ChatGPT

Defense Mechanisms Against RF-Based Attacks: V2K, Ultrasonic, and AM Radio Threats

1. Overview of Key RF Threats

Voice-to-Skull (V2K) – Microwave Auditory Effect

Illustration of the microwave auditory effect (Frey effect), where pulsed RF energy directed at a person's head induces audible sensations internally. The **voice-to-skull (V2K)** phenomenon refers to transmitting sound directly into a target's head using radio-frequency (RF) energy. It leverages the *microwave auditory effect*, also called the Frey effect, in which pulsed or modulated RF signals (typically in the microwave band) cause thermoelastic expansion in cranial tissues, generating pressure waves that are perceived as sound **inside** the head [1] [2]. First reported near WWII radar systems and studied by Allan Frey in 1961, subjects could hear buzzing or clicking from RF pulses at 1.2 GHz with peak power densities as low as ~80 mW/cm² [3]. Notably, in 1975 researchers **transmitted voice modulated microwaves** and found subjects could discern words (reportedly recognizing 9 out of 10 words) delivered via this method [4]. In essence, a high-power, pulsed microwave beam can "beam" audio into a person's mind without any receiver device. This has led to speculation about its use as a covert communication or harassment tool – hence the term V2K in some military or conspiracy contexts [5]. The practical challenges are significant: effective ranges of a few meters to a few hundred meters were demonstrated in lab settings [3], but delivering intelligible speech at long range requires *very high peak powers* and focused antennas. Nonetheless, V2K is considered a potential **non-lethal weapon** or psy-op method. For example, the U.S. Navy funded a prototype named MEDUSA (Mob Excess Deterrent Using Silent Audio) in the early 2000s to incapacitate targets with microwave sound [6]. While experts debate its feasibility (pointing out that power levels needed for strong effects would cause tissue heating before audible noise [7]), the *threat* is that an attacker with specialized microwave transmitters could cause disturbing sounds or voices in a target's head. This can be used to **harass, distract, or psychologically torment** an individual without any visible attack vector.

Ultrasonic Transmission Attacks

Concept of an ultrasonic "Near-Ultrasound Inaudible Trojan" (NUIT) attack: malicious inaudible commands are played via a device's speaker and picked up by its own or another device's microphone, covertly triggering voice assistant actions. Ultrasonic attacks exploit **high-frequency acoustic waves (above ~20 kHz)** that are inaudible to humans but can still interact with microphones and other sensors. A prominent example is the use of **inaudible voice commands** to hijack voice-controlled devices. In so-called *"DolphinAttack" or "SurfingAttack"* scenarios, attackers modulate ordinary voice commands onto an ultrasonic carrier. Devices' microphones (which often have non-linear responses) demodulate these signals, causing the voice assistant to register them as legitimate commands – all while the human user hears nothing [8]. Early demonstrations required an attacker's ultrasonic speaker to be within line-of-sight of the target device (e.g. a phone on a table) [9]. More recent research has shown **remote attack vectors**: for instance, the NUIT (Near-Ultrasound Inaudible Trojan) technique embeds malicious ultrasonic signals into videos, apps, or voice messages [10] [11]. A victim can be compromised simply by playing a seemingly normal media clip on a

device – the device's own speaker then emits an inaudible command that its microphone (or a nearby device's mic) picks up, triggering actions on voice assistants (Siri, Alexa, Google Assistant, etc.) without the user's knowledge [11] [12]. Attackers have used this to perform actions like unlocking smart locks, visiting malicious websites, or snooping on conversations. Beyond voice assistants, ultrasonic transmissions pose other threats. **Ultrasonic beacons** have been used for covert tracking (e.g. cross-device tracking in advertising), and high-intensity ultrasound can disrupt or spoof sensors. Researchers found that MEMS sensors (gyroscopes, accelerometers, etc.) and even hard disk drives can be manipulated with ultrasonic or acoustic resonance attacks, potentially causing faults in drones or other devices. While these ultrasonic signals don't directly traverse network firewalls, they represent a *side-channel* into devices' control. Overall, ultrasonic attacks are appealing to adversaries because they are stealthy (silent to humans) and can be delivered through innocuous channels (audio output on videos, etc.), effectively bypassing traditional security boundaries.

AM Radio Signal Threats and EMI Attacks

"AM radio" threats encompass any attack leveraging **amplitude-modulated RF signals**, especially in lower frequency bands, to compromise systems. One classic example is **side-channel eavesdropping** via unintentional emissions. Many electronic devices (monitors, cables, keyboards) emit radio-frequency interference that can be AM-modulated by the data they process. In *Van Eck phreaking*, an attacker uses a radio receiver to capture these stray emissions and reconstruct sensitive information (e.g. reading a CRT monitor's display from afar) [13] [14]. Since the 1980s it's been known that an ordinary TV or radio tuned to certain frequencies can pick up these signals – in one case, a CRT screen was snooped from hundreds of meters with only ~$15 of equipment [15] [16]. This demonstrates that **AM radio-based spying** on electronics (also called TEMPEST attacks) is a real threat, enabling data exfiltration without any network contact. Another major category is **EMI (Electromagnetic Interference) injection attacks** on sensors and circuits. Here, an attacker broadcasts a purposely crafted RF signal that is *amplitude-modulated* with a malicious waveform (e.g. a false sensor reading or voice command). If the target device's analog front-end is insufficiently shielded or filtered, it can demodulate this injected signal and accept it as legitimate input. For instance, researchers showed that *low-power AM radio waves* can inject audio into microphones: using <100 mW of power at 1–2 m distance, they induced microphones to output chosen tones, DTMF dial tones, and even human speech and music [17]. The microphone's circuitry inadvertently rectified the RF carrier (in the tens to hundreds of MHz range), recovering the embedded audio signal. Similarly, attacks have been demonstrated on medical devices (e.g. pacemaker leads) by injecting fake bio-signals via RF, and on analog sensors in drones (causing bogus readings). Because many IoT devices and industrial sensors use simple ASK/OOK (Amplitude Shift Keying / On-Off Keying) radios (e.g. 315 MHz or 433 MHz bands for key fobs, weather stations), an adversary can easily **jam or spoof** these AM-based communications. Duplicating an alarm sensor's 433 MHz unencrypted code, for example, allows an attacker to trigger or silence alarms at will. In summary, AM signal threats range from **eavesdropping on unintended emissions** to **actively injecting signals** into systems. These RF attacks bypass normal network channels, targeting the physical layer vulnerabilities of electronic equipment.

2. Capabilities of RFSec-ToolKit for Detection and Countermeasures

RFSec-ToolKit is an open-source collection of radio frequency security tools and resources, and it can be leveraged to **detect, analyze, or mitigate** the above threats [18] [19]. Rather than a single application, it's a

curated toolbox of hardware, software, and tutorials for RF hacking and defense. Key relevant capabilities include:

- **Wide-Spectrum Signal Monitoring:** The toolkit highlights several **Software Defined Radios (SDRs)** such as HackRF, bladeRF, USRP, and RTL-SDR, which cover broad frequency ranges [20] [21]. For instance, the HackRF One can transmit/receive from ~1 MHz up to 6 GHz, spanning HF, VHF, UHF and microwave bands. This means a security practitioner can use HackRF or USRP to scan for unusual signals associated with V2K (e.g. pulsed 1–3 GHz microwave beams) or unauthorized transmitters in the AM and ultrasonic frequency ranges. The RFSec-ToolKit also lists **spectrum analyzer software** like *QSpectrumAnalyzer* and *Spektrum*, which work with SDRs to visualize RF energy across frequencies in real time [22] [23]. These tools allow detection of anomalies such as a spike of pulsed energy in the 2.4 GHz band (which might indicate a microwave auditory attack in progress) or unexpected carriers in the sub-20 MHz range (potentially illicit AM transmissions).

- **Signal Analysis and Decoding:** Once an RF signal is captured, understanding it is crucial. RFSec-ToolKit includes software for analyzing recorded signals, such as **Inspectrum** (interactive signal analysis) and **Baudline** (a time-frequency spectrogram tool) [24] [25]. For example, if an ultrasonic command is suspected, one could record audio from an ultrasonic detector or SDR baseband and use Baudline to visualize spectral content above 20 kHz [25]. A sharp modulation in that range could reveal the presence of hidden voice commands. There's also **Universal Radio Hacker (URH)** for demodulating and decoding wireless protocols [26]. URH could be applied to decode simple AM/OOK signals from devices – e.g. capturing a 433 MHz door sensor's transmissions and identifying if an attacker is replaying or spoofing them. In short, the toolkit provides the **framework to reverse-engineer RF signals**, whether they are malicious commands or unknown emissions.

- **Tools for Specific Bands/Threats:** The repository lists specialized utilities that align with certain threat vectors. For instance, *rtl_433* is a tool that uses an RTL-SDR to decode common ASK/OOK signals in the ISM bands (like wireless thermometers, tire-pressure monitors, etc.) [27]. This could detect unauthorized signals imitating sensors (an attacker injecting false data into an IoT network). Similarly, *OOKtools* is a set of scripts for handling on-off keyed transmissions [27] – useful for auditing the security of alarm systems or garage remotes that use amplitude modulation. For ultrasonic/acoustic analysis, the inclusion of **Audacity** (a multi-track audio recorder/editor) is notable [28]. Audacity can record from an ultrasound-capable microphone and apply filters or Fourier analysis to spot ultrasonic beeps or patterns in the environment. While not an RF tool per se, it complements RF analysis by handling baseband acoustic data (important for threats like voice assistant attacks that bridge RF and audio domains).

- **Transmission and Jamming Capabilities:** Defending against RF attacks sometimes means *reproducing* them in a controlled way (for testing) or *jamming* them. RFSec-ToolKit highlights projects like **rpitx**, which turns a Raspberry Pi's GPIO into a wideband RF transmitter (5 kHz to 500 MHz) [29]. With rpitx or an SDR transmitter, one can emit test signals: e.g. generating the ultrasound modulations to test if a voice assistant is vulnerable, or broadcasting pulses at microwave frequencies to gauge equipment shielding. It's conceivable to use these tools to **jam** certain signals as well – for instance, transmitting broadband noise in the ultrasonic range to drown out any covert commands (much like a defensive countermeasure).

In summary, RFSec-ToolKit doesn't provide a push-button "RF shield" but it arms security researchers with the **building blocks to detect and counter RF-based attacks**. By using the listed SDR hardware and analysis software, one can scan a facility's spectrum for suspicious activity, record and decode potential attack signals, and even experiment with mitigations (like custom filters or jammers). The toolkit's breadth – from low-frequency radio up through microwave and even audio-spectrum analysis – is well-aligned to addressing V2K, ultrasonic, and AM signal threats in a holistic way.

3. Known and Proposed Defense Mechanisms

Mitigating RF-based attacks requires a combination of **hardware, software, and procedural defenses**. We review measures in each category, noting current implementations and research proposals:

Hardware-Based Defenses

Shielding and Filtering: A fundamental defense against malicious RF or ultrasonic signals is preventing them from reaching sensitive components or people. This is typically done through **Faraday shielding** and RF absorption. For example, placing critical equipment in a *Faraday cage* or using shielded enclosures/cables will block or attenuate external radio waves [30]. High-security facilities follow TEMPEST standards (EMSEC) that include metallic shielding of rooms and filters on cables to thwart Van Eck phreaking and other eavesdropping [30]. On a smaller scale, even personal shielding can be effective: in the original Frey effect experiments, a simple 2-inch square of copper mesh ("fly screen") held next to the head **completely silenced** the microwave auditory effect for that person [31]. This demonstrates that **RF energy can be blocked or redirected** with conductive barriers – implying that a targeted individual could use metallic-lined materials (RF shielding fabric or even the proverbial tinfoil hat) to protect the skull from V2K-style irradiation [31]. Likewise, devices can be outfitted with RF gaskets or coated windows to close off RF leakage paths.

In the case of **ultrasonic attacks**, physical acoustic filters are a hardware solution. Manufacturers can install low-pass acoustic filters or dampers on microphones and speakers so that frequencies above the human hearing range are greatly attenuated. Some modern voice assistants have moved towards MEMS microphones that are less sensitive beyond ~20 kHz, but as research shows, many still pick up near-ultrasound commands [32]. Adding an ultrasonic filter (either in the microphone hardware or as a foam insert that absorbs ultrasounds) could effectively **deafen** the device to malicious ultrasonic cues while not impacting normal voice operation. Similarly, for analog sensors susceptible to EMI, adding **input filtering circuits** (high-frequency notch filters, RF chokes, or ferrite beads on wiring) can block out-of-band signals. Many well-designed sensors include anti-aliasing filters that should in theory remove RF energy, but the persistence of EMI injection vulnerabilities [17] [33] suggests that more robust or carefully tuned filters are needed in practice.

Jamming and Emission Countermeasures: Another hardware approach is to **overwhelm or neutralize** the attack signals. For ultrasonic threats, researchers have proposed actively broadcasting ultrasonic *noise or counter-signals* as a form of jamming. One recent defense, *SUAD Defense*, emits tailored ultrasonic perturbation signals in the environment to "break" any inaudible voice commands an attacker tries to send [34]. These ultrasonic defensive signals are themselves inaudible to humans (e.g. masking in a high band) but they effectively interfere with and corrupt the malicious command before the device can interpret it. In experiments, this method **blocked 98%+ of inaudible voice attacks** on smartphones [35]. The concept is analogous to noise-cancelling but for ultrasounds: by flooding the air with a benign random ultrasonic

background, an attacker's hidden signals can't get through cleanly. For RF attacks like V2K, active jamming is more challenging (since you'd need to jam potentially high-power microwave pulses), but broad-spectrum RF noise generators could be used in a localized area to raise the noise floor. This might deter a microwave auditory attack by forcing the attacker to use even higher power (which would be more noticeable and dangerous, or trigger safety sensors). In the AM band context, cheap **RF jammers** can thwart simplistic remote triggers or eavesdropping devices – for example, a security team might deploy an *433 MHz jammer* temporarily if a suspected rogue device on that frequency is active, buying time to locate it. Care must be taken, as jamming can also disrupt legitimate communications. Overall, hardware countermeasures create an environmental shield: **stop the hostile signal before it hits its target** (whether that target is a human ear, a microphone, or a sensor circuit).

Software-Based Defenses

On the software and firmware side, defenses focus on **detecting or correcting malicious signals** and hardening device behavior against them. One important strategy is **signal validation and filtering in software**. For instance, voice assistant platforms can implement a digital audio filter to automatically discard any input above a certain frequency. If the microphone ADC still captures ultrasounds, the voice recognition software could simply ignore frequencies >20 kHz (or require a parallel audible component for any command). This was not standard initially – which is why attacks succeeded – but awareness is leading to changes. In addition, software can look for telltale patterns of inaudible attack: e.g., a burst of microphone input with energy only in ultrasonic bands might raise a flag. Some research papers note that completely eliminating the hardware non-linearity exploit is hard (since it's an inherent mic design issue) [36], but runtime detection of *when* it's happening is feasible.

Another approach is **authentication and context-checking** for voice commands. Modern devices have started offering optional voice recognition (unlocking only for the owner's voice). If enabled, an ultrasonic attack using a generic synthesized voice might fail because it doesn't match the owner's voiceprint. Researchers like Chen et al. recommend users enable such authentication on their voice assistants [37]. They also suggest software limits like requiring a physical confirmation for sensitive actions (so even if a silent command says "unlock door", the system might ask for a manual confirmation). These procedural software interlocks can mitigate damage if an ultrasonic command injection occurs.

For **EMI sensor attacks**, software can perform **sensor fusion and consistency checks**. Since a malicious RF injection often only affects one sensor's reading (and not the actual environment), the system can compare inputs: e.g., if a pressure sensor suddenly spikes but a correlated temperature or motion sensor does not, it could suspect an EMI spoofing and ignore the anomaly. Researchers who demonstrated EMI injection also proposed software defenses that leverage the physical coupling constraints – for example, sending a known test signal or prompt through the system and seeing if the sensor responds correctly can reveal if an outside signal is manipulating it [33]. Essentially, the device can periodically run a self-check (emitting a benign stimulus and verifying the expected sensor output); an attacker's continuous interference would likely disrupt this expected pattern, triggering an alert.

Machine learning is also being explored: algorithms could be trained to distinguish normal sensor/voice input from tampered input by subtle differences (like waveform shapes or background noise). For instance, an ultrasonic voice command might carry ultrasonic artifacts that a classifier can spot and refuse. In summary, software defenses **monitor and sanitize inputs**, employing filters, anomaly detection, and

authentication to compensate for what hardware let through. They act as the second line of defense if an attack signal reaches the device's digital domain.

Procedural and Operational Defenses

Finally, procedural defenses involve **policies and user behaviors** that reduce exposure to RF threats. One key recommendation is **user education and caution regarding unknown signals**. Since ultrasonic attacks often start with tricking a user into playing a piece of media (malicious video or audio), users and organizations should treat unexpected media links or suspicious attachments as potential malware – extending the usual phishing training to include "audio malware." Keeping devices on *mute or using headphones* can also close the loop that ultrasonic attackers abuse. If you listen to audio through earphones, the device's speakers are not emitting anything externally; this means an inaudible Trojan signal hidden in a video can't propagate into the air to reach another device's mic. Chen's team specifically advises using wired **earphones instead of loudspeakers** for any device that might be near other voice-controlled devices [38]. In sensitive meetings, this could become a recommended practice (similar to disabling voice assistants entirely or putting smartphones in secure bins).

For V2K and general RF harassment, procedural defenses include **surveillance and detection routines**. Security teams can incorporate *RF sweeps* as part of regular security audits – using spectrum analyzers to scan the environment for unfamiliar transmissions. There are now commercial **Wireless Intrusion Detection Systems (WIDS)** (like Bastille networks) that continuously monitor the RF airspace of a facility and alert on unknown or policy-violating signals. These systems provide *"a broader spectrum of wireless threat monitoring than traditional IT security tools"* [39], covering cellular, Bluetooth, IoT frequencies, etc. Deploying such sensors can catch an attacker trying to use a directional microwave emitter or a concealed radio bug; the moment an unusual strong RF signal appears, security can investigate. In a network security context, this is analogous to having IDS/IPS for the wireless physical layer. Organizations dealing with highly sensitive information may also enforce **zoning rules**: e.g., no personal electronics in certain areas (to prevent covert recording or attacks), and maintaining RF isolation for those areas (through architectural shielding or jamming of external signals). These policies, combined with technology, create layered security.

Additionally, **response procedures** are important. If an RF attack is suspected (say, employees reporting strange sounds or devices acting oddly), having a clear protocol – such as powering down equipment, moving to shielded zones, and using RF detectors to locate sources – will limit the damage and gather evidence. From a high-level perspective, robust countermeasures require treating the *"invisible" spectrum as part of the security domain*. Just as firewall logs are monitored, an organization should monitor RF spectrum logs; just as employees are taught about phishing emails, they should be briefed on social engineering via "voice" (like unexpected phone commands or even the possibility of hearing disembodied voices in extreme cases). Procedural defenses ensure that the human and organizational factors do not become the weak link when confronting RF-based threats.

4. Gaps and Limitations in Current Tools and Approaches

Despite growing awareness, there remain significant **gaps in our defensive toolkit** against these unconventional attacks. One major limitation is that **most commercial security frameworks do not cover the RF domain well**. Traditional IT security focuses on network traffic and software; the kinds of attacks discussed (V2K, ultrasonic, EMI) often fall outside the scope of typical monitoring. Open-source collections like RFSec-ToolKit are invaluable, but they require expert operators – they are not turn-key solutions for real-

time protection. There is a lack of integrated, easy-to-deploy RF intrusion detection for the average enterprise. Specialized systems like Bastille's exist, but can be expensive and usually target more common vectors (rogue cellular or Wi-Fi devices) rather than niche threats like microwaves or ultrasounds. This leaves many organizations **blind to RF assaults** unless they have a dedicated RF security team.

Another gap is in **device manufacturer adoption of countermeasures**. The research community has demonstrated attacks and even provided defense techniques (as discussed in Section 3), yet many of these are not yet standard. For instance, as of mid-2025, tests showed that *the majority of smartphones and smart speakers remained vulnerable to ultrasonic command attacks*, with only very limited cases (like an old iPhone model) being invulnerable due to hardware quirks [40] [41]. This indicates that ultrasonic filtering or authentication measures are not uniformly implemented. It often takes years for such defenses to trickle into consumer devices (if at all). Similarly, while EMI injection on sensors has been known for a decade, **many sensors in medical or industrial devices still lack adequate shielding or filtering**, making them soft targets [17] [33]. There is a practical trade-off – adding robust shielding/filters can increase cost or weight, which manufacturers resist unless clearly necessary.

In the case of V2K, one could argue the gap is more about **verification and tools**: if someone suspects a microwave auditory attack, there are few readily available devices to confirm it. Detecting a highly directional microwave beam with pulses might require expensive spectrum equipment and expertise. Law enforcement and security personnel generally do not have protocols for such "psychotropic" attacks, partly because it straddles physical and psychological realms. This lack of mainstream recognition means potential victims of such harassment have limited support or recourse. The literature (and skepticism from experts [7] [42]) suggests V2K is not easily weaponized on a broad scale, which is reassuring, but it also means **little effort has gone into developing specific counter-V2K tech**. In short, current approaches tend to *react* to incidents with ad hoc measures rather than providing preventive tools.

Another limitation is that **countermeasures themselves have side-effects**. Jamming ultrasounds or RF can interfere with normal operations or violate regulations (RF jamming is illegal in many jurisdictions except for authorized agencies). Heavy shielding can impede desired communications (e.g. your building might block the attack but also block cellular signals for users). Striking a balance between security and functionality is non-trivial, and many defenses (like constantly running an ultrasonic jammer) have not been field-tested for long-term safety or compliance.

Finally, usability and awareness remain gaps. Users might find it inconvenient to use earphones all the time or might forget to mute a device. Security staff may not be trained in RF forensics, so even if tools are available, a subtle attack could go unnoticed. RFSec-ToolKit provides the means to *research* these issues, but not a turnkey "RF firewall." There's an **education gap** in the industry about RF threats: many IT professionals are only beginning to learn about things like TEMPEST or inaudible attacks, so organizational policies and budgets often overlook these vectors.

In summary, while the state of the art in research is advancing, **current defenses are piecemeal and not uniformly implemented**. This leaves exposures – especially in consumer and IoT domains – where attackers can still find success. Bridging these gaps will require concerted effort to integrate RF security into the standard cybersecurity framework.

5. Recommendations for Robust Countermeasures in a Network Security Context

To build robust countermeasures against V2K, ultrasonic, and AM radio signal attacks, a **multi-layered strategy** should be adopted, integrating technical controls with policies. Here are key recommendations:

- **Integrate RF Monitoring into Security Operations:** Just as networks are continuously monitored for intrusions, organizations should deploy continuous RF spectrum monitoring in critical areas. This could involve installing spectrum sensors that feed into a Security Operations Center (SOC) dashboard. Modern WIDS/WIPS solutions (e.g. enterprise RF monitoring like Bastille) can be used to detect and locate unknown transmitters on the premises [39] [43]. By logging RF activity, one can establish a baseline "RF fingerprint" of the environment and get alerts on anomalies (e.g. a spike at 2.4 GHz pulsing at audio frequencies might indicate something suspicious). For smaller organizations or personal use, even a periodic sweep with an SDR and open-source tools from RFSec-ToolKit can help maintain awareness of the local spectrum.

- **Harden Devices and Endpoints:** Choose equipment that has been tested for electromagnetic and acoustic robustness. For voice-controlled IoT devices, prefer those that implement ultrasonic filtering or require voice authentication. Encourage or mandate firmware updates that patch known issues (for example, if a vendor releases an update to ignore ultrasounds or to reduce mic gain at high frequencies, apply it promptly). In an industrial or healthcare network, audit sensor modules for EMI susceptibility – if certain sensors are critical (e.g. a pressure sensor that could be spoofed via RF), consider retrofitting additional shielding or using alternative sensing mechanisms less prone to EMI. Implement **TEMPEST-like protections** for systems handling sensitive data: this might include using low-emission monitors, ferrite clamps on cables, and even white noise emitters in the vicinity of classified discussions to mask any gleanable signals.

- **Network Segmentation and Physical Zoning:** Extend the concept of network segmentation to the physical wireless domain. Create **zones of control** where certain wireless technologies are either disabled or tightly monitored. For instance, in a highly secure meeting room, you might deploy an ultrasonic noise generator (to prevent any ultrasonic eavesdropping or attacks) and ban any devices with voice assistants. Likewise, enforce that in sensitive labs, all devices must be in airplane mode and ideally in RF shielded racks – this prevents both exfiltration (via unintended emissions) and infiltration (via malicious signals). Clearly mark these zones and educate personnel that they exist for RF security, similar to how we have EMI-safe zones in hospitals.

- **Implement Procedural Safeguards for Users:** Human awareness is crucial. Conduct training sessions on the risks of "cyber-physical" attacks. For example, employees should know that playing random media from untrusted sources on a device with a voice assistant could be risky (the concept of an "audio Trojan" should be introduced in security training). Advise simple practices like muting smart assistants during confidential work, covering device microphones when not in use (there are slide covers not just for webcams but also for mics in some cases), and using wired headsets or secure communications methods. In contexts where V2K harassment is a concern (e.g. diplomats or military personnel in hostile territories), brief them on the microwave auditory effect – not to induce paranoia, but to ensure they recognize it and report it. If someone knows that a ringing or clicking in their head could be artificially induced, they are less likely to be psychologically destabilized by it.

They should also know to *change locations or get behind thick shielding* if such phenomena occur, and to alert technical security teams who can then scan the area.

- **Enhance Software and Network Layers to React to RF Anomalies:** Even though these are physical attacks, network security appliances can be tuned to pick up secondary signs. For instance, an ultrasonic attack might cause a victim device to suddenly send commands or connect to malicious sites – an IDS could notice an IoT device making unusual requests (triggered by a voice command the owner never actually spoke). Network access control could be set such that voice assistants cannot execute high-privilege actions on other devices without additional verification through the network. Essentially, use the network as a fail-safe: if a smart speaker tries to unlock a door over Wi-Fi, require it to pass a challenge or have the user confirm on their phone (out-of-band verification). This way, even if the device is tricked via RF, the network or cloud service can intervene.

- **Plan for Incident Response and Testing:** Include RF attack scenarios in your incident response plan. For example, define steps for "suspected RF jamming or interference event" – who to call (maybe a spectrum expert or law enforcement liaison), what tools to use (spectrum analyzers, RF direction-finders), and how to preserve evidence (recording signals, etc.). Also, perform *red-team exercises* that include RF attack vectors. A red team might attempt to sneak in an ultrasonic command device or a covert transmitter, and the blue team can practice detecting and mitigating it. Testing the effectiveness of countermeasures like ultrasonic jammers or new filters is important too – these should be validated in real-world conditions (e.g. does the ultrasonic jammer truly block a DolphinAttack without disrupting normal voice commands?).

- **Continued Research and Collaboration:** RF attack techniques are evolving, so staying current is vital. Organizations should keep an eye on research publications and tools (the RFSec-ToolKit itself is periodically updated with new hacktools and techniques across the RF spectrum [44] [45]). Collaborate with the security community – for instance, if a new ultrasonic exploit is found in popular smart TVs or phones, security teams should share detection signatures or mitigation scripts. Participation in industry groups on electromagnetic security or attending conferences (like RFHack, DEF CON Wireless Village, etc.) can provide early warnings of upcoming threats and defenses.

In conclusion, defending against V2K, ultrasonic, and AM RF threats requires **broadening the scope of network security to encompass the electromagnetic domain**. By deploying RF-aware tools, hardening hardware, and educating users, organizations can significantly reduce the risk. The goal is to make the environment as inhospitable as possible to these attacks: *no dark corners in the spectrum that an attacker can quietly exploit*. Through a combination of shield, watch, filter, and educate – "Shield" with hardware, "Watch" the spectrum, "Filter" inputs in software, and "Educate" personnel – we can build a robust defense posture against even the stealthy and unconventional RF-based attacks.

References:

1. Microwave auditory effect (Frey effect) description – Wikipedia [1] [3]
2. Voice-to-skull demonstrations of word transmission [4]; Navy's MEDUSA project and expert commentary [6] [7]
3. Hackaday on microwave auditory effect and shielding (Frey's experiment) [31]
4. Ultrasonic "SurfingAttack" on voice assistants – The Debrief (McMillan, 2023) [8] [11]
5. UTSA Today – Chen et al. NUIT attack and defense insights [46] [37]

6. ArXiv 2025 – SUAD ultrasonic defense with perturbation signals [34] [35]
7. RFSec-ToolKit – Tools for RF analysis (SDRs, spectrum analyzers, Audacity, etc.) [22] [24]
8. EMI injection on analog sensors – Research (Foo Kune et al. 2013) results and mitigation limits [17] [33]
9. Van Eck phreaking overview – Wikipedia [13] [15]
10. Bastille Networks (WIDS) description – broader spectrum monitoring [39] and cellular device detection [43].

---

[1] [2] [3] [4] [5] [6] [7] [42] Microwave auditory effect - Wikipedia
https://en.wikipedia.org/wiki/Microwave_auditory_effect

[8] [9] [10] [11] [32] [40] [41] New Ultrasonic Acoustic Attack Targeting Microphones and Voice Assistants Gives Remote Access to Most Smart Devices - The Debrief
https://thedebrief.org/new-ultrasonic-acoustic-attack-targeting-microphones-and-voice-assistants-gives-remote-access-to-most-smart-devices/

[12] [37] [38] [46] Uncovering the unheard: Researchers reveal inaudible remote cyber-attacks on voice assistant devices | UTSA Today
https://www.utsa.edu/today/2023/03/story/chen-nuit-research.html

[13] [14] [15] [16] Van Eck phreaking - Wikipedia
https://en.wikipedia.org/wiki/Van_Eck_phreaking

[17] [33] spqrlab1.github.io
https://spqrlab1.github.io/papers/fookune-emi-oakland13.pdf

[18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [44] [45] GitHub - cn0xroot/RFSec-ToolKit: RFSec-ToolKit is a collection of Radio Frequency Communication Protocol Hacktools.无线通信协议相关的工具集，可借助SDR硬件+相关工具对无线通信进行研究。Collect with ♥ by HackSmith
https://github.com/cn0xroot/RFSec-ToolKit

[30] Protecting Data at Risk of Unintentional Electromagnetic Emanation: TEMPEST Profiling
https://www.mdpi.com/2076-3417/14/11/4830

[31] Cuban Embassy Attacks And The Microwave Auditory Effect | Hackaday
https://hackaday.com/2017/09/25/cuban-embassy-attacks-and-the-microwave-auditory-effect/

[34] [35] [2508.02116] SUAD: Solid-Channel Ultrasound Injection Attack and Defense to Voice Assistants
https://www.arxiv.org/abs/2508.02116

[36] Inaudible Voice Commands: The Long-Range Attack and Defense
https://www.usenix.org/conference/nsdi18/presentation/roy

[39] [43] Wireless Intrusion Detection - Bastille
https://bastille.net/solutions/wireless-intrusion-detection/