IoT Device Security

Locking Out Risks and Threats to Smart Homes

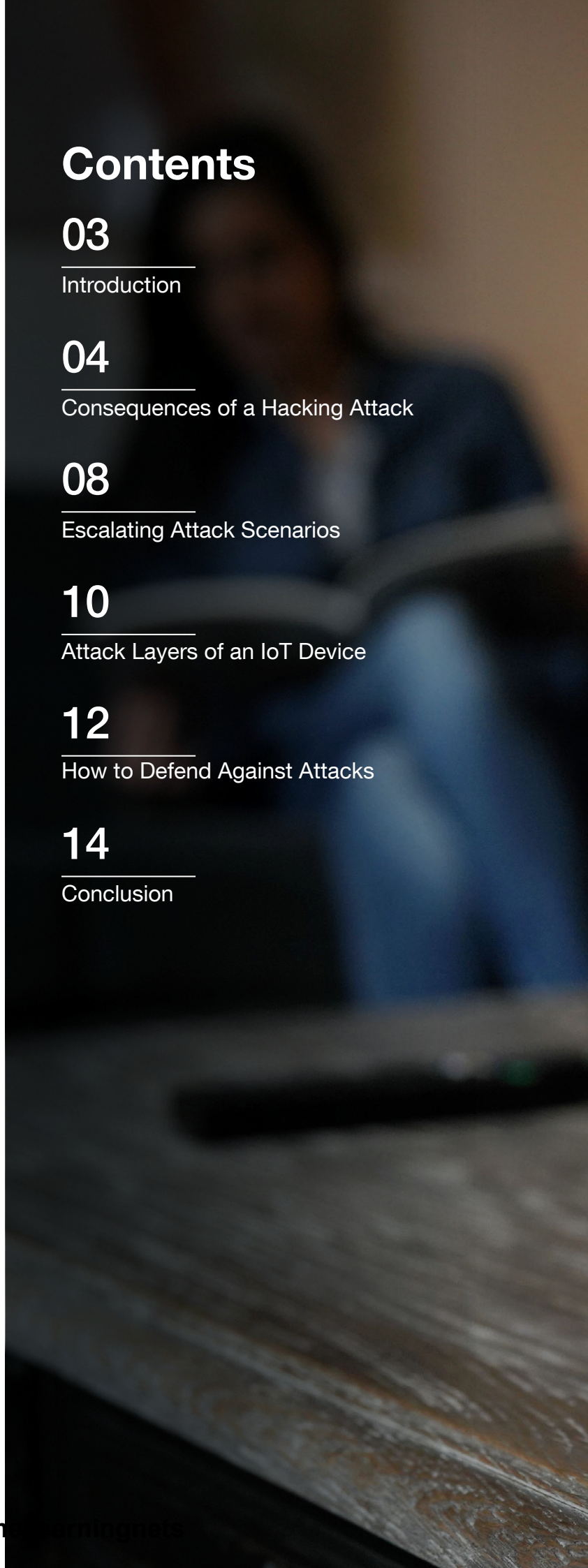
Ziv Chang

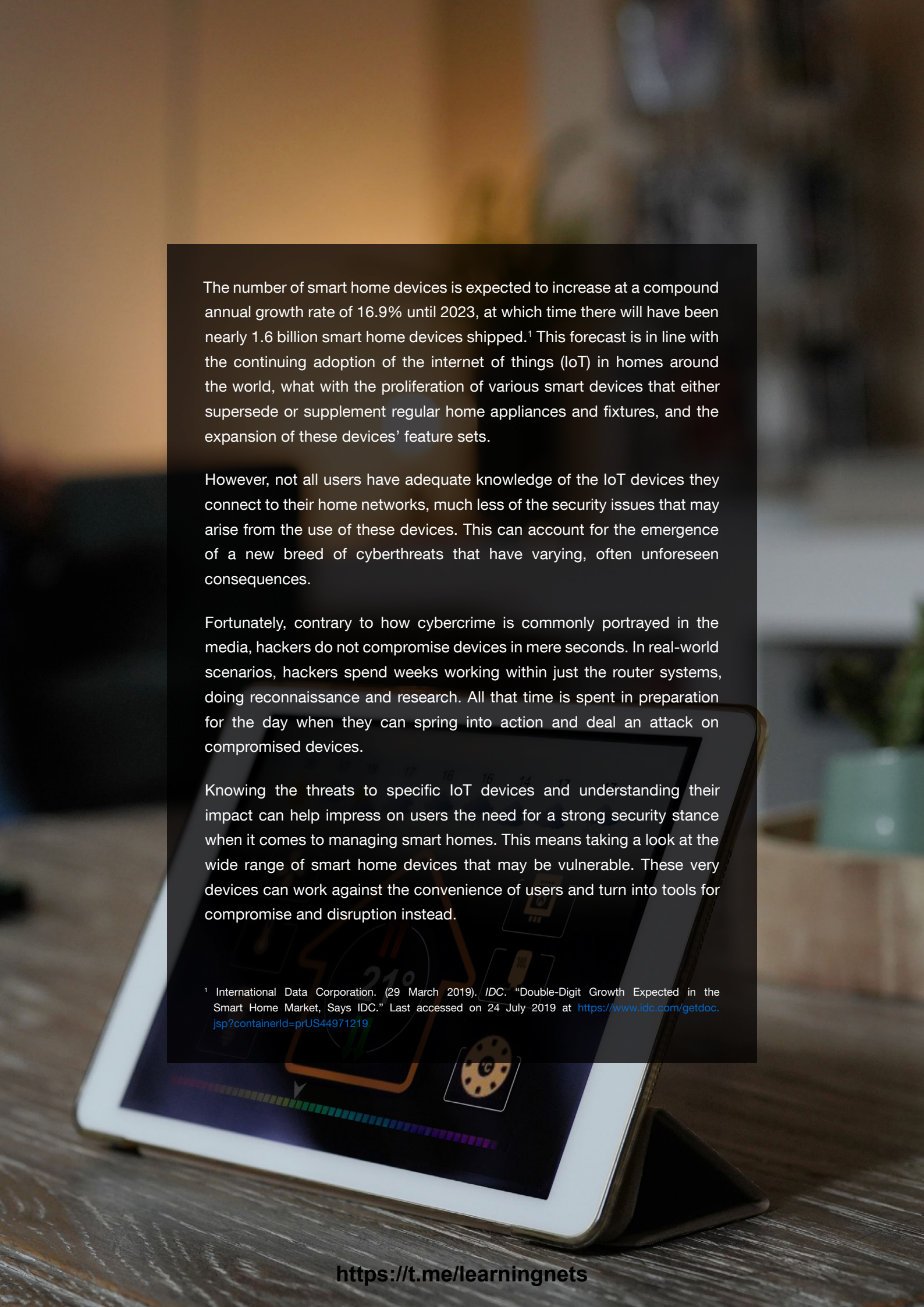
TREND MICRO | research

Published by
Trend Micro Research

Written by
Ziv Chang

Contents





The number of smart home devices is expected to increase at a compound annual growth rate of 16.9% until 2023, at which time there will have been nearly 1.6 billion smart home devices shipped.[1] This forecast is in line with the continuing adoption of the internet of things (IoT) in homes around the world, what with the proliferation of various smart devices that either supersede or supplement regular home appliances and fixtures, and the expansion of these devices' feature sets.

However, not all users have adequate knowledge of the IoT devices they connect to their home networks, much less of the security issues that may arise from the use of these devices. This can account for the emergence of a new breed of cyberthreats that have varying, often unforeseen consequences.

Fortunately, contrary to how cybercrime is commonly portrayed in the media, hackers do not compromise devices in mere seconds. In real-world scenarios, hackers spend weeks working within just the router systems, doing reconnaissance and research. All that time is spent in preparation for the day when they can spring into action and deal an attack on compromised devices.

Knowing the threats to specific IoT devices and understanding their impact can help impress on users the need for a strong security stance when it comes to managing smart homes. This means taking a look at the wide range of smart home devices that may be vulnerable. These very devices can work against the convenience of users and turn into tools for compromise and disruption instead.

[1] International Data Corporation. (29 March 2019). *IDC*. "Double-Digit Growth Expected in the Smart Home Market, Says IDC." Last accessed on 24 July 2019 at https://www.idc.com/getdoc.jsp?containerId=prUS44971219

Consequences of a Hacking Attack

To illustrate the security issues present in smart homes, in Figure 1 and Table 1, we highlight several common yet potentially vulnerable smart devices along with their functions, and give examples of how hackers can use these devices, if successfully compromised, in attacks.

Figure 1. Visualization of a smart home with potentially vulnerable IoT devices

Device	Functions	Actions hackers can take once compromised
Smart refrigerator	• Send out order for groceries through the internet when supplies are low • Suggest recipes based on available ingredients • Set expiration dates and display notifications for users to consume the food while it's still fresh • Create grocery lists that sync with users' mobile devices (e.g., smartphones or tablets) in real time • Function as the message board where users can leave notes for other residents • Connect to a smart TV in another room so users can watch shows from the kitchen	• Order as much grocery as possible from the refrigerator • Ruin food in the refrigerator by turning the temperature up to as high as possible • Modify set expiration dates to always indicate that the food in the refrigerator is fresh
Smart toilet	• Allow remote-controlled water temperature and pressure to meet user preference • Clean itself • Eliminate odor and freshen air • Save water by sensing the right amount needed for flushing waste • Notify users when needed supplies are low (e.g., toilet paper and air freshener)	• Turn the water on and leave it flowing • Raise and lower the smart toilet's lid remotely • Operate the bidet and flush nozzles remotely
Smart toy	• Interact with its players in an educational manner • Base its actions on environmental stimuli • Function on remote-controlled commands from parents • Provide remote video and audio access for parents • Allow a wider range of actions should its install scripts be removed	• Record the voices of the toy's players and leak the recordings online • Communicate with the toy's players • Scare or distress the toy's players by controlling or destroying the toy • Play loud sounds remotely through the toy • Infiltrate the home network through the smart toy • Find the location of the house • Use the toy as an entry point for other attacks

Device	Functions	Actions hackers can take once compromised
Smart robot vacuum cleaner	• Conduct automatic and scheduled cleaning • Provide several cleaning modes for users to choose from, such as wet mopping and dry sweeping • Take anti-twining and anti-dropping maneuvers • Map the home's layout automatically • Recharge automatically when low on power	• Steal the home layout • Monitor room activities remotely • Attack users or residents using the vacuum's stored water • Dirty the home by deliberately creating a mess
Smart lock	• Lock and unlock through a simple icon tap on a mobile device or web interface • Unlock even without a physical key • Record permanent and temporary users and set access schedules for specified days and times • Turn on forced entry alarms to warn users of possible break-ins • Automatically lock after being unlocked for a specified period of time	• Unlock for intruders to enter the home or facility • Lock out users or residents and block the house remotely • Change the lock password remotely • Turn on the alarm when no break-in or intrusion occurred
Smart bulb	• Be controllable by a mobile app or a virtual assistant • Let users select from various lighting colors • Turn on or off as scheduled	• Turn the light on or off at unpredictable times • Turn all of the lights on in the home or facility to overload the power system • Flash lights as quickly as possible to blind people or cause seizures in people with photosensitive epilepsy
Smart coffee machine	• Brew coffee based on a set timer or remote command • Brew higher-quality coffee while giving users more control over the process • Be controllable and configurable through mobile apps	• Disrupt the brewing process • Stop the machine's function completely • Brew coffee continuously even when there are no more coffee beans loaded in the machine
Smartwatch	• Monitor the user's heart rate • Track the user's activity • Send out reminders and alarms • Provide a fitness tracker • Allow users to reply to messages and receive calls from a paired mobile phone	• Spoof the user's smartphone from the smartwatch • Steal the user's health data • Send fake text messages from the smartwatch

Device	Functions	Actions hackers can take once compromised
Home gateway	• Serve as the entry point to the internet • Connect devices through Wi-Fi or other wireless protocols • Perform device control • Provide gateway functions like WAN-to-LAN bridging, Network Address Translation (NAT), IPv4 and IPv6 forwarding, wireless access point (WAP) management, and Voice over IP (VoIP) processing	• Connect to a fake or malicious URL to download malware • Steal credentials or personally identifiable information (PII) through the gateway • Control connected devices remotely from the gateway by either disabling device functions or meddling with them • Block or modify connections to redirect them toward hidden malicious behaviors
Voice-activated home automation device	• Reduce human effort and errors, thus increasing efficiency • Turn devices on or off based on voice commands • Run tasks based on an AI-enabled voice recognition system • Provide the connected virtual assistant data when commanded by its user	• Play voice commands at strategic times to cause inconvenience for residents or users, like “brew coffee at 3 a.m.” or “turn on all lights at 4 a.m.” • Order unwanted stocks by voice commands • Steal voice data as credentials for use in other voice command systems

Table 1. Common smart home devices, their functions, and possible attacks against them once compromised

Escalating Attack Scenarios

Individually many of the attacks mentioned above can be overlooked as harmless by many users. However, once a device or system has been compromised, hackers can strategize and formulate a combination of actions to escalate their attacks in hopes of exacting direr consequences. We illustrate this point by describing two scenarios that can result from a compromised smart robot vacuum cleaner within a smart home.

Thinking that the device is connected only to the home network, the owner of the smart home does not fear exposure through the smart robot vacuum cleaner. In truth, however, the vacuum's Universal Plug and Play (UPnP) function automatically connects to the home router, thereby exposing it to the internet. With no security measures in place against such an exposure, attackers are free to compromise the device as part of their campaign.

Once the vacuum is compromised, at the outset the hackers use the device to familiarize themselves with the layout of the house, and then they move laterally to compromise other devices in the network. Using a combination of different possible actions and compromised devices inside the home, the hackers can strategize and plan a number of different attacks, two of which we detail below.

Break-in

The hackers can monitor residents using IP cameras installed in the house. By making a smart toy act up, the hackers can lure residents into a room or away from their planned entry point. The hackers will then open the necessary smart locks to let an intruder or accomplice in, while turning off the alarm system to avoid alerting the residents and the authorities. While the intruder is inside the house, the hackers can take the extra measure of turning off smart bulbs to hide the intruder in the shadows. Once the intruder is out, the hackers can control the smart locks to lock in residents and subsequently allow the intruder to evade a chase or delay the residents from taking action.

Espionage

Hackers can opt to carry out a campaign where the end goal is the prolonged monitoring or surveillance of a home. Once the hackers have gained control over many, if not all, of the devices inside the house, they can begin to very intimately cyberstalk the residents.

The hackers can access the residents' real-time locations, through devices such as the smart robot vacuum cleaner or a smartwatch. They can also record the residents' activities through photos or videos; they can do so mainly using the IP cameras installed in the smart home, with other devices that are equipped with cameras and microphones, like smart toys, also at their disposal for this task. Using voice-activated devices, the hackers can listen to and even record conversations inside the home. They can even go as far as monitoring food preferences and shopping lists using the smart refrigerator and home gateway, should this information prove useful.

As made apparent in this second scenario, even without a physical break-in, the silent monitoring and surveillance of hackers is no less intrusive because of the rich information these devices are privy to.

Other attack scenarios

In addition to gathering sensitive information, accessing restricted areas, performing lateral movement within the network, and spying on victims, common actions and end goals that hackers can incorporate into their campaigns to compromise smart homes include:

- Gain monetary profit
- Create a hub for cryptocurrency mining
- Carry out denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Create a botnet
- Steal PII or financial credentials
- Destroy connected devices
- Cause chaos and destruction inside homes
- Mislead victims by making devices send or display wrong information
- Trigger false alarms

Attack Layers of an IoT Device

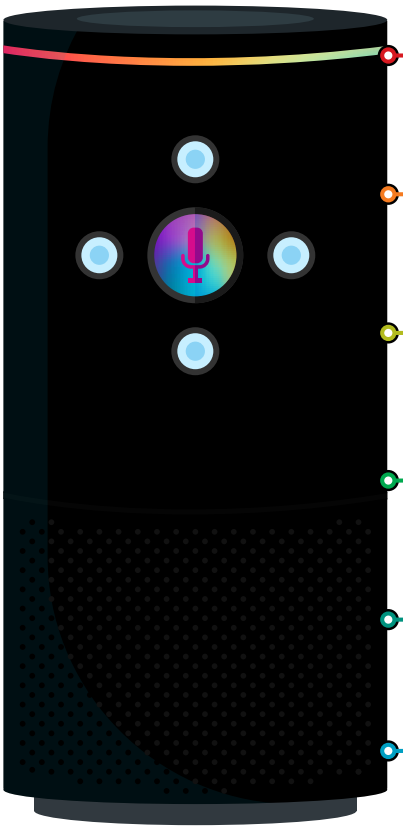
What makes it possible for hackers to compromise IoT devices in the first place? One factor is that security has not been present from the design phase of many IoT devices in the market. Another is the poor configuration of many online devices, which may be set up according to the users' convenience rather than for the sake of security. The lack of security by design can lead to more vulnerabilities and poor configuration can lead to weak security credentials. The persistence of these two factors exacerbates the problem, especially since many hackers are determined to find vulnerabilities from all possible angles.

Hackers can begin from the deepest layer of an IoT device, the physical motherboard. There they can find the hardware debug port or communication port, e.g., JTAG UART, I2C, and SPI. From there, they can search for hard-coded passwords, hidden backdoors, and vulnerabilities in its dumped firmware.

They can also look for entry points in the form of operating system and application bugs. And they can go to the web interface of the device to look for web bugs.

Further, they can try looking for vulnerabilities in communication protocols, such as Bluetooth, Zigbee, Z-Wave, NFC, 4G, 5G, and IEEE 802.1x. Hackers can also go for the policies, which may contain sensitive information or hold settings that may expose the device outside the home network.

We summarize the different attack layers of an IoT device in Figure 2.



Attack layer	Security issues	Risks
Hardware	› Ease in being dismantled and further examined › Existing debug port	› Hackers can connect to the JTAG UART, I2C, and SPI of the system without any security limitations.
Firmware	› Credential issues › Backdoor issues › Unpatched firmware › Buffer overflow issues › Privilege escalation	› Hackers can use the default and hard-coded passwords in the firmware. › Hackers can easily predict these passwords and access the system easily.
Operating system and application	› Unpatched operating system › Buffer overflow issues › Privilege escalation › Possibility of man-in-the-middle (MitM) attacks	› Buffer overflow (stack, heap, and integer) can allow hackers to gain privilege or control over the system.
Web interface	› SQL injection › Directory traversal › Buffer overflow issues › Cross-site scripting (XSS) › Cross-site request forgery (CSRF) › Use of default or sample pages › Privilege escalation issues › Other OWASP issues	› Hackers can gain access to the system without the need for a password. › Hackers can get information that the web interface should not provide (e.g., internal IP address, system structure, directory name, and database configuration).
Protocol	› DoS or DDoS › Session hijacking › Authentication bypass › Media access control (MAC) spoofing attacks › PIN cracking attacks › MitM attacks › Hard-coded key attacks › Replay attacks	› Hackers can disable the device function by flooding the connection bandwidth. › Hackers can initiate hijacking sessions to send forged data. › Hackers can steal data or credentials through MitM attacks. › Hackers can replay stolen data to bypass authentication.
Policy	› Misconfigured policies › Policy violations	› Hackers can leak sensitive data, such as credentials, connection strings, IP addresses, and internal network topology. › Hackers can gain unlimited access to the system. › Unknown exposure outside the network through settings like enabled UPnP in devices.[2]

Figure 2. The attack layers of an IoT device and their security issues and risks

[2] Tony Yang. (6 March 2019). *Trend Micro Security Intelligence Blog*. "UPnP-enabled Connected Devices in the Home and Unpatched Known Vulnerabilities." Last accessed on 24 July 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/upnp-enabled-connected-devices-in-home-unpatched-known-vulnerabilities/.

How to Defend Against Attacks

That these attacks are possible within the confines of the home makes it critical to secure IoT devices against them. With that in mind, we list some questions for users to consider along with corresponding pointers to help improve the security of smart homes.

1. What devices are used in the smart home?

The first thing users must do is to map all their devices. From there users can evaluate the security risks their home may face, based on the full list of connected devices.

2. How many are vulnerable devices?

Answering this question is a form of vulnerability scanning. Having made a list of their smart home devices, users can begin to evaluate the number of known vulnerabilities each device may have using a security scanner app. They can also look up vulnerabilities in the Common Vulnerabilities and Exposures (CVE) database using the device names and versions. This information can help in evaluating the security scores and severity ratings of the vulnerabilities that the users are facing. Creating a list with the vulnerabilities, CVE information, device names, and versions can be a good reference for users.

3. What vulnerable devices can be patched easily?

Users can refer to the list they have created to find and download the needed patches from the respective device vendors' official websites. This step is called vulnerability management. At this point, users should have some idea of the risks against their home security environment.

4. How much information do the users hold?

To truly answer this question, users must take a deeper look into their devices, which means reading device manuals and checking the settings of each device. Although the information gathered by this point is significant, it is not enough to fully evaluate the home environment's security risks. This is because users do not yet know the configuration of the device, including its security credentials. Users should now study each device manually and carefully, even consulting the device's package and manual. They should note and heed all the warning messages, if any. They should also change all default passwords and configurations to more secure ones.

5. How many devices can be protected using a security gateway?

Patching a device can cause problems in some cases. A patch can cause a device to brick or fail to perform its original functions. A good option is to conduct a virtual patch from the gateway. This means that users will not need to patch the actual device, but rather block attacks from the gateway.

6. How much time will be needed to replace or remove risky devices?

At this point, users should have all the information they need to know the full security risks their home faces. The next step is evaluating the time they will need to replace or retire the vulnerable devices that cannot be patched or protected anymore. This evaluation is the beginning of a process called risk management.

7. What should users do?

Based on the information the users have gathered from the questions above, they should be able to determine the weak points of their home and think of possible solutions. We simplify these steps into three.

- **Patch vulnerabilities.** Timely patches and firmware updates are two initial actions users can take, since updates are usually related to security issues. Users can opt to enable the auto-update feature on supported devices to ensure that updates are applied as soon as they become available.
- **Change default settings and passwords.** When users go through the settings of their devices one by one, they can take the opportunity to make necessary modifications to make the devices more secure. They should change default or easy-to-guess passwords immediately, and use unique and strong passwords for multiple accounts. In setting up the devices, users should avoid using PII, especially with the router settings.
- **Isolate devices.** Users should also consider implementing network segmentation for certain devices and isolating them from the entire home network. This is especially needed for vulnerable devices that cannot be patched and yet cannot be replaced or removed by users for whatever reason.

Users can also consider using security solutions that can help them identify and defend against the threats their smart homes may encounter. The Trend Micro™ HouseCall™ for Home Networks tool, for instance, scans home networks for vulnerabilities and suggests ways to deal with them,[3] thereby helping address several of the questions above.

[3] Trend Micro. (n.d.). *Trend Micro*. "HouseCall™ for Home Networks." Last accessed on 24 July 2019 at https://www.trendmicro.com/en_us/forHome/products/housecall/home-networks.html

Conclusion

People living in smart homes should know their homes better than anyone, which in this context means being knowledgeable of all of the devices inside their homes. They should also be able to identify the normal baseline of their devices' network traffic to better monitor for aberrant behavior that can be a sign of a rogue network. Just as the users should be knowledgeable about their implemented devices, home security should aid in this visibility and be transparent to the users.

At the same time, knowing what hackers are capable of doing can help in estimating possible risks and losses from an attack. Ignoring the risks of a hacker attack can lead to disastrous consequences that users may be ill-equipped to mitigate.

As more smart home devices hit the market, the smart home attack surface gets wider. Fortunately, users can adopt a number of measures, such as the ones recommended here, to avoid risks and stay secure inside their smart homes. The ideal smart home security is that which does not impede the availability and functionality of devices, but rather allow users to reap the benefits of the IoT without compromising their security.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research