to Alexa account, it can help the owner use Echo to tweet by saying "Alexa, tell Twitter Bot/Tweet it to tweet···" Therefore, the attacker can spread malicious messages on the victim's account. Also, by applying IFTTT applet which could link to Sina Weibo, one of the most popular social platforms in China, an adversary could also conduct a similar attack.

- Malicious links and photos are also the main spreading routes in the virtual world. IFTTT enables the messages to be sent to Gmail, Linkedin, Google Photo, iOS Photo, OneDrive, Github, etc. Therefore, if the victim has enabled these Applets, the attacker can spread malicious links and photos to these platforms.
- Additionally, with IFTTT applets, an attacker can even command Echo to download the file at a given URL and add it to popular cloud drive service such as Google Drive or Dropbox, which could further lead to the malicious software attack and cause a severe loss for the victim.
- Attackers can add some advertisement on the victim's list with Echo by saying "Alexa, add···on my To-do list", and then ask "Alexa, what is on my To-do list?", so that the information can be sent to his email or phone. Since the email and SMS are sent by Alexa, they cannot be filtered out as junk mail or message. More pernicious, attackers can spread even violent, pornographic, reactionary and other illegal information. In addition, if the victim has enabled the Applet that prints the list with his wireless printer, the malicious information can be printed as well.

Calling or Sending SMS. The "Call and Message" skill makes Echo a free phone to call the owner's friends and family. However, the called subscribers can be their names or phone numbers, and people sometimes save the contacts as their appellations. Thus, after the attacker getting through the contacts by Echo, he can broadcast a help, threaten, extort signal by radio or TV.

To add a person to the contact list, what Echo needs is only the friend's phone number, which enables the attacker to call or message the user's friend on behalf of the user. Making things worse is to attach malicious contents with the message (e.g., a link to download a malicious application). This is very confusing since the message is sent to the friend using the user's account. Once the malicious contents are read by the friend, his machine may be compromised. Sometimes, even a figure (in the content) can trigger a severe vulnerability [22], allowing the device to be fully controlled by the attacker.

More recently, Alexa added "Phone.com Audio Interface" skill into the list. By using this skill, an attacker can easily talk to Echo like "Alexa tell phone dot com to call 888-280-4331" to call one US phone number without any authentication. If the called number is not toll free, the victim may face financial problems later.

Online Purchasing. Through voice commands, a user can ask Echo to order selected Prime-eligible products from the prime catalog or from her order history. After the order is placed, Echo uses the default payment method and shipping address in 1-Click setting to finish the order. Such an order can even be a service such as Uber. People can make a payment, get Amex Offers, check the balance with a 4-digit PIN.

From an attacker's point of view, besides shopping using the user's credit cards, he can also directly steal money from the user. For example, the attacker can pretend to be a Uber driver, stop around the user's house, command Echo to order Uber and, in the end, receive the Uber order. By default, voice purchasing is activated once the user registers his Echo. Further configurations can be operated in the Alexa app, such as turning off voice purchasing or requiring a confirmation code before every order. For security, a user can set a 4-digit code in Alexa app which Echo will ask for when the user is placing an order from Amazon. Unfortunately, this option is not mandatory. So the attacker can place items in the name of the user if he does not set 4-digit security code.

As the maturity and pervasiveness of Amazon Echo device and Alexa platform, more and more third-party shopping services like Best Buy have launched nowadays. Hence, an attacker can also operate related commands towards victim's Echo and make an order from Best Buy, causing much inconvenience and even money loss for the victim.

4.2. Attack Evaluation in the Physical World

As discussed above, hacking Echo can make a great attack in the virtual world. Similarly, people not only enjoy the convenience of IoT devices, but also take the risks of their vulnerability at the same time. Despite the vulnerabilities listed in Table 1. Unquestionably, even some of them are safe, we still can use Echo to attack them. Amazon Echo, as a hub for controlling IoT devices at home, can naturally send commands to the connected IoT devices, including smart locks, switches, thermostats, doors of garages, security cameras, etc. Such commands, once manipulated by the attacker and successfully interpreted by Echo, can further be executed by the corresponding IoT devices, which could bring serious threats to home. Table 4 shows the main attack in the physical world.

The attacker, after crafting voices of commands to the Echo, is apparently able to do whatever a legitimate user can do at home. Unfortunately for the attacker,

Table 4. Impact of attacking Echo in the physical world.

Target	Attack	Impact level
Car	remotely control vehicle	fatal
Garage	unlock and lock	fatal
Camera	disarm for further actions	moderate
Android Devices	remotely manipulate Bluetooth/Wifi	moderate
Router	wifi on/off	moderate
Switch	power on/off	moderate
Thermostat	control temperature	moderate
Oven	roast, preheat	light
Shower	turn on/off	light
Washer/Dryer	turn on/off	light
Air Purifier	change the air quality settings	light
Light	control light brightness and colour	light

we found that Echo still needs extra authentication for sensitive operations such as requiring a passcode to unlock the door. Below we made several experiments to understand what the attacker can really gain. To our surprise, we found that the attacker can still control most of the IoT devices.

Control smart cars. Vehicles are becoming more and more "smart". For example, a voice responsive door lock system is provided to further automate the open and close operations of doors. In this way, users do not need to stand by the vehicle opening the door. Instead, before coming to the vehicle, he could voice-command the door to open and walk into the vehicle. Many vehicles such as Tesla, BMW and Automatic support this kind of voice operations. Further making the vehicles "smarter" is the connection with "smart hub" like Echo. More functionalities can be supported beyond simply opening and closing the doors within a short distance, such as remotely getting the vehicle's location, which greatly extends the distance that an attacker could reach.

Once Echo is controlled by manipulated voices, an attacker can locate the vehicle no matter where it is. In most cases, such sensitive and even dangerous operations need extra authentications such as supporting a PIN code to Echo. An attacker without knowing such code cannot operate on the vehicle. An example is Genesis, a vehicle model of Hyundai, which permits a user to remotely start/stop/lock/unlock the vehicle with the PIN code. However, the openness of the platform of smart vehicles and Echo allows third-party developers to build their own skills for operating on the vehicles through Echo. Without considering strict safety and security policies, the developers of these unofficial skills may let attackers easily control the vehicles with no supply of any extra authentication, further exposing the legitimate users to dangers. We found such an app called "My Tesla". Once a manipulated voice command "Alexa, tell my car to flash lights/honk the horn" is sent to Echo, the attacker can remotely control the flash lights and honk of the vehicle, start or stop the charging system, set the temperature inside, etc. Therefore, the attacker gets full control of the vehicle.

Control smart locks/thermostats. Smart locks are one of the most favorite IoT devices that attackers like to control. Sending the voice command "Alexa, ask August to unlock my door" can unlock the door of the home which allows the attacker to walk in. Usually, extra passcode is needed for authentication before opening the door. However, we did find that some smart devices controlling the locks have no such authentication (e.g., Nexx Garage and Garadget products controlling doors of a garage). Once the voice command is sent to Amazon Echo, the smart lock connecting to Echo will let the door open, which allows an attacker outside the door to enter freely.

Another IoT device related to door opening is smart thermostats, which are originally designed to control the temperature at home through the voice commands from Echo. For example, after receiving the voice command "Alexa, set the downstairs temperature to 72", the thermostat will set the home temperature to 72 Fahrenheit if the unit was chosen as Fahrenheit. Also supported is the increase of the temperature at home. The interesting thing is that the high temperature will let some smart windows open itself to lower the temperature, as reported by Jack Jia, etc. [30]. As a result, even if the attacker cannot directly control the lock, he could still enter the home by setting up a high temperature to let the window open.

Control smart camera. Besides the IoT devices related to locks, attackers also care about the security cameras at home. Many of them connect to the Internet, allowing the owner to check the statuses at home anytime and anywhere. As a result, to avoid being found, the attacker should let the smart cameras not be able to work. For example, the attacker could use Echo to control the smart Homeboy cameras by simply crafting a voice command "Alexa ask Homeboy to disarm". Then the camera will stop working.

Until now, there are not so many cameras working with Echo, even though Echo possesses skills to arm or disarm Homeboy camera, but there is nobody enables them yet. However, once the owner enables them, the attacker will have the ability to turn off the camera when the owner is not in home so that owner cannot monitor the house, or turn it on at night and monitor the privacy inside.

Control devices' communication. Alexa skills such as "Find My Phone" can help the user find their phone call somebody. Specifically, "Alexa, ask Find My Phone to add another number" can add and delete the contacts on the address book. In addition, IFTTT can enable Echo to control the communication models of the phone. For example, The Applet "Tell Alexa to turn on your phone's wifi". If the attacker sets up a malicious WiFi hotspot with the same name and password as the victim linked before. The phone can automatically be linked to the malicious WiFi. It can turn on Bluetooth as well. As Table 2 shows that some Bluetooth devices need not require any passcode to pair. Therefore, attacker can monitor and manipulate the data.

Control smart router/switch/oven/light etc. The capability of commands manipulation to Echo can further be extended by other "smart hubs" such as Samsung SmartThings and other third party IoT platforms. These smart hubs, similar to Echo, connect hundreds of smart sensors, lights, locks, cameras, and even more to monitor and control home. In this way, if a smart device at home is not directly operated by Echo, it can be controlled by one of the smart hubs which connect to Echo. In other words, the voice command manipulated by the attacker can finally control the smart device through Echo.

- Echo can control the ASUS Router to pause the Internet, so that the IoT devices are offline, if the victim uses his camera to monitor his house, the video would stay at the last frame, which the victim may not realize that his house has been attacked.

- Another brute way for the attacker is to control the smart switches, again through Echo. Once an "Alexa, turn off my switch" command is sent to Echo, it will let the smart switch shut down by itself, and further all the devices connected to the switch will lose power to run.

- Echo works with Douch oven, Barbecue master. So an attacker can ask oven to roast, heat or stove, which can lead to fire if there is no person in the house.

- Even though people think the smart light is unconsidered for the thread, people can control the light brightness and color to transmit special signals [24].

5. Defense

Usually, researchers use signal processing and machine learning to defense the replay attack [13, 14, 16, 57]. In addition, voice print authentication is believed as an effective method. However, our test results on Echo, Google Assistant and Apple Siri are not very effective, as somebody or recorded audio can control them, which indicates that the root cause that enables the MUTAE attack is lack or weak of 1) user authentication, 2) user awareness and 3) fine-grained authorization for different (security sensitive) services. Therefore, we propose several defense solutions from three aspects.

First, the lack of user authentication in current voice control devices, like Amazon Echo, opens the initial loophole for the MUTAE attack. Therefore, it is critical to provide authentication. One strong and nature approach is to authenticate a user based on his/her *voice pattern*. That is, only a voice control command from an authenticated user can be executed. This kind of check needs to build a model to characterize users' voice. However, this approach also has a problem. It cannot prevent replay attack. The adversary can record the voice of a registered user and replay his/her command accordingly. To prevent the replay attack, we proposed a defense mechanism on the base of voice pattern authentication. We name it as two-factor authentication over the voice channel. That is, besides using the *voice pattern* for authentication, the Amazon Echo will act like a chatbot and ask questions on the fly. The questions can be based on user historical profile that was registered previously. The questions can also be simple questions, like "who is the current president of U.S.?", to test the intelligence and presence of a real user in front of the voice control device. The user must answer the question directly through the device. This type of two-factor authentication must be performed whenever a security critical voice command is received by Echo. In this way, not only the *voice pattern* of the user is matched, the presence and the human user identity will be checked. Hence, it prevents the MUTAE attack and other potential replayed MUTAE attack. Besides above method, Echo could also enable user's location check inside it. If the user's cell phone is not

in house wifi range, Echo will consider the user is out of safe range and will not response any further voice commands.

Second, for most of our proposed attacks, an victim's unawareness is necessary for the adversary, otherwise the victim could stop any dangerous and malicious actions caused by Echo immediately. So it is obvious that a natural defense method is to set user alerts for potential malicious actions. For example, if an adversary is commanding Echo to conduct potential dangerous actions like making a payment, the victim will receive SMS or email alert showing that actions and decide if he/she wants to continue. This way the attacker's action will be revealed to user and the user could stop it immediately.

Finally, the lack of fine-grained authorization for different users and under different contexts, also enlarges the attack surface of various attacks, which has been discussed in Section 3.2. For instance, the system can enforce the fine-grained policy that only authorized users (e.g., parents but not children) can purchase expensive items or media contents from Internet. Also, the system can enforce the fine-grained policy that only certain authenticated users are able to voice control the security critical operations (e.g., open the front door or windows). Furthermore, IFTTT enriches the skills of IoT and social activities, thus Echo can control IoT or online service based on registered IFTTT skills. Therefore, some fine-grained policy enforcement should be deployed with the application context. When MUTAE attacks trigger a set of Applets or leverage an Applet with low security sensitivity to trigger one with high security sensitivity, the fine-grained security policy should prevent these type of privilege escalation. For instance, if the user enables several *applets*: *applet 1*–"If motion is detected in my Homeboy location, turn my Philips Hue bulbs red"; *applet 2*–"If You say 'Alexa trigger switch off', then turn off Wemo switch." Considering that the Philips Hue bulbs are connected with the Wemo switch; *applet 3*–"Switch on Wemo if my Homeboy detects motion." Attackers can use Echo to turn off the switch, and then take actions, even if the Homeboy camera detects something. The bulbs will not turn red, and the owner will not discover it. The development of IFTTT Applets and how to use them should be scrutinized carefully. We also suggest that before a new skill or Applet is enabled, Alexa and IFTTT platform should provide a security vetting automatically based on the usage context.

6. Discussion

Comparison with other attacks. During last few years, different types of voice spoofing attacks have emerged towards intelligent voice controlled systems and devices. We hereby showed a overview plus comparison among MUTAE attack and other similar voice attacks. We define three metrics including effective distance, target systems and practicality. For attack distance, we consider 10 meters is the bar for long attack range which is enough for an attacker to be outside the room safely, with distance between 1 to 10 meters as medium and distance smaller than 1 meters as short. Target systems refer to the target of the attack, and practicality refers which type of the attack. For a practical attack in the real world, an over-the-air attack would be expected. **As we can see in Table 5, to the best of our knowledge, MUTAE Attack is the first long-range and practical attack which could compromised Amazon Echo devices.**

Limitations of our attack. Although our attack can control Amazon Echo in a long distance expectedly and may lead potential physical damage and financial loss for victims, there are two main limitations of our attack. First, in order to launch our attack in more aspects, we tried our best to do a comprehensive analysis for existing Alexa skills and IFTTT Applets for evaluation of the attacking consequences, and the results strongly indicate that our attack is promising for potential harmful issues in both virtual world and physical world. However, to successfully finish the whole attack, an adversary must ensure the victim has already enabled corresponding skills/applets, which means the adversary can only target one certain group of users. Second, despite the fact that our attack can be conducted remotely, the effective range is still not long enough to cover large amount of target devices and cause severe impact. Currently, our FM and TV signal injection attack can only be effective to 20 meters, which would only allow us initiate our attack for 2 to 3 houses normally. This distance range is highly related with our SDR device power limit, so we would believe a more powerful equipment can make us attack range much larger.

Future work. In this work, we explored Alexa skills and IFTTT Applets and revealed many potential security concerns if an adversary could conduct MUTAE attack and control victim's Amazon Echo. With the rapid development of AI and smart home technologies, Internet of Things have been increasingly equipped in our home and we could ask Echo to control more devices in the future. However, such communication channels not only remain between Echo and devices, but also among those smart devices. For example, an oven may be automatically turned on to prepare the dinner if the kitchen light is on. By now, we have little knowledge how such channels in smart home ecosystem work and whether vulnerabilities exist that an attacker could exploit to control those machines. Therefore, a potential future direction would be to develop a comprehensive and effective security vetting

Table 5. Comparison among voice spoofing attacks.

Attack Name	Effective distance	Target Devices/Systems	Practicality
Dolphin Attack [57]	Medium	iOS/Android Devices, Laptops, Amazon Echo, etc	over-the-air
IEMI Attack [31]	Medium	iOS/Android Smartphones	over-the-air
Hidden Voice Attack [16]	Not Given	CMU Sphinx (white-box attack) Google Speech API (black-box attack)	over-the-air (white-box attack) wav-to-API (black-box attack)
Practical Hidden Voice Attacks [7]	Not Given	Bing Speech API, Google Speech API, IBM Speech API	over-the-air
Carlini Attack [17]	Not Given	Mozilla Deepspeech	wav-to-API
Commandersong [56]	Short	Kaldi, iFlytek	over-the-air
MUTAE Attack	Long	Amazon Echo, Google Home, etc	over-the-air

system which could automatically evaluate the control flow and security issues in one smart home environment controlled by voice console like Echo.

7. Related Work

There are many research related to our topic, which can be summarized as four main categories: (1) voice command injection, (2) audio adversarial samples, (3) voice authentication for voice-based Internet of Things (IoT), (4) smart devices interacting with IFTTT.

Voice commands injection. Many researchers have demonstrated that it is feasible to inject voice commands remotely without raising victim's awareness. Kasmi et al. [31] introduced a new technique for remote silent voice command injection in smart phones based on smart IMEI. Diao et al. [23] and Jang et al. [29] proposed that malicious apps could play voice commands to control victim's cell phones. Zhang et al. [57] realized the inaudible attack on voice control systems by the carrier of ultrasonic. The inaudible attack could be interpreted as commands by voice-based devices. Our work differs with them: The previous works mainly targeted voice control system in a short range, but our attack can be performed in the long distance. Most similar to our work is that R.Martin [2] found Amazon Echo could be influenced by public radio stations while in our attack, we build a radio stations and extend the voice-generate equipment to more kinds of devices including TV, radio, speakers, etc.

We note that a shorter conference version of this paper appeared in [55]. In this manuscript, we proposed a new physical-world attack to inject coaxial signal towards TV. We further did a detailed analysis of Echo's voice control channel and the corresponding impacts if being compromised, in both physical and virtual world (e.g., social network). We also mentioned several feasible defense solutions to mitigate our attack, then users could further trust Echo to command other smart home devices or online services.

Audio adversarial samples. With the significant improvement of state-of-the-art deep learning [26] technologies, more current speech recognition systems are adopting neural network which could bring more accuracy. However, such deep learning technologies show vulnerabilities to adversarial sample [47], which is usually normal object added with small and unnoticeable perturbation but could be misclassified by machine as other target. Recently, researchers have proved such adversarial examples also exist in speech recognition systems. Vaidya et al. [52] and Carlini et al. [16] observed that attackers could issue hidden voice commands which were unrecognizable to human listeners but can be interpreted as desired commands by CMU Sphinx speech system, also in their black-box attack, the voice commands can be understood by Google Speech API. Similarly, Hadi et al. [7] use four methods to generate the noisy audios to practically attack several speech recognition models. Yuan et al. [56] successfully embedded voice commands into regular songs stealthily, which can compromise Kaldi, one popular open-sourced speech recognition system. They also showed that such samples could be played over-the-air and even transfered to another commercial black-box speech model. In addition, [44] use psychoacoustic hiding method to inject command into audios and attack Kaldi without human realization. Our work differ with them as our attack could compromise Amazon Echo and can be launched in a long range.

Voice authentication. Signal processing and machine learning can be used to defense the replay attack [13, 14, 16, 57]. In addition, many previous works demonstrate that the training data for victim's voice sample can

be collected and a voice biometric can be built for speech recognition [10, 15, 20]. However, no theoretical guarantee is provided to ensure the security of these models and replay attacks could compromise some cases. Huan et al. [25] proposed the body-surface vibrations of the user gathered by wearable devices, which can be further analyzed to determine if it matches the speech signal received by a voice assistant. This implementation would enhance the security concerns if the victim is in the noise-around situation or is conducting some confidential work. In our attack scenario, the victim is more likely to be far away from their house and Echo devices. So the wearable equipment would be unsuitable due to the transmit distance limitation.

Smart devices interacting with IFTTT. A considerable number of researches have been conducted to show that connecting a wide range of functionalities of IoT devices in smart home to each other and to different online services using trigger-action programming is feasible for ordinary users [21, 48, 51]. Surbatovich et al. [46] have proposed that IFTTT Applets can lead to privacy risks and potential harm in case that the attacker is able to exploit some trigger channels. In our attacks, this can also be achieved, considering the attacker can control Echo and use it to further trigger smart devices, which would then activate some Alexa-related IFTTT Applets.

8. Conclusion

Echo is one of the first always ready, voice controlled intelligent home appliances that connect to the social and IoT services. Based on Amazon's cloud-based voice service, Amazon provides a collection of APIs and tools such as ASK (Alexa Skills Kit), which allows third-party developers to build new functions into the Amazon Echo. Designers, developers, and brands can build engaging skills and reach millions of customers with ASK. So that Alexa can hear, comprehend, and resolve questions or commands. Besides, IFTTT Applets enrich the skills of Alexa tremendously. However, as people trust and enjoy the convenient voice control of Alexa skills via Echo, Echo dot and etc., unpredictable potential risks may be taken advantaged by injecting voice control commands to take over Echo, so that the attacker can process social network and control IoT devices stealing the owner's sensitive information, threatening his property even lives safety.

We reveal and implement the MUTAE attacks based on HackRF One, which can to inject voice commands to control Echo remotely. Moreover, We have further analyzed the impact of MUTAE attacks for IoT and social network services according to kinds of important skills. We propose to add voice pattern and answering questions as a two-factor authentication, to prevent the MUTAE attack and other potential replay MUTAE attack. Besides, we also suggest that Alexa and IFTTT platform provide a security vetting automatically based on the usage context.

Acknowledgments

IIE authors are supported in part by National Key R&D Program of China (No.2016QY04W0805), NSFC U1836211, National Top-notch Youth Talents Program of China, Youth Innovation Promotion Association CAS, Beijing Nova Program, Beijing Natural Science Foundation (No.JQ18011), National Frontier Science and Technology Innovation Project (No. YJKYYQ20170070).

References

[1] *Hacking the Samsung NX300 'Smart' Camera*. https://op-co.de/blog/posts/hacking_the_nx300/.

[2] *Listen Up: Your AI Assistant Goes Crazy For NPR Too*. http://www.npr.org/2016/03/06/469383361/listen-up-yourai-assistant-goes-crazy-for-npr-too/.

[3] *Morgan Stanley says Amazon has sold more than 11 million Echo devices*. http://www.seattletimes.com/business/amazon/amazon-has-sold-more-than-11-million-echo-devices-morgan-stanley-says/.

[4] *Belkin Wemo Home Automation devices contain multiple vulnerabilities*, 2017. http://www.kb.cert.org/vuls/id/656302.

[5] *CVE-2017-9765*, 2017. https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-9765.

[6] *Vulnerability Details : CVE-2017-9212*, 2017. https://www.cvedetails.com/cve/CVE-2017-9212/.

[7] Hadi Abdullah, Washington Garcia, Christian Peeters, Patrick Traynor, Kevin RB Butler, and Joseph Wilson. Practical hidden voice attacks against speech and speaker recognition systems. *Network and Distributed Systems Security (NDSS) Symposium*, 2019.

[8] VS Abhayawardhana, IJ Wassell, D Crosby, MP Sellars, and MG Brown. Comparison of empirical propagation path loss models for fixed wireless access systems. In *2005 IEEE 61st Vehicular Technology Conference*, volume 1, pages 73–77. IEEE, 2005.

[9] Tripwire Guest Authors. *My SecTor Story: Root Shell on the Belkin Wemo Switch*, 2015. https://www.tripwire.com/state-of-security/featured/my-sector-story-root-shell-on-the-belkin-wemo-switch/.

[10] Mossab Baloul, Estelle Cherrier, and Christophe Rosenberger. Challenge-based speaker recognition for mobile authentication. In *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the*, pages 1–7. IEEE, 2012.

[11] Ian Barker. *HomeHack vulnerability could allow your LG robot vacuum to spy on you*, 2017. https://betanews.com/2017/10/26/lg-hom-bot-homehack-vulnerability/.

[12] Mark Barnes. *A new hack can turn an Echo into a live microphone*, 2017. https://www.theverge.com/2017/8/1/16079044/amazon-echo-hack-microphone-listen-in-mark-barnes.

[13] Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2ma: Verifying voice commands via two microphone authentication. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 89–100. ACM, 2018.

[14] Logan Blue, Luis Vargas, and Patrick Traynor. Hello, is it me you're looking for?: Differentiating between human and electronic speakers for voice interface security. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 123–133. ACM, 2018.

[15] Rudolf Maarten Bolle, Sharon Louise Nunes, Sharathchandra Pankanti, Nalini Kanta Ratha, Barton Allen Smith, and Thomas Guthrie Zimmerman. Method for biometric-based authentication in wireless communication for access control, November 16 2004. US Patent 6,819,219.

[16] Nicholas Carlini, Pratyush Mishra, Tavish Vaidya, Yuankai Zhang, Micah Sherr, Clay Shields, David Wagner, and Wenchao Zhou. Hidden voice commands. In *USENIX Security Symposium*, pages 513–530, 2016.

[17] Nicholas Carlini and David Wagner. Audio adversarial examples: Targeted attacks on speech-to-text. *arXiv preprint arXiv:1801.01944*, 2018.

[18] Catalin Cimpanu. *WikiLeaks Claims CIA Could Turn Samsung Smart TVs Into Listening Devices*, 2017. https://www.bleepingcomputer.com/news/hardware/wikileaks-claims-cia-could-turn-samsung-smart-tvs-into-listening-devices/.

[19] Lucian Constantin. *Researchers Find Vulnerability in Smart Home Control Apps*, 2017. https://motherboard.vice.com/en_us/article/pak3zg/wink-hub-insteon-hub-hacks.

[20] Amitava Das, Ohil K Manyam, Makarand Tapaswi, and Veeresh Taranalli. Multilingual spoken-password based user authentication in emerging economies using cellular phone networks. In *Spoken Language Technology Workshop, 2008. SLT 2008. IEEE*, pages 5–8. IEEE, 2008.

[21] Luigi De Russis and Fulvio Corno. Homerules: A tangible end-user programming interface for smart homes. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, pages 2109–2114. ACM, 2015.

[22] CVE Details. *Heap-based buffer overflow in IrfanView before 4.32*, 2012. http://www.cvedetails.com/cve/CVE-2011-5233/.

[23] Wenrui Diao, Xiangyu Liu, Zhe Zhou, and Kehuan Zhang. Your voice assistant is mine: How to abuse speakers to steal information and control your phone. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, pages 63–74. ACM, 2014.

[24] Adi Shamir Eyal Ronen. Extended functionality attacks on iot devices: The case of smart lights. In *2016 IEEE European Symposium on Security and Privacy*, pages 1–12. 2016 EuroSP, 2016.

[25] Huan Feng, Kassem Fawaz, and Kang G Shin. Continuous authentication for voice assistants. *arXiv preprint arXiv:1701.04507*, 2017.

[26] Geoffrey Hinton, Li Deng, Dong Yu, George E Dahl, Abdel-rahman Mohamed, Navdeep Jaitly, Andrew Senior, Vincent Vanhoucke, Patrick Nguyen, Tara N Sainath, et al. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. *IEEE Signal Processing Magazine*, 29(6):82–97, 2012.

[27] Dr. Shankar Banik Ike Clinton, Lance Cook. *A Survey of Various Methods for Analyzing the Amazon Echo*, 2016. https://vanderpot.com/Clinton_Cook_Paper.pdf.

[28] ISACA. *Alexa, Can You Hear Me? Demystifying the Amazon Echo Through Theoretical Bug Hunting*, 2016. http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/alexa-can-you-hear-me.aspx.

[29] Yeongjin Jang, Chengyu Song, Simon P Chung, Tielei Wang, and Wenke Lee. A11y attacks: Exploiting accessibility in operating systems. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–115. ACM, 2014.

[30] Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Z Morley Mao, Atul Prakash, and Shanghai JiaoTong Unviersity. Contexiot: Towards providing contextual integrity to appified iot platforms. In *Proceedings of The Network and Distributed System Security Symposium*, volume 2017, 2017.

[31] Chaouki Kasmi and Jose Lopes Esteves. "iemi threats for information security: Remote command injection on modern smartphones". *IEEE Transactions on Electromagnetic Compatibility*, 57(6):1752–1755, 2015.

[32] Swati Khandelwal. *Bluetooth Hack Affects 20 Million Amazon Echo and Google Home Devices*, 2017. https://thehackernews.com/2017/11/amazon-alexa-hacking-bluetooth.html.

[33] David Lodge. *Steal your Wi-Fi key from your doorbell?*, 2016. https://www.pentestpartners.com/security-blog/steal-your-wi-fi-key-from-your-doorbell-iot-wtf/.

[34] Guaranty Media. *95 percents OF US HOUSEHOLDS HAVE AT LEAST ONE RADIO RECEIVER*, 2017. http://guarantymedia.com/95-of-u-s-households-have-at-least-one-broadcast-radio-receiver/.

[35] Mitre. *CVE-2017-9765 Detail*, 2017. https://nvd.nist.gov/vuln/detail/CVE-2017-9765.

[36] Nicole Casal Moore. *Hacking into homes: 'Smart home' security flaws found in popular system*, 2016. http://ns.umich.edu/new/multimedia/videos/23748-hacking-into-homes-smart-home-security-flaws-found-in-popular-system.

[37] Mike Newton. *gSOAP remote code execution*, 2017. https://netvu.org.uk/is-the-gsoap-vulnerability-really-a-surprise/.

[38] Pierluigi Paganini. *Flaws in BMW ConnectedDrive Infotainment System allow remote hack*, 2016. http://securityaffairs.co/wordpress/49149/hacking/bmw-connecteddrive-hacking.html.

[39] Sheng-Lung Peng, Souvik Pal, and Lianfen Huang. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. Springer, 2020.

[40] Zinaida Benenson Philipp Morgner, Stephan Mattejat. All your bulbs are belong to us: Investigating the current state of security in connected lighting systems. pages 1–13, 2016.

[41] Ian Poole. *Radio Signal Path Loss*. http://www.radio-electronics.com/info/propagation/path-loss/rf-signal-loss-tutorial.php.

[42] Dikla Barda Roman Zaikin and Oded Vanunu. *HomeHack: How Hackers Could Have Taken Control of LG's IoT Home Appliances*, 2017. https://blog.checkpoint.com/2017/10/26/homehack-how-hackers-could-have-taken-control-of-lgs-iot-home-appliances/.

[43] Rafael Scheel. *Smart TV Hacking (Oneconsult Talk at EBU Media Cyber Security Seminar)*, 2017. https://www.youtube.com/watch?v=b0J_8QHX60A.

[44] Lea Schönherr, Katharina Kohls, Steffen Zeiler, Thorsten Holz, and Dorothea Kolossa. Adversarial attacks against automatic speech recognition systems via psychoacoustic hiding. *Network and Distributed Systems Security (NDSS) Symposium*, 2019.

[45] Bob Sorokanich. *Researcher: BMW, Mercedes Vulnerable to Remote-Unlocking Hack*, 2015. https://blog.caranddriver.com/researcher-bmw-mercedes-vulnerable-to-remote-unlocking-hack/.

[46] Milijana Surbatovich, Jassim Aljuraidan, Lujo Bauer, Anupam Das, and Limin Jia. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of ifttt recipes. In *Proceedings of the 26th International Conference on World Wide Web*, pages 1501–1510. International World Wide Web Conferences Steering Committee, 2017.

[47] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199*, 2013.

[48] Kazuki Tada, Shin Takahashi, and Buntarou Shizuki. Smart home cards: tangible programming with paper cards. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pages 381–384. ACM, 2016.

[49] Scott Tenaglia. *Breaking BHAD: Abusing Belkin Home Automation Devices*, 2016. https://www.blackhat.com/docs/eu-16/materials/eu-16-Tenaglia-Breaking-Bhad-Abusing-Belkin-Home-Automation-Devices.pdf.

[50] Iain Thomson. *Backdooring the Frontdoor Hacking a perfectly secure smart lock*, 2016. https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Jmaxxz-Backdooring-the-Frontdoor-UPDATED.pdf.

[51] Blase Ur, Elyse McManus, Melwyn Pak Yong Ho, and Michael L Littman. Practical trigger-action programming in the smart home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 803–812. ACM, 2014.

[52] Tavish Vaidya, Yuankai Zhang, Micah Sherr, and Clay Shields. Cocaine noodles: exploiting the gap between human and machine speech recognition. *Presented at WOOT*, 15:10–11, 2015.

[53] Mathy Vanhoef. *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*, 2017. https://papers.mathyvanhoef.com/ccs2017.pdf.

[54] Vijay. *Hackers can spy on what you say by hacking Sony made Android TVs*, 2016. https://www.techworm.net/2016/05/hackers-can-spy-say-hacking-sony-made-android-tvs.html.

[55] Xuejing Yuan, Yuxuan Chen, Aohui Wang, Kai Chen, Shengzhi Zhang, Heqing Huang, and Ian M Molloy. All your alexa are belong to us: A remote voice control attack against echo. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2018.

[56] Xuejing Yuan, Yuxuan Chen, Yue Zhao, Yunhui Long, Xiaokang Liu, Kai Chen, Shengzhi Zhang, Heqing Huang, Xiaofeng Wang, and Carl A Gunter. Commandersong: A systematic approach for practical adversarial voice recognition. *USENIX Security 2018*, 2018.

[57] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–117. ACM, 2017.

[58] Steve Zurier. *Wemo IoT Vulnerability Lets Attackers Run Code On Android Phone*, 2016. https://www.darkreading.com/iot/wemo-iot-vulnerability-lets-attackers-run-code-on-android-phone-/d/d-id/1327362?