Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone

Andrew Kwong, Wenyuan Xu, Kevin Fu

andrewkwong.org, usslab.org, spqr.eecs.umich.edu, kevinfu@umich.edu

IEEE Symposium on Security and Privacy 2019
Grand Ballroom B -- 1:10Pm
Sensors Intrude on Privacy

• Accelerometers can leak keystrokes [1], gyroscopes can leak voice [2], etc.

• What is the threat from devices never intended to be sensors in the first place?

Accelerometers: [1] Marquardt et al., CCS '11, "(sp)iPhone..."
Hard Drive as a Microphone?

Challenges:

• HDDs are not designed as microphones
• Large quantity of self-noise
• Low signal-to-noise ratio
Contributions

HDD as a microphone

- Used SNReval measurements to evaluate extracted speech quality
- Used Shazam to recognize song recovered through HDD

Mitigations

- Ultrasonic aliasing
- Firmware signatures
Threat Model

Firmware Resident Malware
• Drive firmware can be flashed from software

Flashing:
• MITM attacks (POODLE, LOGJAM, DROWN)
• Any compromise granting root access to a machine

2007

Malware found on new hard drives
The Taipei Times is reporting that around 1,800 new 300GB and 500GB external hard drives manufactured by Maxtor shipped with malware on them. What makes this story even more interesting is that Taiwanese authorities suspected that Chinese authorities were involved.

By Adrian Kingsley-Hughes for Hardware 2.0 | November 13, 2007 -- 14:10 GMT (06:10 PST) | Topic: Security

Andrew Kwong (https://andrewkwong.org)
Apple's T2 security chip disconnects a MacBook's microphone when users close the lid

Feature only available for MacBook Pro and MacBook Air models released in 2018.

By Catalin Cimpanu for Zero Day | October 30, 2018 — 20:00 GMT (03:00 PDT) | Topic: Security

2018

http://stahlke.org/dan/phonemute/

Andrew Kwong (https://andrewkwong.org)
HDD as a microphone

- Head stack assembly actuates the read/write head as the disk spins beneath it
  - Head follows a track
  - can tolerate only tiny errors
- Position Error Signal (PES):
  - Head's offset from center of current track

Andrew Kwong (https://andrewkwong.org)
Head Tracking

• Utilizes Feedback-Control Loop to keep head on track
• Generates PES by reading out magnetic burst from servo sectors
  • Fixed number of servo sectors per track
Similarities to Microphone

Microphone:
- Output measures diaphragm displacement
- Sound waves displace diaphragm

HDD:
- PES measures read/write head displacement
- Sound waves displace write head?

Andrew Kwong (https://andrewkwong.org)


PES approximates microphone output??
Measuring the PES

• Under our threat model, attacker would read it through firmware resident malware
  • Zaddach et al. [3] developed HDD firmware malware

• Proof of concept: suffices to read PES by tapping a debug pin
  • Used serial diagnostic port to output PES

HDD Malware: [3] Zaddach et al., ACSAC '13
Sampling Rate

\[ \text{frequency}_{\text{sampling}} = \text{frequency}_{\text{rotation}} \times \text{num\_servo\_sectors\_per\_track} \]

\[ = 120 \text{ Hz} \times 288 \]

\[ = 34,560 \text{ Hz} \]

Nyquist-Shannon Sampling theorem:
• need sample at 2x the frequency of signal
Audible sound: 20 Hz-20 kHz
• Male fundamental: 85-180 Hz
• Female fundamental: 156-255 Hz
• POTS: 8 kHz

Andrew Kwong (https://andrewkwong.org)
demo
Experimental Setup

Speaker

Hard Drive

Andrew Kwong (https://andrewkwong.org)
Speech Recovery

Must recover speech from PES readings

• PES values approximate instantaneous air pressure readings

• Wrote normalized PES values to WAV file

Noise from:

• Platter eccentricity

• Thermal drift
  • Errors 300X width of track

• turbulence

Andrew Kwong (https://andrewkwong.org)
Signal Analysis

From HDD:

Original:

Cross Correlation:

- Harvard Sentence male speaker with drive enclosed in case and fan powered at max (42W)
Quantitative Measures

PESQ MOS: Perceptual Evaluation of Speech Quality.
- Estimates intelligibility of speech
- Baseline: 1.7dB
- From exposed HDD: 1.4 dB
- Inside external hard drive enclosure: 1.6 dB

Enclosure actually improved results!
- Container presents a larger surface area to oncoming waves
Speech Sample

Transcription:

• Paint the sockets in the wall dull green.
• The child crawled into the dense grass.
• Bribes fail where honest men work.
• Trample the spark, else the flames will spread.
Shazam Recognition

• Played Iron Maiden’s “The Trooper” at hard drive
Success, but ...

Required higher volume (90 dBA), filtering didn’t work

- Noise-gating discrimination errors ruined spectral fingerprint
- Recovered audio extremely poor
- Still enough information to be recognized
Potential Improvements

Multiple Hard drives
- Make use of signal averaging
- White noise averages to zero, signal averages to itself

Use auto-correlation to find repetitions of same utterance, average them
Mitigations

• Ultrasonic masking can protect deployed systems
• Sign firmware!
  • Zaddach et al. [3] didn’t find signatures in use in any HDDs they examined

[3] [HDD Malware, ACSAC '03]
Conclusion

Our research sheds light on overlooked threat of devices that weren’t designed as sensors.

Defenses for already deployed systems are challenging.

Hard drives can approximate crude microphones.

Other Applications: other devices, such as printers; mechanical coupling.

Andrew Kwong (https://andrewkwong.org)
Shipments of hard and solid state disk (HDD/SSD) drives worldwide from 2015 to 2021 (in millions)

<table>
<thead>
<tr>
<th>Year</th>
<th>HDD</th>
<th>SSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>470</td>
<td>105</td>
</tr>
<tr>
<td>2016</td>
<td>425</td>
<td>140</td>
</tr>
<tr>
<td>2017*</td>
<td>395</td>
<td>190</td>
</tr>
<tr>
<td>2018*</td>
<td>370</td>
<td>235</td>
</tr>
<tr>
<td>2019*</td>
<td>360</td>
<td>280</td>
</tr>
<tr>
<td>2020*</td>
<td>350</td>
<td>320</td>
</tr>
<tr>
<td>2021*</td>
<td>330</td>
<td>360</td>
</tr>
</tbody>
</table>

Sources:
Statista estimates; IHS (IHS Markit)
© Statista 2018

Additional Information:
Worldwide; 2016
Granularity

- PES is a 16-bit value
- Granularity: $1/(2^{12})$ of a track
- Only get 8 bits from AMUX pin
  - Chose bits 3-10
Accessibility to MCU

- Proof-of-Concept attack demonstrates what an attacker with firmware-resident malware can do
- First confirmed MCU's access to PES

Andrew Kwong (https://andrewkwong.org)
Frequency Response
Spectral Analysis

- Heavy bands of persistent noise around 8 kHz and 1900 kHz
- Responds well to 2.5 kHz tone
Reading PES
Digital Signal Processing

- Linearly filtering out 8 kHz and 1.9 kHz removes the heaviest bands of noise
- Made use of spectral noise gating for further filtering
  - Find noise thresholds at smaller sub-bands, only pass frequencies above the threshold