CSE509 Computer System Security

Stony Brook University

2023-05-04

Physical Security

Michalis Polychronakis

Stony Brook University

Physical Security

Very broad area spanning various threats beyond information security

- Commercial espionage
- Theft
- Sabotage
- Acts by foreign powers
- Terrorism

Our focus: *physical attacks against IT security*

- Complementary to non-physical attacks
- *"Physical security protects people, data, equipment, systems, facilities and company assets" (Harris, 2013)*

IT Physical Security

An often-underestimated aspect of IT security

We will focus on two main areas:

Premises

How to gain unauthorized physical access to computing and networking assets

Hardware

How to compromise a device or network once physical access has been achieved

Various threat models

Outside attacker, insider threats, spouse, …

Physical Penetration Testing

Main focus is usually on technology-oriented countermeasures

- Firewalls, intrusion detection systems, AV, access control, …
- What good are these if an attacker can just walk into a building and compromise an unlocked terminal?

Physical penetration testing assesses the security weaknesses of a client's physical security

Major threats

- Unauthorized access into areas
- Tampering/physical access to computing devices
- Access to internal networks
- Theft of devices and other equipment (valuable mostly for the data on them)

Main Engagement Phases

Receiving the assignment: sign contracts and clear legal issues

Rules of engagement: negotiate what is in scope and what is off limits

Preliminary research

Human Intelligence (HUMINT): information from human sources
(innocuous interactions, social engineering, …)

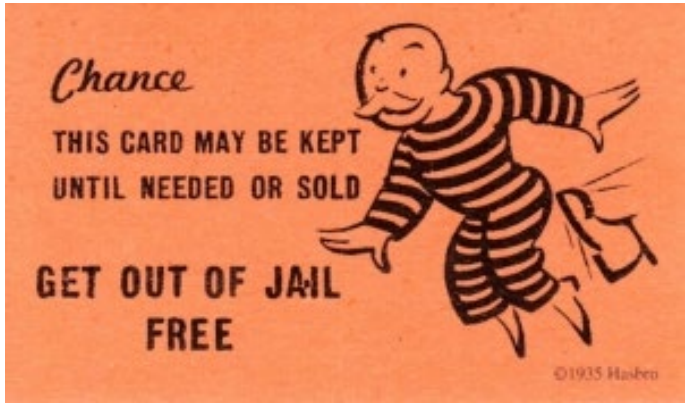
Signals Intelligence (SIGINT): interception technologies
(network sniffing, breaking into WiFi networks, RF communication, …)

Open Source Intelligence (OSINT): information from public sources
(online directories, dumpster diving, …)

Imagery Intelligence (IMINT): photo/video
(google maps, drones, binoculars, discrete photography, …)

Provide documentation and legal requirements

Test plan, signed contracts, copies of ***"get out of jail free"* cards**,
IDs of team members, clearance information, …



Physical Controls

Perimeter security

Guards, barriers, gates, turnstiles, door locks, …

Badges

Simple paper/plastic, proximity tokens, magnetic cards, RFID, …

Surveillance

CCTV, computer cameras, presence sensors, …

Intrusion alarms

Motion detectors, security lighting, …

Bypassing Physical Controls

Perimeter security

Tailgating/piggybacking, social engineering (delivery person, cleaning crew, new employee, etc.), lock picking, …

Badges

Fabrication, cloning, jamming, …

Surveillance

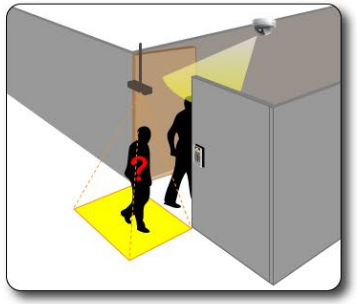
Blend in, avoid, jam, …

Intrusion alarms

Avoid triggering (e.g., engage during working hours), disable, …

Single Door In-Swing doors

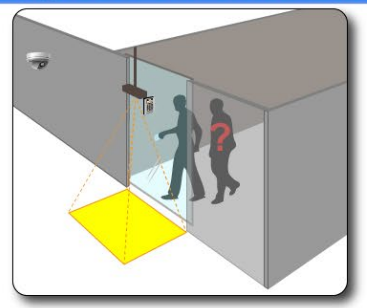
Tailgating detection



Tailgater Image recorded

Tailgater Alarm

Single Door Bi-Fold doors



Tailgating detection

Tailgater Image recorded

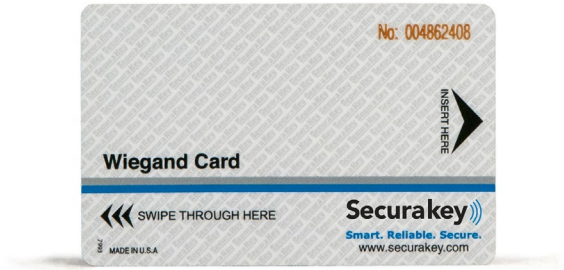

LOGO
定制

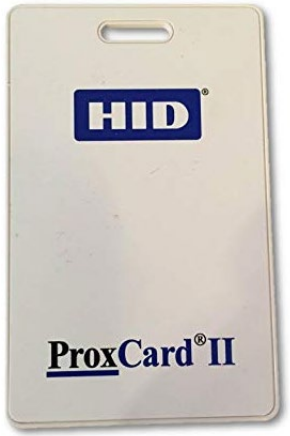
Badge Types

Minimal amount of data: just a small binary blob containing user-identifying information

Many different types

- Magnetic Stripe
- Wiegand (swipe)
- 125 kHz Prox (HID & Indala)
- MIFARE contactless smart cards
- iCLASS contactless smart cards





RFID (Radio-frequency Identification)

Uses radio waves produced by a *reader* to detect the presence of (and then read the data stored on) a *tag*

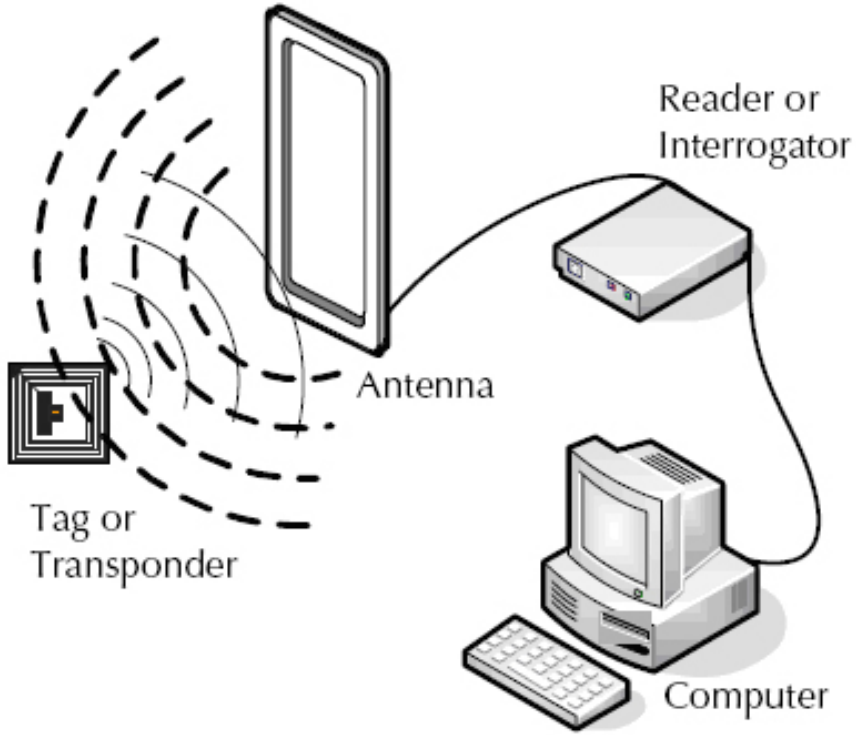
Can be embedded in cards, stickers, buttons, capsules, …

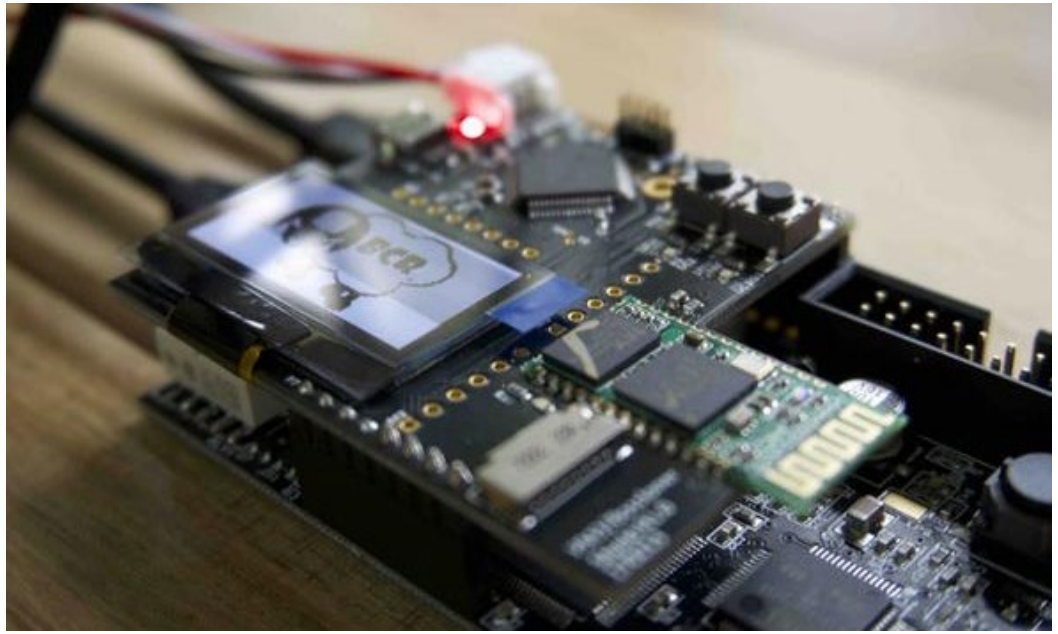
Passive

Use the interrogator's radio wave energy to relay its stored information back to the interrogator

Active

Battery powered to increase range





"The Boscloner Premium Kit includes everything you need to start capturing and cloning RFID out of the box"

- Support for the most widely used RFID technology (125kHz HID Proxcard)
- Capturing and cloning of RFID cards from up to three feet away

approx. 1 meter/3.3ft

Special long range card

approx. 70cm/2.3ft

General thickness 1.8mm card

approx. 50cm/1.6ft

Thickness 0.8mm card

approx.30cm/1ft

Keyfob

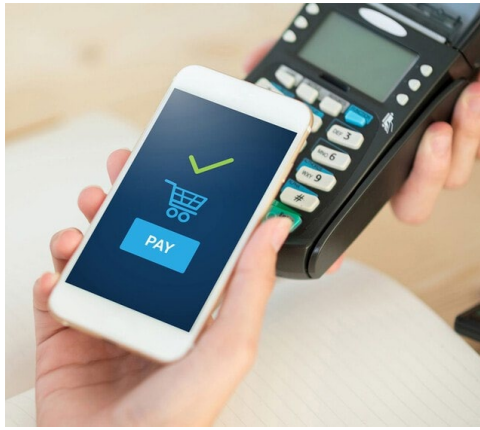
NFC (Near-field Communication)

Subset of RFID: designed to be a secure form of data exchange

- Modern smartphones support NFC: payments, access control, data transfer, …
- Built-in encryption and authentication protocols
- Much shorter range: up to 4cm
- Higher data transfer rate: up to 424 Kbit/s
- Bi-directional communication

In essence

- RFID: wireless barcodes
- NFC: wireless smartcards

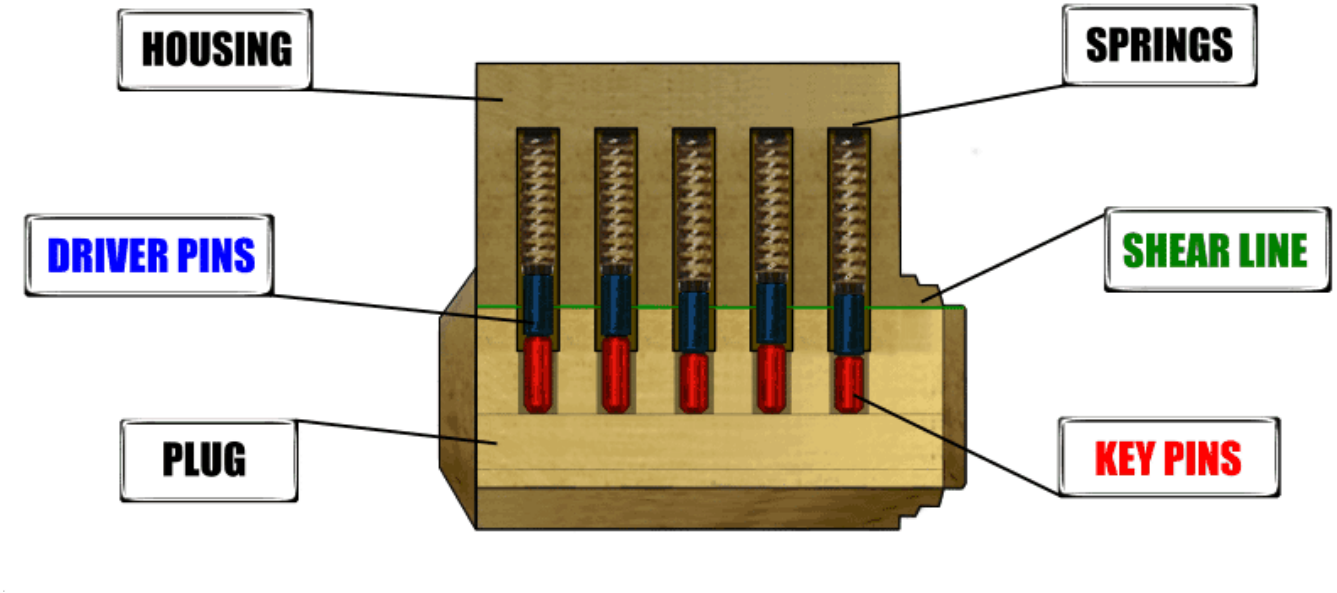


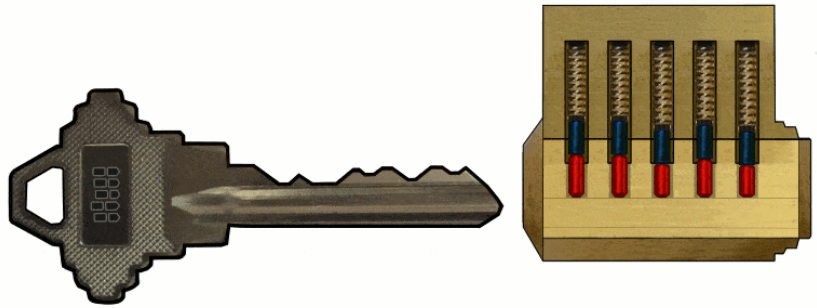
https://www.researchgate.net/figure/NFC-operation-modes_fig1_325162487

Lock Picking

Non-destructive way to open a lock without using its key

Most common type: pin tumbler lock

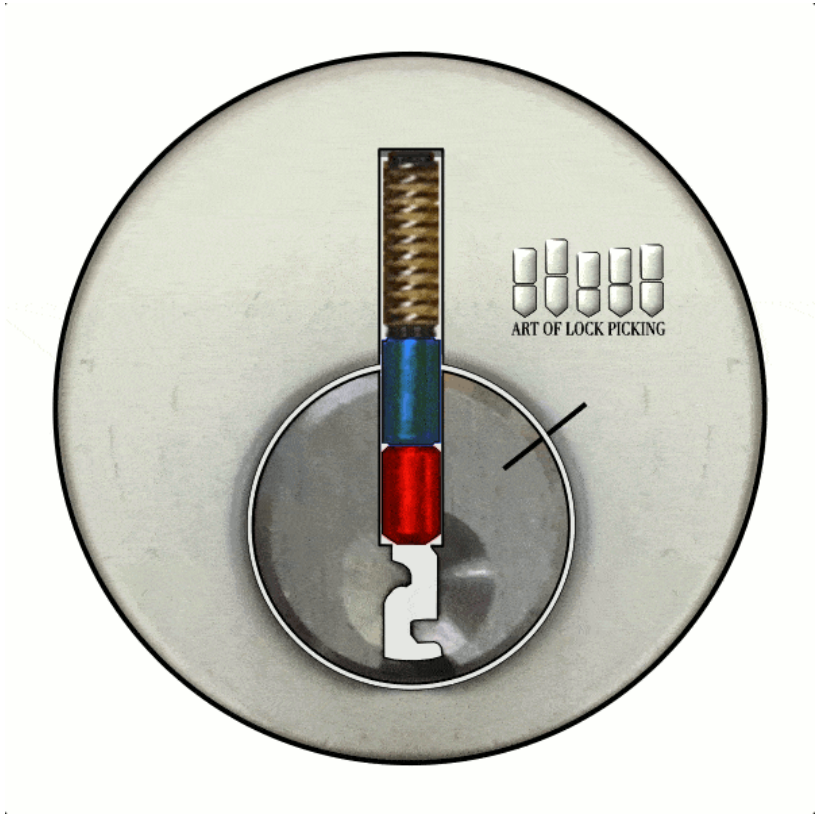




Lock Picking: Tension Wrench

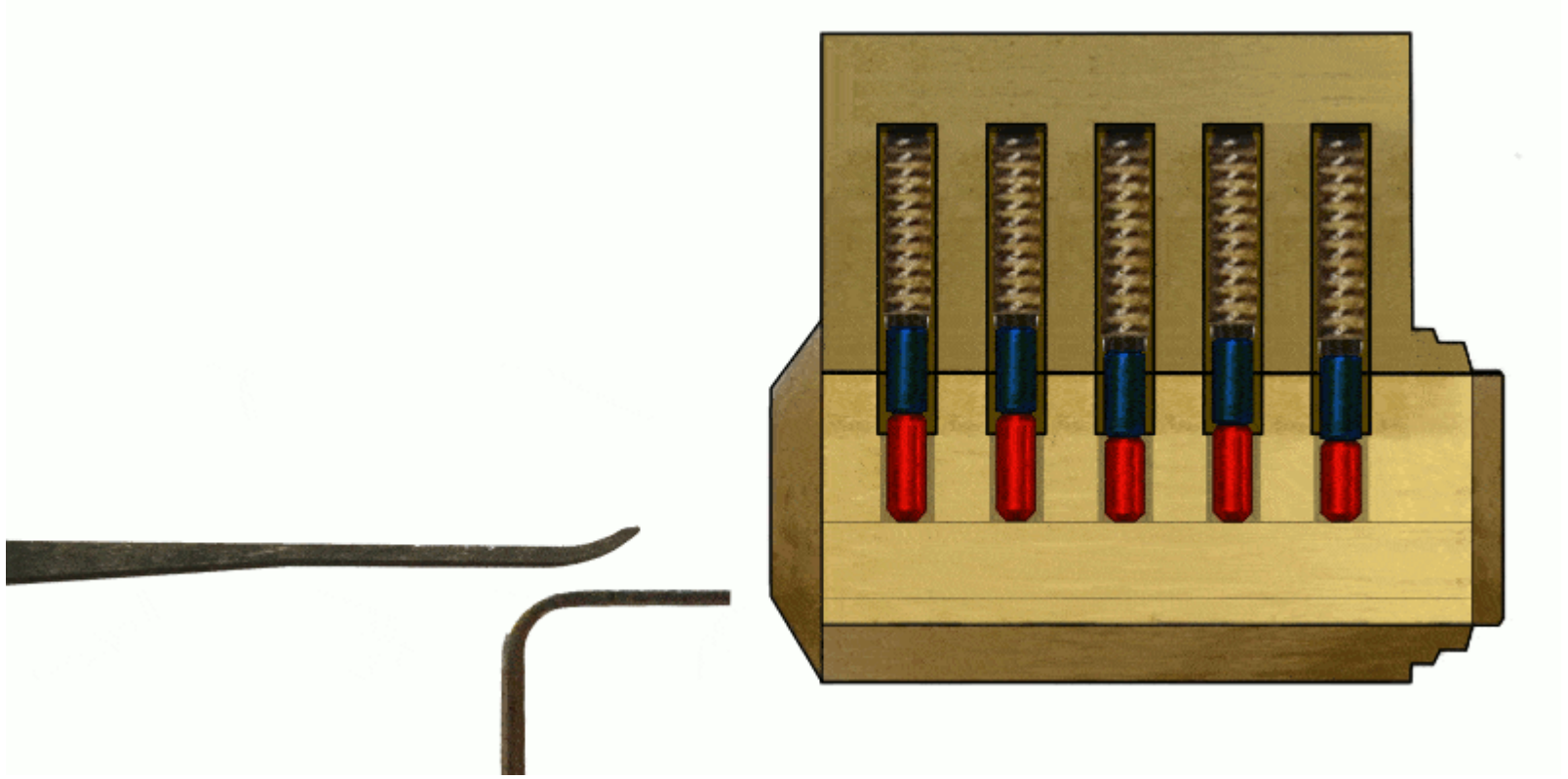
Bent piece of metal acting similar to the key: leverage to turn the plug

- Helps keeping the pins at the shear line during picking

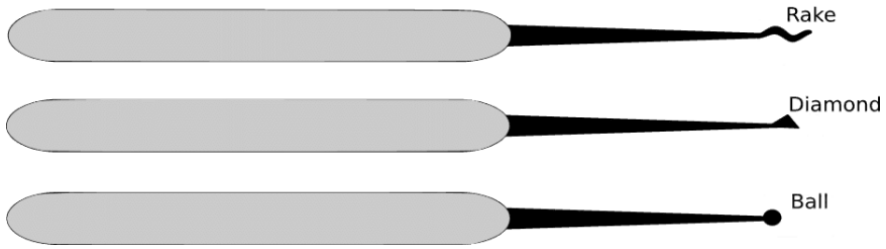


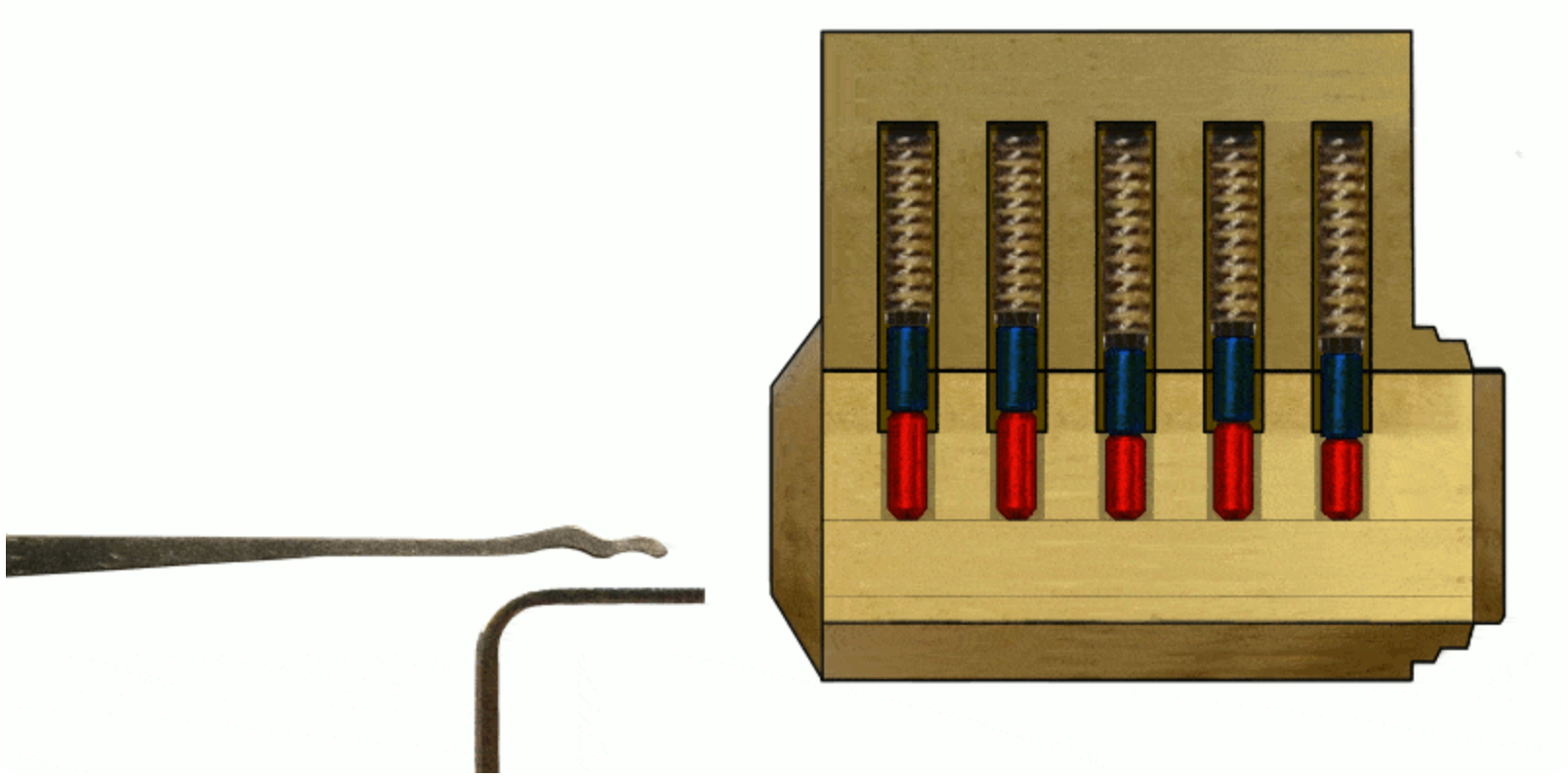
Technique #1: Single Pin Picking

Binding pin

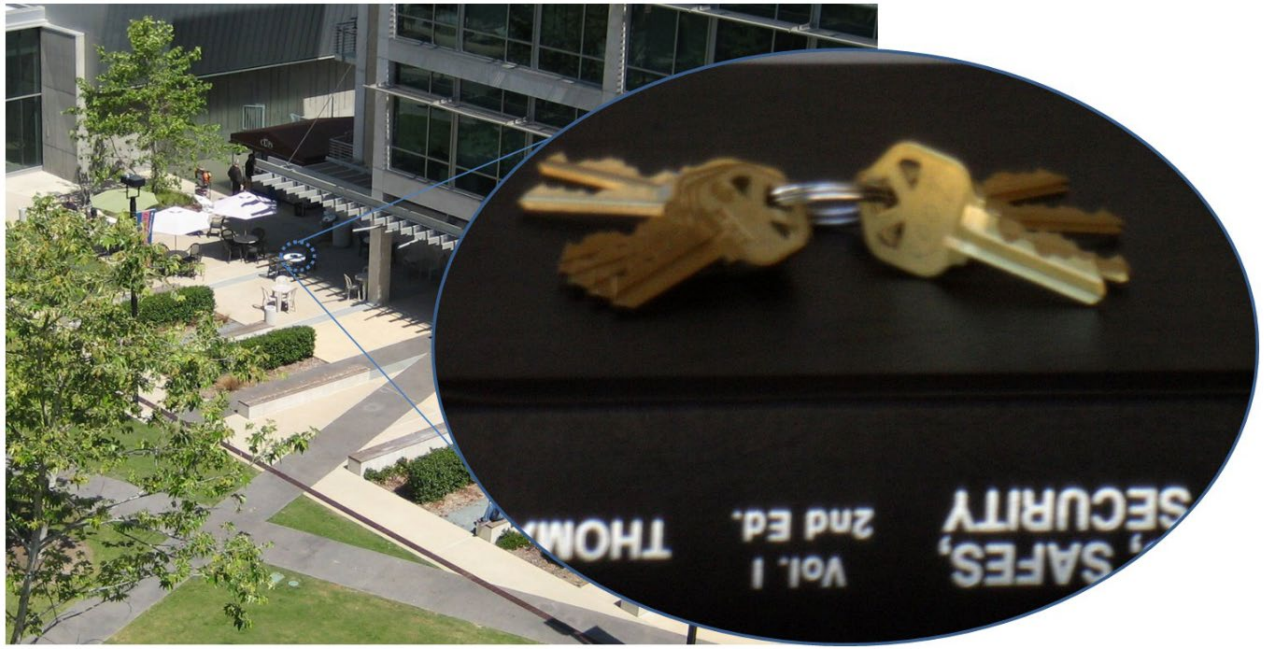


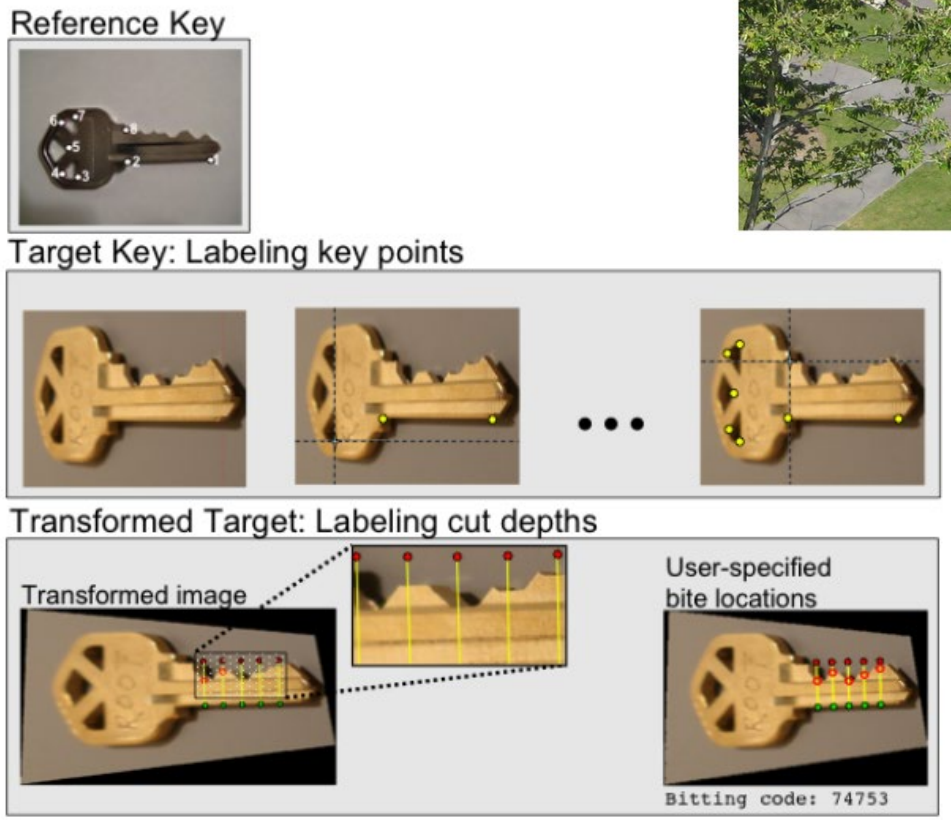
Technique #2: Raking





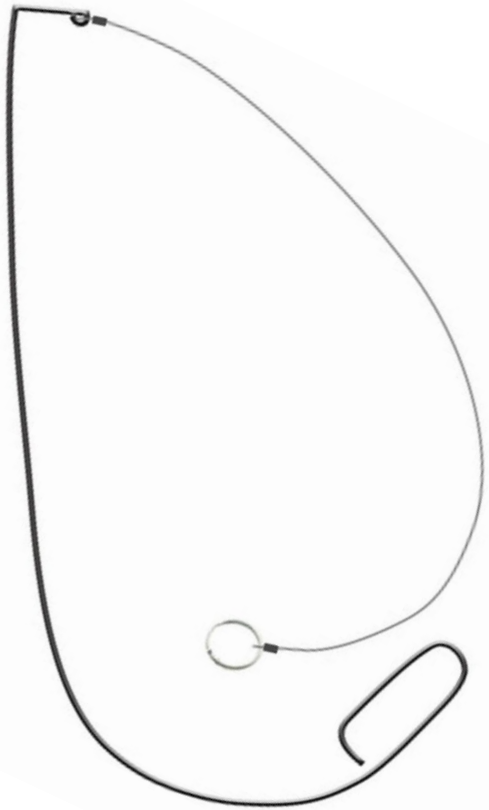
Key Cloning

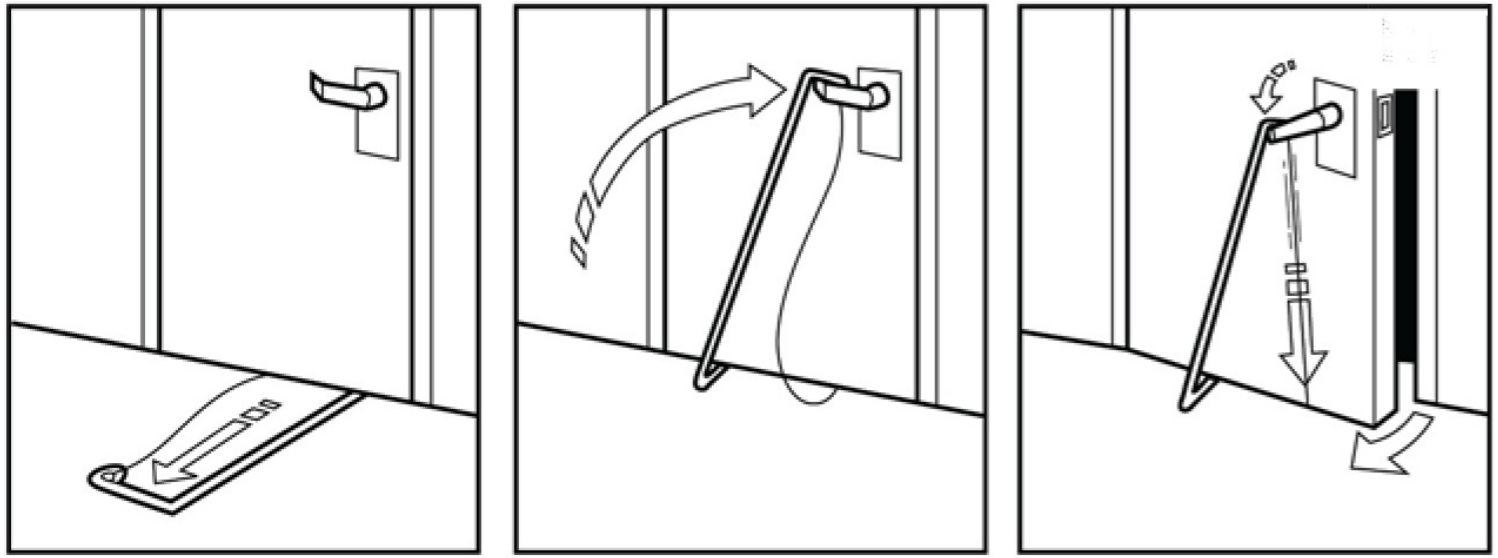

SECURITY
2nd Ed.
Vol. 1


Reference Key
Target Key: Labeling key points
Transformed Target: Labeling cut depths
Transformed image
User-specified
bite locations
Bitting code: 74753


CELESTRON

Under The Door Tool





Anti-theft Systems

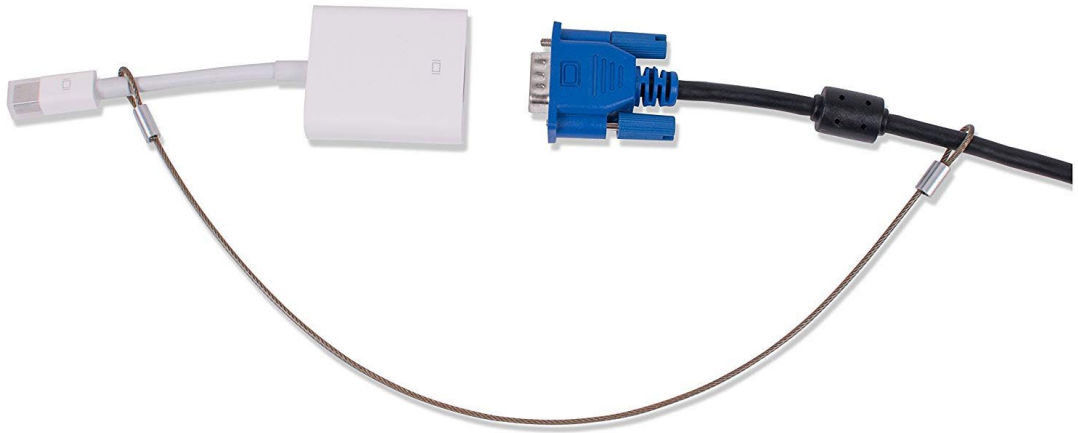
Kensington locks

Tracking tags

Forensic marking

Find my iPhone

…



Physical Access

Machine

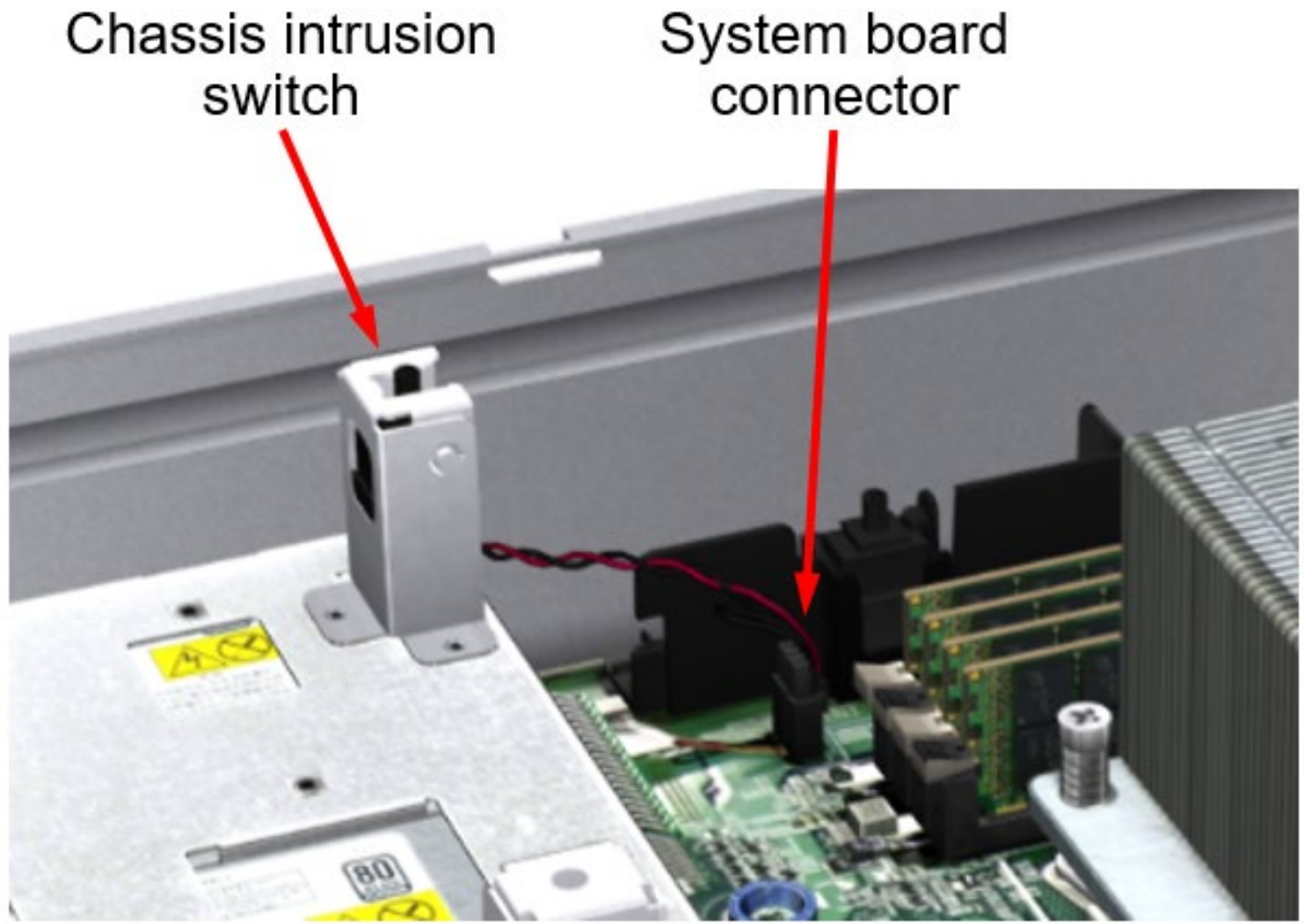
- Plug malicious USB stick, hardware keylogger, …
- Bypass boot process (F8 in Windows, `init=/bin/sh` in Linux)
- Boot from ~~CD/~~USB and read unencrypted data off the HD
- Physical memory attacks (DMA, cold boot, …)
- Malicious devices/peripherals (physically plug device, ship "gift" device, …)
- Walk off with machine/HD (steal it or return it back)

Network

- Plug a new device into the internal network (e.g., Raspberry Pi)
- Bring a rogue access point
- Sniff traffic (WiFi, network tap, …)

Space

- Install spy cameras (e.g., pointing to keyboards/screens), mics, long-range RF readers, …


Chassis intrusion switch
System board connector

Linux Root Access

1. As soon as the boot process starts, press ESC to bring up the GRUB boot prompt
2. When GRUB prompt appears, press "e" to edit the first boot option
3. Find the kernel line (starts with: `linux /boot/`)
4. Add `init="/bin/bash"` at the end of the line
5. Press CTRL-X or F10 to boot and enjoy root access

```
mount -rw -o remount /
passwd user
```

Filesystem-level Encryption

`/home` folder, individual files, encrypted partition, …

Not sufficient protection if not applied for all files

- Infect non-encrypted executables, copy files when decrypted, …

Full Disk Encryption

Everything is encrypted (incl. swap file, temp files, …)

- Destroying the key "erases" all the data

Still not bulletproof

- Cold boot attacks: steal key from memory
- Suspend/sleep mode: some data may remain unencrypted
- Keyloggers and similar threats are still effective

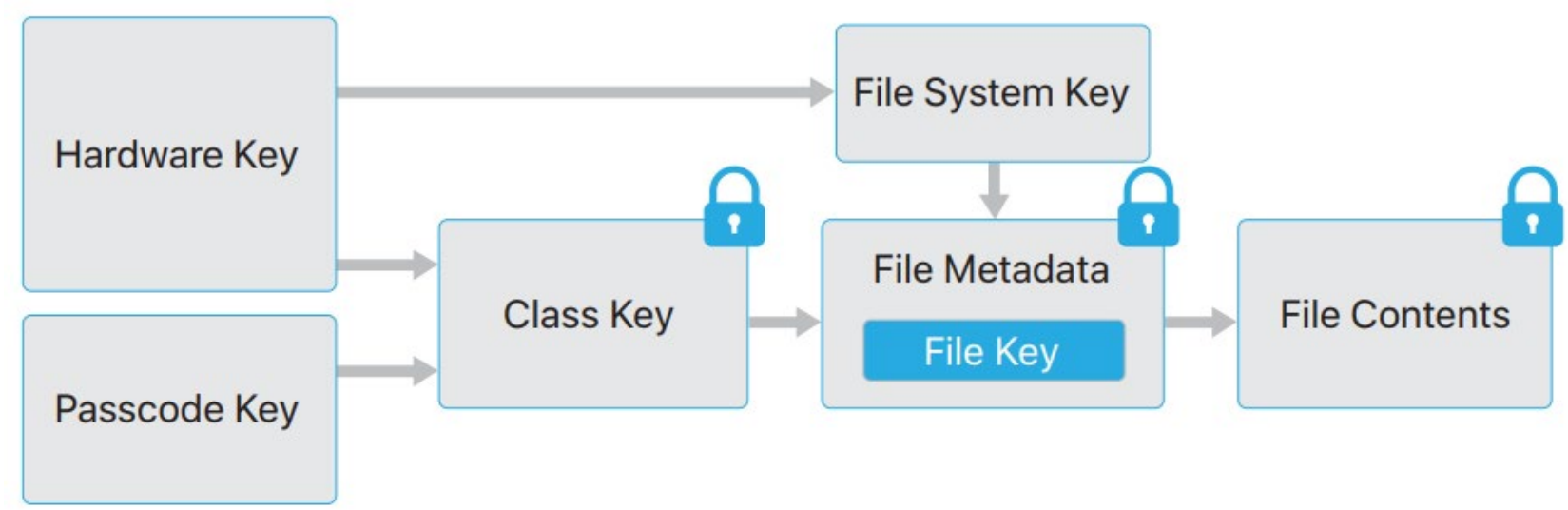
Example: iOS Data Protection

Per-file encryption by assigning each file to a class

- Each file's content is encrypted using a unique per-file key
- File metadata is encrypted separately through the secure enclave

Per-file key is encrypted with one of several "class keys"

- Derived from the user passcode and some hardware secrets embedded in the CPU



iOS Data protection classes

Complete protection: class key is protected with a key derived from the user passcode and the device UID

Discarded shortly after device is locked (10 sec, if the Require Password setting is Immediately)

Protected Unless Open: class key is protected using public key encryption

Some files may need to be written while the device is locked (e.g., mail attachment being downloaded, taking a picture while locked)

Protected Until First User Authentication: same as Complete Protection, but key stays in memory when locked

Similar to desktop full-volume encryption: protects data from attacks that involve a reboot

No protection: class key is protected only with the UID

Since all keys stored on the device, main benefit is just fast remote wipe

Cold Boot Attacks

DRAM retains its content for several seconds after power is lost

Cold reboot (just hit the restart switch): OS doesn't have the chance to cleanup anything

- Immediately boot a lightweight imaging tool (instead of the normal OS) to dump DRAM contents

Alternative: physically remove the DIMMs (preferably after freezing them to maintain low temperature)

- Then plug them to a compatible machine

Figure 5: Before powering off the computer, we spray an upside-down canister of multipurpose duster directly onto the memory chips, cooling them to −50 °C. At this temperature, the data will persist for several minutes after power loss with minimal error, even if we remove the DIMM from the computer.

"Lest We Remember: Cold Boot Attacks on Encryption Keys." J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, Edward W. Felten. USENIX Security 2008

DMA Attacks

Direct memory access (DMA) allows peripheral devices to access RAM

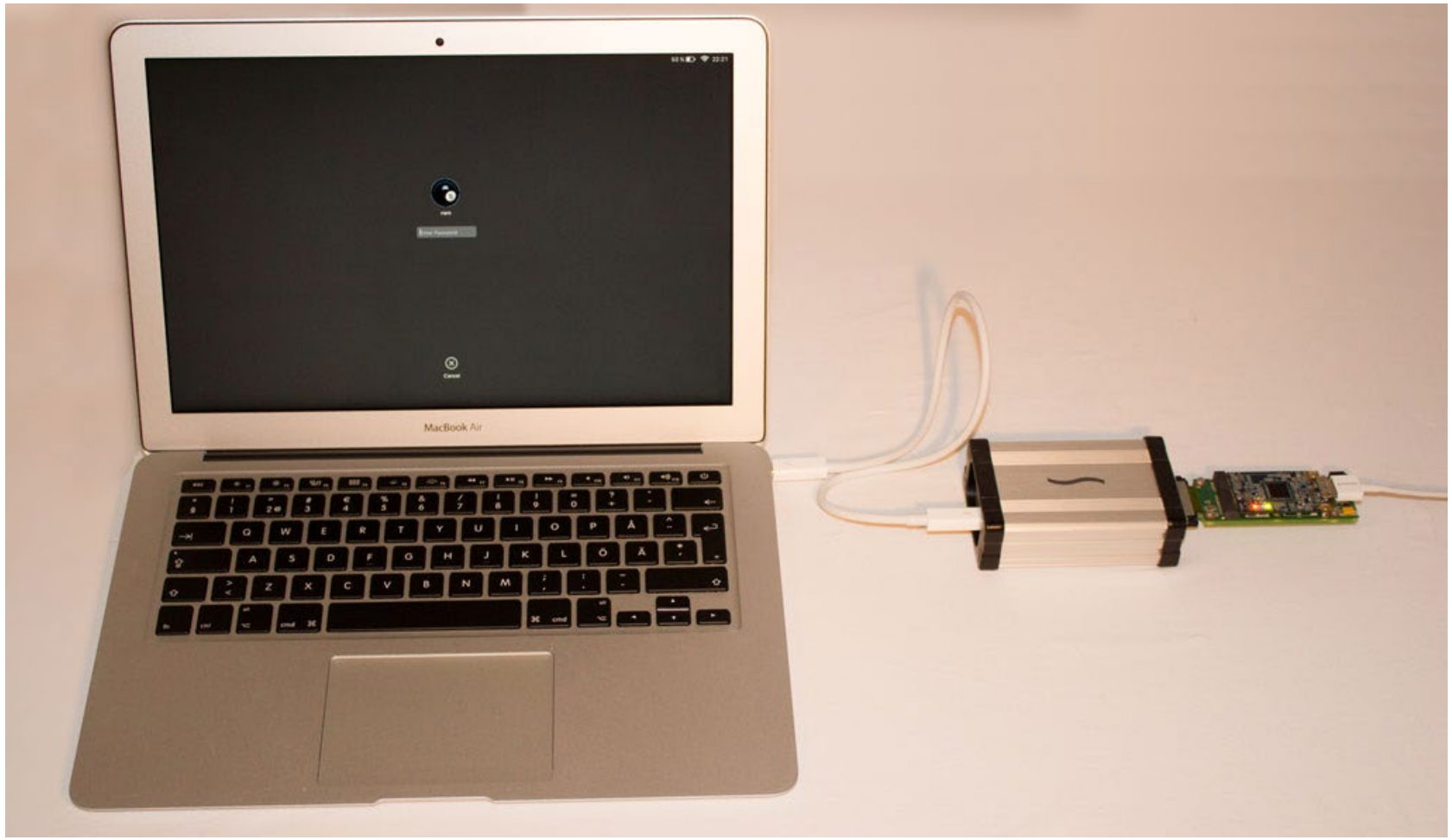
- Copying data through the CPU would be much slower
- FireWire, eSATA, PC Card, Thunderbolt, USB, PCI, …

A malicious device can directly access part or all of physical memory

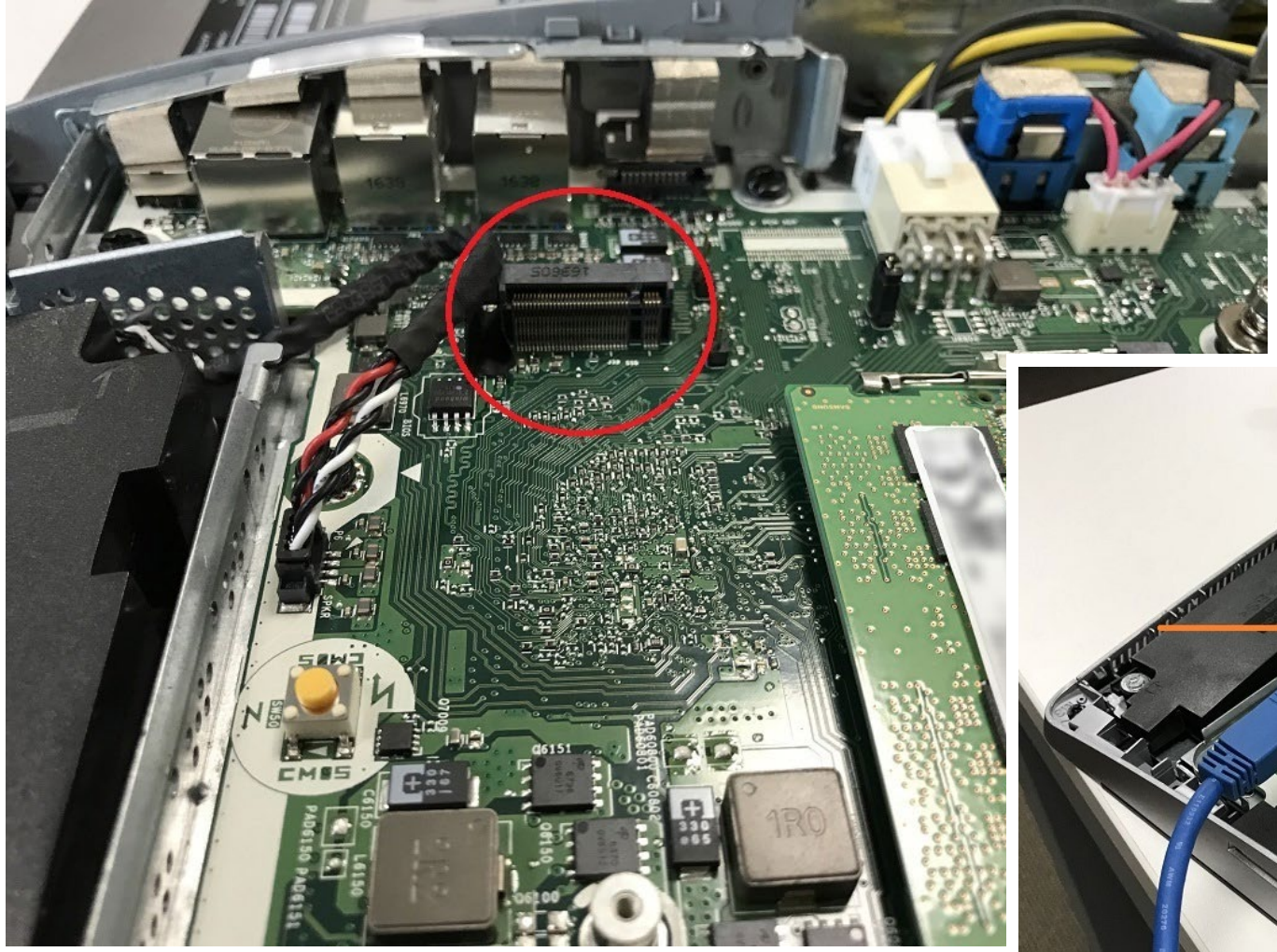
- Bypass OS security mechanisms, lock screen, …
- Read data, install malware/rootkits/backdoors, …

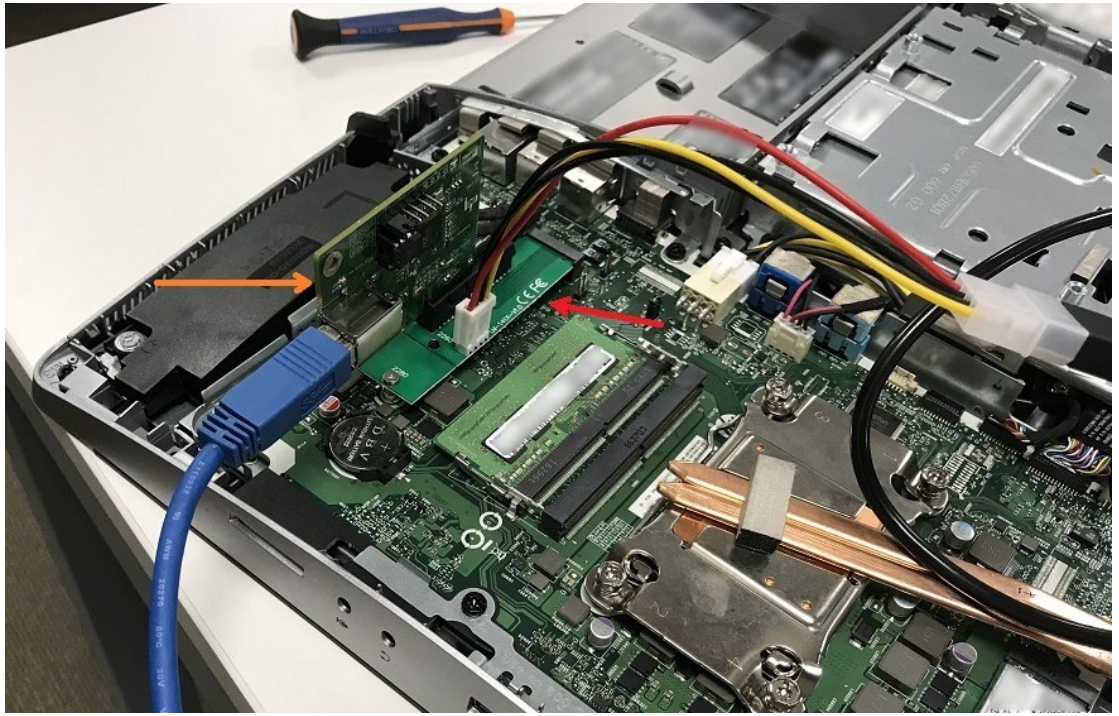
IOMMU provides some additional protection (recent CPUs)

- Translates I/O virtual to physical addresses and applies access control (similar to how the MMU translates virtual addresses from processes)
- *Other types of plug-and-exploit attacks are still possible* (e.g., a USB device pretending to be a keyboard)



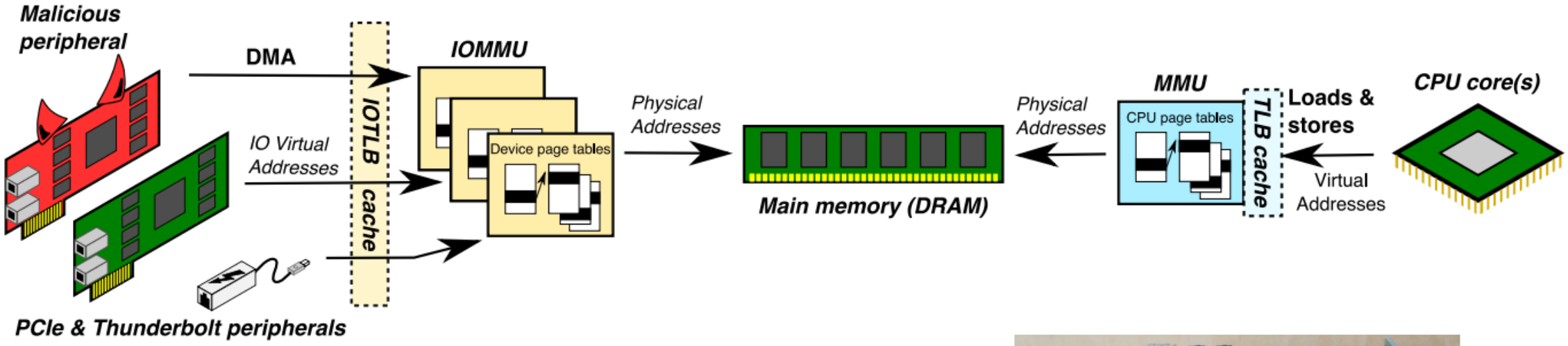
Example: retrieve FileVault2 password from suspended Mac through rogue Thunderbolt device (2016)





Example: compromise Windows 10 workstation

SSD NVMe M.2 connector (NVMe relies on PCIe): USB3 PCIe card ➔ PCIe to M2 adaptor



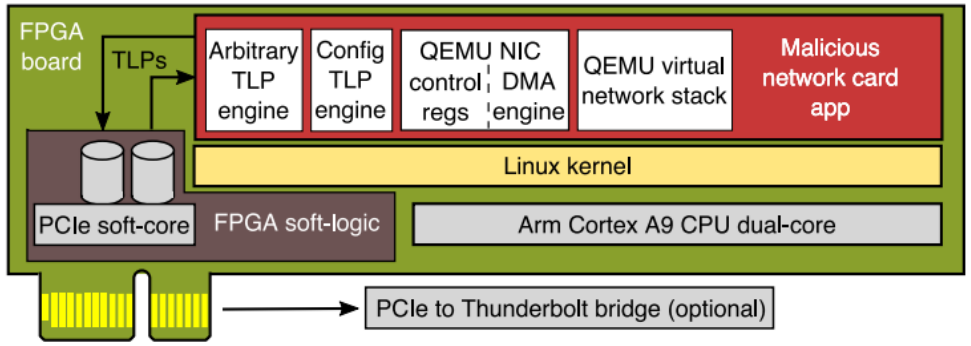


Fig. 4: Implementation of fully-functional network card using a QEMU device model running on FPGA

Fig. 1: Thunderbolt dock with FPGA implant, an implementation of our I/O-security research platform

ThunderClap: bypass IOMMU to Re-Enable DMA Attacks

Mimick the functionality of a legitimate peripheral to trick the OS into granting it access to memory

Inception https://github.com/carmaa/inception

PCI-based DMA physical memory manipulation tool

- Supports FireWire, Thunderbolt, ExpressCard, PC Card, and any other PCI/PCIe hardware interfaces
- Intrusive and non-intrusive memory access against live computers using DMA

Presents a Serial Bus Protocol 2 (SBP-2) unit directory to the victim over an IEEE1394 FireWire interface

- Victim OS thinks that a SBP-2 device has connected to the FireWire port
- SBP-2 devices use DMA for fast bulk data transfers (e.g., FireWire HDs, camcorders) ➔ DMA is enabled for the device
- The tool now has full read/write access to the lower 4GB of RAM

Hardware Keyloggers

Most common type: inline connection

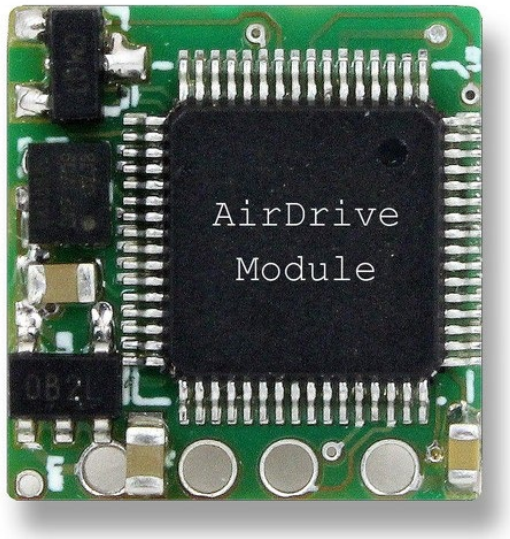
- Typically designed to have an innocuous appearance
- Can also be installed inside the keyboard itself
- On-device or wireless logging

Other types

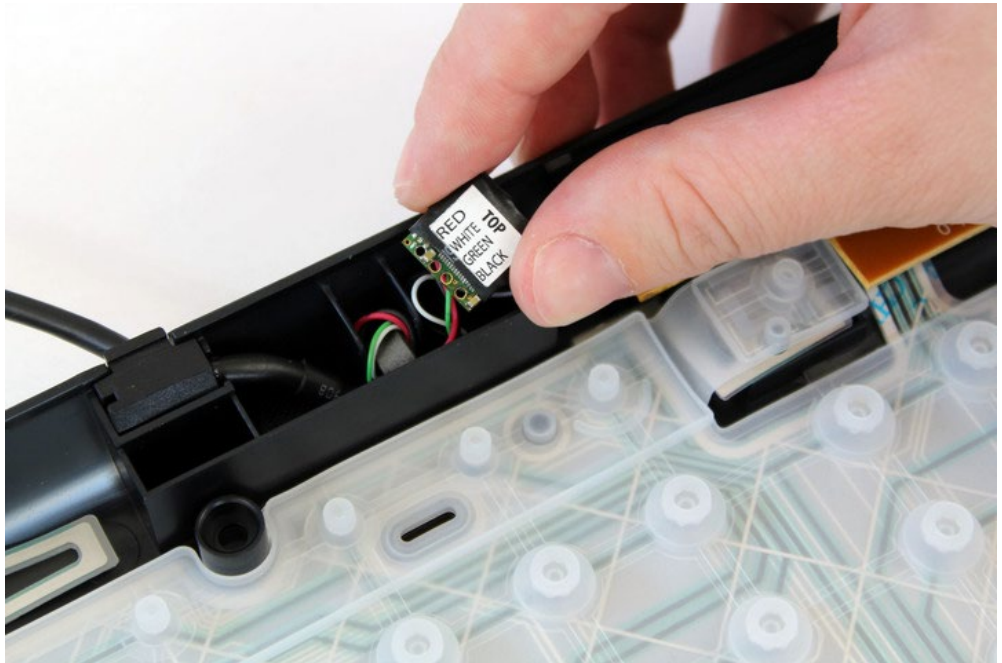
- Wireless sniffers: mostly for wireless keyboards
- Malicious firmware: BIOS handles keyboard events
- Keyboard overlays: fake keypad (mostly used in ATM attacks)
- Side channels (mostly experimental): electromagnetic emanations, powerline leakage, sound, etc.
- *Don't forget that cameras can record keystrokes (!)*

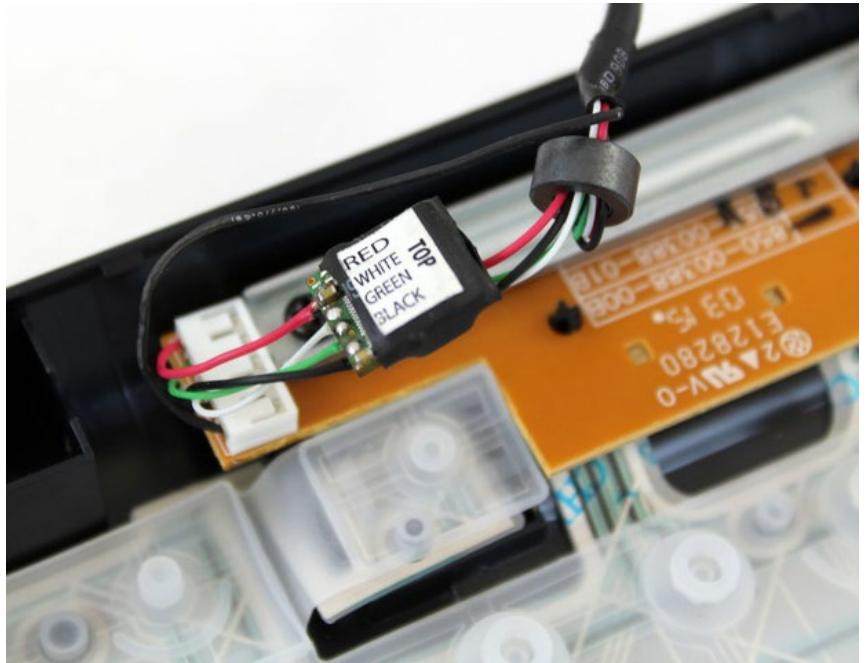

WiFi


KeyGrabber


AirDrive
Module


AirDrive - Data Log
This is the data log area of the AirDrive. You can view it by opening a web browser on any Wi-Fi device, such as a laptop, tablet, smartphone, or desktop computer. Simply enter 192.168.4.1 in the address bar.
Page: 1 / 10
<< Previous
Next >>
AirDrive ©
Settings
UDP Receiver application where streamed data is displayed live


RED
WHITE
GREEN
BLACK
TOP


RED
WHITE
GREEN
BLACK
TOP

USB Drop

Infection strategies

- Social engineering: rely on user action (e.g., open file, run .exe)
- HID spoofing: simulate human interface device (e.g., mouse, keyboard)
- 0-day: Stuxnet-level attack

Example: 297 social-engineered USB keys dropped on the University of Illinois campus ➔ *45% of the keys phoned home*

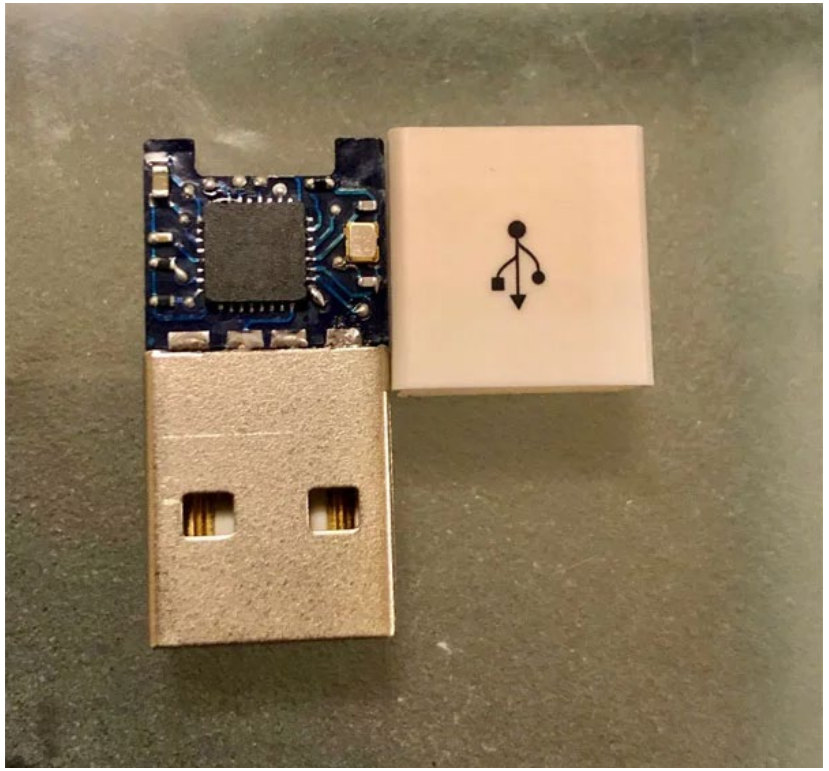
USB Rubber Ducky

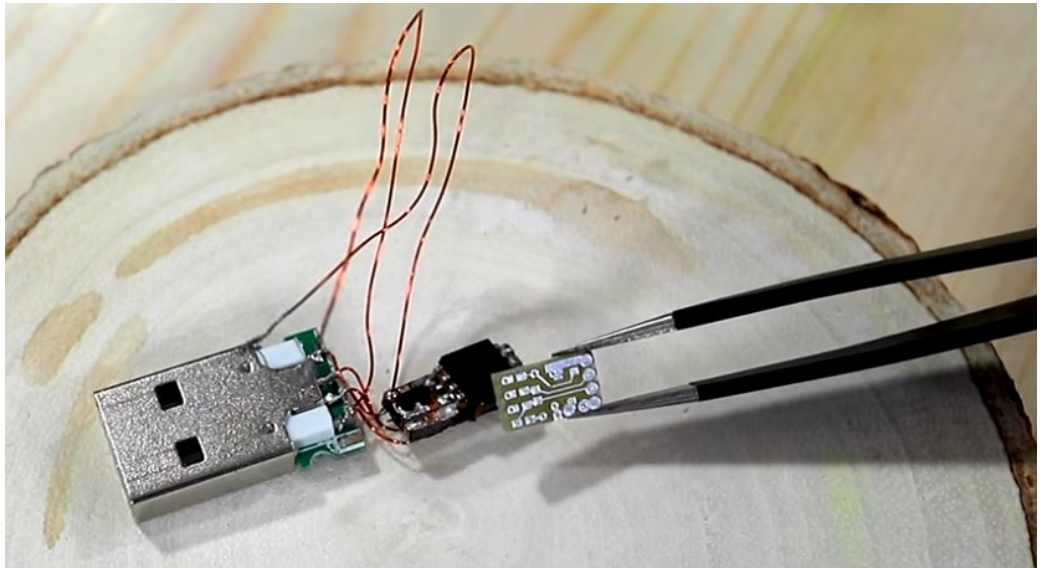
simple ducky payload.txt - Notepad

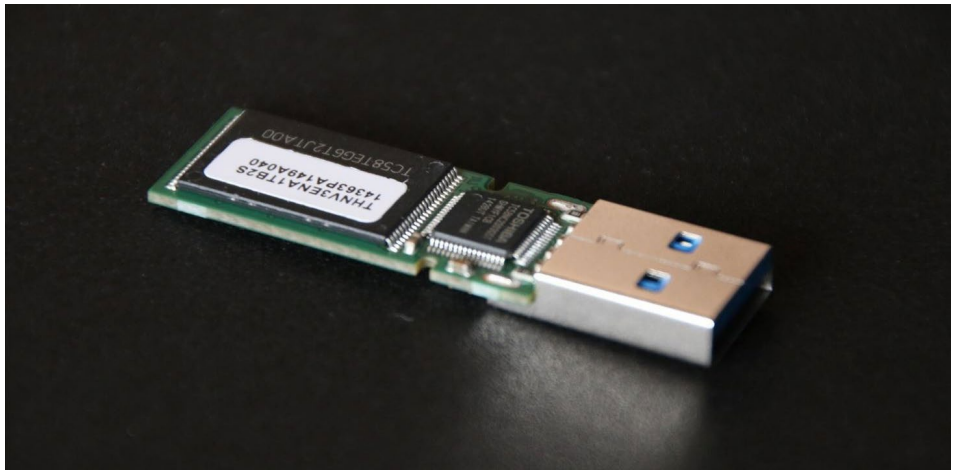
File Edit Format View Help

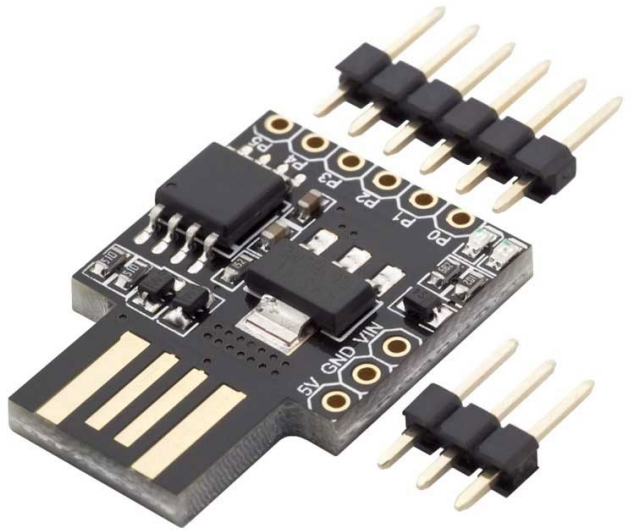
```
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello World! I'm in your PC!
```

Bad USB Cable

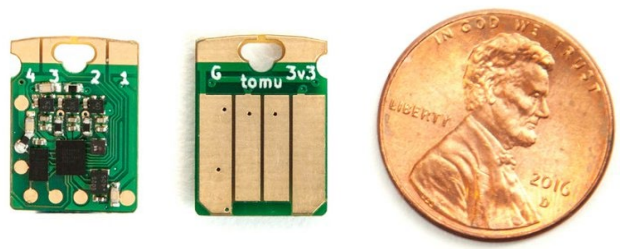







5V GND VIN

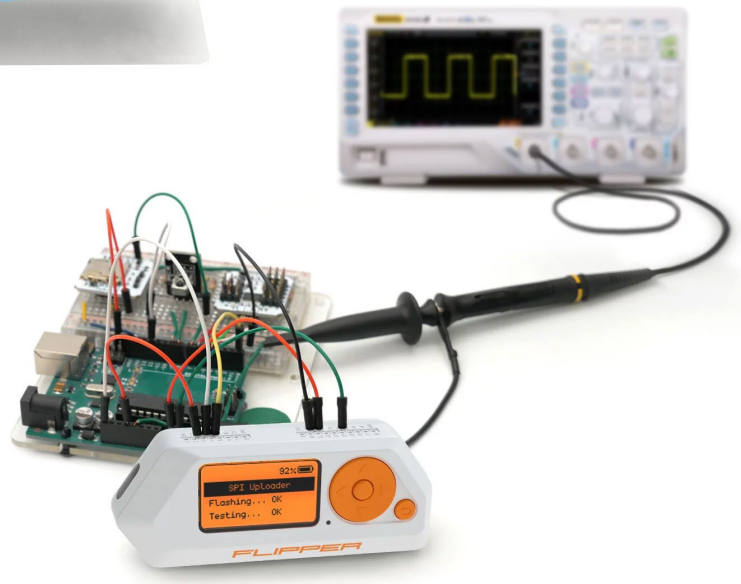

INVERSE PATH
armory
β-3L-NCP


4 3 2 1
G tomu 3v3
LIBERTY
2016

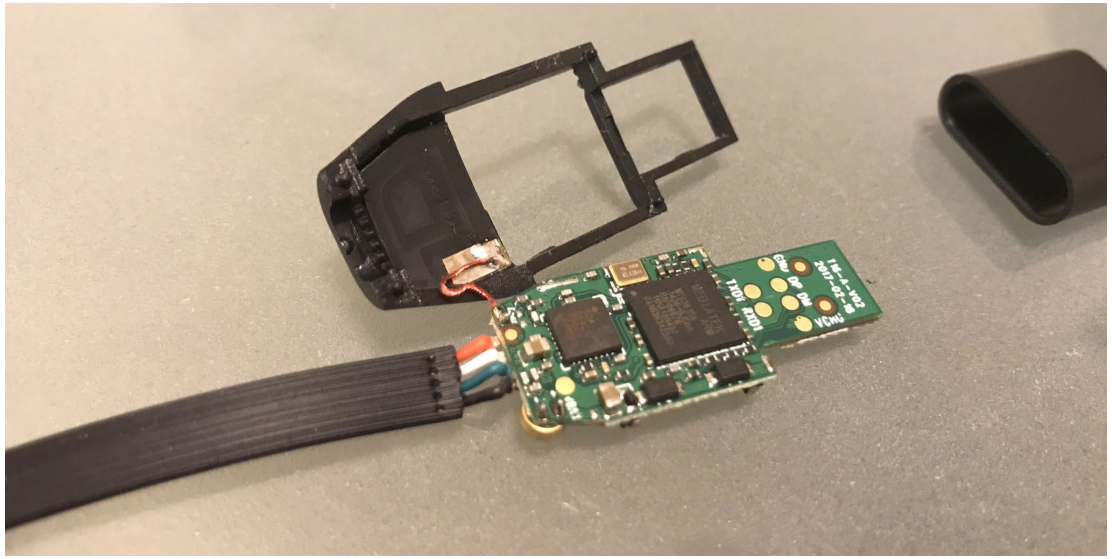
Flipper Zero

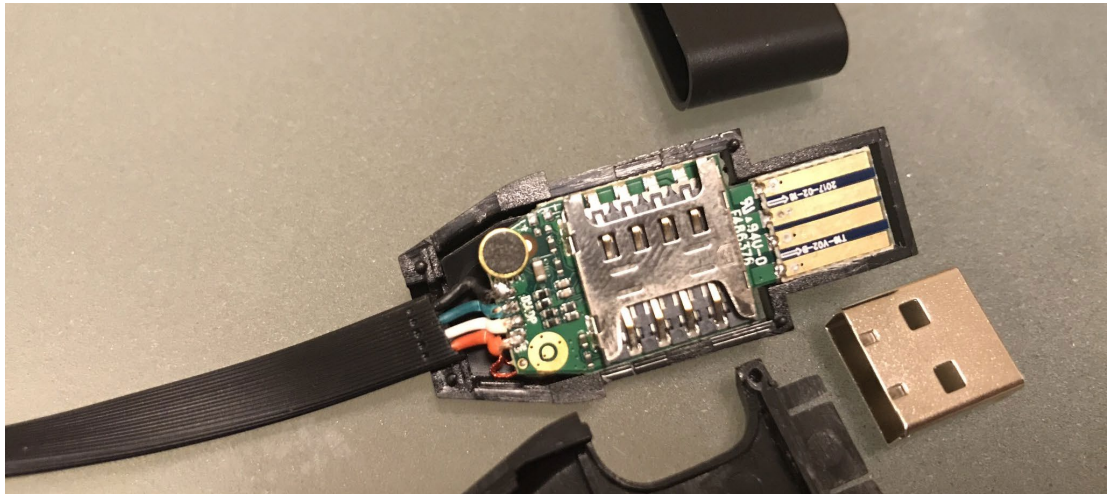
Read/clone/emulate:

- Sub-GHz
- 125 kHz RFID
- NFC
- Bluetooth
- Infrared
- iButton
- Bad USB/HID controller
- U2F
- GPIO pins for external HW



Spy cables: hidden microphones & geolocation ($10)



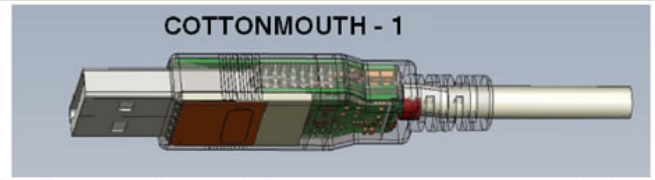


COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

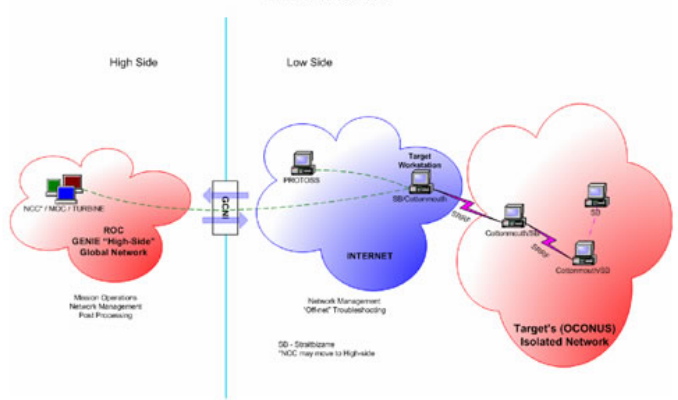
08/05/08



(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP
INTERNET Scenario



Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Student used 'USB Killer' device t

https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers

Incognito

POLICY | US & WORLD | TECH

Student used 'USB Killer' device to destroy $58,000 worth of college computers

46

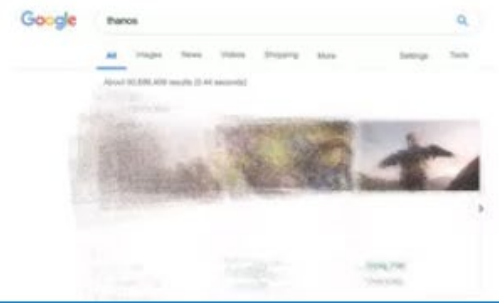
The former College of Saint Rose student faces up to 10 years in prison

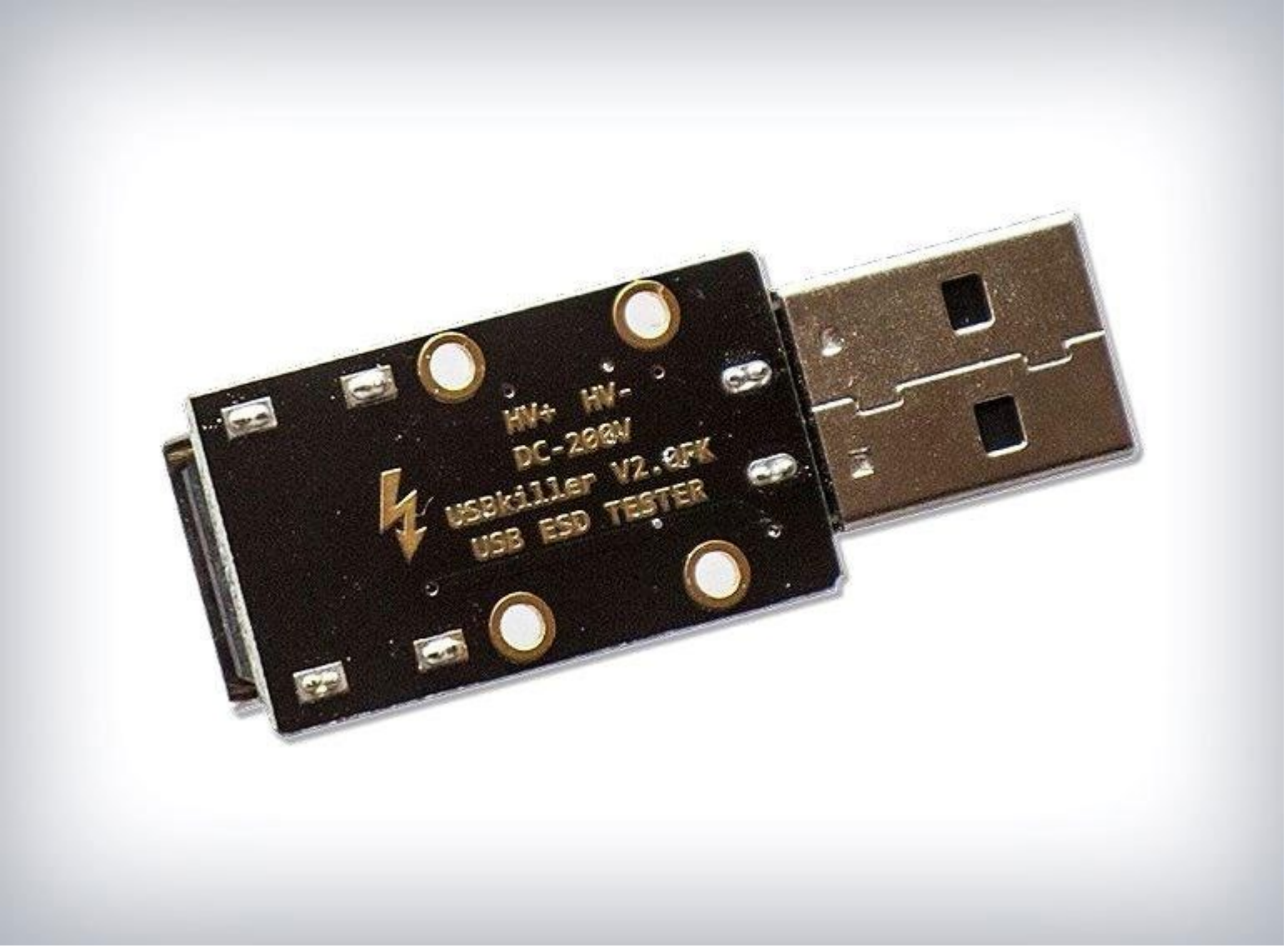
By Chris Welch | @chriswelch | Apr 17, 2019, 3:07pm EDT

SHARE

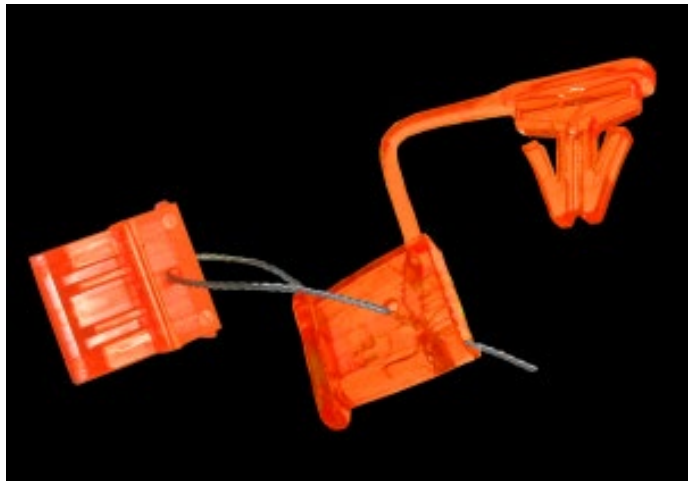
MOST READ

Astell & Kern announces the ridiculously powerful and pricey Kann Cube

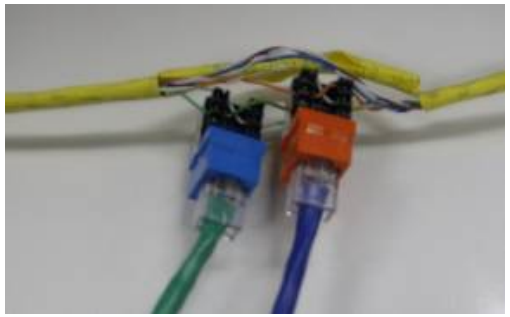



HV+ HV-
DC-200V
USBkiller V2.0FK
USB ESD TESTER

Disable/protect USB ports



Network Sniffing and Interception



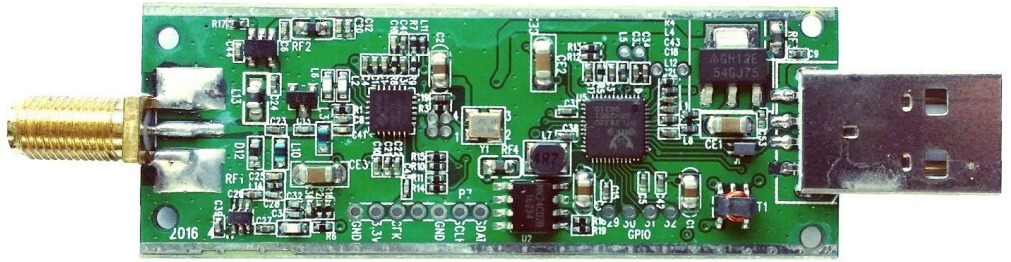
Software-defined Radio

RF communication that uses *software* to perform signal-processing tasks that are typically done by hardware

- Mixers, filters, amplifiers, modulators/demodulators, …

Can be used for a broad range of attacks

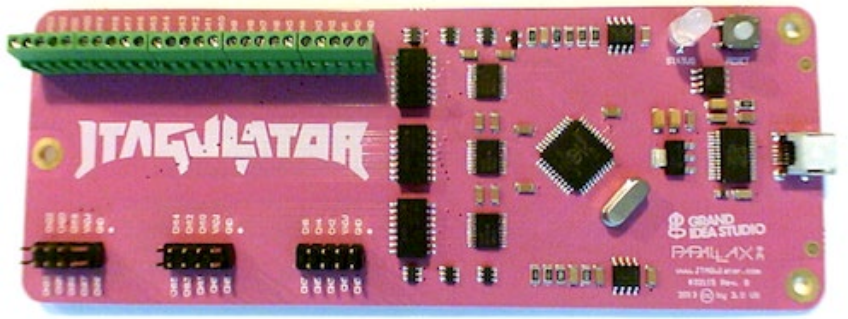
- RDS Traffic Message Channel
- RFID
- IMSI catcher
- GSM sniffing
- Restaurant pagers
- IoT devices
- Car key fobs
- Medical devices



Embedded Hardware Hacking

Main steps

- Research the device
- Identify the components
- Identify debugging ports
- Dump the flash
- Extract/analyze firmware



Common ports

- JTAG: dedicated debugging port implemented as a serial interface (typically hidden or present only in early/prototype models)
- UART: serial communication easily bridged over USB via any UART-to-USB bridge


lenovo