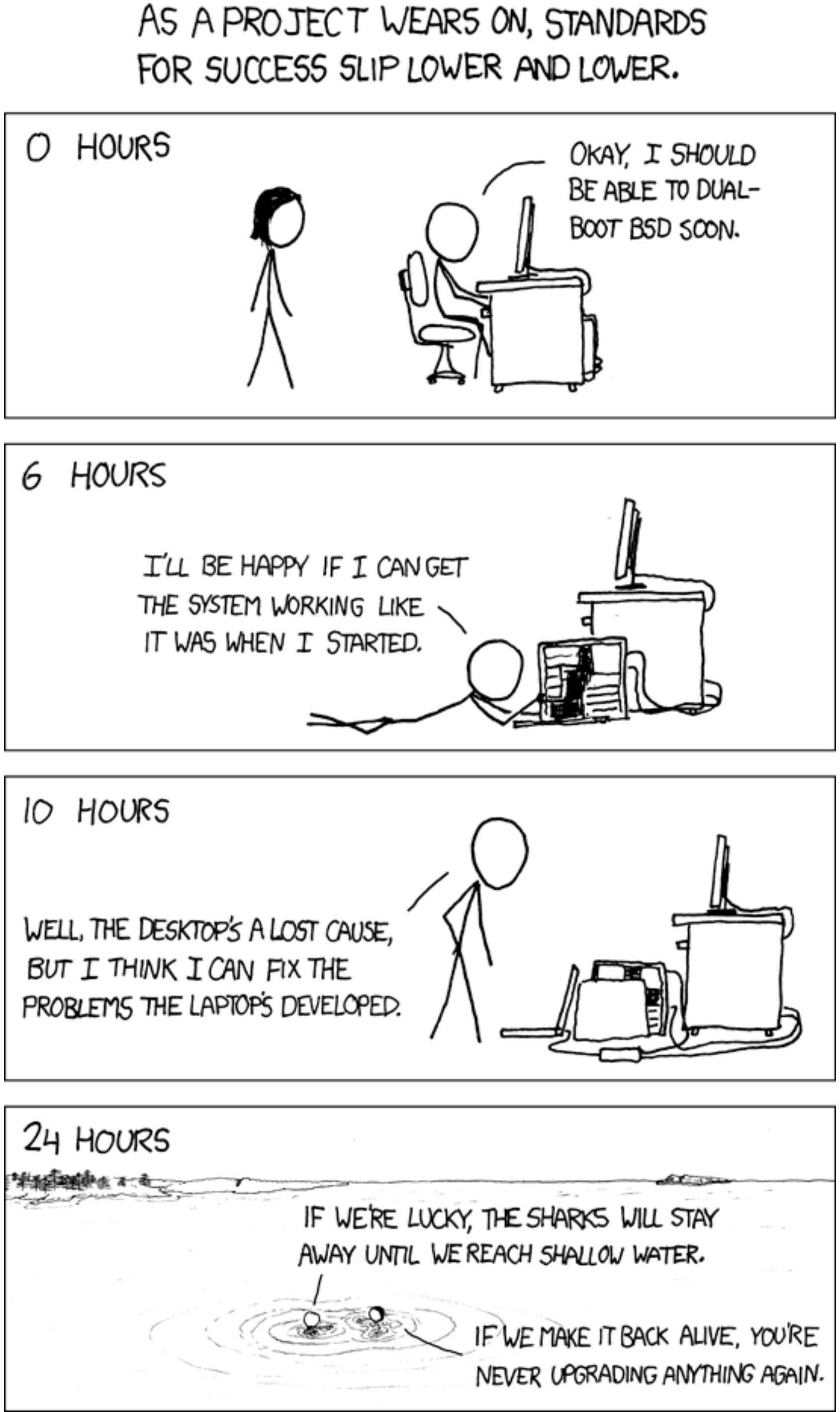

AS A PROJECT WEARS ON, STANDARDS FOR SUCCESS SLIP LOWER AND LOWER.
0 HOURS
OKAY, I SHOULD BE ABLE TO DUAL-BOOT BSD SOON.
6 HOURS
I'LL BE HAPPY IF I CAN GET THE SYSTEM WORKING LIKE IT WAS WHEN I STARTED.
10 HOURS
WELL, THE DESKTOP'S A LOST CAUSE, BUT I THINK I CAN FIX THE PROBLEMS THE LAPTOP'S DEVELOPED.
24 HOURS
IF WE'RE LUCKY, THE SHARKS WILL STAY AWAY UNTIL WE REACH SHALLOW WATER.
IF WE MAKE IT BACK ALIVE, YOU'RE NEVER UPGRADING ANYTHING AGAIN.

https://xkcd.com/349/

CS 55:
Security and Privacy

Side channels and countermeasures

Agenda

1. Terminology

2. Listening devices and defenses

3. Side channel attacks

4. Hacking humans

5. Securing hardware from side channels

Emanations can be intentional or unintentional

Unintentional

Side channel: information leaks accidentally via some medium not intended for communication

Example: Use audio to recover RSA private key

Intentional

Covert channel: a deliberate leak via some medium not intended for communication

Example: Use screen brightness on computer to exfiltrate message without detection

Adapted from Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.
https://thehackernews.com/2020/02/hacking-air-gapped-computers.html

Emission security (EMSEC) attempts to prevent compromising emissions

Examples

EMSEC is part of the broader COMSEC

- Control emissions to prevent observation
- Military aircraft going radio silent after crossing FEBA

Tempest

- Stray RF emissions picked up by opponent and information reconstructed
- Also refers to shielding equipment from such attacks

Interference

- Electromagnetic compatibility (EMC)/interference (EMI)
- Radio Frequency Interference (RFI)/crosstalk
- Electromagnetic Pulse (EMP)

Adapted from Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

SCIFs are facilities designed to protect against bugs and side channel attacks

Sensitive Compartmentalized Information Facility (SCIF)

- Physical access tightly controlled
- Must have appropriate security clearance to enter
- Shielded against side channels
- Regularly swept/monitored for bugs

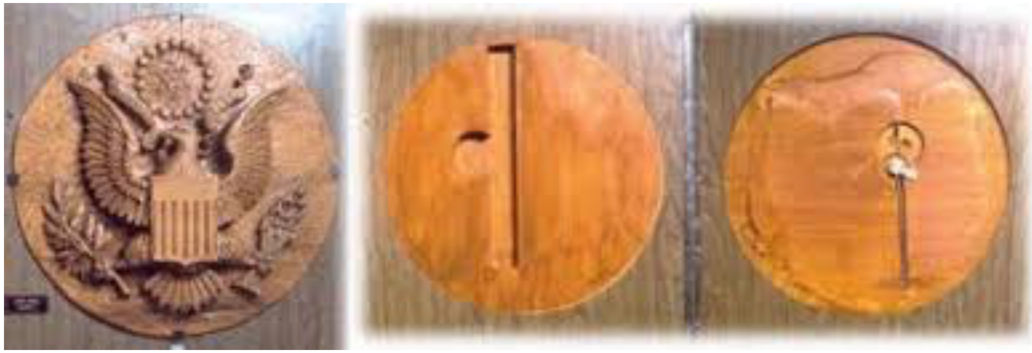
Adapted from Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

Agenda

1. Terminology
2. ➡ Listening devices and defenses
3. Side channel attacks
4. Hacking humans
5. Securing hardware from side channels

Bugs capture audio, video, and/or keystrokes

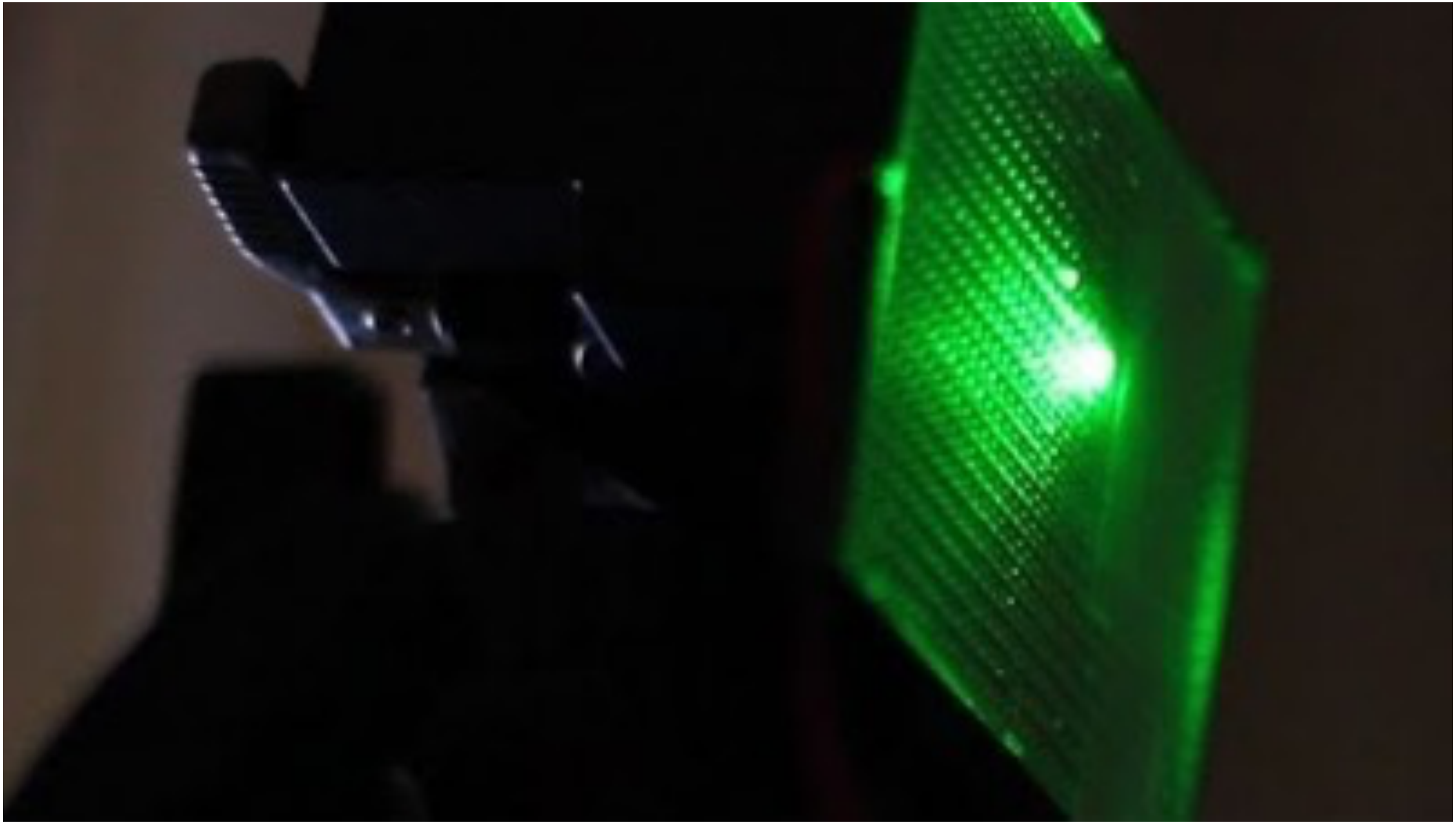
- Simple bugs use AM or FM
- Battery driven, last days/weeks
- Cost a few dollars
- Easy to detect?



- Great Seal bug
- Resonate cavity acted as microphone
- Worked when hit by RF

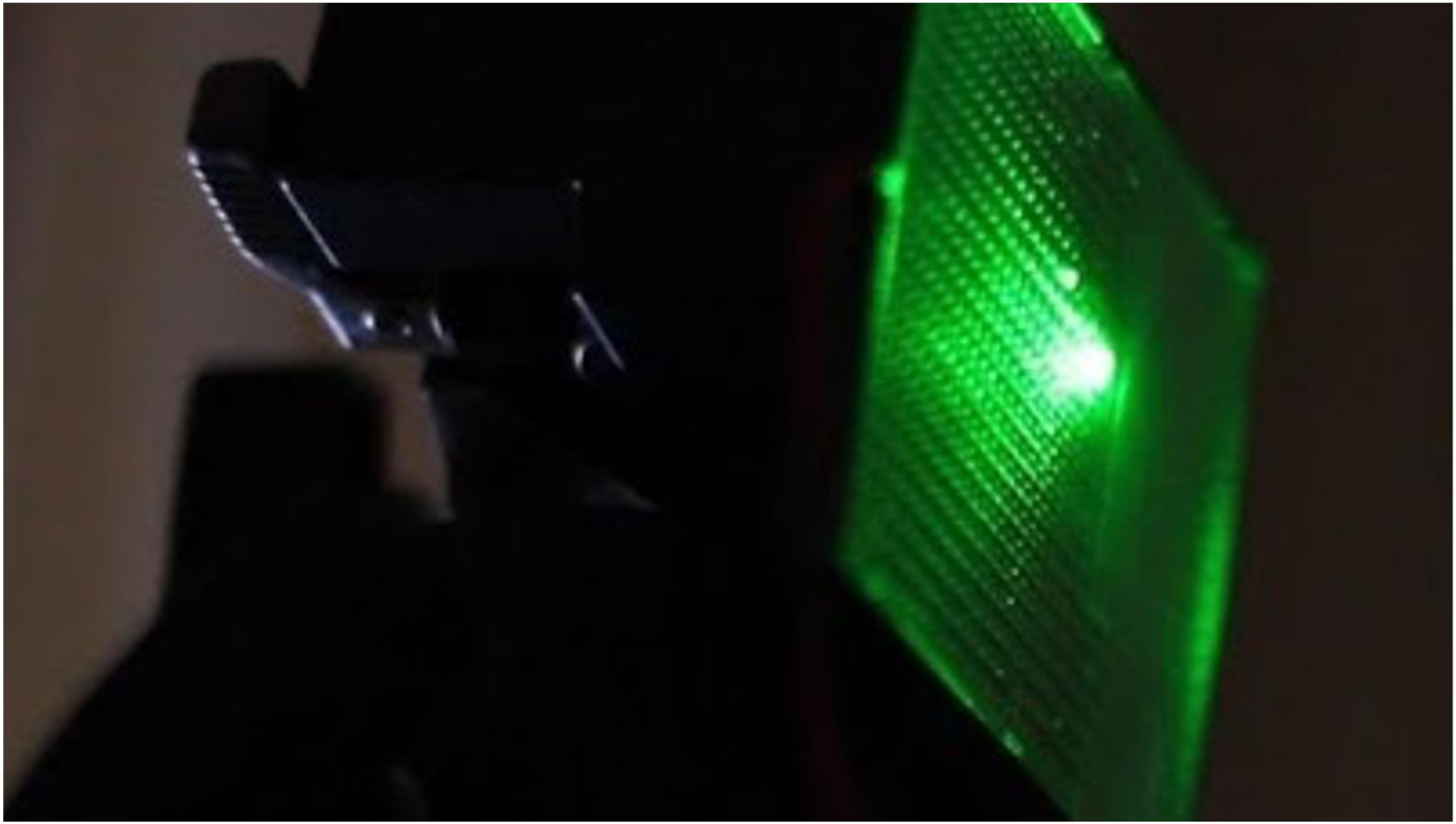
- Laser microphone
- Shines laser against windows
- Accurate distance measurement detects vibrations caused by speech

Laser microphone demo



https://www.youtube.com/watch?v=1zGU_30l6eU&start=270

Laser microphone demo



https://www.youtube.com/watch?v=1zGU_30l6eU&start=270

Countermeasures?

Bugs can be found in unexcepted places, but not always by design!

- Keystroke logger
- Inserted into cable on desktop
- Hard to discover

- Furby toy listens and randomly repeats conversations
- Banned by NSA
- Cayla talking doll banned in Germany, could talk to children

- Roomba maps home
- Can pick up voice conversations

Sami, Sriram, et al. "Spying with your robot vacuum cleaner: eavesdropping via lidar sensors." *Proceedings of the Conference on Embedded Networked Sensor Systems (Sensys)*. 2020.

The greatest bug might be one you are probably carrying right now!

- Phone has many sensors (microphone, 3 radios, accelerometer, light sensor, battery indicator)
- Many academic papers use accelerometer or microphone to determine keystrokes
- Reflections of screen from glasses or eyeballs can reveal keystrokes[1]
- Battery level can indicate route of travel[2]
- Generally, assume the phone is infected with malware

[1] Raguram, Rahul, et al. "iSpy: automatic reconstruction of typed input from compromising reflections." *Proceedings of the ACM conference on Computer and communications security*. 2011.

[2] Michalevsky, Yan, et al. "Powerspy: Location tracking using mobile device power analysis." *USENIX Security Symposium (USENIX Security)*. 2015..

To be useful, bugs must exfiltrate their data

Sometimes data is stored locally on the bug

Adversary returns later to retrieve it

Often data is transmitted using Radio Frequencies (RF)

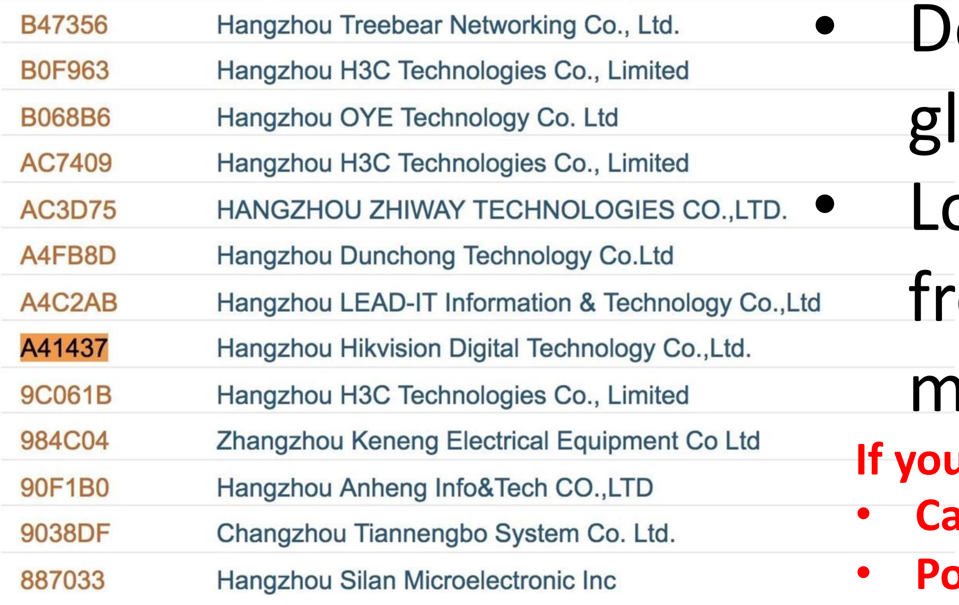
- AM
- FM
- Wi-Fi

Technical Surveillance Countermeasures (TSCM) can detect RF data exfiltration

Bug sweeps

- Surveillance receivers
  - Sweep radio spectrum from about 10KHz to 6 GHz every few seconds
  - Look for unexplained signals
  - Problems with frequency hoppers, spread spectrum, burst transmitters, LPI
- Non-linear junction detectors (NLJD)

Wireless cameras can often be detected from their communications



B47356	Hangzhou Treebear Networking Co., Ltd.
B0F963	Hangzhou H3C Technologies Co., Limited
B068B6	Hangzhou OYE Technology Co. Ltd
AC7409	Hangzhou H3C Technologies Co., Limited
AC3D75	HANGZHOU ZHIWAY TECHNOLOGIES CO.,LTD.
A4FB8D	Hangzhou Dunchong Technology Co.Ltd
A4C2AB	Hangzhou LEAD-IT Information & Technology Co.,Ltd
A41437	Hangzhou Hikvision Digital Technology Co.,Ltd.
9C061B	Hangzhou H3C Technologies Co., Limited
984C04	Zhangzhou Keneng Electrical Equipment Co Ltd
90F1B0	Hangzhou Anheng Info&Tech CO.,LTD
9038DF	Changzhou Tiannengbo System Co. Ltd.
887033	Hangzhou Silan Microelectronic Inc

Cameras

Airbnb room sometimes have hidden cameras[1]

Visual search looking for anything out of place

- Detect cameras by looking for glint from lens
- Look for camera video feeds from known camera manufacturers (OUIs)[2]

If you discover a hidden camera:

- **Call the authorities**
- **Possible to execute a deauthentication attack to repeatedly knock camera off Wi-Fi (dropkick.sh)**

[1] https://nymag.com/intelligencer/2017/11/you-should-probably-check-your-airbnb-for-hidden-cameras.html

[2] https://null-byte.wonderhowto.com/how-to/hack-wi-fi-disabling-security-cameras-any-wireless-network-with-aireplay-ng-0185435/

Wi-Fi cameras (or other devices) can be taken offline easily

https://www.youtube.com/watch?v=kXm8f9fhaxQ&start=349

Agenda

1. Terminology

2. Listening devices and defenses

3. Side channel attacks

4. Hacking humans

5. Securing hardware from side channels

Tempest: spying on leaking emissions; Van Eck phreaking is a famous example

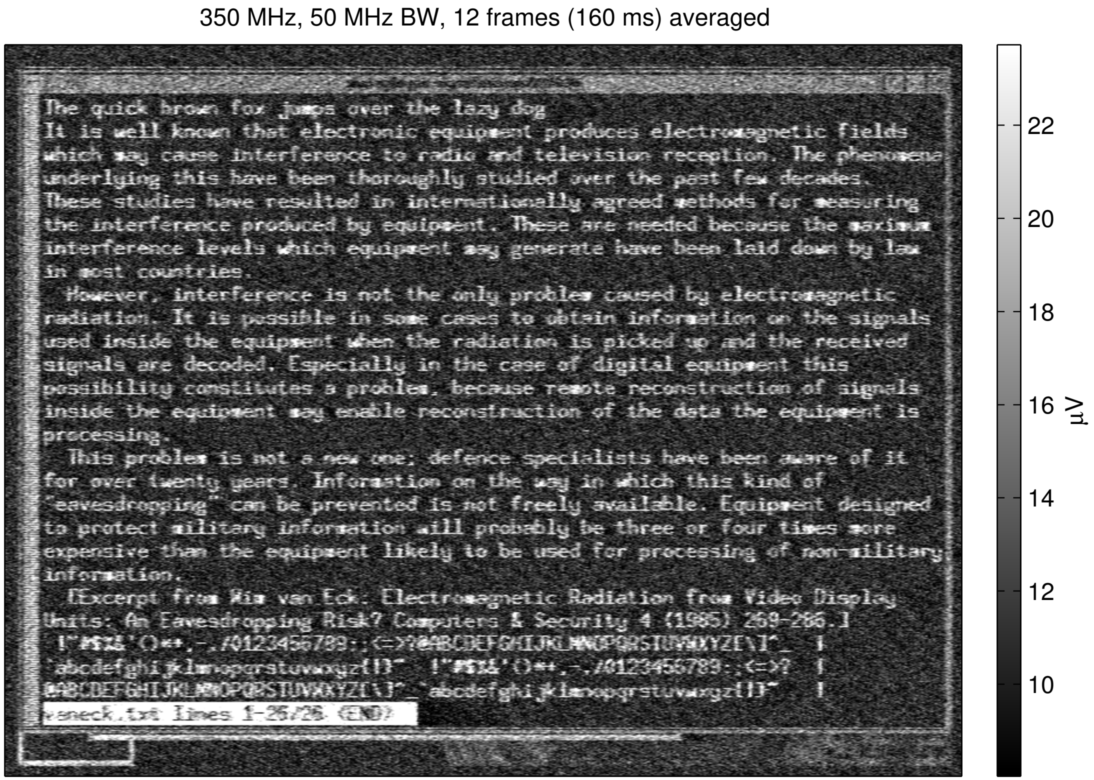
Tempest covers sound and vibrations, but is often thought of as related to RF

Wim Van Eck published research that reconstructs text displayed on a CRT from leaky RF

- Electron gun moves across screen hits phosphors on screen with electron to light up
- Creates emanation that can be picked up remotely
- Through walls, via sprinkler pipes, power lines

Van Eck, Wim. "Electromagnetic radiation from video display units: An eavesdropping risk?." *Computers & Security* 4.4 (1985): 269-286.

Flat screens often considered to be immune from Van Eck attacks, but are not!



```
The quick brown fox jumps over the lazy dog
It is well known that electronic equipment produces electromagnetic fields
which may cause interference to radio and television reception. The phenomena
underlying this have been thoroughly studied over the past few decades.
These studies have resulted in internationally agreed methods for measuring
the interference produced by equipment. These are needed because the maximum
interference levels which equipment may generate have been laid down by law
in most countries.
  However, interference is not the only problem caused by electromagnetic
radiation. It is possible in some cases to obtain information on the signals
used inside the equipment when the radiation is picked up and the received
signals are decoded. Especially in the case of digital equipment this
possibility constitutes a problem, because remote reconstruction of signals
inside the equipment may enable reconstruction of the data the equipment is
processing.
  This problem is not a new one; defence specialists have been aware of it
for over twenty years. Information on the way in which this kind of
"eavesdropping" can be prevented is not freely available. Equipment designed
to protect military information will probably be three or four times more
expensive than the equipment likely to be used for processing of non-military
information.
  [Excerpt from Wim van Eck: Electromagnetic Radiation from Video Display
Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286.]
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_  |
`abcdefghijklmnopqrstuvwxyz{|}~  !"#$%&'()*+,-./0123456789:;<=>?  |
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~   |
vaneck.txt lines 1-26/26 (END)
```

Text recovered from Toshiba laptop via RF emanation

Attacker must be close physical proximity

Cannot exploit over the Internet

Tempest zones

Zone	Range
0	1 meter
1	20 meters
2	120 meters
3	1200 meters

Expensive

Most commercial equipment

Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

Timing attacks are another side channel; RSA keys can be recovered

RSA exponentiation done one bit at a time

- If bit =1, then multiply
- Faster if bit=0 than if bit=1
- Guess exponent one bit a time
- Measure time
- Repeated decrypt observations reveals the private key
- OpenSSL private key guessed in 1 million decryptions on Apache servers
- Can use blinding to defeat attack (OpenSSL had it, Apache didn't use it)

Symmetric algorithms also vulnerable to timing attacks

- Cache misses

Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

Brumley, David, and Dan Boneh. "Remote timing attacks are practical." *Computer Networks* 48.5 (2005): 701-716.

Power usage can also be exploited

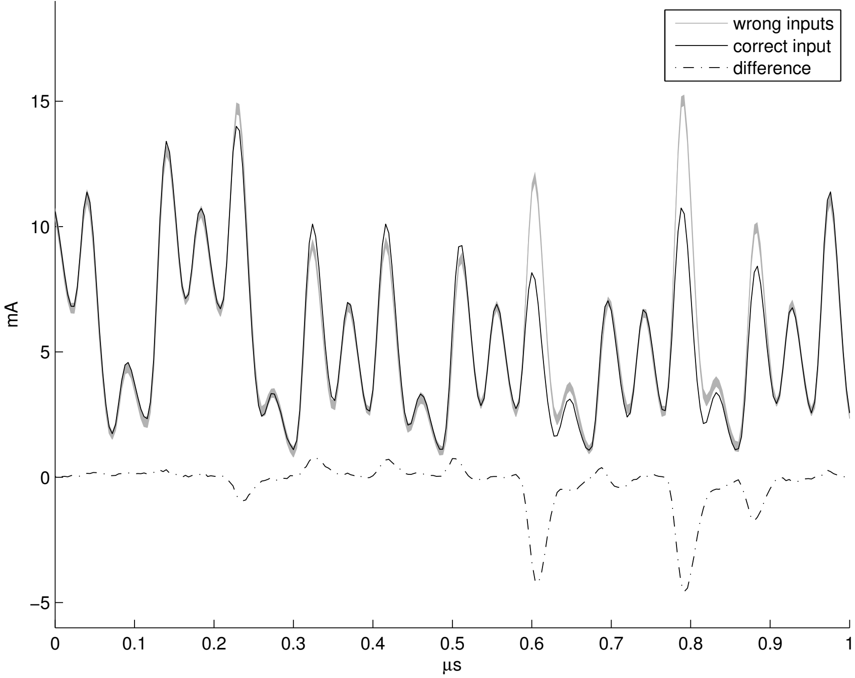
Power analysis (rail noise analysis) measures power draw

- Simple to implement
- Put resistor on ground line and connect digital scope to observe current draw

Guess password one byte at at a time

Home in on correct password by watching current draw

Another use: detect malware on medical equipment



Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020
Clark, Shane S., et al. "Wattsupdoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices." *HealthTech*. 2013.

Glitching involves introducing unanticipated inputs into a chip

Glitching involves injecting a short transient voltage at just the right time

- Typically ranges 1V to tens of volts
- Normally only lasts a few nanoseconds
- Can disrupt chip operation
  - Skip a few lines of boot code
  - Skip authentication step (e.g., skip code that asks for pin)
- Examples: Xbox 360 and PlayStation
- Only need an FPGA and hobbyist hardware

https://www.invia.fr/pages/tutorials/how-a-voltage-glitch-attack-could-cripple-your-soc-or-mcu-and-how-to-securely-protect-it.aspx

Glitching can also be done using a laser against Google Home and Amazon Alexa

Target MEMS microphone with laser

Can inject voice commands from across the street

Research project called Light Commands

Sugawara, Takeshi, et al. "Light commands: laser-based audio injection attacks on voice-controllable systems." *USENIX Security*. 2020.

Light Commands demo

https://www.youtube.com/watch?v=ozIKwGt38LQ&start=520

Optical side channels are more than just shoulder surfing!

Kuhn read information on screen from light on face and shirt[1]

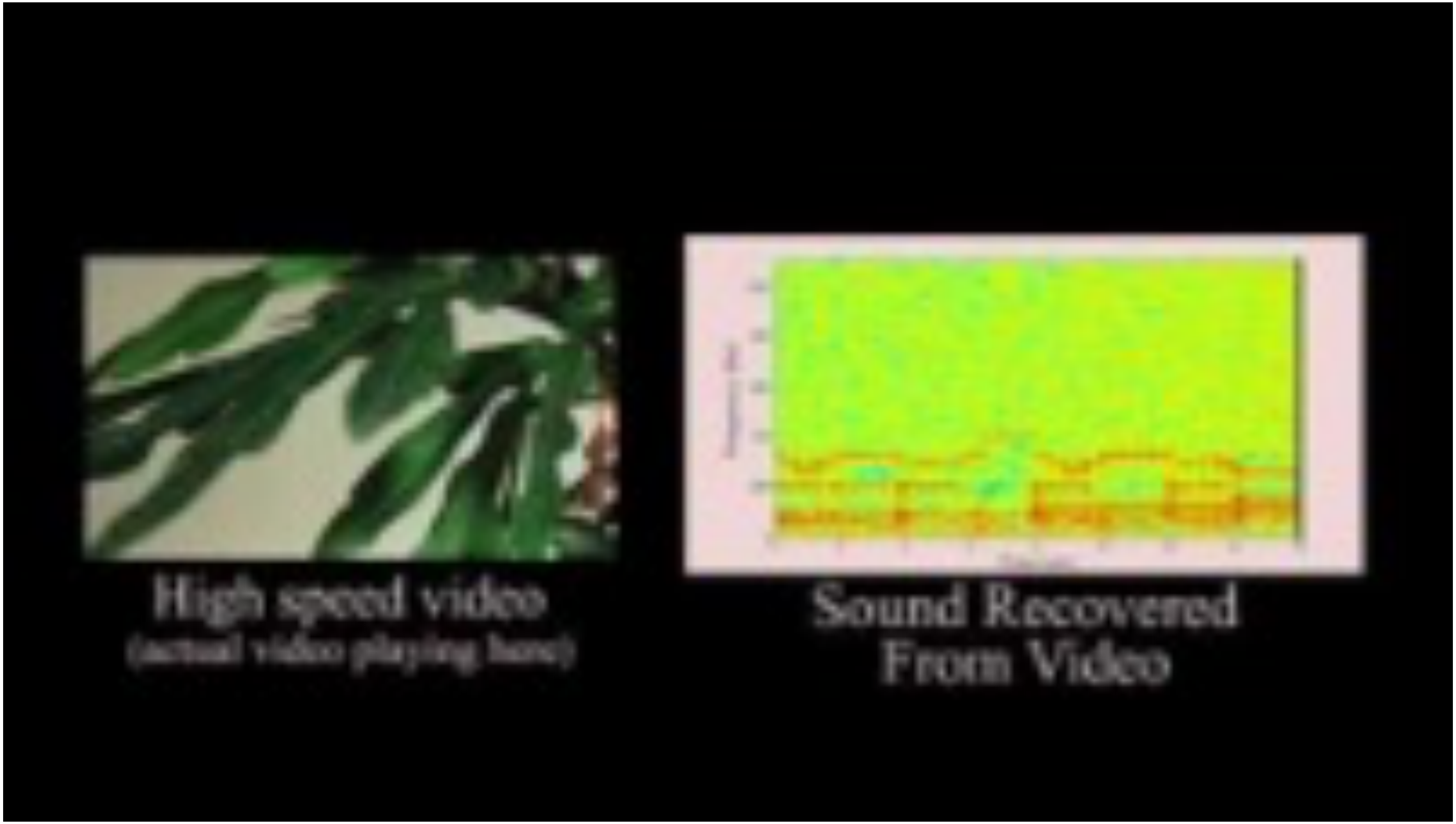
Snowden says this was used to spy on foreign embassies (code name Ocean)

Nassi and colleagues recovered speech and music from vibrations in hanging lightbulb[2]

(MIT did it 6 years ago with a bag of potato chips[3])

[1] MG Kuhn, “Optical Time-Domain Eavesdropping Risks of CRT Displays” in IEEE Symposium on Security and Privacy (2002)
[2] B Nassi, Y Pirutin, A Shamir Y Elovici, B Zadov, “Lamphone – Real-Time Passive Sound Recovery from Light Bulb Vibrations” BlackHat USA (2020)
[3] https://news.mit.edu/2014/algorithm-recovers-speech-from-vibrations-0804

Audio recovered by optically observing a bag of chips



High speed video
(actual video playing here)

Sound Recovered
From Video

https://www.youtube.com/watch?v=FKXOucXB4a8&start=92

Acoustics are another potential side channel

Acoustic emanations from a chip have been used to steal crypto keys[4] (so has RF!)

Can tell which key was pressed based on sound (or motion of the device) caused by press[1]

Given a small sample of someone typing, can determine which key was pressed based on inter-key timing from typing sound[2]

Others propose acoustics as an authentication scheme[3]

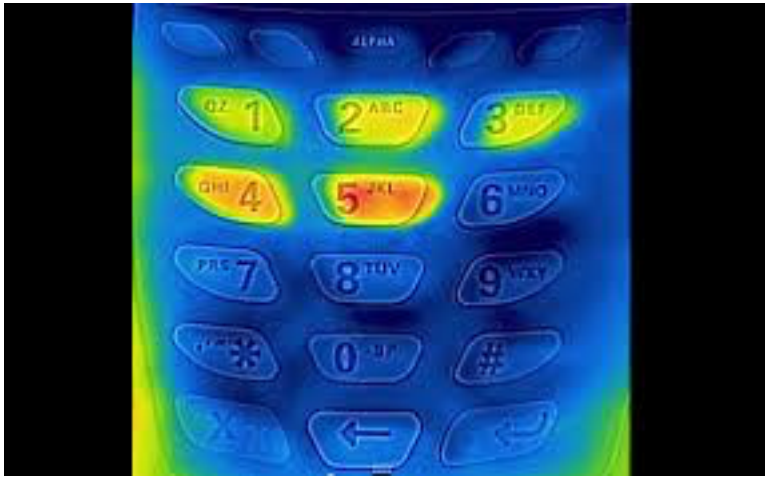
[1] Asonov, Dmitri, and Rakesh Agrawal. "Keyboard acoustic emanations." *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*. IEEE, 2004.
[2] Zhuang, Li, Feng Zhou, and J. Doug Tygar. "Keyboard acoustic emanations revisited." *ACM Transactions on Information and System Security (TISSEC)* 13.1 (2009): 1-26.
[3] Jan, Mian Ahmad, et al. "A robust authentication scheme for observing resources in the internet of things environment." *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2014.
[4] E Tromer, 'Hardware-Based Cryptanalysis', PhD Thesis, Weizmann Institute of Science (2007), at http://www.wisdom.weizmann.ac.il/~tromer/ papers/tromer-phd-dissertation.pdf

If something can be observed in any way, there is a good chance it can be exploited

Other side channels and attacks

- Smudge and residual heat attacks recover pins
- Clock skews to identify devices
- Physical layer manufacturing imperfections identify devices
- Many, many other types of keystroke recovery schemes including vibration
- Smart watch detects activity
- Lots more

Adversaries are clever!



Attack vectors

- RF
- Timing/Power
- Optical
- Acoustics
- Heat
- Vibration

Adapted from Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

Agenda

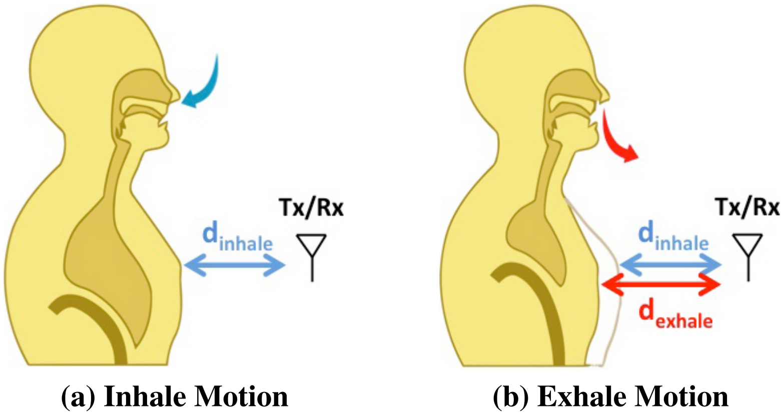
1. Terminology
2. Listening devices and defenses
3. Side channel attacks
4. ➡ Hacking humans
5. Securing hardware from side channels

Pulse and respiration rate can be detected via video

Implications if your employer knows this information?

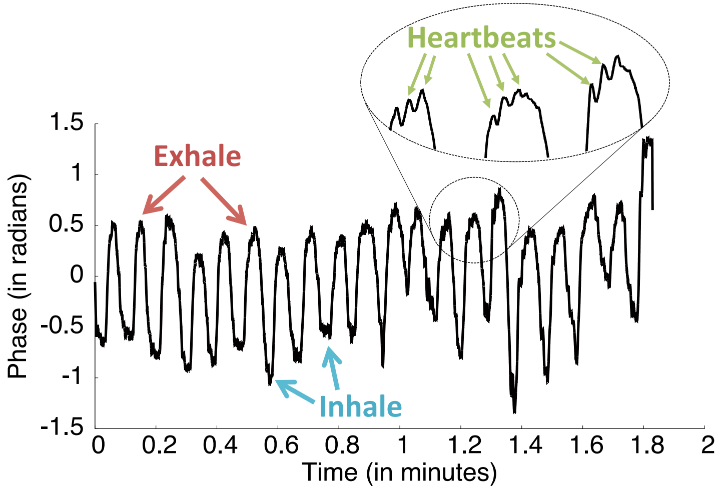
https://www.youtube.com/watch?v=e9ASH8IBJ2U&t=21s

Wireless transmissions can reveal pulse and respiration rate also!



(a) Inhale Motion

(b) Exhale Motion



Vital-Radio transmits FMCW

System measures time of flight

Detects small differences in distance when someone breathes

Also measures heart rate!

This approach is purposefully trying to collect information with single-purpose transmission

Newer research collects data from data background transmissions

Other uses in business setting?

Adib, Fadel, et al. "Smart homes that monitor breathing and heart rate." *Proceedings of the ACM conference on Human Factors in Computing Systems*. 2015.

Channel State Information (CSI) from data transmissions can be a side channel

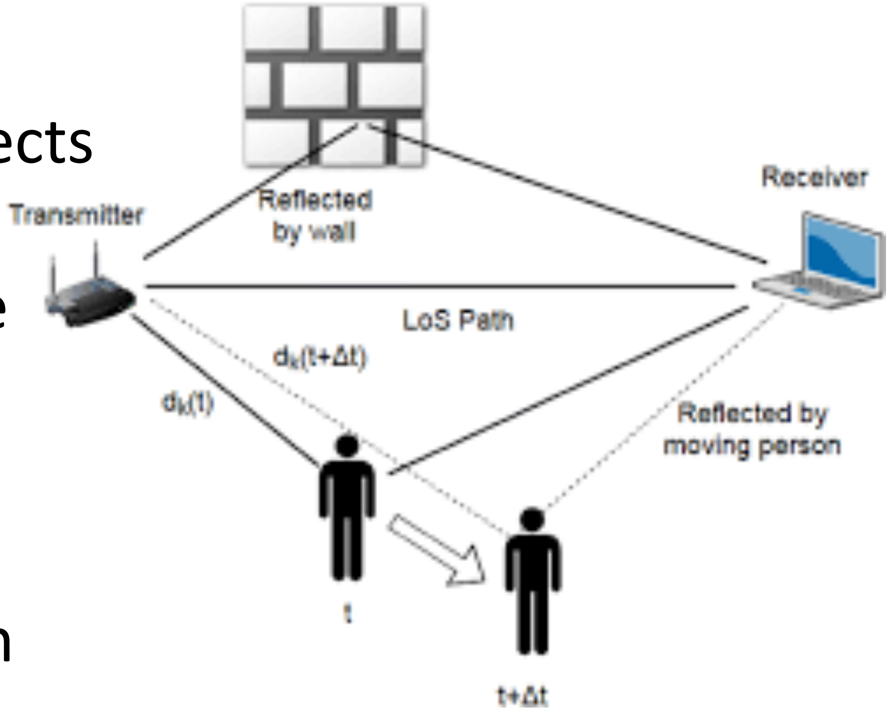
Signal sent to receiver will be modified by the environment

Receiver can estimate channel effects with preamble

Changes caused by channel can be used for[1]:

- Device-free fall detection
- Key presses on keyboard
- Gesture and smoking detection
- Identification

Backscattered background data transmissions can power devices without batteries[2]



My prediction: many health devices go away in the future

Data transmissions are all around us (all the time)

Intended for info exchange but can be side channel to infer other things

[1] Ma, Yongsen, Gang Zhou, and Shuangquan Wang. "WiFi sensing with channel state information: A survey." *ACM Computing Surveys (CSUR)* 52.3 (2019): 1-36.

[2] Liu, Vincent, et al. "Ambient backscatter: Wireless communication out of thin air." *ACM SIGCOMM Computer Communication Review* 43.4 (2013): 39-50.

Social activities can also leak information

- Military pizza orders
- Cell phone location data can reveal
  - Trips to medical specialists
  - Political affiliation
  - Demonstration/protest participation
  - Murder suspects
  - Associates
- USAF uniform story

https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

Agenda

1. Terminology
2. Listening devices and defenses
3. Side channel attacks
4. Hacking humans
5. Securing hardware from side channels

The US federal government sets a standard for physical security

Federal Information Processing Standards (FIPS) 140-2

Establishes requirements for computer security and interoperability

Level 1

Product grade

Ordinary snap bottle

- Limited testing required
- Algorithm compliance (AES)
- State transition diagrams

Level 2

Tamper evident

Tamper evident caps

Level 1 plus

- Crypto users and roles identified
- Must authenticate user’s role
- Not particularly useful, do not resist tampering

Level 3

Tamper resistant

Tamper resistant caps

Level 2 plus

- Infeasible for practical software unless protected by Level 3+ enclosure
- Additional, expensive testing required
- More user/role identification

Level 4

Tamper responding

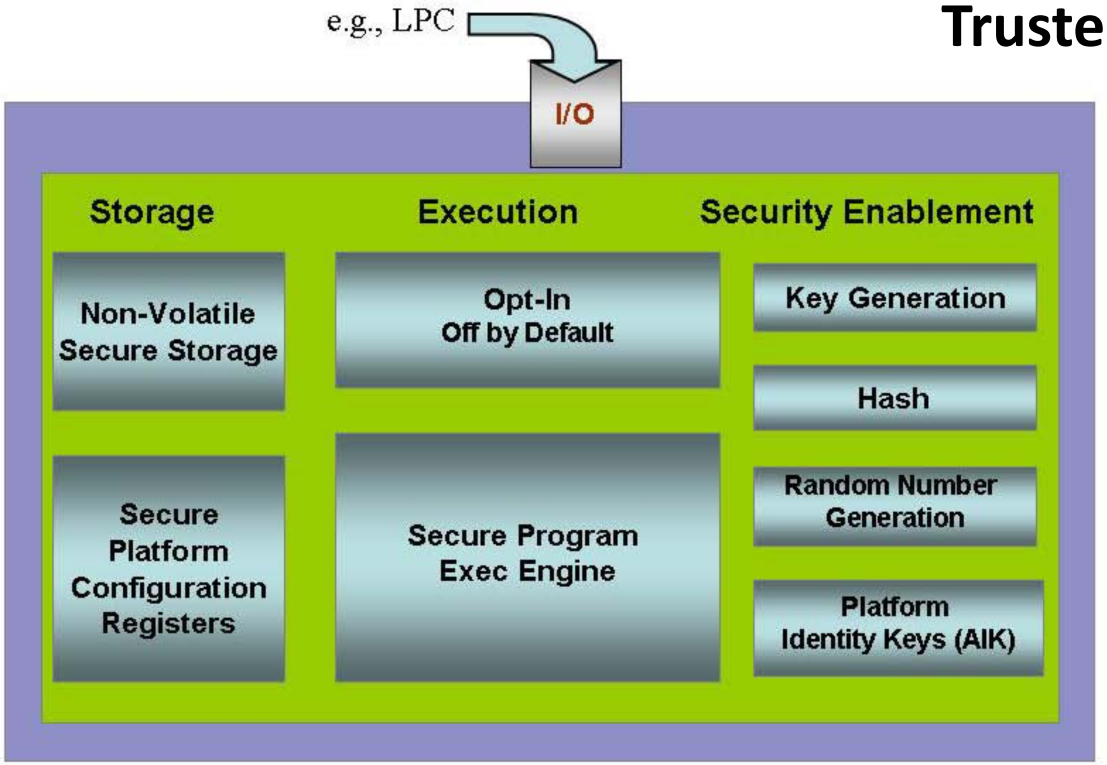
PillSafe protects itself

Level 3 plus

- Protects against physical intrusion, side channels
- Active testing/formal verification
- Few devices exist (most from IBM)
- Can deploy in untrusted environments

Source: Prof. Palmer lecture slides

FIPS-140 Level 4 requires specialized hardware and extensive testing


e.g., LPC
I/O
Storage
Execution
Security Enablement
Non-Volatile Secure Storage
Opt-In Off by Default
Key Generation
Hash
Secure Platform Configuration Registers
Secure Program Exec Engine
Random Number Generation
Platform Identity Keys (AIK)

Trusted Platform Module (TPM)

Separate hardware for crypto responsible for

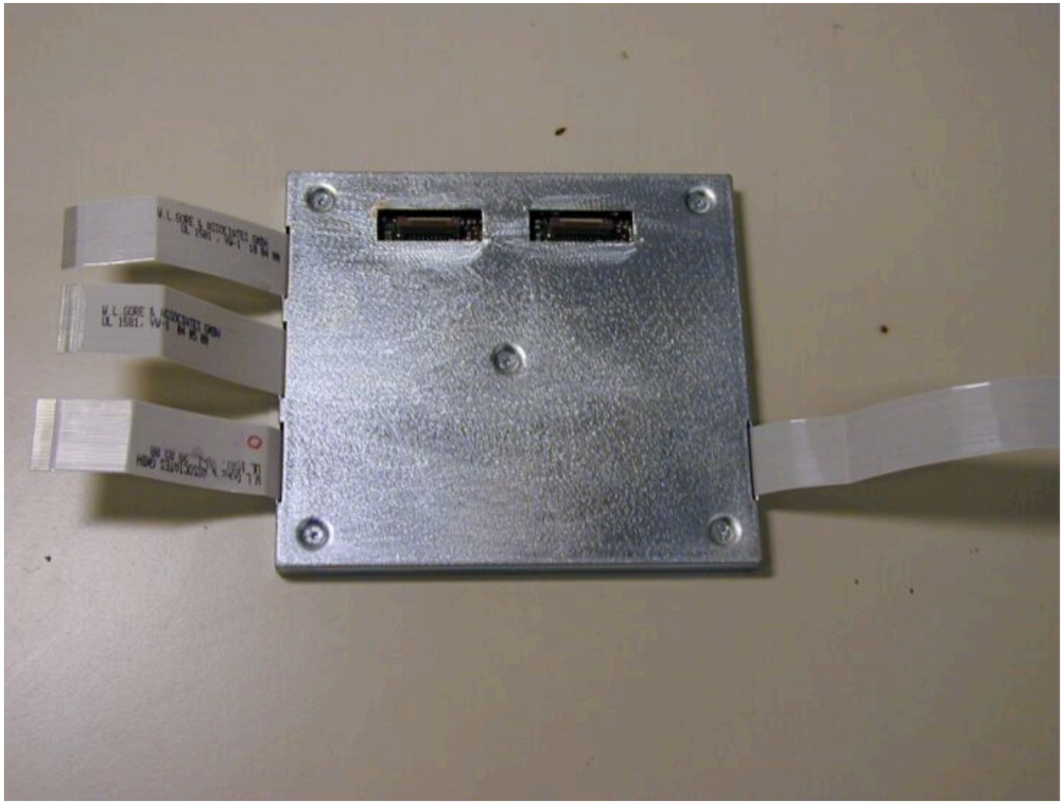
- Random numbers
- Key generation
- Storing platform keys

Used to be a separate chip installed on motherboard

Now baked into motherboard/SOC

Source: Trusted Computing Group

FIPS Level 4 requires specialized hardware and extensive testing


W.L.GORE & ASSOCIATES GMBH
UL 1581, VW-1
W.L.GORE & ASSOCIATES GMBH
UL 1581, VW-1
W.L.GORE & ASSOCIATES GMBH
UL 1581, VW-1

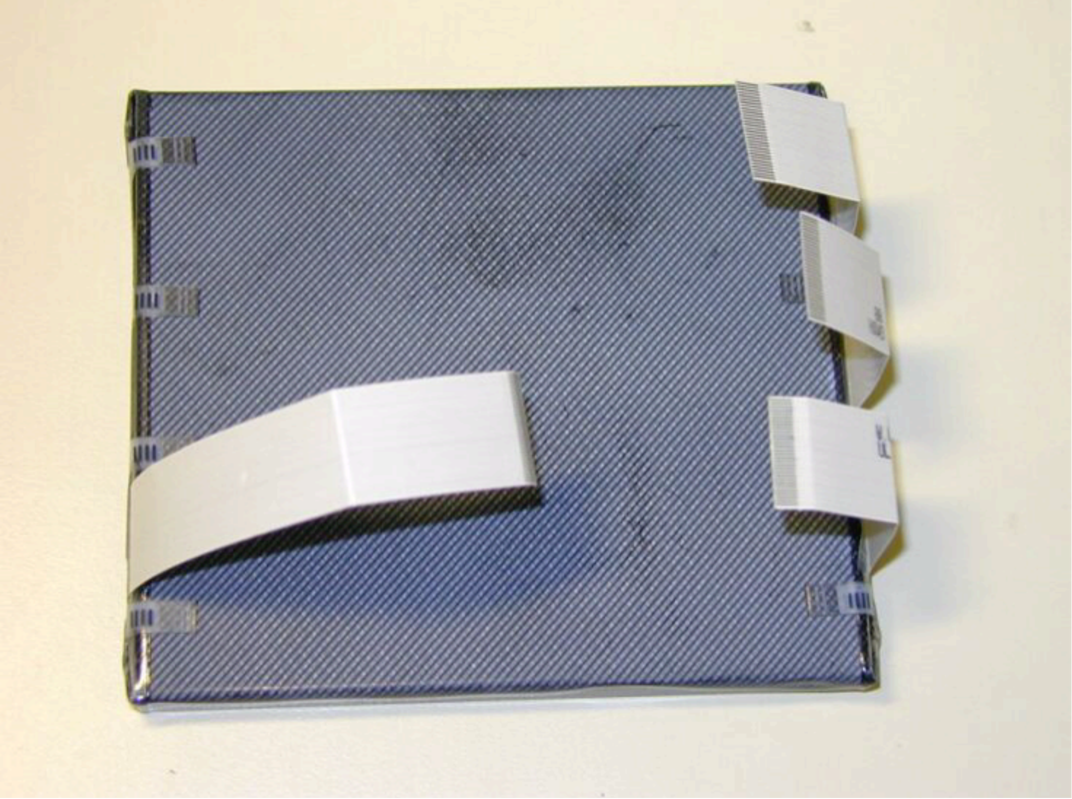
Inner copper enclosure

Resists

- Unintended emissions
- Radio Frequency Interference (RFI)

Source: Prof. Palmer lecture slides

FIPS Level 4 requires specialized hardware and extensive testing

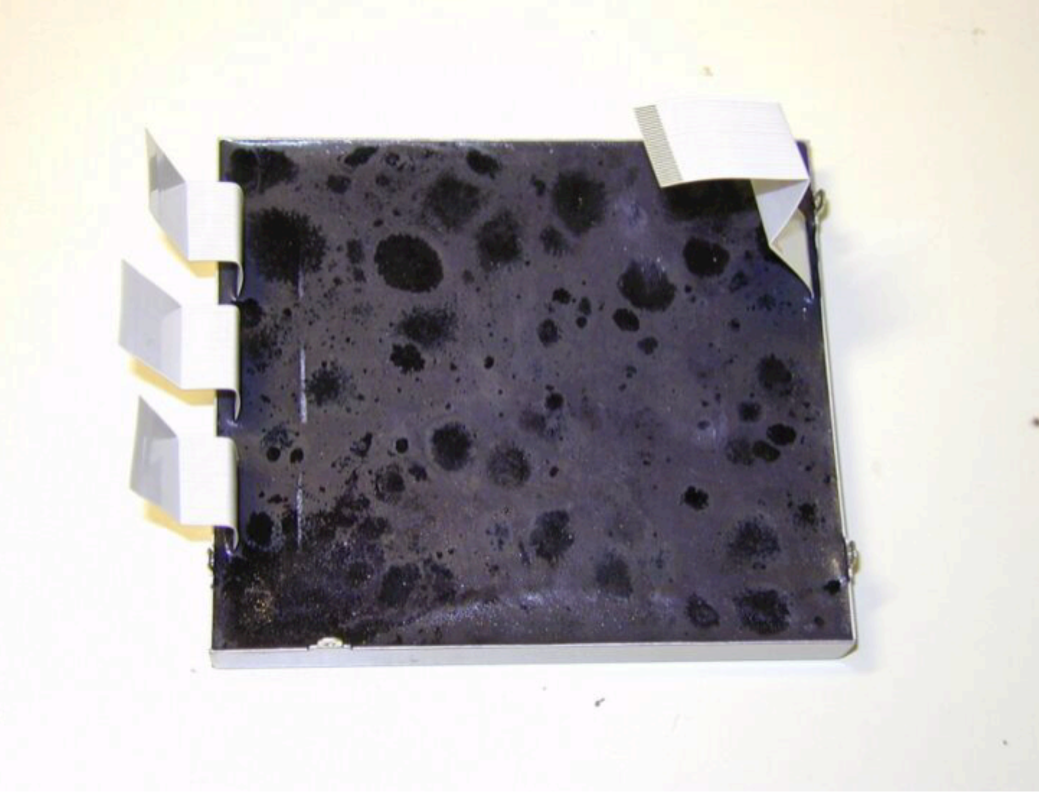


Tamper-sensing mesh/membrane

Detect physical intrusion attempts

Source: Prof. Palmer lecture slides

FIPS Level 4 requires specialized hardware and extensive testing



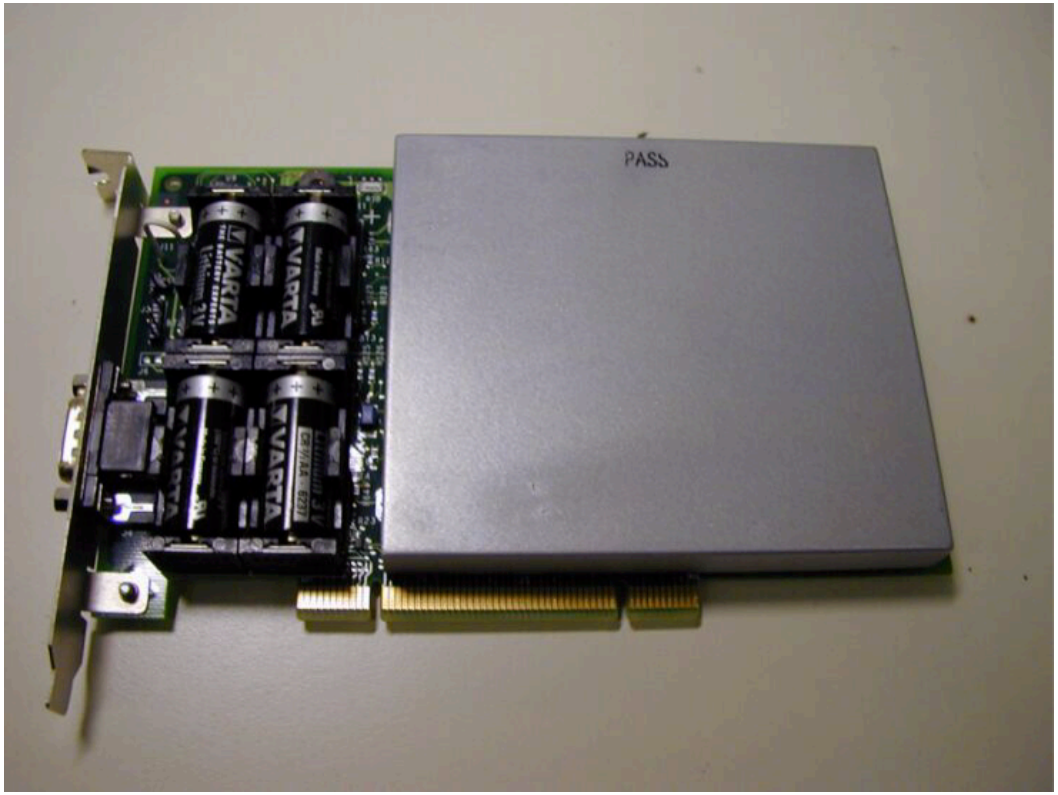
Outer copper shell and potting material

- Environmental protection

Source: Prof. Palmer lecture slides

FIPS Level 4 requires specialized hardware and extensive testing

Completed assembly



FIPS-140 Level 4

Source: Prof. Palmer lecture slides