Sound Effects

Exploring acoustic cyber-weapons

Matt Wixey
August 2019

All references cited are at the end of the slide deck, available on the DEF CON media server!
Matt Wixey

- Research Lead for the PwC UK Cyber Security practice
- PhD student at UCL
- Previously worked in LEA doing technical R&D
- Black Hat USA, DEF CON, ISF Congress, BruCon, 44Con, BSides, etc
Disclaimer

- Undertaken as part of my PhD research at UCL
- Supervisors & co-authors:
  - Prof. Shane Johnson ([https://www.ucl.ac.uk/jill-dando-institute/about-us/people/academic-staff/shane-johnson](https://www.ucl.ac.uk/jill-dando-institute/about-us/people/academic-staff/shane-johnson))
  - Assoc. Prof. Emiliano De Cristofaro ([https://emilianodc.com/](https://emilianodc.com/))
- The following is presented for educational purposes only
Why this talk?

- DEF CON 25: “See no evil, hear no evil”
  - https://www.youtube.com/watch?v=gFTiD7EnVjU
- Interested in unconventional uses of sound, applied to security
Why should you care?

• Novel class of attack
• Empirical experimentation
• Increasing attack surface
• Building on previous work on:
  – Malware and physical harm
  – Acoustic harm
  – Digital/physical crossover attacks
Background
Malware and physical harm – some examples

- Digital/physical malware: Stuxnet, Mirai, Mirksy et al, 2019
- Malware inadvertently affecting physical kit: Conficker, Wannacry
- Medical implant vulnerabilities
  - Halperin et al, 2008; Rushanan et al, 2014; Williams & Woodward, 2015; Rios & Butts 2019
- Vehicle vulnerabilities (Othmane et al, 2013; Valasek & Miller 2015)
Malware and harm - effects

• Typically, there’s an indirect relationship

• What about malware that *directly* affects humans?

  – Poulsen, 2008; Oluwafemi et al, 2013; Ronen & Shamir, 2016; Rios & Butts, 2017
Sound as a weapon

Continuous dB

85 dB
88 dB
91 dB
94 dB
97 dB
100 dB
103 dB
106 dB
109 dB
112 dB
115 dB

Permissible Exposure Time

8 Hours
4 hours
2 hours
1 hour
30 minutes
15 minutes
7.5 minutes
3.75 minutes (< 4 min)
1.875 minutes (< 2 min)
.9375 min (~ 1 min)
.46875 min (~ 30 sec)

http://dangerousdecibels.org/education/information-center/decibel-exposure-time-guidelines/

Sound Effects: Exploring acoustic cyber-weapons

PwC
Sound Effects: Exploring acoustic cyber-weapons


Background

- Floor fan
- Lawn mower
- Chainsaw
- Jet taking off
- Windows XP start-up sound

<table>
<thead>
<tr>
<th>dB Level</th>
<th>Sound Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 dB</td>
<td>Threshold of normal hearing</td>
</tr>
<tr>
<td>10 dB</td>
<td>Normal sound</td>
</tr>
<tr>
<td>89 dB</td>
<td>Sound becomes irritating</td>
</tr>
<tr>
<td>90 dB</td>
<td>Can damage hearing if prolonged</td>
</tr>
<tr>
<td>100 dB</td>
<td>Eyes begin to twitch</td>
</tr>
<tr>
<td>110 dB</td>
<td>Vision impaired</td>
</tr>
<tr>
<td>130 dB</td>
<td>Lose ability to understand speech</td>
</tr>
<tr>
<td>140 dB</td>
<td>Can feel pain</td>
</tr>
<tr>
<td>150 dB</td>
<td>Feel nauseous</td>
</tr>
<tr>
<td>166 dB</td>
<td>Difficulty breathing</td>
</tr>
<tr>
<td>177 dB</td>
<td>Abnormal respiration</td>
</tr>
<tr>
<td>188 dB</td>
<td>Lungs collapse and death imminent</td>
</tr>
<tr>
<td>190 dB</td>
<td>Upper range of LRAD acoustic generator</td>
</tr>
<tr>
<td>194 dB</td>
<td>Bones shatter and internal organs rupture</td>
</tr>
<tr>
<td>200 dB</td>
<td>Instant death</td>
</tr>
</tbody>
</table>

Acoustics and harm
What can we hear?

- Ultrasound & infrasound: above/below human hearing threshold
- Traditionally 20Hz – 20kHz (Durrant & Lovrinic, 1995)
  - This is a misconception: thresholds vary widely
  - This talk:
    - High-frequency noise (HFN): 17 - 21kHz
    - Low-frequency noise (LFN): 60 - 100Hz
Imperceptibility

• Basing a definition on a lack of a property is problematic
  – Duck & Leighton, 2018
• Perceptibility not a case of arbitrary cut-off points
• Mechanisms not fully understood (Koch, 2017)
• Significant variation in thresholds
  – Leighton, 2018; Leventhall et al, 2003; van Wieringen & Glorieux, 2018
Imperceptibility

- Depends on volume, background noise, previous exposure, etc
- Sound may be perceived as vibration (Leventhall et al, 2003)
  - Or audible ‘subharmonics’ (Ashihara et al, 2006; Howard et al, 2005)
- Likelihood declines non-linearly (Muhlhans, 2017)
- For HFN, threshold increases with age
  - Macca et al, 2015; van Wierengen & Glorieux, 2018
Adverse physiological effects - HFN

- Susceptibility differs (Leighton, 2016; Qibai & Shi, 2004)
- No reports of high frequencies causing hearing loss, but:
  - Adverse effects on hearing (Duck & Leighton, 2018)
  - Temporary threshold shifts (Acton and Carson, 1967)
  - Neurasthenia, cardiac neurosis, hypotension, bradycardia, functional changes in CV and CNS (Smagowska & Pawlaczyk-Łuszczyńska, 2013)
Adverse psychological effects - HFN

• Nausea, fatigue, headaches
  – Duck & Leighton, 2018; Howard et al, 2005; Von Gierke & Nixon, 1992
• Tinnitus and ear pain (Chopra et al, 2016; Fletcher et al, 2018a)
• Irritation (Ueda et al, 2014)
• Somnolence, dizziness, palpitations, decreased concentration (Smagowska & Pawlaczyk-Łuszczyńska, 2013)
Adverse physiological effects - LFN

- Temporary threshold shifts (Leventhall et al, 2003)
- Some correlation with:
  - Heart ailments, chronic insomnia (Mirowska & Mroz, 2000)
  - Elevated cortisol levels (Bengtsson, 2003)
Adverse psychological effects - LFN

• Annoyance (Pawlaczyk-łuszczy´nska et al, 2005; Persson & Rylander, 1988; Storm, 2009) most common, but also:
  – Headaches and palpitations (Møller & Lydolf, 2002)
  – Deterioration in performance & productivity (Bengtsson, 2003; Benignus et al, 1975; Kaczmarska & Łuczak, 2007)
  – Lower levels of cooperation & agreeableness (Waye et al, 1997)
  – Depressive symptoms & distress (Stansfeld & Shipley, 2015)
  – Even at very moderate levels:
    • 40-45dBA (Bengtsson, 2003; Persson & Bjorkman, 1988; Waye et al, 1997)
Caveats

• Data often sparse and anecdotal (Leighton, 2018)
• Easily misinterpreted (Duck & Leighton, 2018)
• Detailed knowledge of “noise dose” not always present
  – Andringa & Lanser, 2013; Donder et al, 2018
• Many effects not reproducible in labs (Fletcher et al, 2018b)
  – Ethical restrictions (Fletcher et al 2018a, 2018b; Leighton, 2018)
  – Possible “nocebo” effect
• But significant base for adverse effects in subset of population
Exposure guidelines - HFN

- Significant differences in methodology and implementation
- Mostly in occupational context
- Often based on small samples
- Samples often made up of mostly adult males (Leighton, 2018)
<table>
<thead>
<tr>
<th></th>
<th>8kHz</th>
<th>10kHz</th>
<th>12.5kHz</th>
<th>16kHz</th>
<th>20kHz</th>
<th>25kHz</th>
<th>31.5kHz</th>
<th>40kHz</th>
<th>50kHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parrack 1966</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>140</td>
<td>140</td>
<td>140</td>
<td>140</td>
<td>140</td>
</tr>
<tr>
<td>Grigor’eva 1966</td>
<td>80</td>
<td>85</td>
<td>90</td>
<td>90</td>
<td>120</td>
<td>120</td>
<td>120</td>
<td>120</td>
<td>120</td>
</tr>
<tr>
<td>Acton 1968</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Parrack 1969</td>
<td>-</td>
<td>80</td>
<td>80</td>
<td>80</td>
<td>105</td>
<td>110</td>
<td>115</td>
<td>115</td>
<td>115</td>
</tr>
<tr>
<td>Japan 1971</td>
<td>90</td>
<td>90</td>
<td>90</td>
<td>90</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>USSR 1975</td>
<td>-</td>
<td>-</td>
<td>75</td>
<td>85</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>Acton 1975-6</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>110</td>
<td>110</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>USAF 1976</td>
<td>-</td>
<td>-</td>
<td>85</td>
<td>85</td>
<td>85</td>
<td>85</td>
<td>85</td>
<td>85</td>
<td>-</td>
</tr>
<tr>
<td>ILO 1977</td>
<td>-</td>
<td>-</td>
<td>75</td>
<td>85</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>Sweden 1978</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>105</td>
<td>110</td>
<td>115</td>
<td>115</td>
<td>115</td>
</tr>
<tr>
<td>Norway 1978</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td>120</td>
<td>120</td>
<td>120</td>
<td>120</td>
</tr>
<tr>
<td>ACGIH 1979</td>
<td>-</td>
<td>80</td>
<td>80</td>
<td>80</td>
<td>105</td>
<td>110</td>
<td>115</td>
<td>115</td>
<td>115</td>
</tr>
<tr>
<td>Canada 1980</td>
<td>80</td>
<td>80</td>
<td>80</td>
<td>80</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>Australia 1981</td>
<td>-</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>USSR 1983</td>
<td>-</td>
<td>-</td>
<td>80</td>
<td>90</td>
<td>105</td>
<td>105</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>INIRC-IRPA 1984</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>75</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>INIRC-IRPA 1984</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>70</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Health Canada 1991</td>
<td>-</td>
<td>-</td>
<td>75</td>
<td>75</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>Poland 2002</td>
<td>-</td>
<td>80</td>
<td>80</td>
<td>80</td>
<td>90</td>
<td>105</td>
<td>110</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Poland 2002</td>
<td>-</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>110</td>
<td>125</td>
<td>130</td>
<td>130</td>
<td>-</td>
</tr>
<tr>
<td>ACGIH 2004</td>
<td>-</td>
<td>-</td>
<td>88</td>
<td>89</td>
<td>92</td>
<td>94</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ACGIH 2004</td>
<td>-</td>
<td>105</td>
<td>105</td>
<td>105</td>
<td>105</td>
<td>140</td>
<td>145</td>
<td>145</td>
<td>145</td>
</tr>
<tr>
<td>US DoD 2010</td>
<td>-</td>
<td>80</td>
<td>80</td>
<td>80</td>
<td>105</td>
<td>110</td>
<td>115</td>
<td>115</td>
<td>115</td>
</tr>
<tr>
<td>EARS Project 2015</td>
<td>-</td>
<td>75</td>
<td>75</td>
<td>75</td>
<td>77</td>
<td>102</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
</tbody>
</table>
Weighting

https://www.cirrusresearch.co.uk/blog/2011/08/what-are-a-c-z-frequency-weightings/

Sound Effects: Exploring acoustic cyber-weapons

PwC
Exposure guidelines - HFN

• Consensus that A-weighting is inappropriate
• Underestimates higher frequencies (Lawton, 2001; Leighton, 2018)
• SPL re 20 μPa is commonly used
• As is Z-weighting (flat frequency response from 10Hz – 20kHz, no attenuation for sounds above/below ‘audible range’)

Acoustics and harm
Exposure guidelines - LFN

• Fewer guidelines exist
• Perhaps because primary effects are subjective, at moderate levels?
• Again, methodology differs significantly
Exposure guidelines - LFN

- Reference curve proposed by Defra (Moorhouse et al, 2011)
- Devised after assessment of previously published curves
- G-weighting (ISO 7196:1995) commonly used for 1Hz - 20Hz
  - But not LFN (Koch, 2017)
Exposure guidelines - LFN

<table>
<thead>
<tr>
<th>Frequency (Hz)</th>
<th>Exposure Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Hz</td>
<td>92</td>
</tr>
<tr>
<td>12.5Hz</td>
<td>87</td>
</tr>
<tr>
<td>16Hz</td>
<td>83</td>
</tr>
<tr>
<td>20Hz</td>
<td>74</td>
</tr>
<tr>
<td>25Hz</td>
<td>64</td>
</tr>
<tr>
<td>31.5Hz</td>
<td>56</td>
</tr>
<tr>
<td>40Hz</td>
<td>49</td>
</tr>
<tr>
<td>50Hz</td>
<td>43</td>
</tr>
<tr>
<td>63Hz</td>
<td>42</td>
</tr>
<tr>
<td>80Hz</td>
<td>40</td>
</tr>
<tr>
<td>100Hz</td>
<td>38</td>
</tr>
<tr>
<td>125Hz</td>
<td>36</td>
</tr>
<tr>
<td>160Hz</td>
<td>34</td>
</tr>
</tbody>
</table>
Previous work
Covert communications channels (HFN)
- Mobile devices (Deshotels, 2014)
- Covert mesh networks (Hanspach & Goetz, 2014)
- Dreadphone/Spectregram (Wixey, 2017)
- Many consumer devices capable of emitting HFN (Filonenko et al, 2010)
Sound in security research

- Disruption of echolocation systems for obstacle avoidance
  - Ultrasonic altimeters on drones (Wixey, 2017)
  - Tesla vehicles (Yan et al, 2016)
- Corruption of data written to hard disk drives
  - Blue Note (Bolton et al, 2018)
- Ultrasonic tracking beacons for targeted marketing
  - Filonenko et al, 2010; Cunche & Cardoso, 2018
Acoustic weapons – FAQs

• Brown Note
• Paranormal experiences (Tandy, 2000; Parsons et al, 2008)
• US Embassy in Cuba (Leighton, 2018)
Acoustic weapons

• Many misunderstandings (Muhlhans, 2017; Vinokur, 2004)
• Significant practical issues (Altmann, 2001)
  – Threshold shifts probably not of interest to attackers
  – Challenging to cause targeted, directional effects
  – LFN: high propagation, low directionality, size restrictions
  – HFN: low propagation, size restrictions
• Need close proximity, rapid diffusion (Bartholomew & Perez, 2018)
Our experiment
Hypothesis

• HFN and LFN may be imperceptible to subset of population
• And, above certain levels, may cause adverse effects
• Some consumer equipment can emit HFN and LFN
• Could an attacker develop malware or attacks to:
  – Cause a device to emit HFN or LFN...
  – ... at levels at or exceeding those in maximum permissible guidelines...
  – ... and therefore cause adverse effects?
Experiment outline

- Develop attacks and malware
- Which can control volume and speaker output in consumer devices
- Play/stream tones at a set of high and low frequencies
- Measure output with a sound level meter
- Compare output to maximum permissible levels
Our experiment

- No human subjects involved in experiment
- Ethics exemption granted by UCL Ethics Committee
- Full risk assessment conducted prior to experimentation
- Relevant safety precautions (ear defenders, anechoic chamber)
- Brands/models/code not released, to minimise risk
Attack scenarios

- Attacker seeking to affect performance of employees/staff
- Attacker seeking to affect performance of organisation (at scale)
- Targeted harassment campaigns
- Low-grade cyber-weapons
## Attack scenarios

<table>
<thead>
<tr>
<th>Device</th>
<th>Environment</th>
<th>Price</th>
<th>Attack Vector</th>
<th>Access Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Home, business</td>
<td>$1,000</td>
<td>Malware infection</td>
<td>Remote or local</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>Home, business</td>
<td>$200</td>
<td>Malware infection</td>
<td>Remote or local</td>
</tr>
<tr>
<td>Bluetooth speaker</td>
<td>Home, business, public</td>
<td>$50</td>
<td>Bluetooth</td>
<td>Within range</td>
</tr>
<tr>
<td>Smart speaker</td>
<td>Home, business, public</td>
<td>$200</td>
<td>Vulnerability</td>
<td>Remote or local</td>
</tr>
<tr>
<td>Headphones</td>
<td>Home, business</td>
<td>$400</td>
<td>Multiple</td>
<td>Remote or local</td>
</tr>
<tr>
<td>Vehicle PA</td>
<td>Public</td>
<td>$35</td>
<td>USB</td>
<td>Local</td>
</tr>
<tr>
<td>Parametric speak.</td>
<td>Business, public</td>
<td>$250</td>
<td>Multiple</td>
<td>Local</td>
</tr>
<tr>
<td>Vibration speaker</td>
<td>Home, business, public</td>
<td>$70</td>
<td>Bluetooth</td>
<td>Within range</td>
</tr>
</tbody>
</table>
Test environment

Our experiment
Windows PoC malware

- Tones embedded
- Local mode (plays on lock)
- Remote mode (C2 channel)
- Volume increased to 100%
- Lowered to original level afterwards
PoC Android malware

- Local mode (plays on lock)
- Remote mode (C2 channel)
- Volume increased to 100% for attack
- Lowered to original level afterwards
Smart speaker

- Known vulnerability to control audio
- Attacker on local network, or do DNS rebinding attack
- Python script to scan for speakers
- If inactive, stream tone from attacker’s web server at 100% volume
- Then restore volume to original state
Headphones

• Over-ear design
• Connected to laptop over Bluetooth
• Placed closer to SLM (1cm)
Vibration & Bluetooth speakers

• Vibration speakers
  – No diaphragm cone
  – Uses a coil on a movable plate which pushes against surface
  – Smaller profile, possibly attractive as localised acoustic weapons

• Paired over Bluetooth (same as Bluetooth speaker)
Parametric speakers

- Ultrasonic carrier waves
- High-intensity directional audio (Pompei, 2002)
- No smart capabilities
- Connected to laptop
- Low profile and cost, and directional properties
- Could be attractive as portable acoustic weapon
Vehicle-mounted PA system

- No network interfaces
- Autoplays audio from an inserted storage device (USB/SD)
Additional attacks – HTML5

- HTML5 audio tag
- Autoplay on visit to site
- Now disabled in some browsers
- Depends on currently set system volume (can’t change client-side)
Additional attacks – manipulation of audio
Additional attacks - manipulation of audio

Our experiment
Measurement

- Class I sound level meters
- “Precision grade”: narrower tolerances, wider frequency range
- Spot-calibrated
- Very expensive
- But you can hire them and send them back via courier
  - That awesome time I almost lost ~£20,000
Measurement

- Each device placed in anechoic chamber with Class I SLM
- Via attacks, played a sine wave tone at 44.1kHz sample rate
- Single frequency (checked with spectrograms)
- Each tone on each device played for 10 minutes
- Surface temperature also measured before/after attack
Measurement

- Z-weighting used for 17kHz and 19kHz
- Proprietary high-pass filter weighting used for 21kHz
- Z-weighting used for LFN
### Results - HFN

<table>
<thead>
<tr>
<th></th>
<th>17kHz</th>
<th>19kHz</th>
<th>21kHz (HPE)</th>
<th>40kHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>63</td>
<td>64.5</td>
<td>45.5</td>
<td>-</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>59.4</td>
<td>58.3</td>
<td>16.9</td>
<td>-</td>
</tr>
<tr>
<td>Bluetooth speaker</td>
<td>59.4</td>
<td>48.5</td>
<td>54.5</td>
<td>-</td>
</tr>
<tr>
<td>Smart speaker</td>
<td>86</td>
<td>35.2</td>
<td>43.8</td>
<td>-</td>
</tr>
<tr>
<td>Headphones</td>
<td>87.5</td>
<td>81.2</td>
<td>79.8</td>
<td>-</td>
</tr>
<tr>
<td>3 laptops</td>
<td>65.6</td>
<td>63.8</td>
<td>57.5</td>
<td>-</td>
</tr>
<tr>
<td>3 phones</td>
<td>59.8</td>
<td>61.1</td>
<td>45.3</td>
<td>-</td>
</tr>
<tr>
<td>Vehicle PA</td>
<td>75.3</td>
<td>20.5</td>
<td>18.5</td>
<td>-</td>
</tr>
<tr>
<td>Vibration speaker</td>
<td>47.7</td>
<td>36.1</td>
<td>27.3</td>
<td>-</td>
</tr>
<tr>
<td>Parametric speaker</td>
<td>85.1</td>
<td>84.2</td>
<td>97.1</td>
<td>117.7</td>
</tr>
<tr>
<td>Parametric (no music)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>89.7</td>
</tr>
<tr>
<td>Parametric (music)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>84.9</td>
</tr>
</tbody>
</table>
### Results - LFN

<table>
<thead>
<tr>
<th></th>
<th>60Hz</th>
<th>80Hz</th>
<th>100Hz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>2</td>
<td>0.1</td>
<td>3</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>1</td>
<td>1.2</td>
<td>6.5</td>
</tr>
<tr>
<td>Bluetooth speaker</td>
<td>38.2</td>
<td>51</td>
<td>64.2</td>
</tr>
<tr>
<td>Smart speaker</td>
<td>47.5</td>
<td>59</td>
<td>71.6</td>
</tr>
<tr>
<td>Headphones</td>
<td>37.5</td>
<td>39.9</td>
<td>40.2</td>
</tr>
<tr>
<td>3 laptops</td>
<td>1.4</td>
<td>-0.3</td>
<td>4.7</td>
</tr>
<tr>
<td>3 phones</td>
<td>3.3</td>
<td>1.6</td>
<td>12.5</td>
</tr>
<tr>
<td>Vehicle PA</td>
<td>13.7</td>
<td>22.6</td>
<td>33.7</td>
</tr>
<tr>
<td>Vibration speaker</td>
<td>24</td>
<td>21.1</td>
<td>18.4</td>
</tr>
<tr>
<td>Parametric speaker</td>
<td>-0.6</td>
<td>0.5</td>
<td>28.6</td>
</tr>
</tbody>
</table>
Other results of interest

- Vibration speaker vibrated so much that it continuously fell over
- Burning smell from smart speaker
  - Further testing showed it was permanently damaged...
Sound Effects: Exploring acoustic cyber-weapons

- Damage
- Critical event
- No recovery
Smart speaker damage

Our experiment
• Reported to manufacturers, who were responsive and cooperative
• Informed updates had been rolled out to address the issue
Audible components - headphones

Our experiment

125Hz - 12500Hz
Audible components – parametric speaker

Our experiment

125Hz – 12500Hz
Headphones are a significant concern:
- Increasingly used (Henderson et al, 2011)
- At high volumes, by young people (Herrera et al, 2016; Vogel et al, 2007)

Also device-agnostic to some extent

Variations of laptop/phone malware could be adapted
- Only trigger sound when headphones are connected

Audio manipulation attack could also succeed with headphones
Implications – parametric speaker

• May be attractive as a portable, low-cost acoustic weapon
• Use in public may constitute significant health risk
Implications – Bluetooth and smart speakers

- Could be used to produce LFN consistent with annoyance
- Smart speaker could be permanently damaged
- ‘Burning-out’ of components could be a fire hazard
- Other models may be vulnerable
Feasibility

- Attacks viable on some devices
  - Any attack/malware capable of arbitrary code execution could deploy this
- Reliant on imperceptibility, susceptibility, exposure duration
- And on no audible components (subharmonics, distortion, etc)
  - Could be attenuated with multiple fade ins/fade outs
Feasibility

- Some attacks require physical/local access, Bluetooth attacks, etc
- Attackers may be more interested in other avenues
  - Espionage, sabotage, financial, etc
Countermeasures
Device-level

• Deshotels, 2014
  – Limit frequency range of speakers
  – Visibly alerting users when speakers are in use
  – Filtering files during processing to remove high/low frequency noise
  – Mobiles: permission restrictions on use of speakers by apps

• Heuristic detection
  – Rarely, if ever, should an application need access to volume levels
  – Maybe muting apps
  – Some legitimate uses for ultrasound (Google Nearby Messages, comms)
Environment-level

• Monitoring environment for HFN/LFN
  – SLMs (most consumer models won’t go that high/low)
  – Requires specialist equipment
  – Android: Ultrasound Detector and Infrasound Detector
  – We used both for our pilot study (Kardous & Shaw, 2014)
  – Modern smartphones *may* be suitable for occupational noise measurement
  – Within limitations of a given device
  – And accepting a certain loss of accuracy
Environment-level

- SoundAlert for HFN detection – PoC only!
- Modified open source application (link below)
- Simple alerts when noise over a threshold is detected

Do not use to evaluate if there is risk of damage or adverse effects, or for safety/compliance assessments (employ a trained professional with appropriate equipment)

Environment-level

- github.com/catz3/SoundAlert-example


Countermeasures
Policy-level

• Review guidelines:
  – Often inadequate due to methodology
  – Or underestimation of effects
  – Or lack of clarity on implementation outside of occupational contexts
• Employers must comply with applicable legislation
• Should conduct regular checks
Conclusion
Limitations

• Small scale
• Limited number of devices
• Short exposure times
• Constant emission of HFN/LFN may degrade audio equipment
• No human experimentation on perceptibility/susceptibility
  – Frequent limitation of research in this area
  – Ethical and safety concerns have to come first
Future work

- In general, more research needed on the risk of HFN and LFN
- Wider range of equipment, larger-scale, longer durations
- Test overheating effects on other devices
  - Take appropriate safety precautions!
- More work on countermeasures, especially detection
- Ethical restrictions make extrapolation challenging
- Get in touch to discuss more!
Summary

• As digital and physical worlds become more integrated:
  – Attackers may become increasingly interested in leveraging vulns against humans
  – Attack surface likely to grow
  – Attacks are (at the moment) often trivial
  – And may become possible/more effective at scale
  – Lack of consensus for adequate safety guidelines is a challenge

• However:
  – Countermeasures are available
  – Real-world consequences are difficult to assess
Thank you!

Q&A: In corridor

@darkartlab
matt.wixey@pwc.com
References


L. Deshotels. Inaudible Sound as a Covert Channel in Mobile Devices. In WOOT, 2014.


