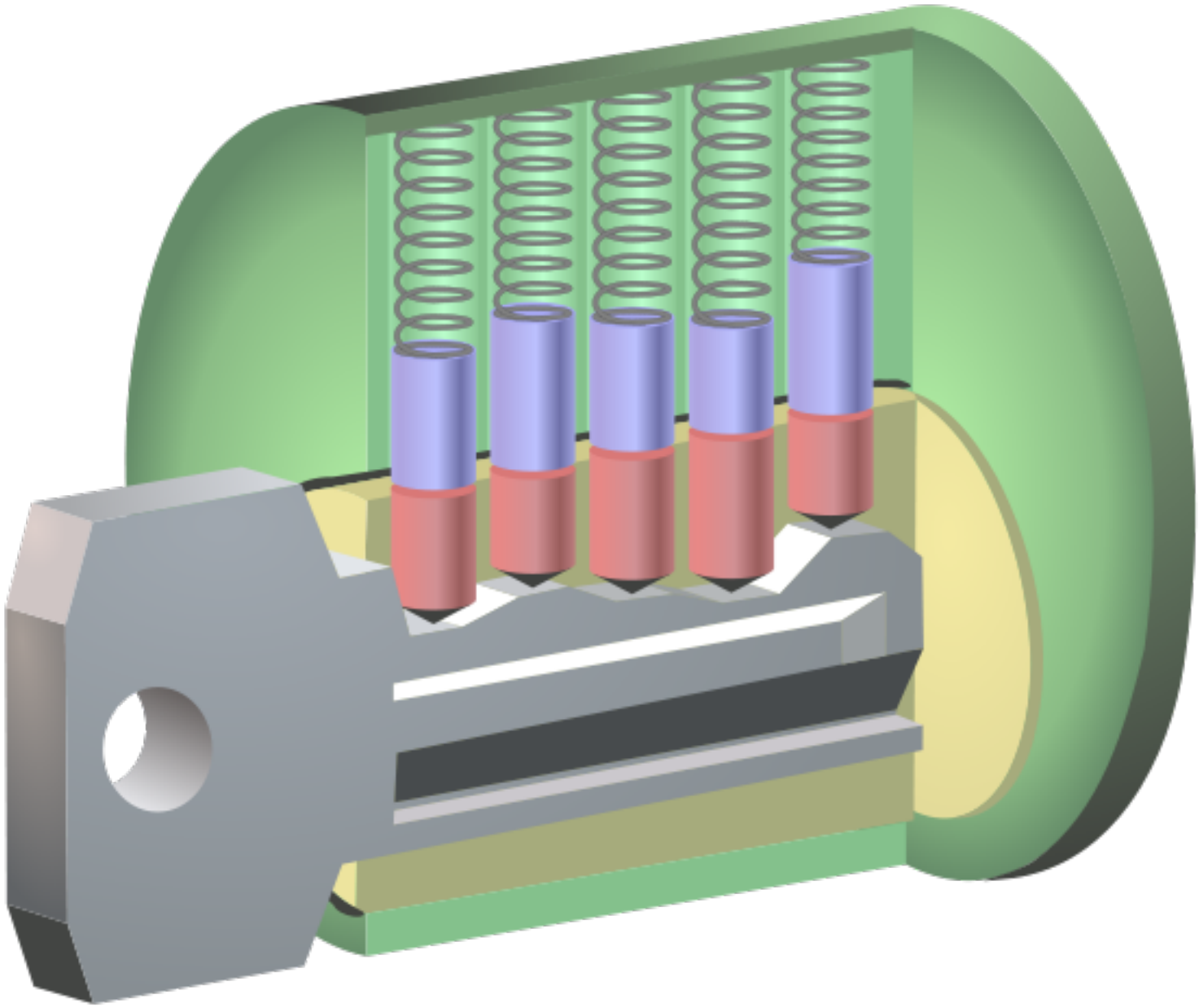
Public domain image from http://commons.wikimedia.org/wiki/File:Motion_Picture_Production_Code.gif

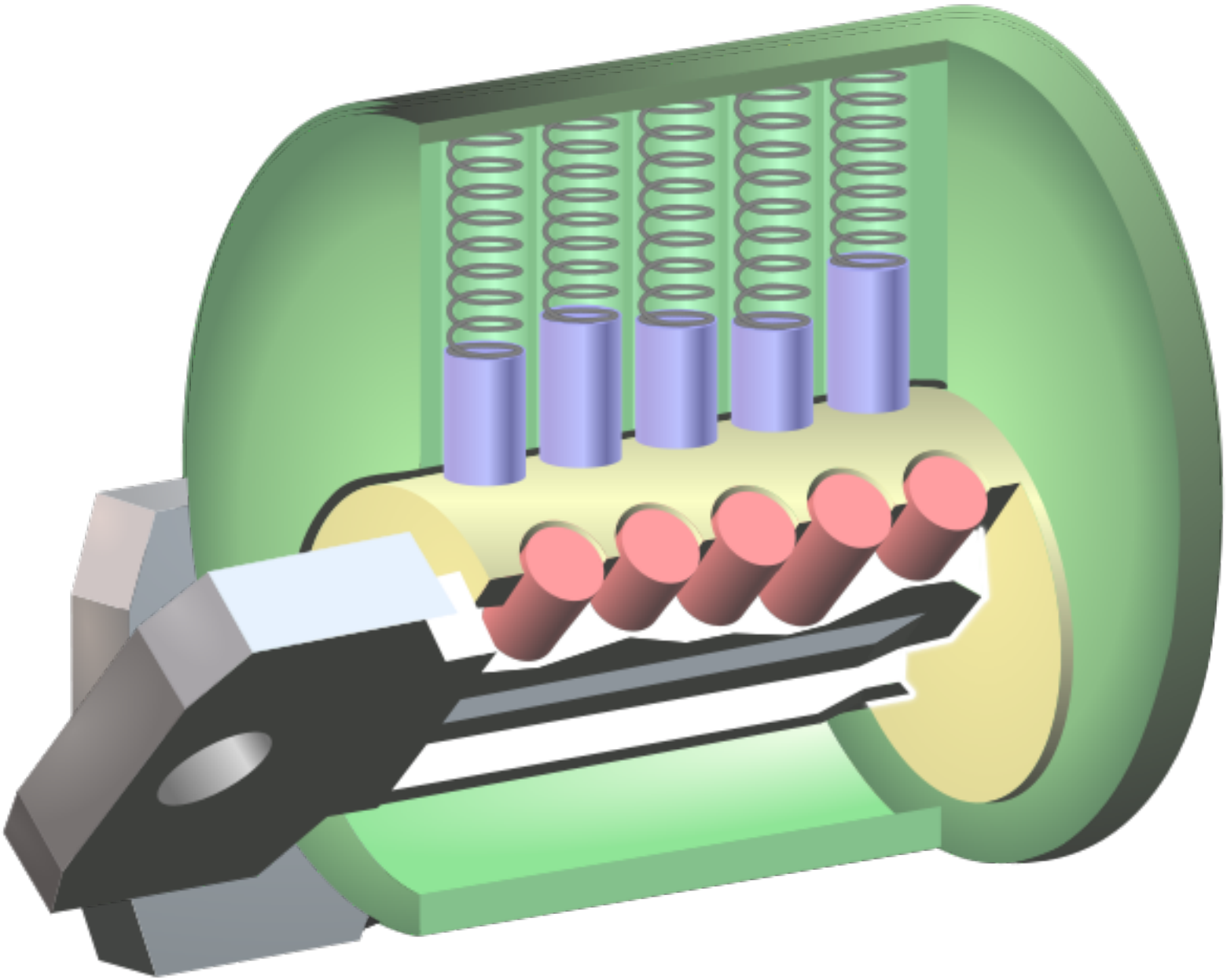
Pin Tumbler Lock

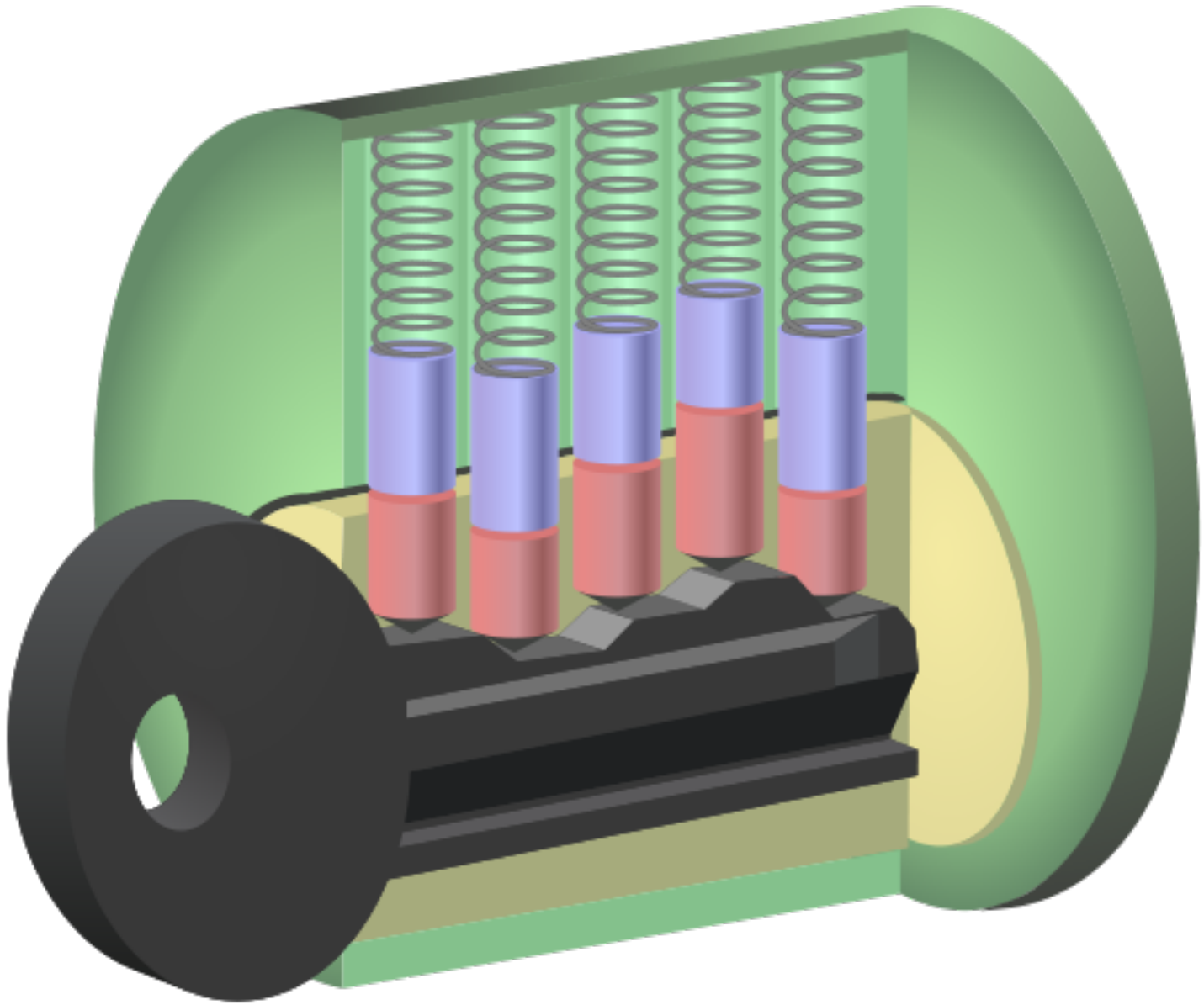


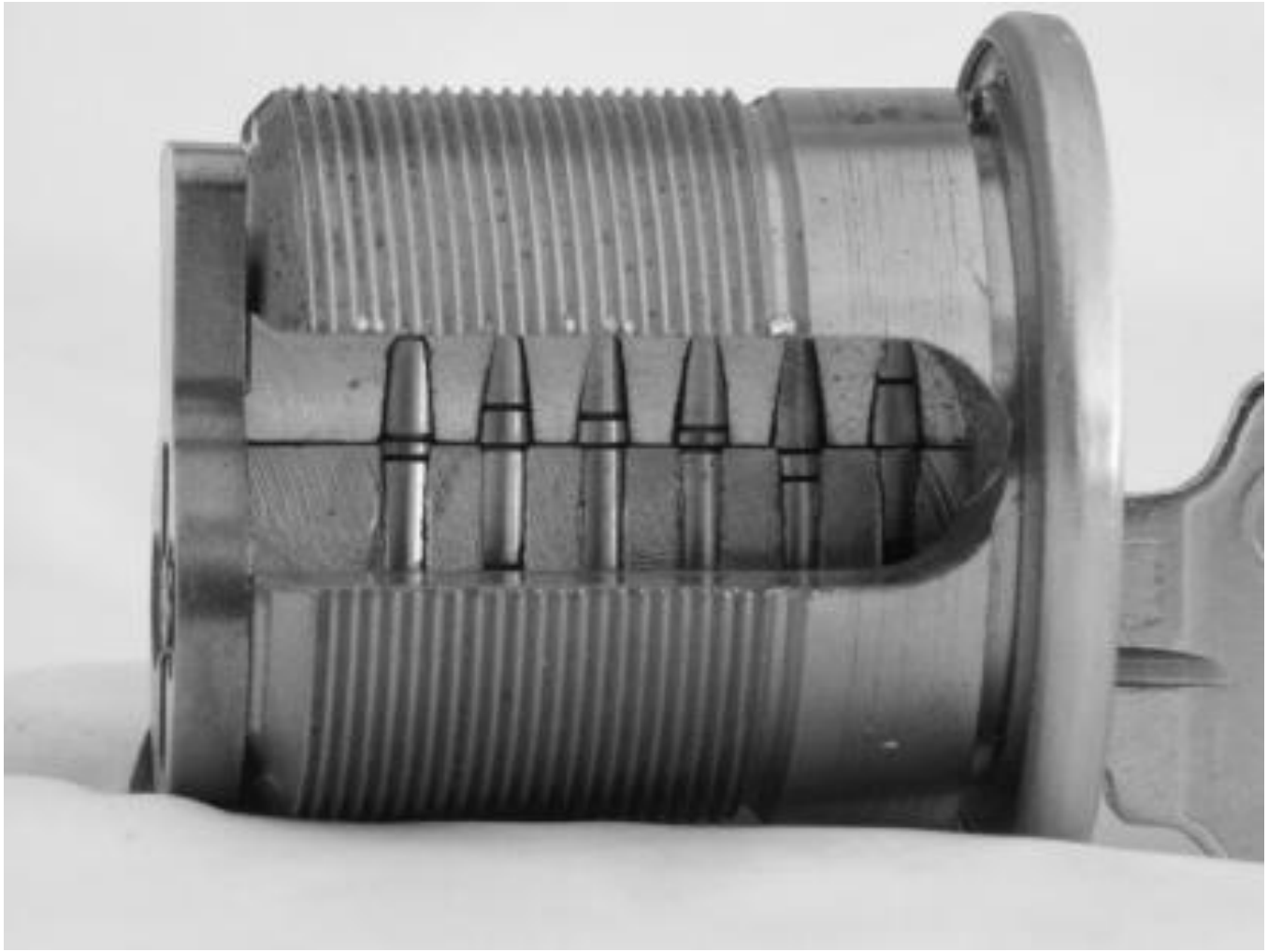


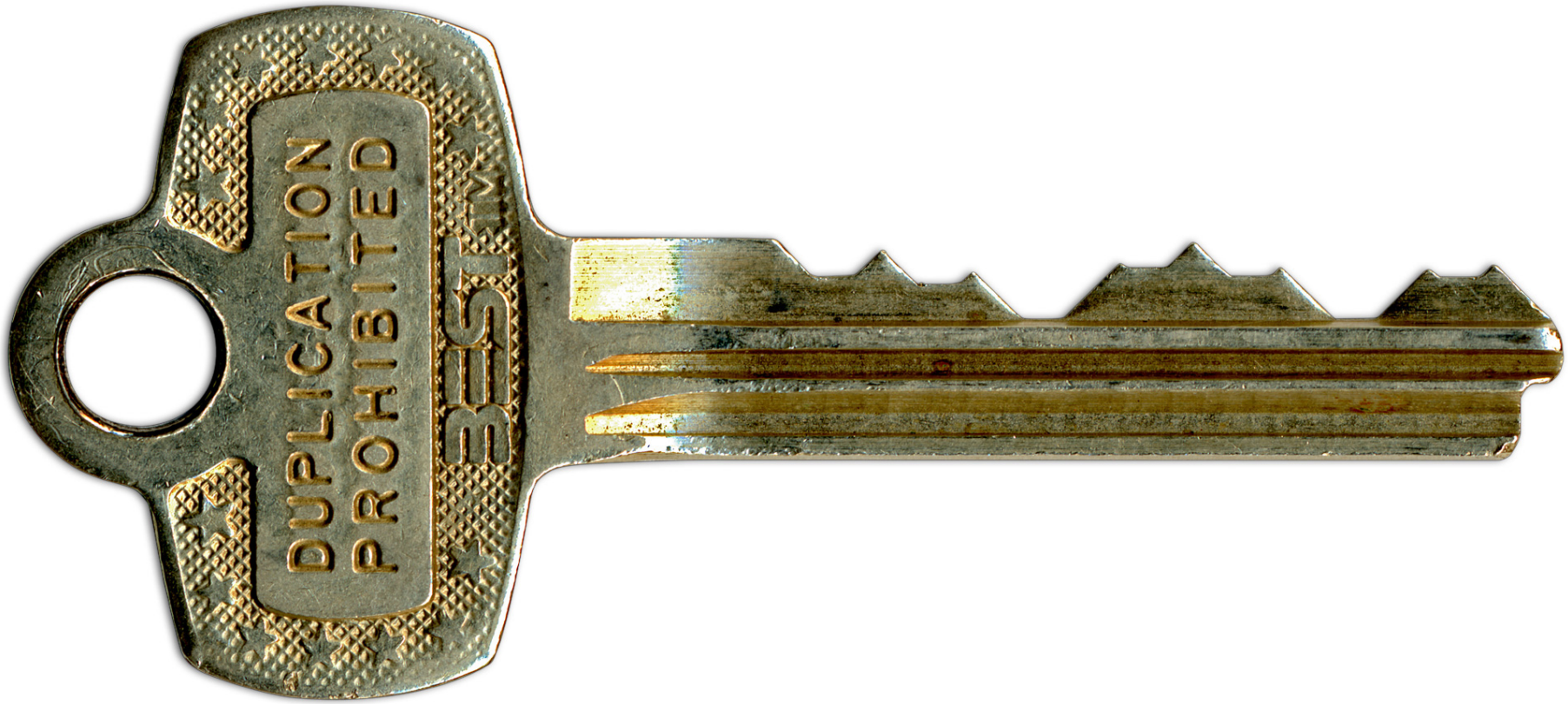












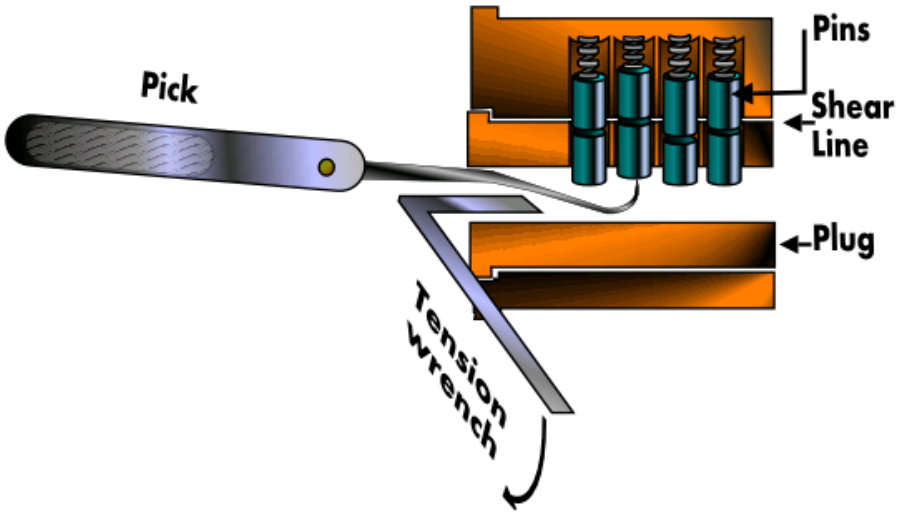
$8^7 = 2{,}097{,}152$

Compromising Locks

- For centuries, the lock has been one of the cornerstones of physical security
  - We rely on dozens of them every day to protect people and assets
- The trust most people place in locks is unwarranted
  - Most locks can be easily compromised with nondestructive methods
  - Sometimes within seconds and with readily available tools
- **“Locks keep honest people honest”**

Feeler Picking

- Apply light tension
- Lift one pin at a time
  - Identify binding pin
- Lift binding pin until it reaches the shear line
- Setting the binding pin will rotate the lock slightly
- Find next pin and repeat the process



Scrubbing / Raking

- Apply light tension
- Work over pins back to front in a circular motion
  - attempting to pop them into the shear line with the combination of tension
- Good for beginners
- Usually employ snake pick or half diamond

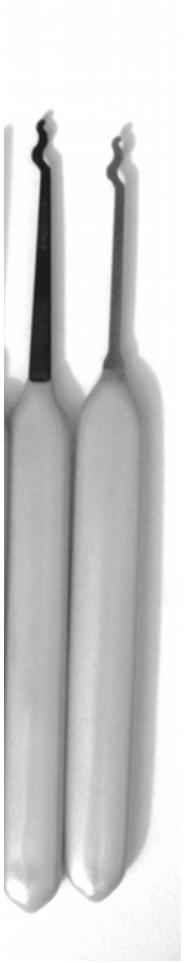


Photo by Jennie Rogers included with permission.

Bump Keys

- Driver pins “jump” higher than the cylinder just for an instant
- If a light rotational force is applied, the cylinder will turn
- Lock bumping is a very fast method for opening the lock
- The lock is not damaged
- Defense: different weighted pins

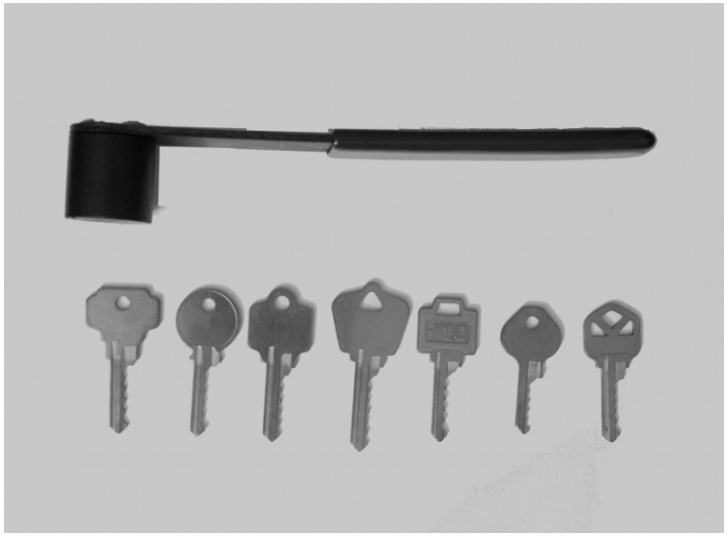


Photo by Jennie Rogers included with permission.

How many of you have your keys sitting out?


Speedy
Rewards

keysduplicated.com

ECE 422 (2 unread) ECE 422, CS...ter Security University of.../ Self-Service American Airl...ts at AA.com TEM Resour...- OBFS Home Michael Bailey My.ECE Portal - U of I Google Scholar

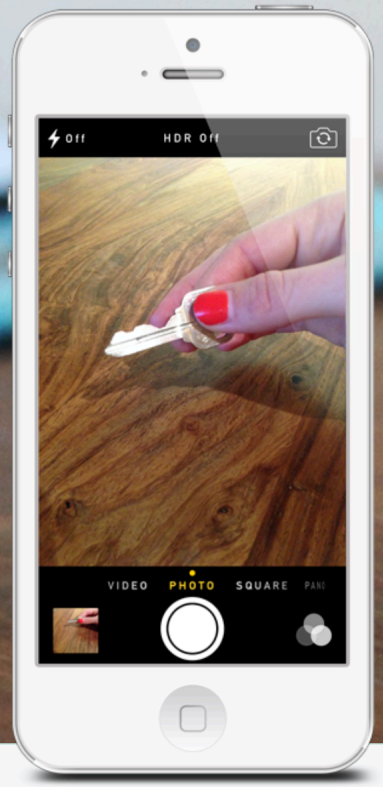
KEYS DUPLICATED

FAQ SECURITY BUSINESS API

Copy your house keys with your phone

No time for the hardware store?
Get your keys delivered to you

Get Started



Diebold Election Systems - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.diebold.com/nasadmk/cgi-bin/desi_catalog.pl?section=8&ic

Google

DIEBOLD
ELECTION SYSTEMS

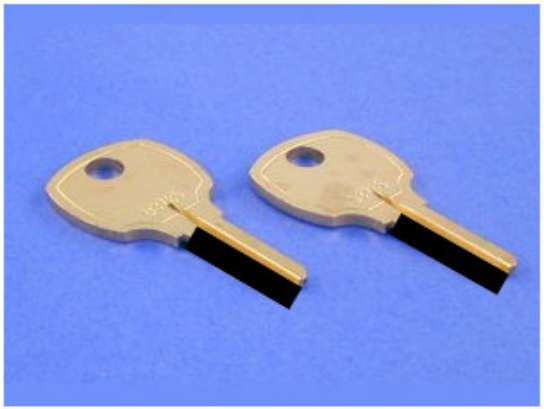
SHOPPING CART : ORDER FORM :

0 items in my cart | CHECKOUT

- AccuVote-OS
- AccuVote-TS
- AccuVote-TSX
- Documentation & Help Cards
- Election Extras
- Electrical Accessories
- ExpressPoll 2000/4000
- Networking & Printer Supplies
- Office Furniture & Storage
- Office Supplies
- Polling Station Supplies
- Signs
- Transfer & Transport Cases
- DIMS-NeT/Voter Registration
- Voting Booths & Ballot Boxes

ACCUVOTE-TS

The votes are in and Diebold supplies take the lead for accuracy and simplicity of use with this dependable touch-screen technology. //



Replacement Access Keys

- 2 keys that allow easy service access to the Tally Printer and replacement battery compartment

GS-567311-1000 **$5.90** USD per set
$6.90 CAD per set

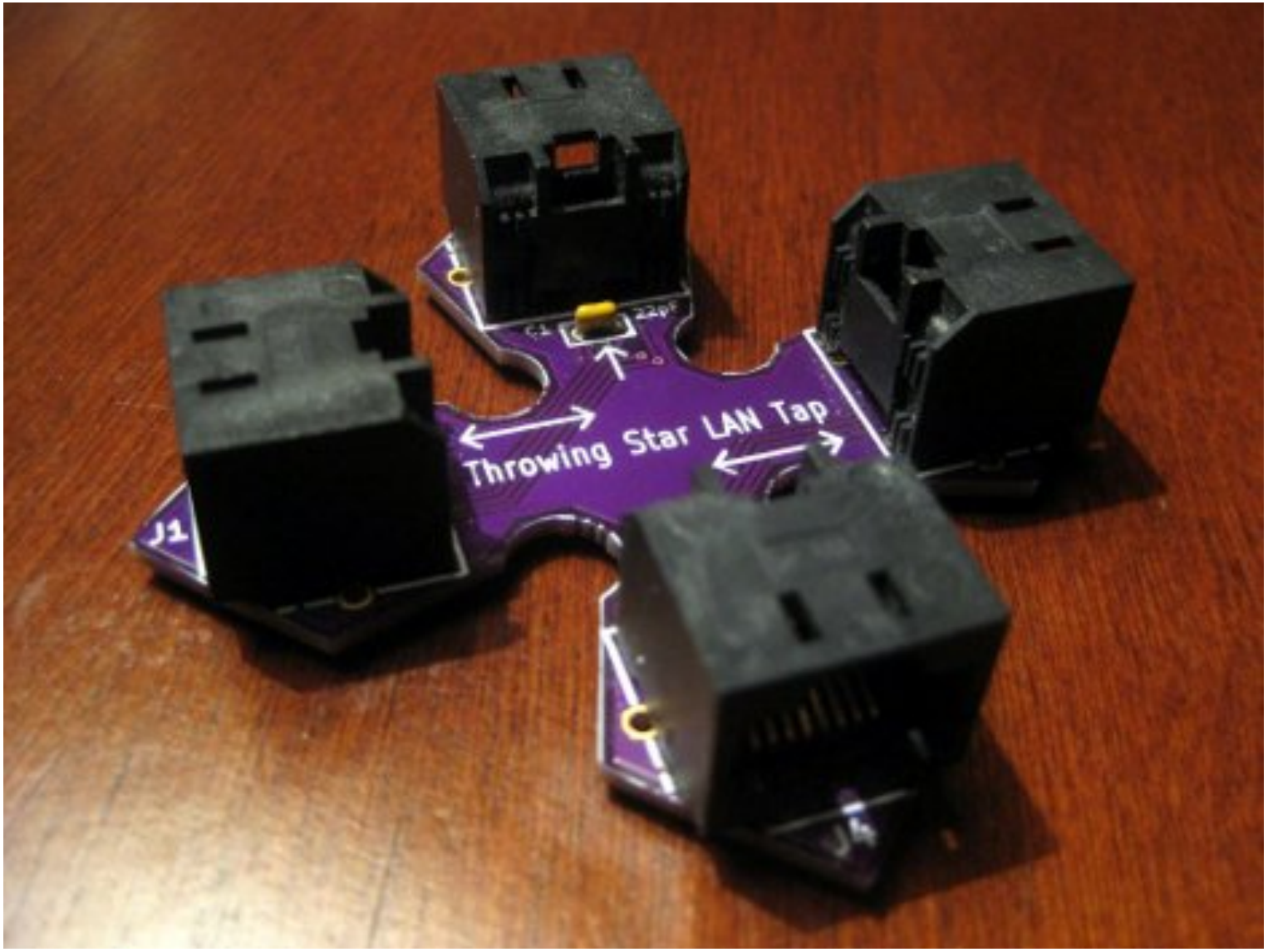
Enter a quantity

add to your order ▸

ORDER BY PHONE 800.769.3246

Why is physical security an IT concern?

physical access == total access?


Throwing Star LAN Tap
J1


Insert Card
Receipt
Visit us online
at www.bankofamerica.com
24 hours a day,
seven days a week.
Deposit
Cash


Insert Card
Receipt

What about Encryption?

Hibernation

- Modern machines have the ability to go into a powered-off state known as **hibernation.**
- While going into hibernation, the OS stores the contents of machine's memory into a **hibernation file** (such as hiberfil.sys) on disk so the computer can be quickly restored later.
- But… without additional security precautions, hibernation exposes a machine to potentially invasive forensic investigation.

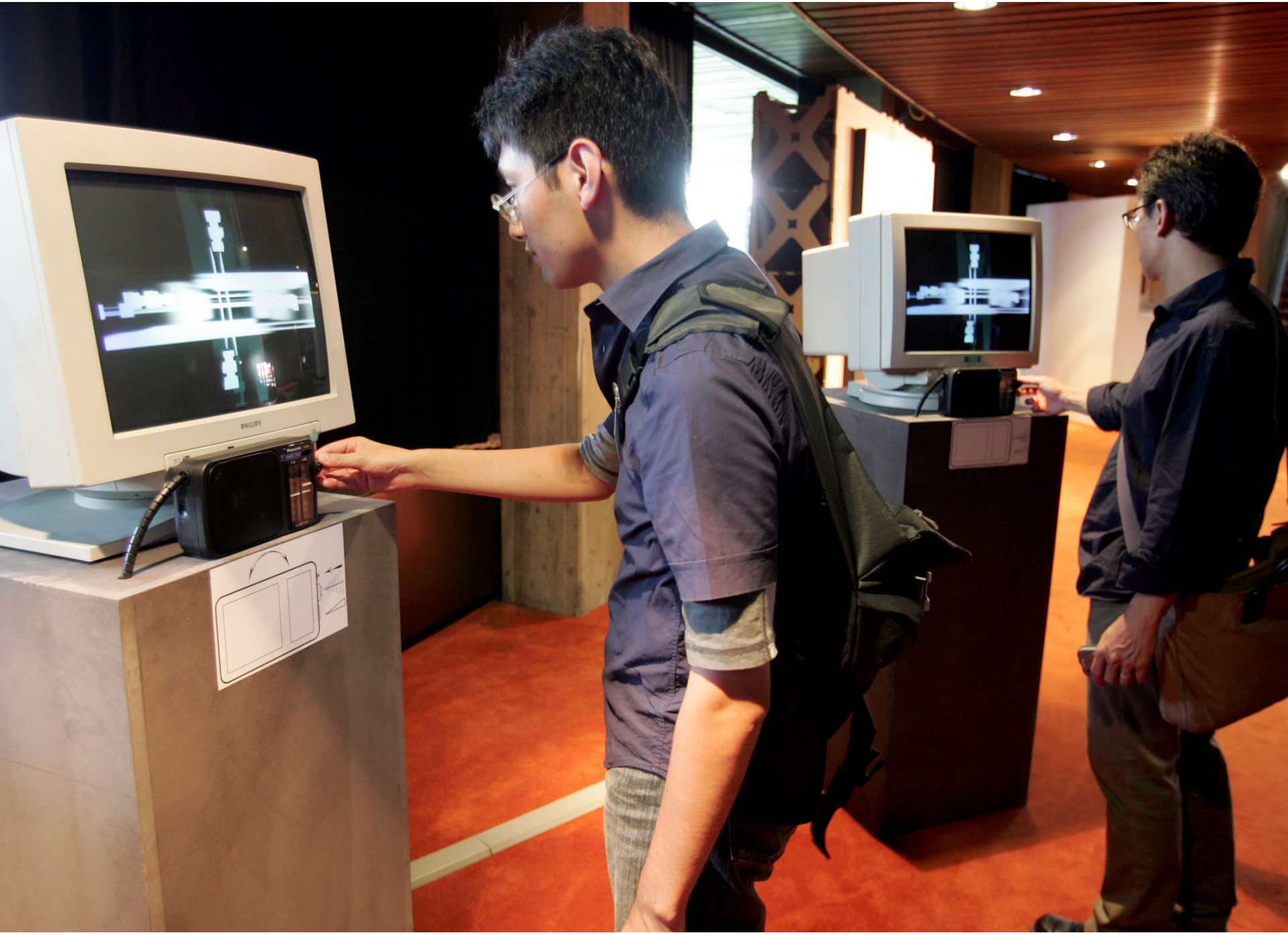
1. User closes a laptop computer, putting it into hibernation.

2. Attacker copies the hiberfil.sys file to discover any unencrypted passwords that were stored in memory when the computer was put into hibernation.

Proximity

Signal Emissions

- Computer screens emit **radio frequencies** that can be used to detect what is being displayed.
- **Visible light** reflections can also be used to reconstruct a display from its reflection on a wall, coffee mug, or eyeglasses.
- Both of these require the attacker to have a receiver close enough to detect the signal.

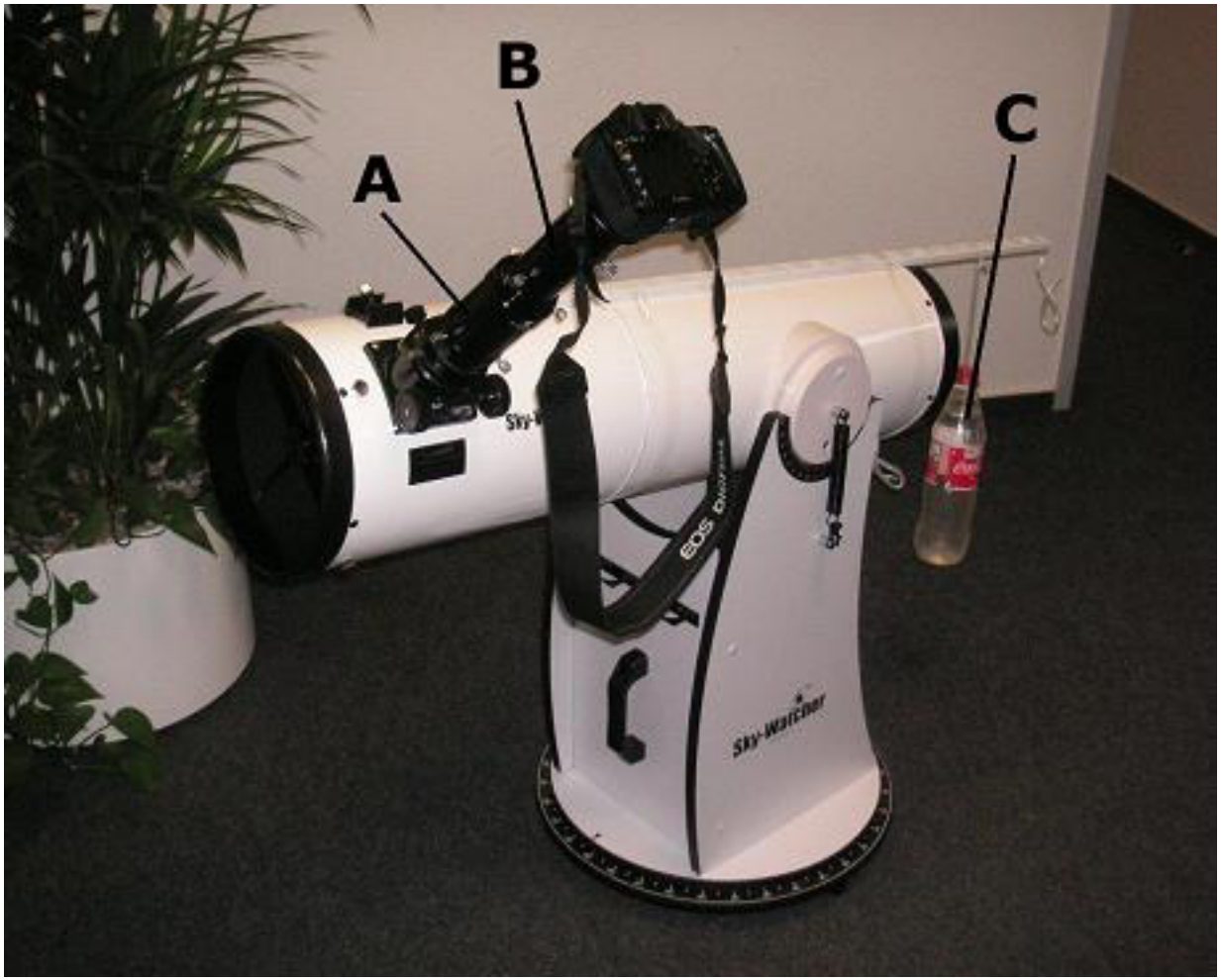

PHILIPS

Faraday Cages

- To block electromagnetic emanations in the air, we can surround sensitive equipment with metallic conductive shielding or a mesh of such material, where the holes in the mesh are smaller than the wavelengths of the electromagnetic radiation we wish to block.
- Such an enclosure is known as a **Faraday cage.**

Acoustic Emissions

- Dmitri Asonov and Rakesh Agrawal published a paper in 2004 detailing how an attacker could use an audio recording of a user typing on a keyboard to reconstruct what was typed.


A
B
C
Sky-Watcher

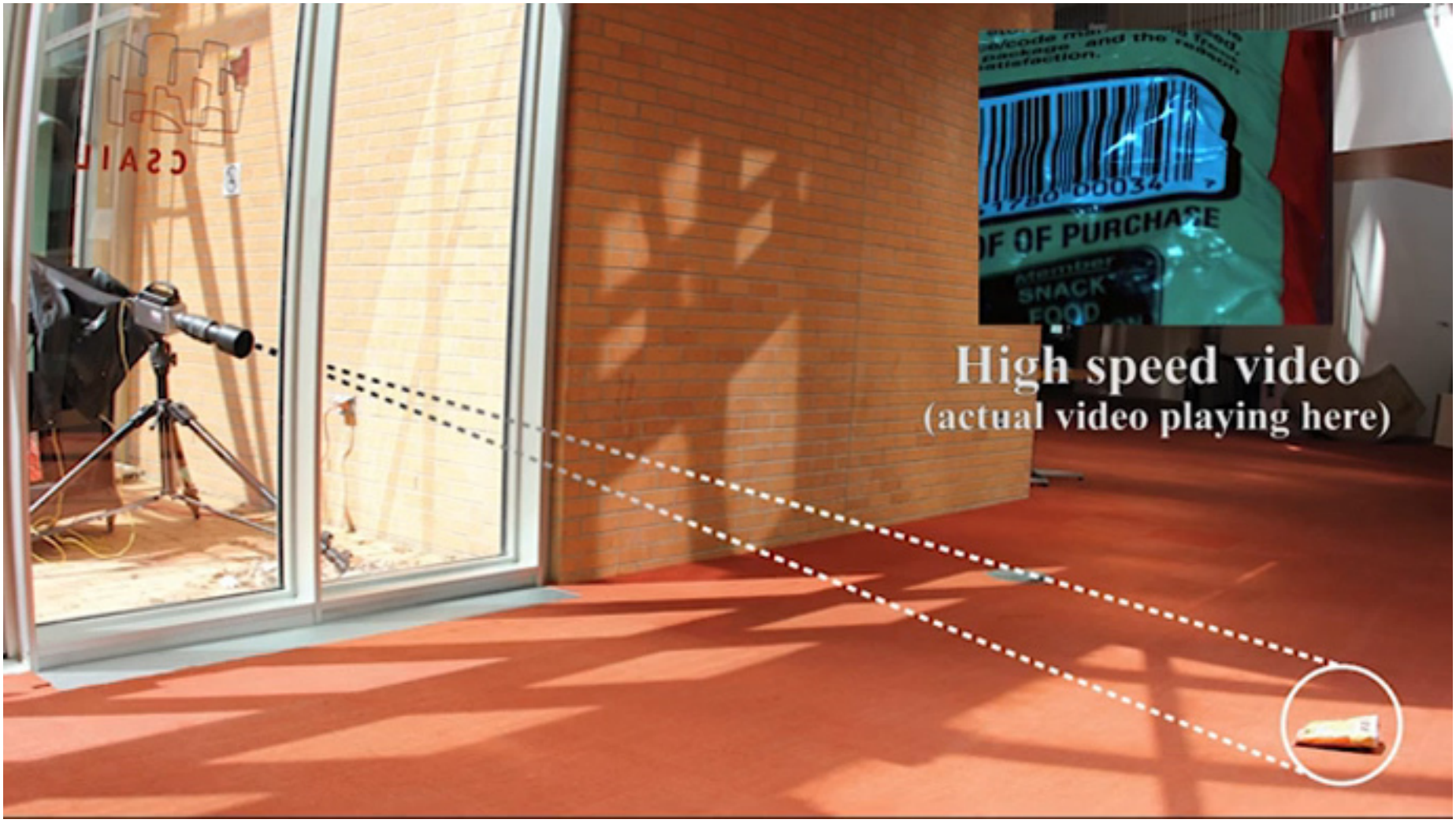
Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?

Wim van Eck
PTT Dr. Neher Laboratories, St. Paulusstraat 4, 2264 XZ
Leidschendam, The Netherlands

This paper describes the results of research into the possibility of eavesdropping on video display units by picking up and decoding the electromagnetic interference produced by this type of equipment. During the research project, which started in 1982, it became more and more clear that this type of ... committed very easily using a normal

1. Introduction

It is well known that ... electromagnetic fields ... radio and television ... underlying this have been ... past few decades. ... internationally agreed ... interference produced ... because the maximum ... equipment may generate ... a ... countries.


High speed video
(actual video playing here)