CS 1699
Privacy in the Electronic Society

William Garrison
bill@cs.pitt.edu
6311 Sennott Square
http://cs.pitt.edu/~bill/1699

08: More side-channel attacks

Continuing: Why isn't crypto enough?

Audio side-channels

- CPUs
- Dot-matrix printers
- 3D printers
- Keyboards

More unique side-channels

- Accelerometer
- Reflections

Thought experiment

Consider the shell game

- Place a ball under one of three cups while player watches
- Shuffle the cups
  - Hard mode: Don't let player watch this step
- If done well, player should have no information about which cup contains ball
- If done even better, player should be convinced of a guess that is incorrect
  - (i.e., worse than chance)
- How hard could it be?

Spreitzer et al. proposed a taxonomy of side-channel attacks

Passive vs. active

- Passive simply observes, active participates or manipulates

Physical vs. logical properties

- What available information is exploited?
- Physical: hardware, power, EM
- Logical: software, data-usage statistics, cache, memory footprint

Local vs. vicinity vs. remote attacker

- Local must be in close proximity
- Vicinity can wiretap or eavesdrop on network
- Remote need no co-location

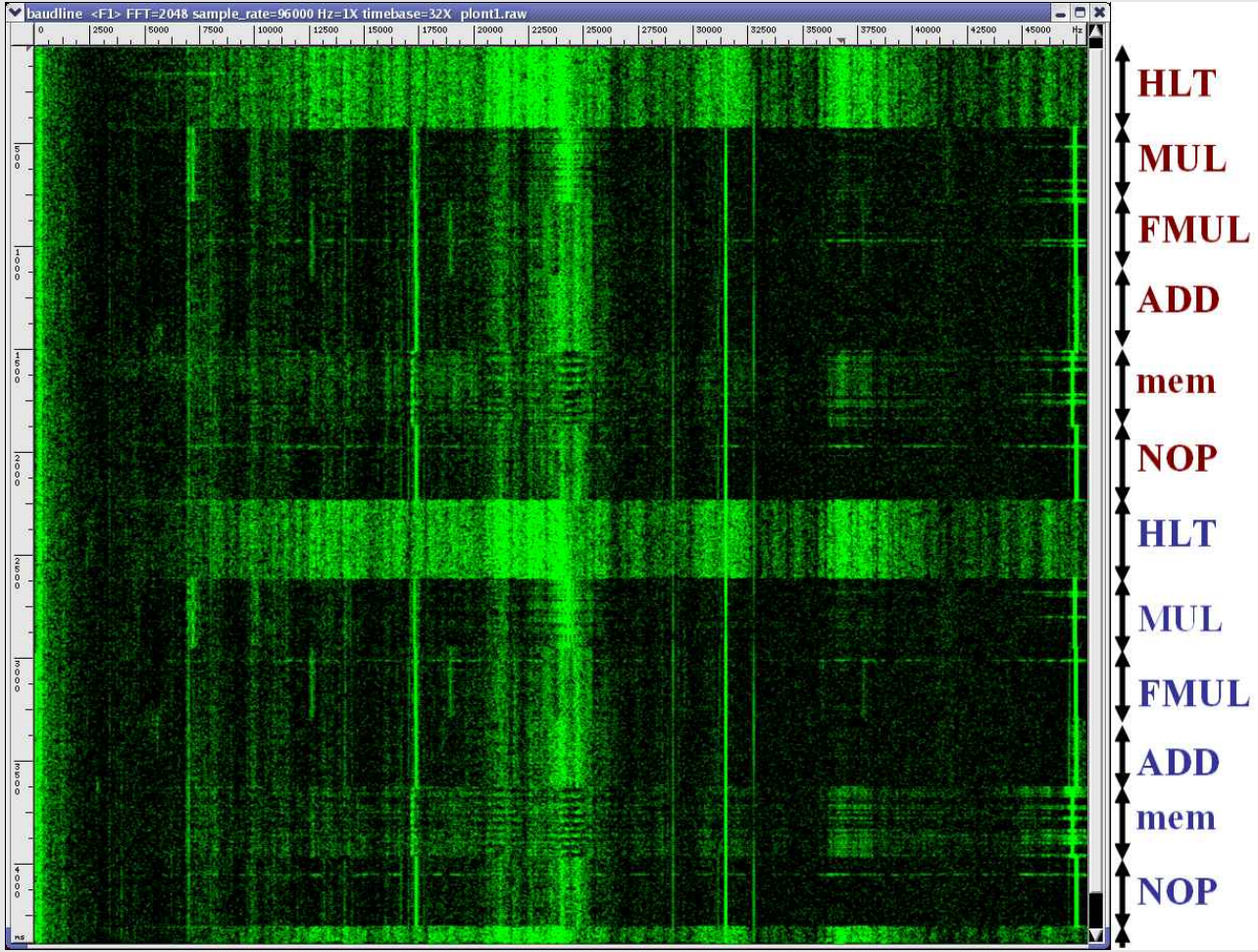
How can audio reveal information?

First, let's think about CPUs

- Electronics vibrate, vibrations create noise
- Different operations cause different vibrations
- Idea: Can we reveal operations from audio?

Adi Shamir and Eran Tromer (2004): Probably

- Easy to distinguish idle from busy
- Can we do more? Will decryption sound different with different keys?
- Can resolution save us? Audio is kHz, CPUs are GHz
  - Think about Kocher's timing attack



Different instructions are recognizable!

Ten years later: Full key recovery

Full key extraction using only low-bandwidth audio

- GnuPG: Well-studied, open-source implementation of PGP
- 4096-bit RSA keys recovered in under one hour
- Smartphone recorded audio from beside computer
  - Or, sensitive microphone 10 meters away
- Specially-crafted RSA ciphertexts that cause cancellations in modexp, causing a recognizable 0-iteration loop
- Attack type? Feasibility?

Live demo on stage!

Also showed the same is possible using the electric potential of the computer chassis

Quick idea behind the attack

Algorithm 1. GnuPG's modular exponentiation (see function mpi_powm in mpi/mpi-pow.c).

Input: Three integers c, d and q in binary representation such that $d = d_n \cdots d_1$.
Output: $m = c^d \mod q$.

```
1:  procedure MODULAR_EXPONENTIATION(c, d, q)
2:      if SIZE_IN_LIMBS(c) > SIZE_IN_LIMBS(q) then
3:          c ← c mod q
4:      m ← 1
5:      for i ← n downto 1 do
6:          m ← m^2                          ▷ Karatsuba or grade-school squaring
7:          if SIZE_IN_LIMBS(m) > SIZE_IN_LIMBS(q) then
8:              m ← m mod q
9:          t ← m · c                        ▷ Karatsuba or grade-school multiplication
10:         if SIZE_IN_LIMBS(t) > SIZE_IN_LIMBS(q) then
11:             t ← t mod q
12:             if d_i = 1 then
13:                 m ← t
14:         return m
15:     end procedure
```

What else can audio give away?

Backes et al. (2010) studied dot matrix printers

- Commonly used in health care environments, banks
  - Some countries require carbon-copy printers for narcotics prescriptions
- Microphone near printer, dictionary attack at the word level
- Training in similar environment, feature selection/extraction, noise reduction, HMMs
- 70% accuracy (72.5% with domain-specific dictionary)

Results were quite robust

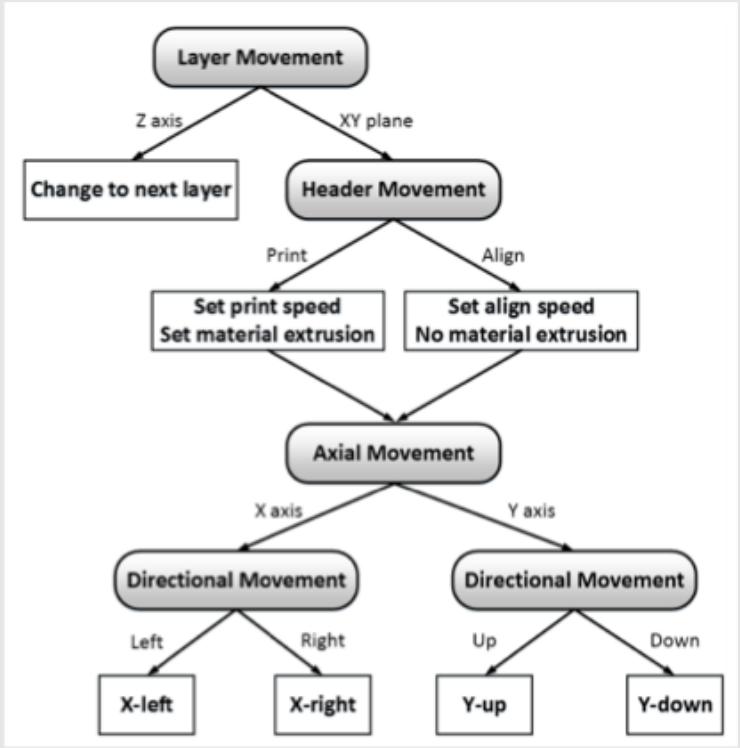
- No special effort to dampen external noise (e.g., traffic)
- Cheap microphones, different printer reduce accuracy by <10%

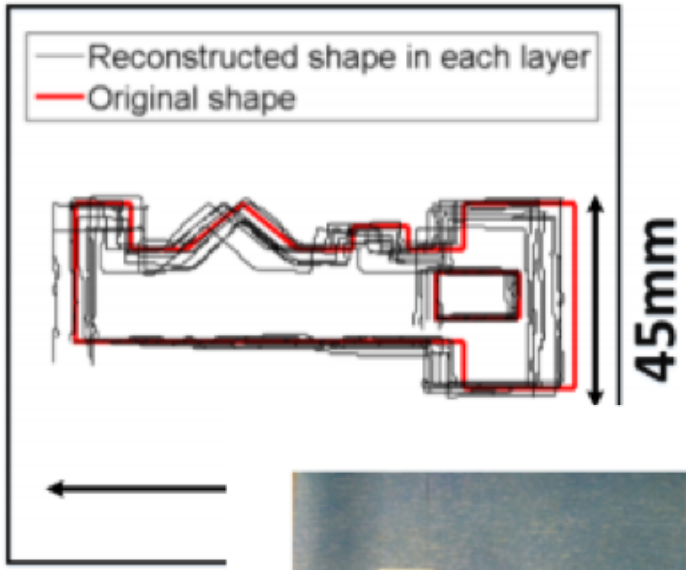
Countermeasures?

Dot matrix printers are old tech; this could never work on newer technology… (?)

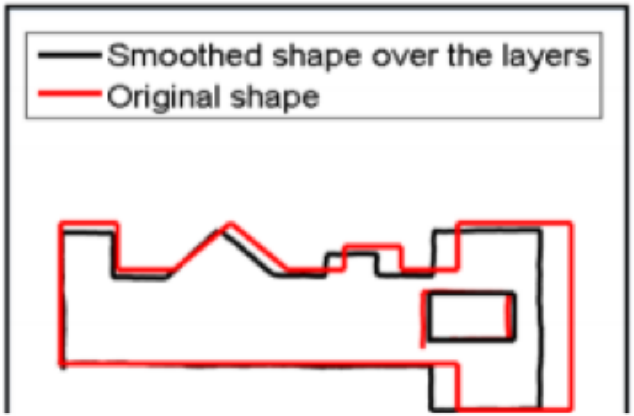
Song et al. (2016) studied similar techniques on 3D printers

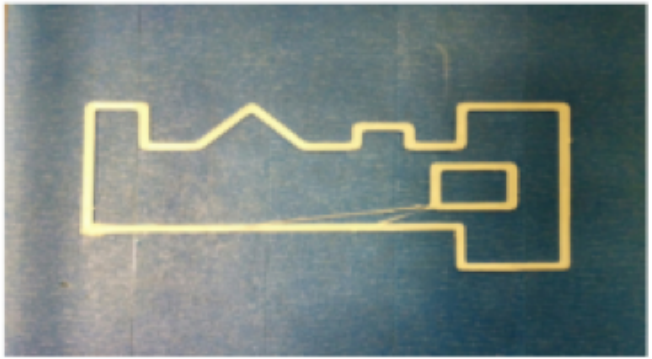
- … aka additive manufacturing
- Recorded using a Nexus 5 smartphone, but audio is lower quality than expensive microphone
- Rotors in printer are moved with electromagnets
- Observe audio and magnetic field!
  - Magnetometer aka compass
- Clever feature extraction, off-the-shelf SVM



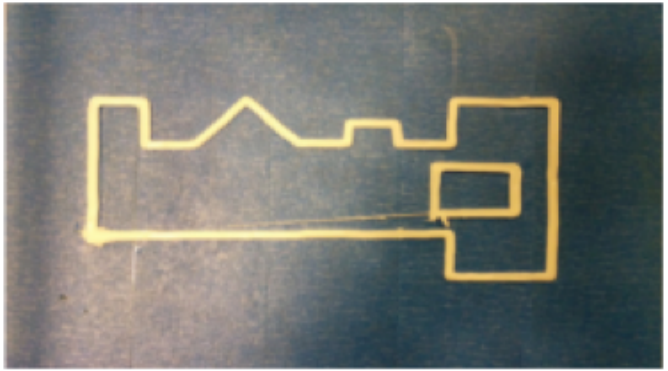


(a) The
the compl
reconstru
layers.





(a) The original designed complex shape.



(b) The replicated object based on the smoothed reconstruction result.

By now, it's probably not surprising that keyboard sounds can identify typed text…

Asonov and Agrawal (2004)

- Two different keys can be distinguished with high accuracy
- …with a neural network and lots of training

Zhuang et al. (2005)

- Unsupervised training, thanks to language characteristics
  - Recall cryptanalysis for single substitution
- 96% of characters identified, passwords identified with high accuracy over multiple trials

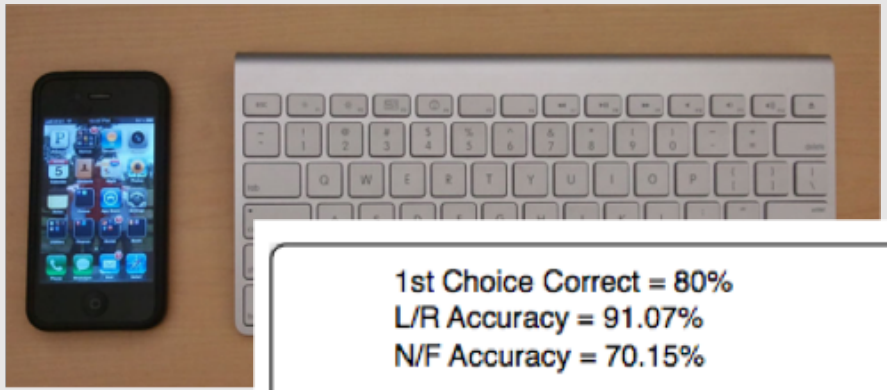
Berger et al. (2006)

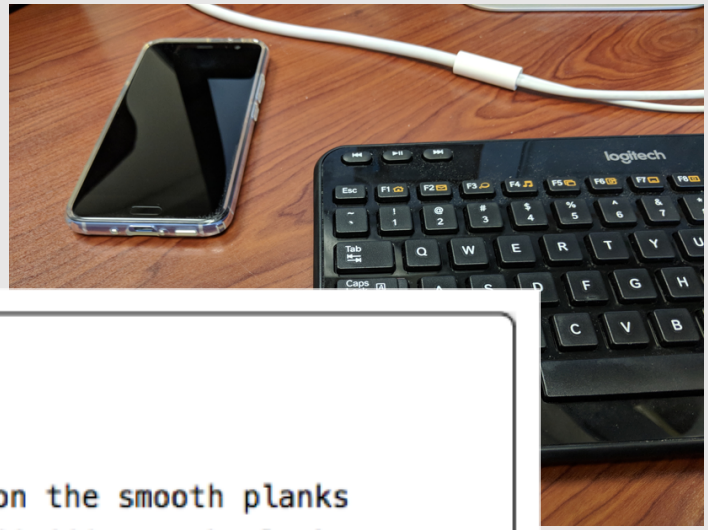
- Dictionary attack, operates on entire words
- Considers word length, press vs. release, etc.
- No need for (even unsupervised) training

But what about other types of side-channel?

(sp)iPhone, Marquardt et al. (2011)

- Idea: Use the accelerometer to detect vibrations
- Why is this particularly dangerous?
  - Consider permissions needed





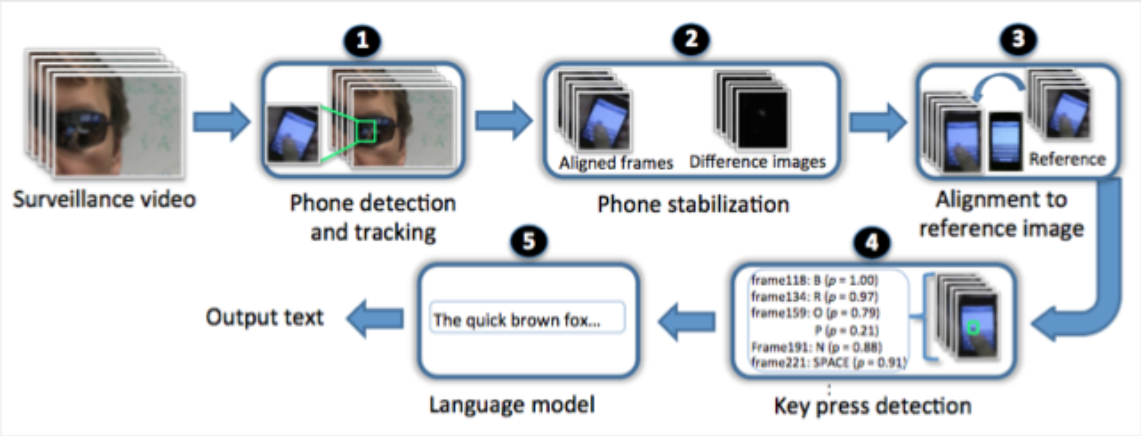
1st Choice Correct = 80%
L/R Accuracy = 91.07%
N/F Accuracy = 70.15%

Typed Text: The birch canoe slid on the smooth planks
Recovered Text: *** punch canoe slid ** *** smooth planks

How else might my typing be eavesdropped upon?

Raguram et al. (2011) used classic over-the-shoulder spying

- … with a twist
- Instead of looking over the victim's shoulder, use reflections



Using 66x104-pixel frames from sunglasses reflection:

- Typed: "to be prepared beforehand for any contingency is the greatest of virtues"
- Hypothesis: "to be prepared beforehand for any contingency [?] the greatest of virtues"

This is terrifying and exhausting, what can we do?

Don’t forget that all electronic systems exist in the real world

Physical access should be protected, even when using other good practices

Don’t implement your own cryptography

Lots of information can be inferred from low-bandwidth channels