Lend Me Your Ear:
Passive Remote Physical Side Channels on PCs

Daniel Genkin, Noam Nissan, Roei Schuster, Eran Tromer

USENIX Security 2022
Software vs. Physical Side Channels

Software

- Attacker
- Victim
- Shared resource
- Power analysis

Physical

- Attacker
- Victim
- Electromagnetic
- Acoustic
Physical side channels

“Passive”
✓ No need to execute code on the target
✓ No need to interact with the target
✓ Only measure target’s emissions

✗ ... But require physical proximity

Today:
! Remote physical side channel, without attack code running on the target

? ... Or do they?
Observation I: laptops can measure themselves

Internal microphone
Observation I: laptops can measure themselves

measurement happens whenever **audio recording** is on
Self measurement
Self measurement

while True:
    [0.8s] MUL
    [0.4s] HLT

0.8 sec
0.4 sec
Observation II: audio is recorded and shared by common apps.
Case study: website identification

Use ConvNets

94% accuracy for 14-way classification

https://twitter.com
VoIP call
Case study: cryptographic key extraction

Libgcrypt signing
VoIP call

WWW
Crypto - ECDSA

- Key Generation
  \[ n, \mathbb{G} \]
  \[ sk: d \leftarrow [1, n - 1] \]
  \[ vk: Q \leftarrow [d] \mathbb{G} \]

- Signing
  \[ z = HASH(m) \]
  \[ k \leftarrow [1, n - 1] \]
  \[ (x, y) = [k] \mathbb{G} \]
  \[ r = x, s = k^{-1}(z + r \cdot d) \]
  signature is \( (r, s) \)

- Verification
  \[ u_1 = -zr^{-1}, u_2 = sr^{-1} \]
  \[ (x, y) = [u_1] \mathbb{G} + [u_2] Q \]
  verify \( x \equiv r \)

- Scalar-by-point multiplication
- Constant-time implementation bug [JSS+’20]
Nonce leaks via timing [JSS+’20]

The bug: skipping leading zeros bits in K
Result: linear dependency between bit length of K and signing time
Signal processing

“valley” duration: signature-time estimate

too noisy to use 😞
Denoising

- Random ECDSA nonces prevent averaging across traces
- Deterministic ECDSA (RFC 6979): nonce derived from key and $m$

Attacker method:
1. Group traces by message
2. Reject outliers
3. Average to denoise
4. Select shortest signatures

Sufficient for lattice attack of Albrecht and Heninger ‘20

Result: key extraction from traces of 20,000 signed messages, each repeated 91 times
Case study: Counter-Strike ("the killer app")

- One of the best-known, successful FPS games
- *E-sport* played competitively, orchestrated league with large awards and millions of viewers
Case study: Counter-Strike ("the killer app")

Victim is hiding behind the corner!
Counter Strike

Key observation: victim machine is rendering attacker’s avatar even when attacker not in field-of-vision
Counter Strike
check out the paper!

Lend Me Your Ear: Passive Remote Physical Side Channels on PCs

Daniel Genkin
Georgia Tech
genkin@gatech.edu

Noam Nissan
Tel Aviv University
noamnissan@post.tau.ac.il

Roei Schuster
Tel Aviv University and Cornell Tech
rs864@cornell.edu

Eran Tromer
Tel Aviv University and Columbia University
tromer@tau.ac.il

Abstract
We show that built-in sensors in commodity PCs, such as microphones, inadvertently capture electromagnetic side-channel leakage from ongoing computation. Moreover, this information is often conveyed by supposedly-benign channels such as applications.

Thus, we channel attack analysis of computers for the duration of the attack. Consequently, physical side-channel attacks on PCs can no longer be excluded from remote-attack threat models.

Questions?