CIS 700/002 : Special Topics : Physical-Cyber Attacks

Sangdon Park

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

January 27, 2017

Physical-Cyber Attacks

- Definition

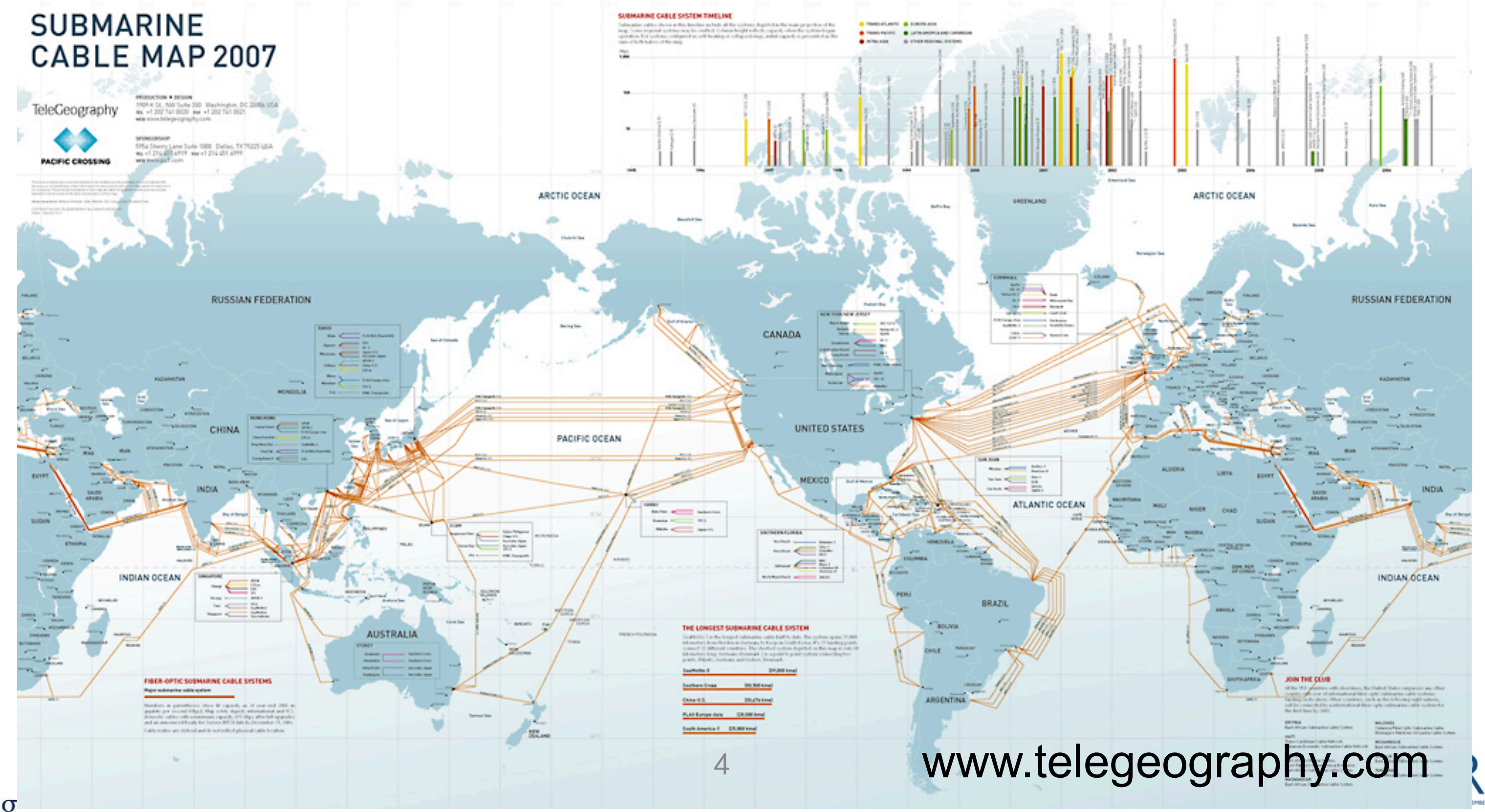
A physical-cyber attack is an attack performed in physical space that adversely affects cyberspace.

CIA

- Confidentiality, Integrity, Availability (CIA)
- CIA are properties of system that a designer wants to implement
  - Authentication
  - Encryption

Breaching Availability

- Direct physical damage
  - Physically damage cyber systems (e.g., network cable)



www.telegeography.com

Breaching Availability:
Direct physical damage

- Incidents and attacks
  - (Incident, 2001) Fire on fiber-optic cables → loss Internet connectivity for 2 days
  - (Incident, 2006) Earthquake near undersea cables → No Internet connection in Hong Kong
  - (Incident, 2008) ship anchors cut network cables → Egypt lost Internet connectivity.
  - (Incident, 2011) Damage a fiber-optic cable → loss Internet connectivity for 5 hours
  - (Attack, WW1) Britain tried to cut German telecommunication cable
  - (Attack, 2013) Divers tried to cut Egypt's main telecommunication provider
  - …

Breaching Availability:
Direct physical damage

- Analysis: finding “areas of failure”
  - Gorman et al., 2004; Neumayer et al., 2011; Agarwal et al., 2011

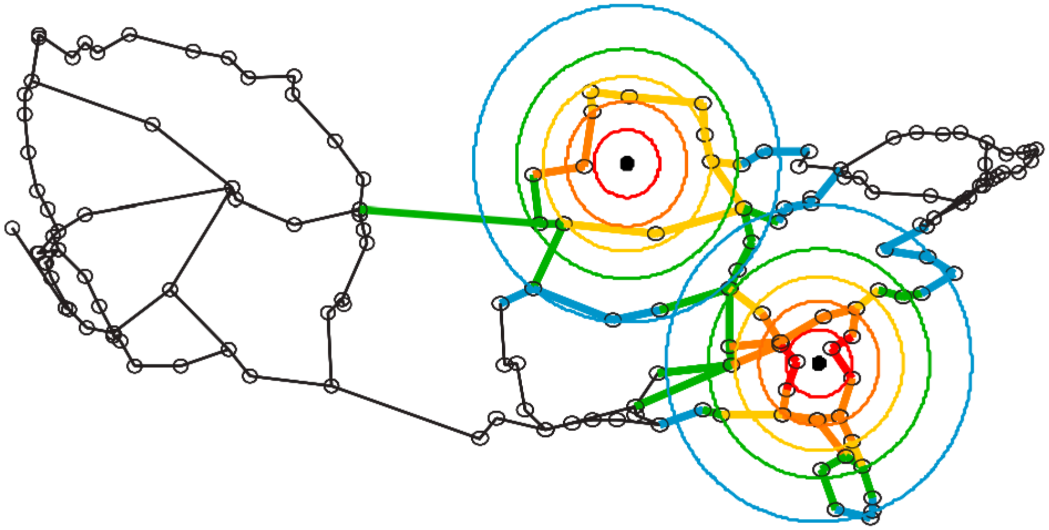


Fig. 1. The fiber backbone operated by a major U.S. network provider [30] and an example of two attacks with probabilistic effects (the link colors represent their failure probabilities).

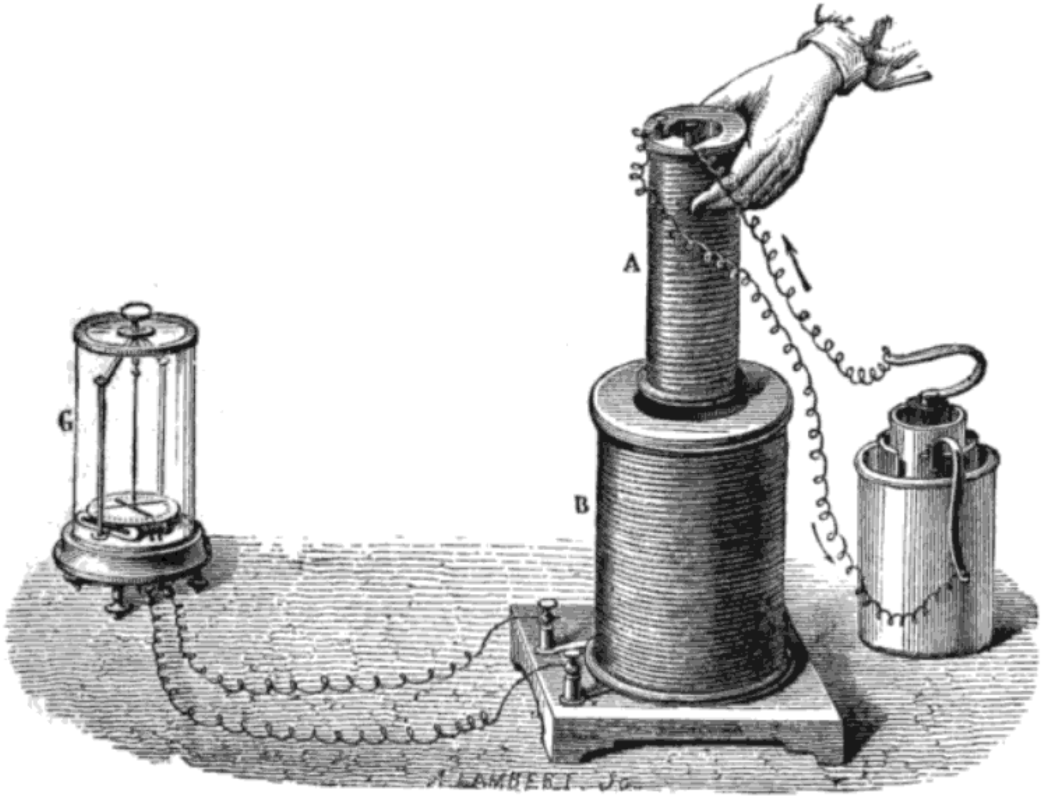
Agarwal, P. K., Efrat, A., Ganjugunte, S., Hay, D., Sankararaman, S., and Zussman, G. The resilience of WDM networks to probabilistic geographical failures. In Proceeding of INFOCOM, IEEE, pp. 1521 1529, April 2011.

Breaching Availability:
Direct physical damage

- Countermeasures
  - Redundant network devices and cables
  - Maximize the network’s resilience by considering geographical distribution

Breaching Availability

- Electromagnetic damage
  - Electromagnetic Pulse (EMP) effect



www.wikipedia.com

Breaching Availability:
Electromagnetic Damage

- Electromagnetic Damage
  - (Incident, 1962) nuclear test → an EMP damages electrical installations in Hawaii
  - (Incident, 1989) a solar flare → a 12-hour electrical power blackout in Quebec, Canada
  - (Attack, 2003) a US Air Force used High Power Microware devices → may be disabled Iraqi satellite TV during Iraq War

Breaching Availability:
Electromagnetic Damage

- Analysis: Report of the Commission, 2004
  - terrorists may use unsophisticated nuclear weapons for an EMP attack on U.S. infrastructure

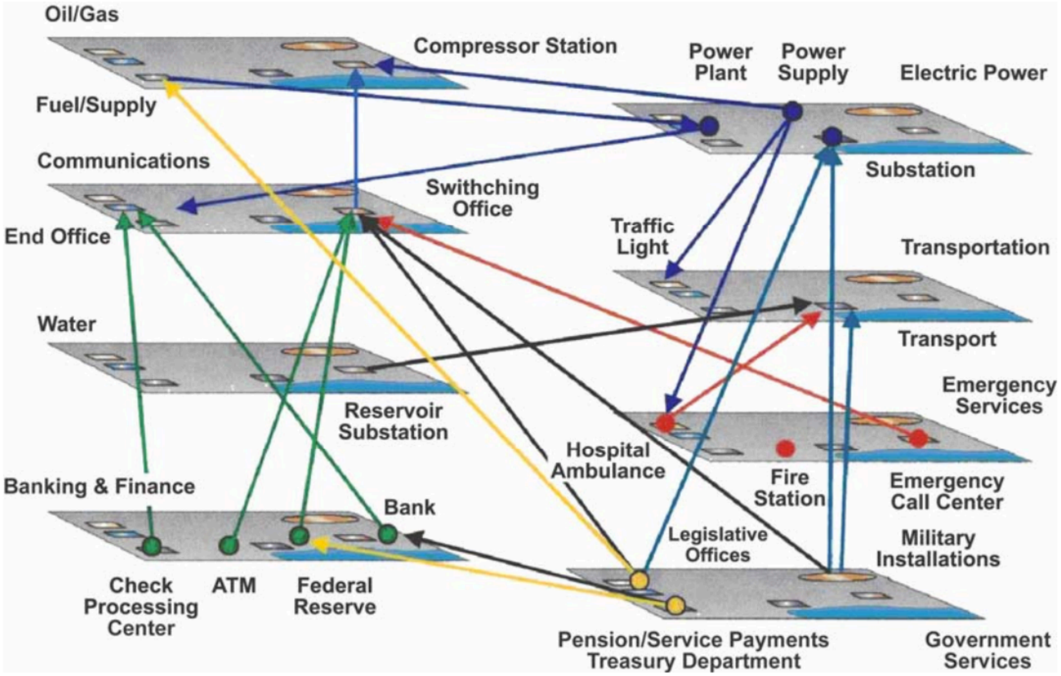
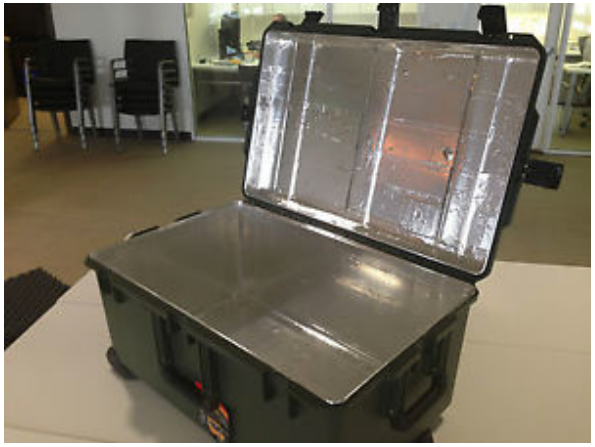


Figure 4. Interdependent Infrastructure Sectors

http://www.empcommission.org/docs/empc_exec_rpt.pdf

Breaching Availability:
Electromagnetic Damage

- Countermeasures
  - Outer EMP protector



  - Copper network cables → Optical fibers

Breaching Integrity

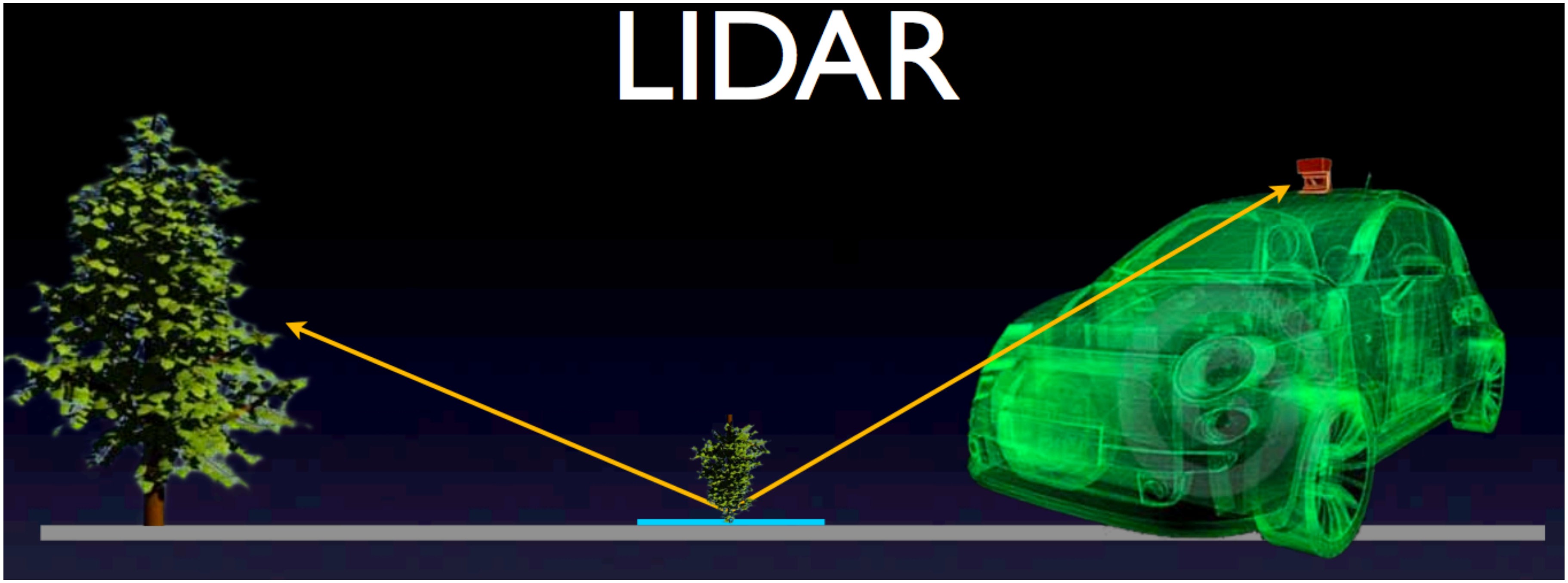
- Physical manipulation of sensor input

LIDAR

Backscatter X-ray

Breaching Integrity:
Sensor Failures

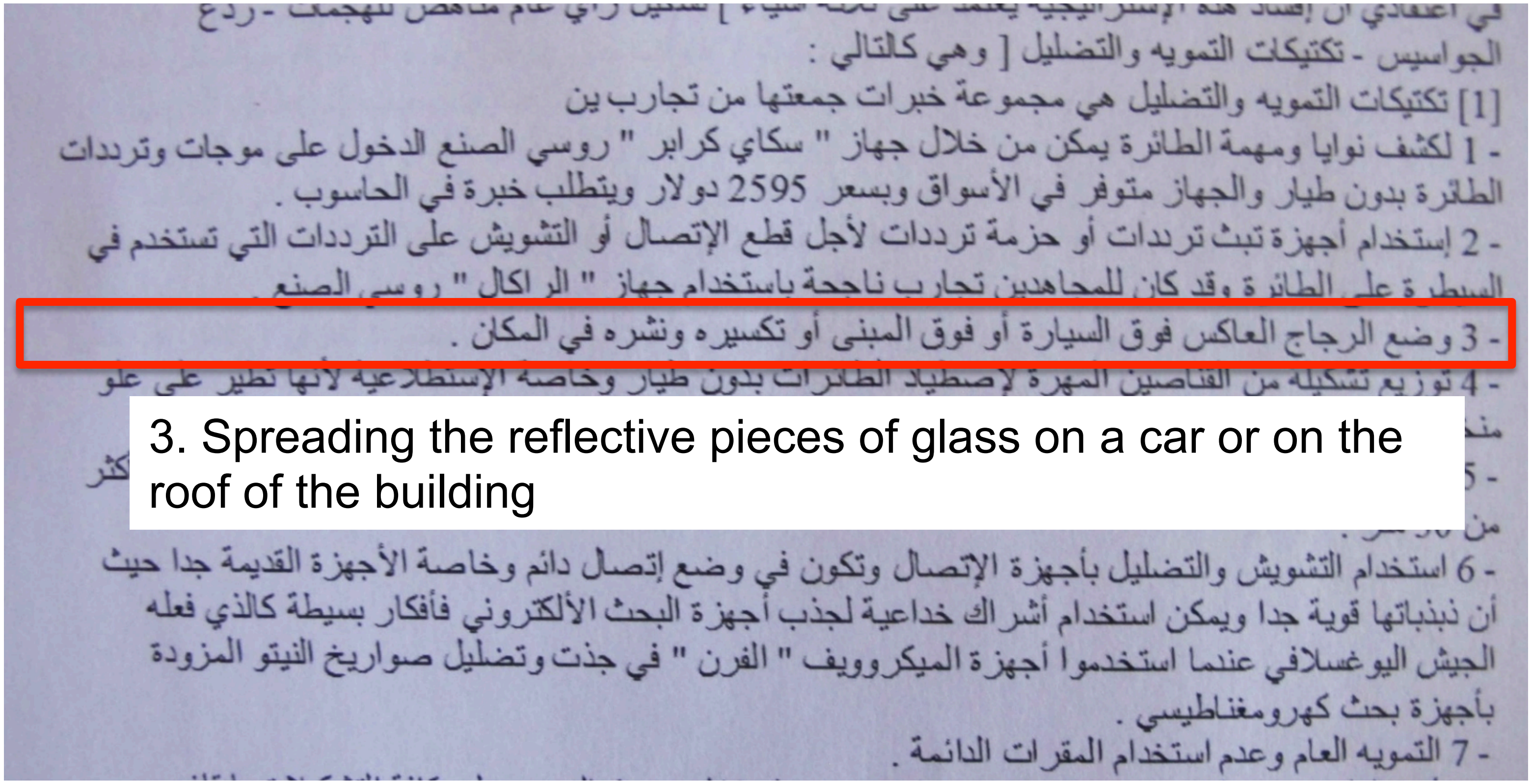
- Attack: Zoz, DEFCON 2013
  - Fool LIDAR sensors



Zoz. Hacking Driverless Vehicles. DEFCON 21, 2013.

Breaching Integrity:
Sensor Failures

- Attack: Al-Qaida Papers - Drones, 2013
  - 22 tips on avoiding UAV missile strikes



في اعتقادي أن إفساد هذه الإستراتيجية يعتمد على ثلاثة أشياء [تشكيل رأي عام مناهض للهجمات - ردع
الجواسيس - تكتيكات التمويه والتضليل] وهي كالتالي :
[1] تكتيكات التمويه والتضليل هي مجموعة خبرات جمعتها من تجارب ين
- 1 لكشف نوايا ومهمة الطائرة يمكن من خلال جهاز " سكاي كرابر " روسي الصنع الدخول على موجات وترددات
الطائرة بدون طيار والجهاز متوفر في الأسواق وبسعر 2595 دولار ويتطلب خبرة في الحاسوب .
- 2 إستخدام أجهزة تبث ترددات أو حزمة ترددات لأجل قطع الإتصال أو التشويش على الترددات التي تستخدم في
السيطرة على الطائرة وقد كان للمجاهدين تجارب ناجحة باستخدام جهاز " الراكال " روسي الصنع .
- 3 وضع الرجاج العاكس فوق السيارة أو فوق المبنى أو تكسيره ونشره في المكان .
- 4 توزيع تشكيله من القناصين المهرة لإصطياد الطائرات بدون طيار وخاصة الإستطلاعية لأنها تطير على علو
منخ
- 5 أكثر
من 50 متر .
- 6 استخدام التشويش والتضليل بأجهزة الإتصال وتكون في وضع إتصال دائم وخاصة الأجهزة القديمة جدا حيث
أن ذبذباتها قوية جدا ويمكن استخدام أشراك خداعية لجذب أجهزة البحث الألكتروني فأفكار بسيطة كالذي فعله
الجيش اليوغسلافي عندما استخدموا أجهزة الميكروويف " الفرن " في جذت وتضليل صواريخ النيتو المزودة
بأجهزة بحث كهرومغناطيسي .
- 7 التمويه العام وعدم استخدام المقرات الدائمة .

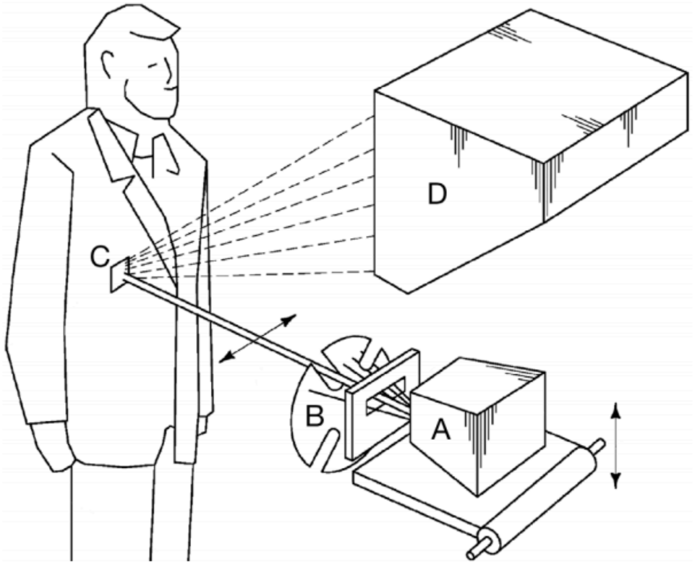
3. Spreading the reflective pieces of glass on a car or on the roof of the building

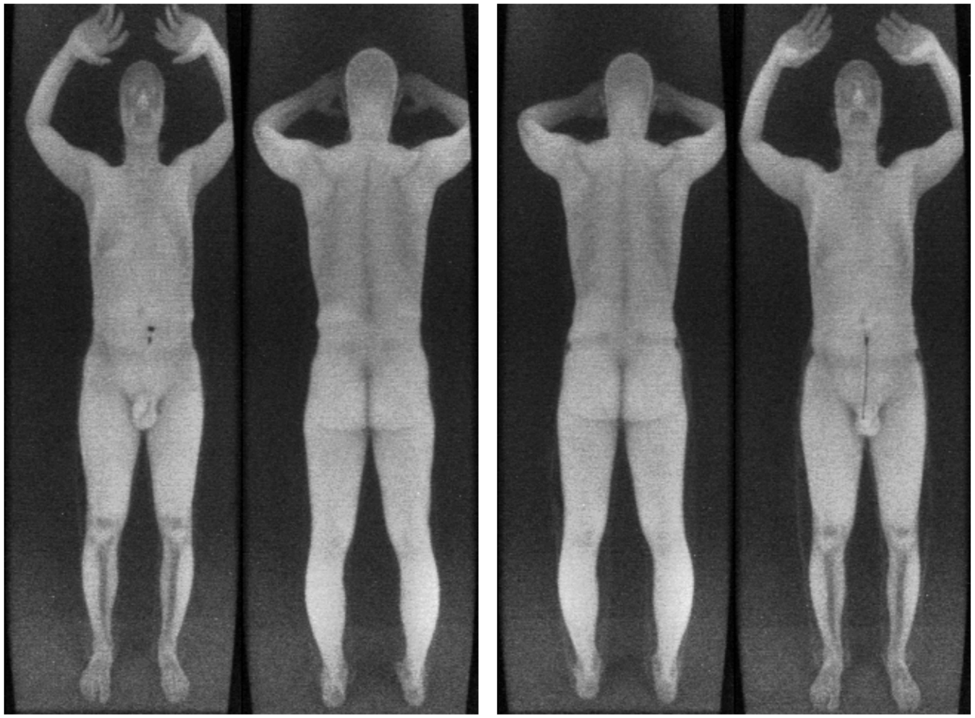
Breaching Integrity:
Sensor Failures

- Countermeasures
  - Infrared radiation
    - Attack: evade detection by hiding behind window glasses
  - Rule-based approaches
    - Set lower and upper limits
  - Learning-based approaches
    - Learn the limits
  - Context-based approaches
    - Temporal context: measurement + forecasted one
    - Redundant sensors

Breaching Integrity:
Sensor Failures

- Attack: Mowery et al., USENIX Security 2014
  - – Fooling backscatter X-ray imagining tech.





(a) Subject with .380 ACP pistol taped above knee.

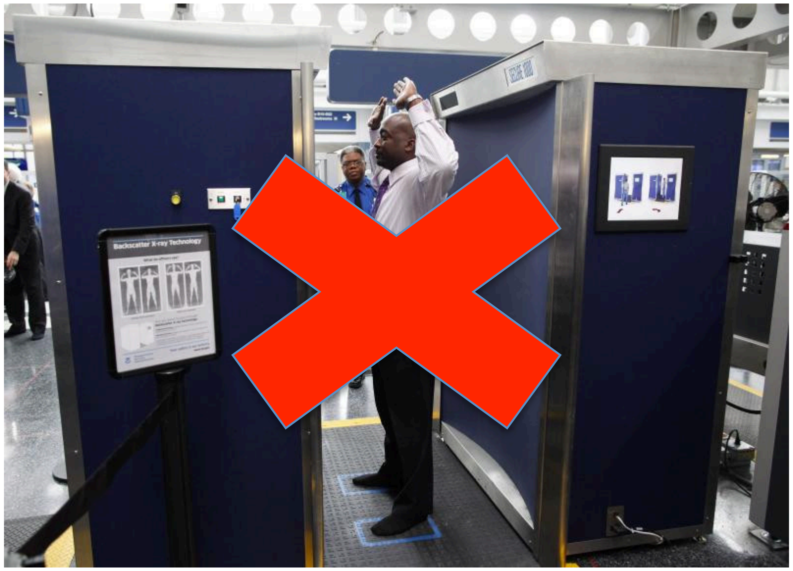
(b) Subject with .380 ACP pistol sewn to pant leg.

Mowery, K., Wustrow, E., Wypych, T., Singleton, C., Comfort, C., Rescorla, E., Checkoway, S., Halderman, J. A., and Shacham, H. (2014). Security analysis of a full-body scanner. In 23rd USENIX Security Symposium, August 20 22, 2014, San Diego, CA.

Breaching Integrity: Sensor Failures

- Countermeasures
  - X-ray: 3D imaging

Backscatter X-ray



Millimeter wave scanner

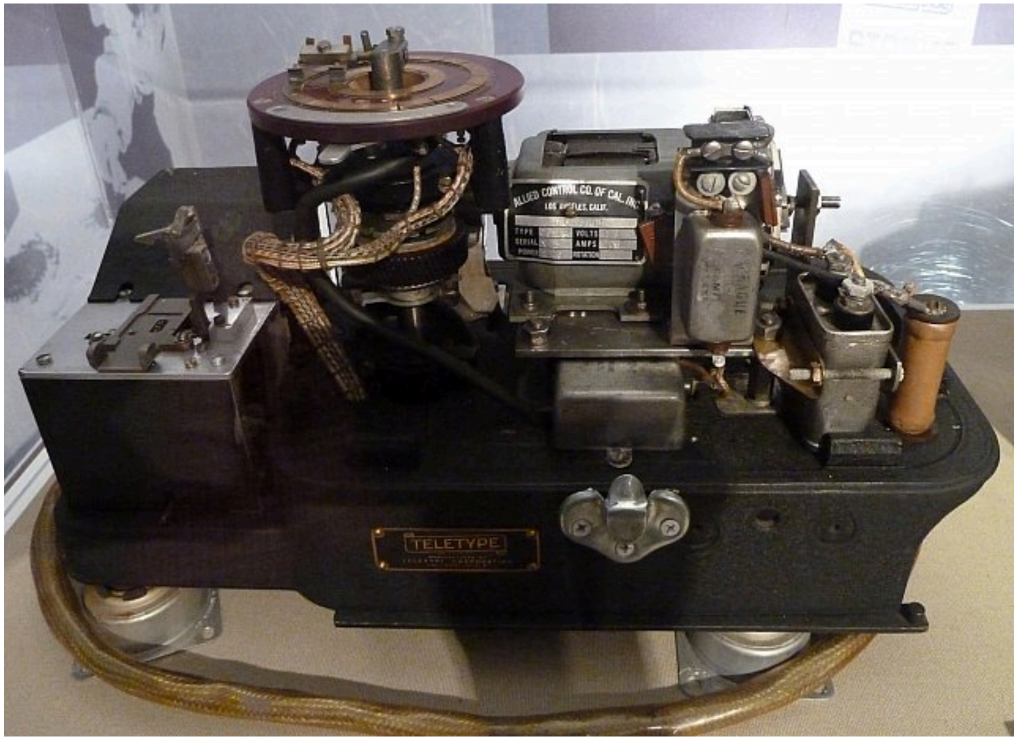
Breaching Confidentiality

- Exploit by-products of computations
  - Heat, electrical signals, electromagnetic radiation, light, sounds, and motion
  - Extract information
- Emsec attack
  - An attack that exploits emanation from systems
  - A.k.a. Side channel attacks

Breaching Confidentiality:
Electromagnetic Emsec Attacks

- Attack: Crypto system (Bell 131-B2), WW2

SIGTOT teletype system



http://ciphermachines.com/otp

Breaching Confidentiality:
Electromagnetic Emsec Attacks

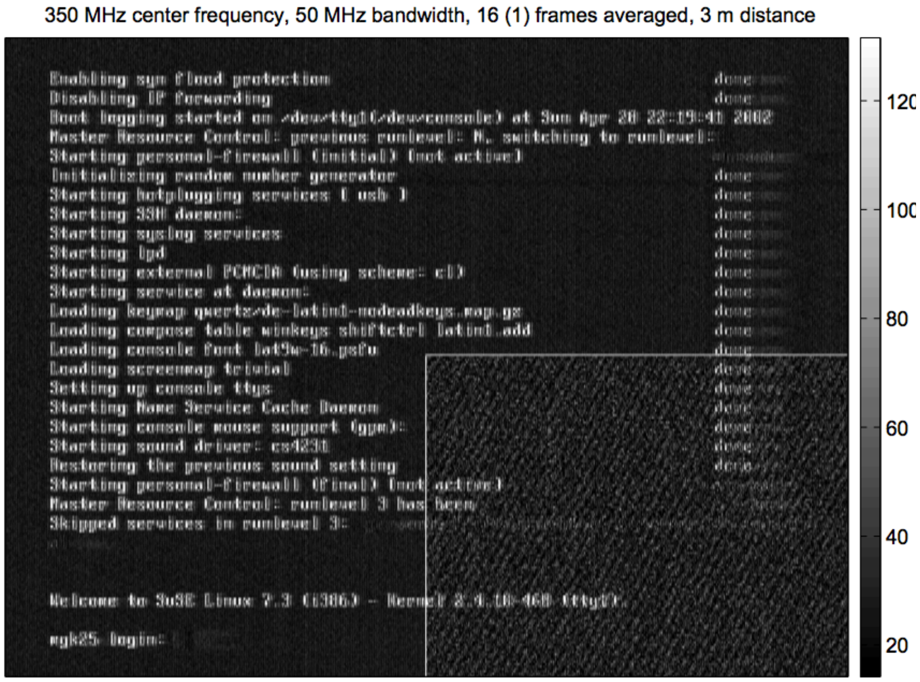
- Attack: Crypto system (Bell 131-B2), WW2
  - electromagnetic from Bell 131-B2 measured by an oscilloscope → decrypt the encrypted texts
    - 75% was recovered
- Countermeasure
  - Use the device only if they had control of an area of 100 feet around them

Breaching Confidentiality:
Electromagnetic Emsec Attacks

- Attack: CRT/LCD display
  - – Van Eck attacks (1985)
    - Electromagnetic from a CRT TV set → reconstruct images displayed on it
  - – Markus Kuhn (2005)
    - Electromagnetic from LCD → reconstruct images

Breaching Confidentiality:
Electromagnetic Emsec Attacks

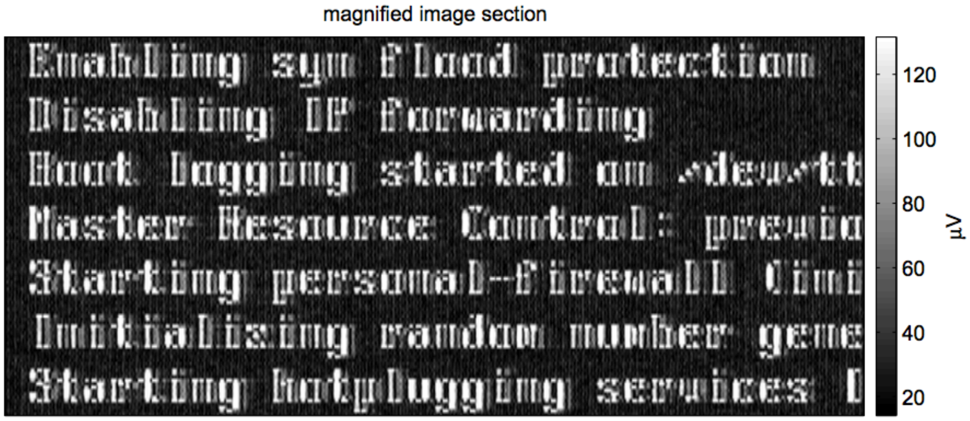
- Attack: Kuhn, LCD monitors, 2005.
  - Electromagnetic from LCD connectors → reconstruct images


350 MHz center frequency, 50 MHz bandwidth, 16 (1) frames averaged, 3 m distance

```
Enabling syn flood protection                                      done
Disabling IP forwarding                                            done
Boot logging started on /dev/tty1(/dev/console) at Sun Apr 28 22:19:41 2002
Master Resource Control: previous runlevel: N, switching to runlevel:
Starting personal-firewall (initial) [not active]
Initializing random number generator                               done
Starting hotplugging services [ usb ]                              done
Starting SSH daemon:                                               done
Starting syslog services                                           done
Starting lpd                                                       done
Starting external PCMCIA (using scheme: c1)                        done
Starting service at daemon:                                        done
Loading keymap qwertz/de-latin1-nodeadkeys.map.gz                  done
Loading compose table winkeys shiftctrl latin1.add                 done
Loading console font lat9w-16.psfu                                 done
Loading screenmap trivial                                          done
Setting up console ttys                                            done
Starting Name Service Cache Daemon                                 done
Starting console mouse support (gpm):                              done
Starting sound driver: cs4236                                      done
Restoring the previous sound setting                               done
Starting personal-firewall (final) [not active]
Master Resource Control: runlevel 3 has been
Skipped services in runlevel 3:


Welcome to SuSE Linux 7.3 (i386) - Kernel 2.4.10-4GB (tty1).

mgk25 login:
```


magnified image section

```
Enabling syn flood protection
Disabling IP forwarding
Boot logging started on /dev/tt
Master Resource Control: previo
Starting personal-firewall (ini
Initializing random number gene
Starting hotplugging services [
```

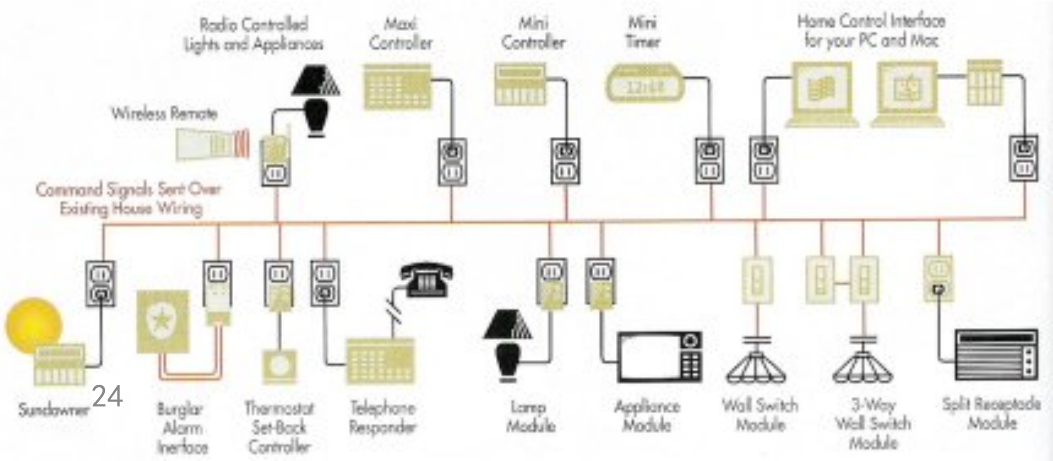
Kuhn, M. G. (2005). Electromagnetic eavesdropping risks of flat-panel displays. In Privacy Enhancing Technologies, Springer Berlin Heidelberg, pp. 88 107, January 2005.

Breaching Confidentiality:
Electromagnetic Emsec Attacks

- Countermeasure
  - Dutch government's regulation
    - Voting equipments should be protected from leaking information up to 5 meters

Breaching Confidentiality: Electromagnetic Emsec Attacks

- Attack: X-10 devices, DEFCON, 2011.
  - X-10 is a protocol for communication among electronic devices through power lines
  - X-10 signals leak through the power grid → pick up by adversaries in the same neighborhood
- Countermeasure
  - encryption



Breaching Confidentiality: Electromagnetic Emsec Attacks

- Attack: crypto system (e.g., smartcards)
  - – Paul Kocher (1999)
    - Power drawn of a smartcard → decrypt
  - – Clark et al. (2013)
    - The power analysis of a computer → identify web pages visited
    - The power drawn fluctuation and web contents are correlated

Breaching Confidentiality:
Electromagnetic Emsec Attacks

- Attack: Kocher et al., CRYPTO, 1999.
  - A smartcard for authentication

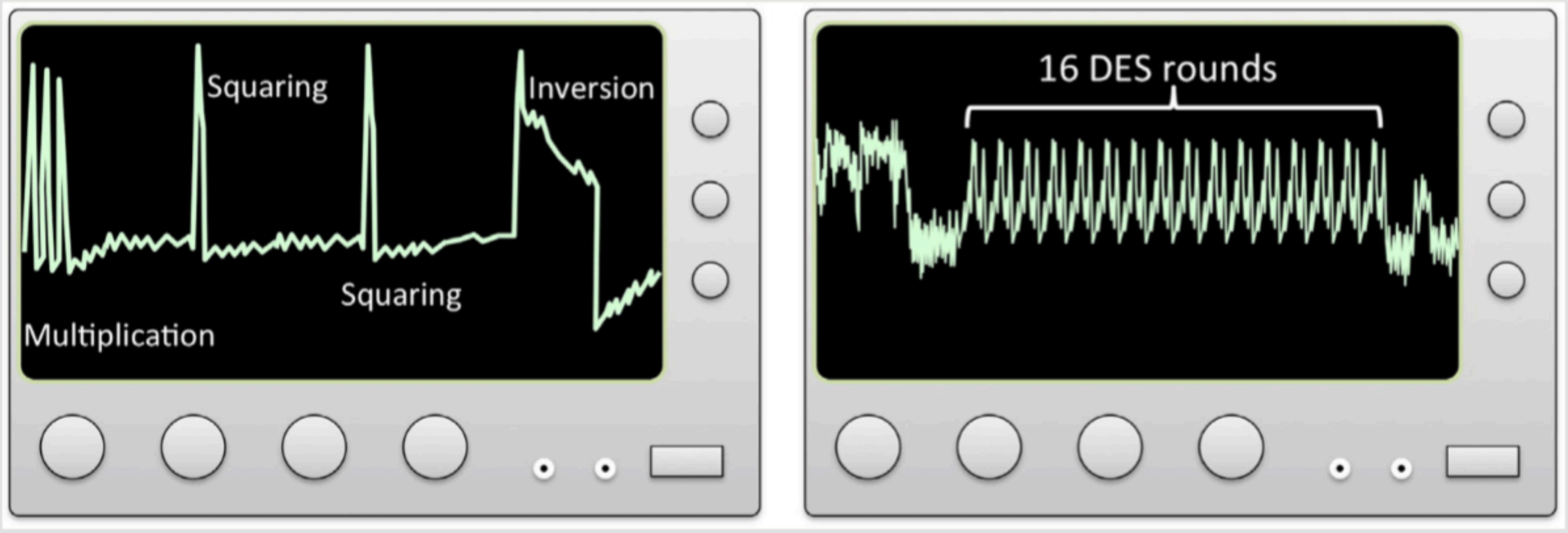


Figure 7.2 The current fluctuates based on the instruction performed by the device’s microprocessor.

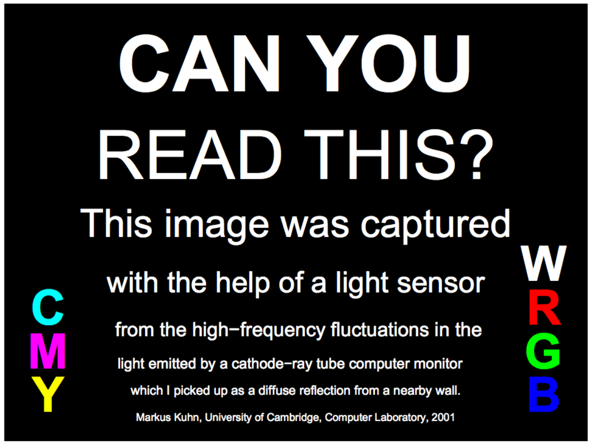
Kocher, P., Jaffe, J., and Jun, B. (1999). Differential power analysis. In Advances in Cryptology CRYPTO’99, Springer Berlin Heidelberg. pp. 388 397, January 1999.

Breaching Confidentiality

- Optical/heat Emsec Attacks
  - Computer monitors
  - Device indicators
  - Human body
  - …

Breaching Confidentiality:
Optical Emsec Attacks

- Attacks
  - Telescope → see monitors
  - (Attack, S&P 2002) Markus Kuhn
    - Photodetector, out-of-sight, CRT → reconstruct images



CAN YOU

READ THIS?

This image was captured

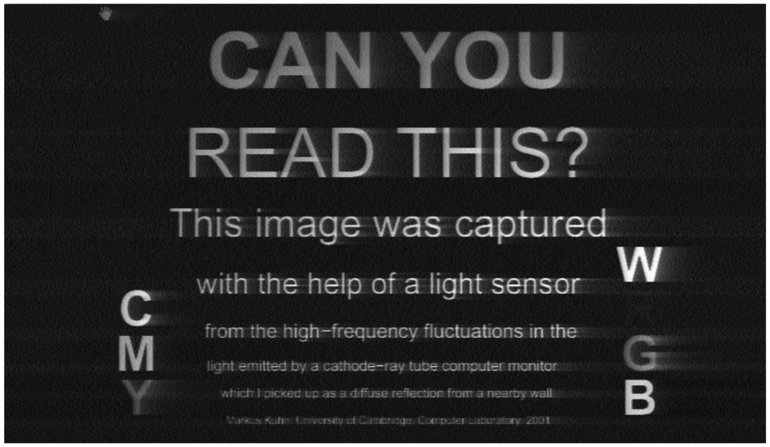
with the help of a light sensor

from the high−frequency fluctuations in the

light emitted by a cathode−ray tube computer monitor

which I picked up as a diffuse reflection from a nearby wall.

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001



CAN YOU

READ THIS?

This image was captured

with the help of a light sensor

from the high−frequency fluctuations in the

light emitted by a cathode−ray tube computer monitor

which I picked up as a diffuse reflection from a nearby wall.

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

- Countermeasure: use LCD

Kuhn, M. G. (2005). Electromagnetic eavesdropping risks of flat-panel displays. In Privacy Enhancing Technologies, Springer Berlin Heidelberg, pp. 88 107, January 2005.

Breaching Confidentiality:
Optical Emsec Attacks

- Attack: Loughry and Umphress, 2002
  - Blink patterns from indicators on modems→ the series of zeros and ones
  - Why? LEDs and data transmission circuits share same power source

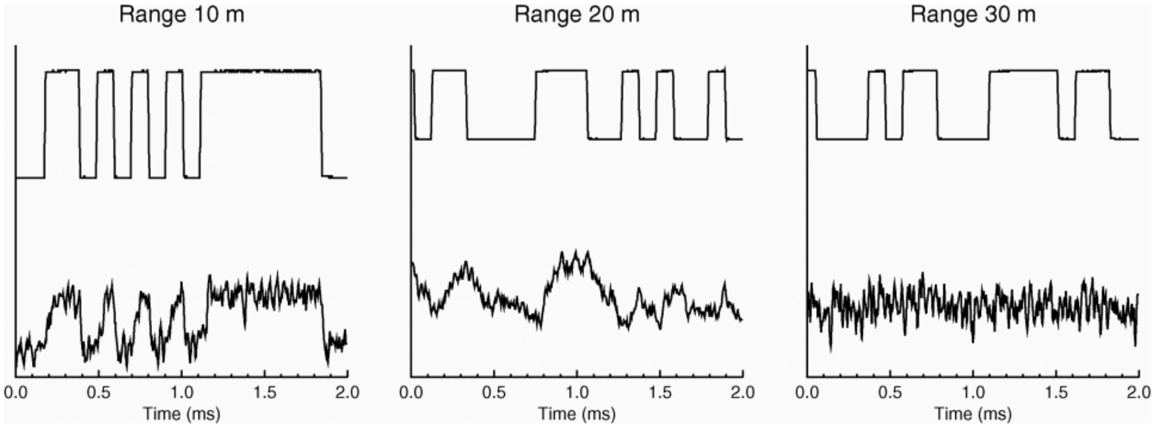


Fig. 4. Degradation of the optical signal with increasing distance from the target. The data rate was 9600 bits/s.

Loughry, J. and Umphress, D. A. (2002). Information leakage from optical emanations. ACM Transactions on Information and System Security (TISSEC), Volume 5, No. 3, pp. 262 289.

Breaching Confidentiality:
Optical Emsec Attacks

- Attack: Mowery et al., 2011.
  - ATM keypads + user's finger + thermal camera → infer keys pressed
  - Why? Thermal residual

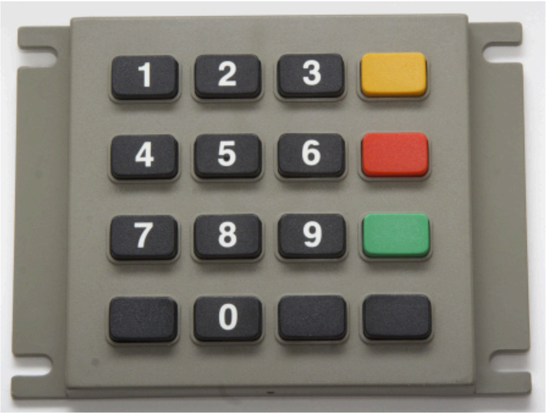
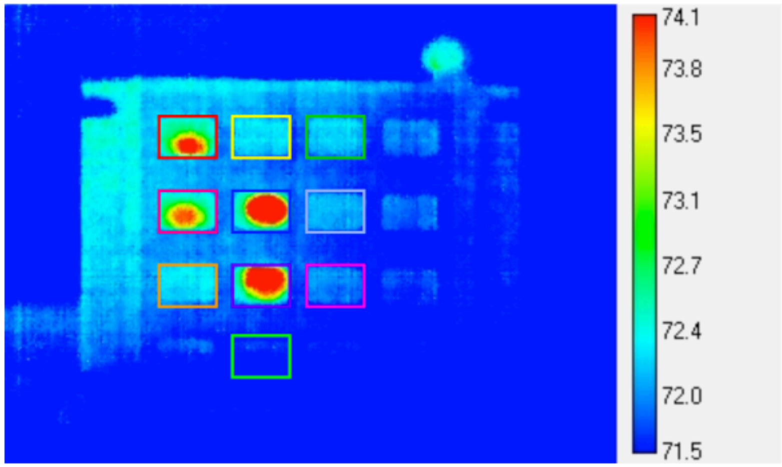


Figure 2: The Diebold plastic ATM keypad with rubber keys, model 19-019062-001M REV1.



- Countermeasures
  - Use metal keypads

Mowery, K., Wustrow, E., Wypych, T., Singleton, C., Comfort, C., Rescorla, E., Checkoway, S., Halderman, J. A., and Shacham, H. (2014). Security analysis of a full-body scanner. In 23rd USENIX Security Symposium, August 20 22, 2014, San Diego, CA.

Breaching Confidentiality

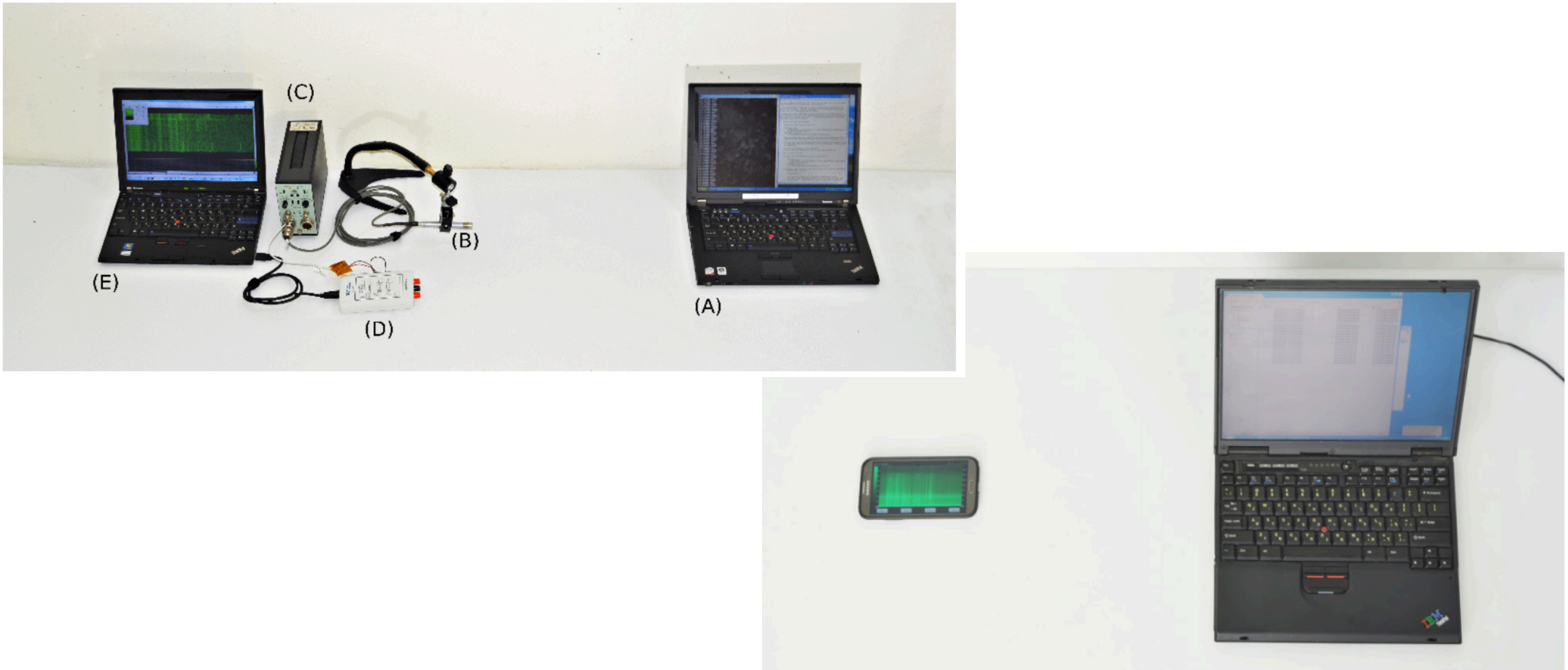
- Acoustic Emsec Attacks
  - Key typing sounds
  - Sounds from devices

Breaching Confidentiality
Acoustic Emsec Attacks

- Attack: British spy, 1956
  - – British collects the sounds from encryption devices → spy for Egyptian embassy
- Attack: Asonov and Agrawal, S&P2004; Zhuang et al., 2005
  - – Sounds from keyboards → infer keys pressed
  - – Recover up to 96% of characters
  - – Why?
    - Keys are not identical
    - Different physical locations of keys

Breaching Confidentiality
Acoustic Emsec Attacks

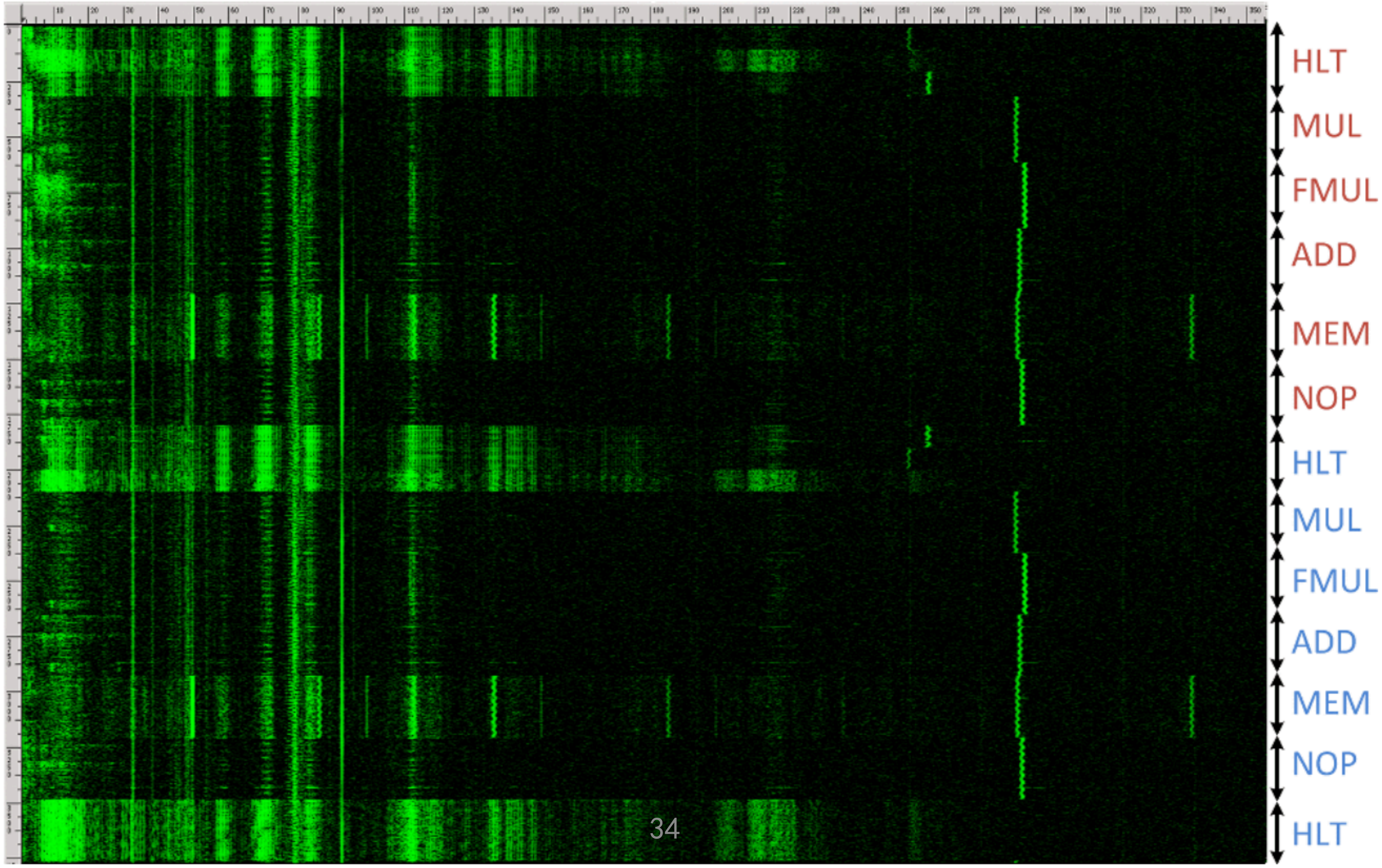
- Attack: Genkin et al. CRYPTO 2014
  - Sounds from computers → extract RSA key



Genkin, Daniel, Adi Shamir, and Eran Tromer. "RSA key extraction via low-bandwidth acoustic cryptanalysis." International Cryptology Conference. Springer Berlin Heidelberg, 2014.

Breaching Confidentiality
Acoustic Emsec Attacks

- Attack: Genkin et al. CRYPTO 2014
  - Why? Correlation between sounds and ops

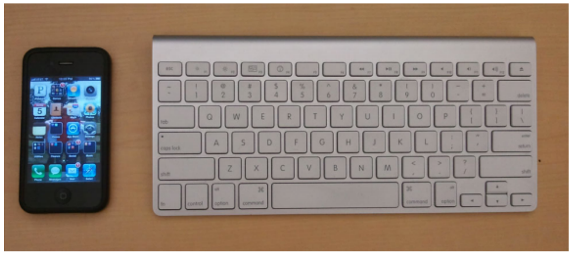


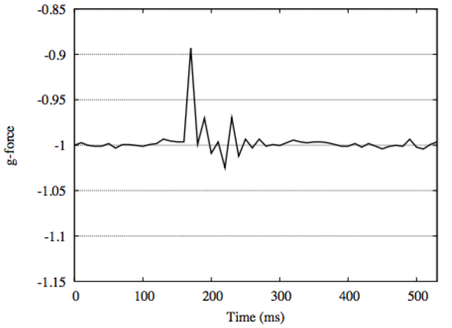
Breaching Confidentiality

- Motion Sensor-based Side Channel Attacks
  - – Gyroscopes in smartphones
  - – Accelerometers in smartphones

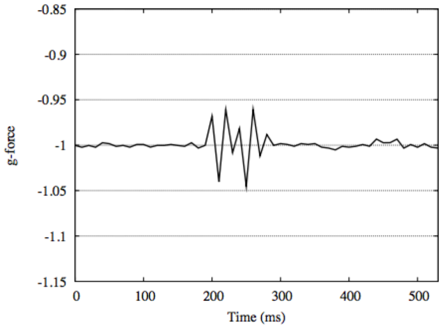
Breaching Confidentiality
Motion Sensor-based Attacks

- Attack: Marquardt et al., CCS 2011
  - Vibration from accelerometers → identify the words typed
  - Why?

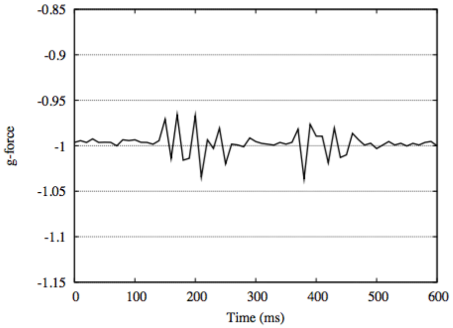




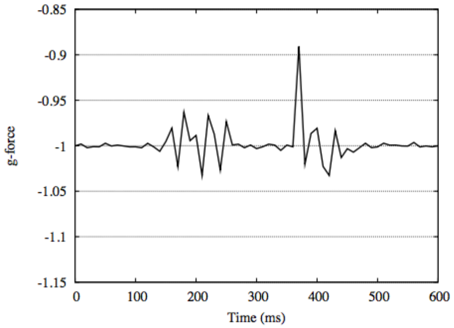
Single character "a"



Single character "l"



Character pair "nm"

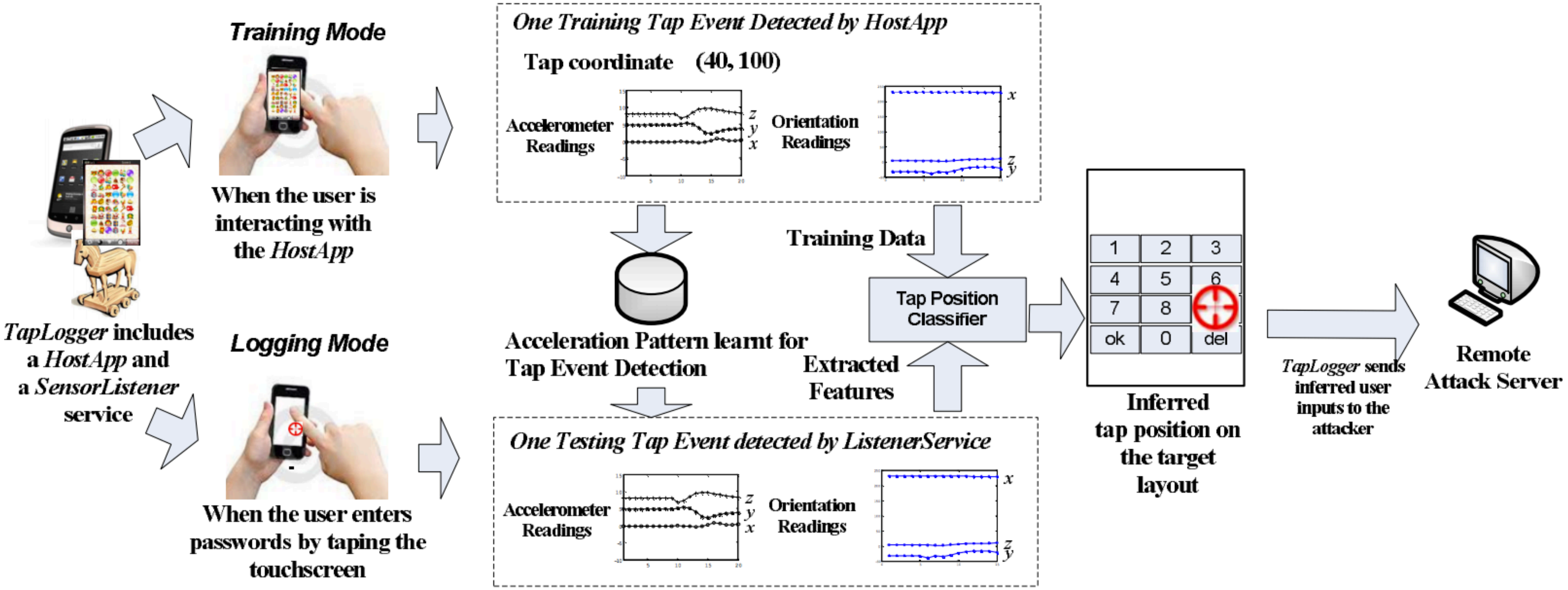


Character pair "pq"

Marquardt, P., Verma, A., Carter, H., and Traynor, P. (2011). (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In Proceedings of the 18th ACM conference on Computer and communications security, ACM, pp. 551 562, October 2011.

Breaching Confidentiality
Motion Sensor-based Attacks

- Apps: TouchLogger, ACCessary, TapLogger
  - Motion sensors → infer the area tapped

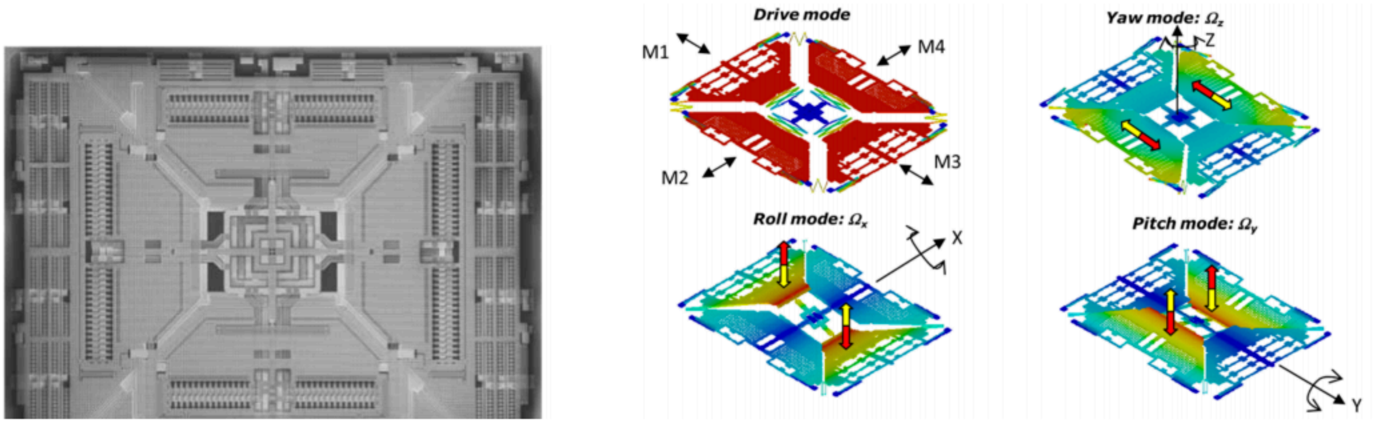

Training Mode
When the user is interacting with the HostApp
TapLogger includes a HostApp and a SensorListener service
Logging Mode
When the user enters passwords by taping the touchscreen
One Training Tap Event Detected by HostApp
Tap coordinate (40, 100)
Accelerometer Readings
z
y
x
Orientation Readings
x
z
y
Training Data
Tap Position Classifier
Acceleration Pattern learnt for Tap Event Detection
Extracted Features
One Testing Tap Event detected by ListenerService
Accelerometer Readings
z
y
x
Orientation Readings
x
z
y
1
2
3
4
5
6
7
8
ok
0
del
Inferred tap position on the target layout
TapLogger sends inferred user inputs to the attacker
Remote Attack Server

Xu, Zhi, Kun Bai, and Sencun Zhu. "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors." Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2012.

Breaching Confidentiality

Motion Sensor-based Attacks

- Attack: Gryophone, USENIX Security 2014.
  - Gyroscopes → identify speakers or words
  - Why? An acoustic signal affects a gyroscopic measurement



(a) MEMS structure

(b) Driving mass movement depending on the angular rate

Figure 1: STMicroelectronics 3-axis gyro design (Taken from [16]. Figure copyright of STMicroelectronics. Used with permission.)

Michalevsky, Y., Boneh, D., and Nakibly, G. (2014). Gyrophone: Recognizing Speech From Gyroscope Signals. In Proceedings of the 23rd USENIX Security Symposium, August 20 22, 2014.

Breaching Confidentiality

- Active Emsec Attacks
  - A system's emanations can be artificially simulated

Breaching Confidentiality

- Active Emsec Attacks
  - Attack, 1996
    - Manipulate the voltage of a device → fault
  - Attack, 2002
    - A virus controls LEDs → reveals user's typing
  - Attack, 2011
    - Cause to generate electromagnetic emanations → transmit signals
  - Attack, 2013
    - Malwares to form acoustical networks → share information

Breaching Confidentiality

- Countermeasures in general
  - “Safety-zone”
  - Shielding for electromagnetic emanations
  - Jamming: generate additional emanations
  - Tempest font (1998)
    - blurring fonts → the info. leak through electromagnetic emanations is reduced
    - A cost-effective software-based solution

PCP Attacks

- Physical-cyber-physical (PCP) attack
  - An EMP attack (physical) → networks with SCADA (cyber) → control a plant (physical)
  - <u>Locate a magnet near an implantable defibrillator (physical) → keep triggering the data transmission (cyber) → exhuast the battary (physical)</u>

CPC Attacks

- Cyber-physical-cyber (CPC) attack
  - Attacks on power grids (cyber) → cut power (physical) → breach network availability (cyber)
  - A virus (cyber) → emanations (physical) → leak information (cyber)
  - (Diao et al., 2014) malware (cyber) → generate voice commands (physical) → initiate actions (cyber)

CPC Attacks

- Attack: Martinovic et al., USENIX Security 2012
  - A malware displays a malicious image (cyber) → triggers the user brain (physical) → brain-computer-interfaces log private information (cyber)

(b) A MindSet device (NeuroSky)

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., and Song, D. (2012). On the feasibility of side-channel attacks with brain-computer interfaces. In Proceedings of the 21st USENIX Security Symposium, pp. 143 158, August 2012.

Take-home message

- Physical-cyber attacks can be distinguishing features of CPS security
- Software-based solutions look attractive as countermeasures