CYBERSECURITY CONSIDERATIONS FOR CONNECTED SMART HOME SYSTEMS AND DEVICES

EXECUTIVE SUMMARY

The concept of the "Internet of Things" (IoT) is no longer the stuff of science fiction but an essential part of the reality of our everyday lives. Today, there are more than 13 billion interconnected digital and electronic devices in operation globally, the equivalent of more than two devices for every human on earth.[1] One of the most common examples of IoT in action include technologies and applications intended to support the deployment of so-called "smart home" systems and devices. Indeed, a brief visit to any technology retailer will reveal the scope and breadth of IoT-based smart home devices already on the market, such as programmable appliances, thermostats and lighting controls.

But the widespread use of connected smart home devices and systems has also provided an attractive platform for targeted cyberattacks by hackers and other unscrupulous operators. In one of the most recent high-profile examples, the operation of a New Hampshire-based internet domain name system company was overrun by millions of requests originating from security cameras, digital video recorders and other connected smart home devices manufactured by a company located halfway around the world. The attacks, which were orchestrated by an outside perpetrator, resulted in the temporary denial of service for many users of Twitter, Spotify, Netflix, Amazon and other social media sites and online retailers across the northeastern seaboard of the United States.[2]

This UL white paper explores the issue of cyberthreats originating from or impacting connected smart home systems and devices, and discusses the steps that smart home device manufacturers can take to reduce the risk to both device users and others. Beginning with a brief overview of the IoT and the application of smart home technologies, the white paper then discusses the key cyber vulnerabilities in the design and implementation of connected smart home systems and devices, and offers specific recommendations that can help device manufacturers achieve effective, foundational cybersecurity hygiene. The white paper concludes with information on UL's unique approach to addressing cybersecurity vulnerabilities in smart home systems and connected devices of all types.

WHAT IS THE "INTERNET OF THINGS"?

Although there is little consensus regarding a specific definition, the "Internet of Things" generally refers to the multiple networks of devices ("things") that communicate with each other via wired and wireless protocols and without direct human interaction. IoT-enabled devices can help to facilitate the rapid and efficient transfer of data used to support a wide range of activities and operations. The application of IoT technologies is expected to result in significant operational improvements, such as increased efficiency, better performance and enhanced safety.

Many think of the IoT as a single global network. But the IoT actually encompasses a multitude of independent but complementary networks in various service sectors, such as:

- **Efficient energy production and distribution (so-called "smart grids")**
- **Machine-to-machine (M2M) and other industrial and manufacturing controls**
- **Vehicular traffic and transportation management**
- **Health and healthcare services**
- **Public safety**

In fact, technology research and consulting firm Beecham Research has identified nine different IoT service sectors and 29 separate applications for current and potential IoT development or expansion. [3]

The anticipated application of IoT technologies is reflected in projections of future IoT market revenue and growth. IDC Research estimates that the global market value for IoT products and devices will reach $737 billion (USD) in 2017, and will increase to $1.29 trillion by the year 2020, a compound annual growth rate (CAGR) of 15.6 percent.[4] A separate projection from advisory firm Gartner, Inc. indicates that the number IoT-connected devices will increase from around 5 billion in 2015 to more than 20 billion by 2020.[5]

These and other projections unmistakably signal the increased adoption of IoT technologies in a wide range of applications and their broad acceptance by buyers and consumers alike. Clearly, leveraging the growth potential of the IoT is likely to be an essential element of the strategy of technology companies in the years to come.

THE IOT AND SMART HOME APPLICATIONS

Like IoT, the term smart home has been widely but inconsistently used. However, in an effort to standardize the meaning of the term in the residential real estate market, Coldwell Banker Real Estate, working in conjunction with technology news source CNET, has defined a smart home as:

"A HOME THAT IS EQUIPPED WITH NETWORK-CONNECTED PRODUCTS (AKA "SMART PRODUCTS") CONNECTED VIA WI-FI, BLUETOOTH® OR SIMILAR PROTOCOLS) FOR CONTROLLING, AUTOMATING AND OPTIMIZING FUNCTIONS SUCH AS TEMPERATURE, LIGHTING, SECURITY, SAFETY OR ENTERTAINMENT, EITHER REMOTELY BY A PHONE, TABLET, COMPUTER OR A SEPARATE SYSTEM WITHIN THE HOME ITSELF."[6]

While there are probably thousands of different IoT smart home devices and applications currently on the market, they typically fall under one of the following categories:

- **ENTERTAINMENT**

  Smart entertainment applications provide on-demand, wireless access to video and audio feeds from conventional broadcast channels, the Internet and enabled storage devices. Smart devices in this category include smart televisions and recording devices, network connection devices and program streaming services.

- **SURVEILLANCE AND SECURITY**

  Smart surveillance and security applications address issues related to the safety of a home and its occupants. Smart devices in this category include smart fire/carbon monoxide detectors, smart door locks and access controls, networked security cameras and monitoring systems, and smart nightlights.

- **ENERGY AND RESOURCE MANAGEMENT**

  Smart energy and resource management applications track and adjust consumption patterns of electricity, natural gas and water to increase efficiency. Smart devices in this category include smart thermostats and environmental controls, smart HVAC systems, smart household appliances and smart outdoor watering systems.

- **HOUSEHOLD MANAGEMENT**

  A number of smart home devices and applications are now available to assist in general household management tasks, such as monitoring available food supplies, compiling shopping lists, placing orders, etc.

- **LIGHTING**

  Smart lighting applications contribute to both energy and resource efficiency and security by monitoring both environmental conditions and actual use patterns. Smart devices in this category include smart lightbulbs and lighting systems.

- **HEALTH**

  Increasingly, smart health applications are expected to play a critical role in monitoring and protecting the health and well-being of a 21st century population. Smart devices in this category include smart monitors and wearable sensors that can track and report vital health indicators, as well as sudden movements indicative of a fall.

Juniper Research projects that spending on smart home devices and applications will reach $195 billion by the year 2021, more than double the projected $83 billion spend in 2017. This growth is expected to be driven by entertainment services, as well as expanded home automation hardware and subscription service offerings.[7] And an estimated 30 million households in the U.S. are expected to add smart home devices and applications during the coming year, as consumers seek the enhanced safety and convenience they provide.[8]

RECENT EXAMPLES OF SMART HOME CYBERSECURITY VULNERABILITIES

While the number of reported instances of malicious cyberattacks on smart home systems and devices are relatively small, university and industry researchers and cybersecurity experts are routinely uncovering vulnerabilities to cyber threats that could compromise consumer privacy, safety and security. Some recent examples include:

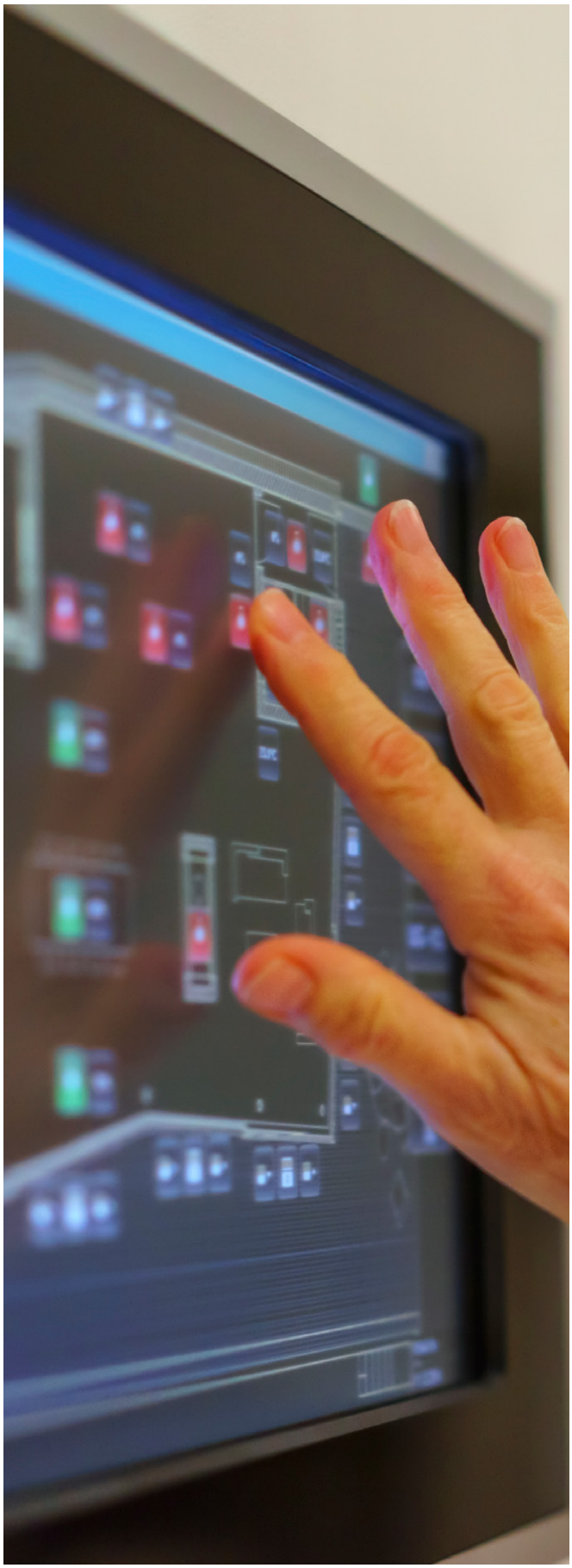
- In a platform-wide study of connected smart home systems, researchers at the University of Michigan were able to able to hack into a widely-available smart home automation system and successfully open electronic locks, change system pre-sets and remotely trigger a false fire alarm. [9]

- At a two-day hackathon sponsored by MIT's Media Lab, more than 150 hackers were tasked with exploiting weaknesses in more than 20 different smart home systems and devices. On the first day, hackers were successful in gaining control of 25 percent of targeted smart home devices in less than three hours. [10]

- Industry consultants identified nine separate security holes in a recently-introduced indoor and outdoor lighting system that would enable hackers to use the system's mobile application to access network configuration information and control the lights without authentication. [11]

- Long a subject of cyberthreats, internet-connected baby monitors remain vulnerable to hacking. In 2015, researchers evaluated nine separate models of baby monitors for security risk and found that only one model was sufficiently secure from a potential cyberattack. [12]

- Finally at DEF CON 24, the annual hacker convention, researchers reviewed their findings on the weaknesses of smart locks from a variety of manufacturers. They found that 12 out of 16 different Bluetooth-enabled smart locks had "insufficient Bluetooth low energy security," and were susceptible to cyberattack. [13]



CYBERSECURITY VULNERABILITIES RELATED TO CONNECTED SMART HOME DEVICES

As the above examples clearly illustrate, cybersecurity vulnerabilities in connected smart home systems and devices are most frequently caused by issues related to product design and implementation. The most common causes of cyber-related vulnerabilities generally fall into one of the following five areas:

- **POOR PRODUCT DESIGN**

  Despite widespread publicity around the cybersecurity threat to connected smart home systems and devices, many designs fail to integrate even basic security measures into the finished product, or fail to separate security functions from other functions. And few standards directly address cybersecurity of smart home systems.

- **NON-SECURE COMMUNICATIONS PROTOCOLS**

  The deployment of connected smart home systems and devices usually depends on local home area networks using Wi-Fi, Bluetooth or Near Field Communications (NFC) protocols. Even though these protocols may operate over relatively short distances, they are vulnerable to hacking from external sources.

- **INADEQUATE AUTHENTICATION PROCEDURES**

  Similarly, because smart home devices are designed to communicate over short distances, password and other authentication procedures may be insufficient. Factory-set passwords like “admin” or “user” contribute to the problem.

- **LIMITED SOFTWARE UPDATING/PATCHING**

  According to one estimate, 97 percent of cybersecurity incidents can be traced back to the failure to patch vulnerabilities in existing software or software applications.[14] The absence of regular system updates or software patches only increases the risk with the passage of time. The use of third party components, such as commercial off-the-shelf (COTS) or open source software, also presents supply chain security issues in which vendors may be unable to trace known vulnerabilities in source components.

- **IMPROPER IMPLEMENTATION OR DEVICE/APPLICATION USE**

  Finally, consumers who install smart home systems and devices may lack a sufficient understanding of device or network-related security considerations. Even the positioning of certain smart devices in the home network can make them more or less vulnerable to hacking. Implementation issues may arise even from simple configuration challenges that a security novice may be unable to address, for example, changing default security parameters such as keys and passwords.

PRINCIPLES FOR CYBERSECURITY OF THE IOT AND CONNECTED SMART HOME DEVICES

Since 2013, the U.S. Federal Government has been actively involved in efforts to help ensure the security of connected devices from cyberattack. The most recent effort in this area was the release in November 2016 of the document "Strategic Principles for Security the Internet of Things." [15] Developed by the U.S. Department of Homeland Security (DHS), the goal of the document is to offer recommended cybersecurity practices to those who "design, manufacture and use Internet-connected systems and devices."

As set forth by the DHS, the six IoT security principles are, as follows:

- **INCORPORATE SECURITY AT THE DESIGN PHASE**

  Security should be evaluated as an integral component of any network-connected device. While there are notable exceptions, economic drivers motivate business to push devices to market with little regard for security.

- **ADVANCE SECURITY UPDATES AND VULNERABILITY MANAGEMENT**

  Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates and vulnerability management strategies.

- **BUILD ON PROVEN SECURITY PRACTICES**

  Many tested practices used in traditional IT and network security can be used as a starting point for IoT security. These approaches can help to identify vulnerabilities, detect irregularities, respond to potential incidents and recover from damage or disruption to IoT devices.

- **PRIORITIZE SECURITY MEASURES ACCORDING TO POTENTIAL IMPACT**

  Risk models differ substantially across the IoT ecosystem, as do the consequences of security failures. Focusing on the potential consequences of disruption, breach, or malicious activity is critical for determining where in the IoT ecosystem particular security efforts should be directed.

- **PROMOTE TRANSPARENCY ACROSS THE IOT**

  Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware provided by vendors outside their organization. Increased awareness can help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies.

- **CONNECT CAREFULLY AND DELIBERATELY**

  IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption.

The DHS document also provides a number of suggested practices that can be used to address each of these strategic principles. As such, it provides an effective framework that can enable developers and manufacturers of connected smart home systems and devices to create a detailed plan tailored to identify and address the specific cybersecurity vulnerabilities in their products.

UL'S APPROACH TO PROTECTING CONNECTED SMART HOME SYSTEMS AND DEVICES

UL's Cybersecurity Assurance Program (CAP) provides a holistic approach to mitigating cybersecurity risks that evaluates both product-specific and systemic protections against cyberthreats. This approach can help to minimize the vulnerability of smart home systems and devices to cyberattacks and provide device manufacturers with greater assurances regarding the security of their products.

UL CAP

consists of a series of UL requirements documents that provide verifiable criteria for assessing the cyber vulnerability of network-connectable products and systems. Specifically, the UL 2900 series, *Standard for Software Cybersecurity of Network-Connectable Devices*, is applicable to a broad range of interconnected devices and systems, and is intended to provide testable cybersecurity criteria to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase overall security awareness.

The UL 2900 series currently consists of standards in the following categories:

- **GENERAL PRODUCT REQUIREMENTS**

  Standards in this category include UL 2900-1, *Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*. UL 2900-1 sets forth requirements to assess software for the presence of security risk controls in its architecture and design, using prescribed testing methods to evaluate vulnerabilities, software weakness and malware.

- **INDUSTRY PRODUCT REQUIREMENTS**

  At present, there are two standards in this category. They are UL 2900-2-1, *Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems*, and UL 2900-2-2, *Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems*. These Part 2 standards address vulnerabilities of software that supports devices and systems used in the specified industry environment. Additional standards in this category are currently under development.

- **GENERAL PROCESS REQUIREMENTS**

  Currently under development is UL 2900-3, *Outline of Investigation for Software Security of Network-Connectable Products, Part 3: General Requirements*. This Part 3 series of standards is expected to address the general testing of organizational systems and processes for conducting the organization's risk assessment necessary to identify applicable, software-based cyber threats and the ability of the organization to include appropriate security in the product development process.

Utilized together, the UL 2900 series of standards complement the DHS's strategic principles and provide an effective approach for evaluating an organization's cybersecurity tactics, as well as the specific vulnerabilities of individual smart home systems and devices. As such, it provides equipment manufacturers and software developers with the necessary criteria to measure and assess the security features of their products and the likelihood that cyber vulnerabilities can be exploited.

SUMMARY + CONCLUSION

Assuring the cybersecurity of connected smart home systems and devices will soon become a market imperative for device developers and manufacturers, as consumers increasingly demand smart home products that are secure from malicious attacks. The DHS's recently published strategic principles for the security of connected devices provides a helpful framework that can be used in the development of a device-specific cybersecurity plan. Together with UL CAP, developers and manufacturers can now effectively address growing concerns regarding the security of connected smart home systems and devices, thereby helping to protect the security and safety of consumers everywhere.

For more information about the cybersecurity of connected smart home systems and devices, and UL's Cybersecurity Assurance Program, please contact **ULCYBER@UL.COM** or visit **UL.COM/CYBERSECURITY**

END NOTES

[1]"'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020," Juniper Research, 28 July 2015. Web. 1 December 2016. http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.

[2]"Cyberattack knocks out access to Twitter, Spotify, Reddit , others," United Press International, October 22, 2016. Web. 1 December 2016. http://www.upi.com/Business_News/2016/10/22/Hackers-used-smart-home-devices-to-carry-out-Dyn-cyberattack/2061477141377/.

[3]"M2M World of Connected Services: The Internet of Things," an infographic prepared by Beecham Research. Web. 1 December 2016. http://www.beechamresearch.com/download.aspx?id=18.

[4]"Internet of Things Spending Forecast to Grow 17.9% in 2016, Led by Manufacturing, Transportation, and Utilities Investment, According to New IDC Spending Guide," IDC Research, Inc., January 4, 2017. Web. 23 January 2017. http://www.idc.com/getdoc.jsp?containerId=prUS42209117

[5]"Gartner Says 6.4 Billion Connected 'Things' Will be in Use in 2016, Up 30 Percent from 2015," press release from Gartner, Inc., November 10, 2015. Web. 1 December 2016. http://www.gartner.com/newsroom/id/3165317.

[6]"Coldwell Banker Real Estate and CNET Define "the Smart home'," press release from Coldwell Banker Real Estate, May 10, 2016. Web. 1 December 2016. https://www.coldwellbanker.com/press-release/coldwell-banker-and-cnet-define-the-smart-home.

[7]"Smart Home Hardware & Services Revenue to Exceed $190BN by 2021, As Big 4 Tighten Grip on Market," press release from Jupiter Research, Inc., January 10, 2017. Web. 21 January 2017. https://www.juniperresearch.com/press/press-releases/smart-home-hardware-services-revenue-to-exceed-$.

[8]"The Safe & Smart Home: Security in the Smart Home Era," a report on results of a 2016 survey of 1300 U.S. consumers conducted by August Home and Xfinity, April 2016. Web. 1 December 2016. Available at http://www.businesswire.com/news/home/20160421005889/en/Million-U.S.-Households-Projected-Add-Smart-Home.

[9]"Hacking into homes: 'Smart home' security flaws found in popular system," Michigan News, University of Michigan, May 2, 2016. Web. 1 December 2016. http://ns.umich.edu/new/multimedia/videos/23748-hacking-into-homes-smart-home-security-flaws-found-in-popular-system.

[10]"Hackers prove how easy it is to invade smart homes—but there's a silver lining," BI Intelligence, Business Insider, March 10, 2016. Web. 1 December 2016. http://www.businessinsider.com/hackathon-for-smart-homes-in-iot-internet-of-things-2016-3.

[11]Osram Lightify light bulbs 'vulnerable to hack'," BBC News, 27 July 2016. Web. 1 December 2016. http://www.bbc.com/news/technology-36903274.

[12]"Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities," a report prepared by cybersecurity consulting firm Rapid7, September 2015. Web. 1 December 2016. https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf.

[13]"Have a smart lock? Yeah, it can probably be hacked," posting on c|net, August 9, 2016. Web. 1 December 2016. https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/.

[14]"2016 Data Breach Investigation Report," Verizon, April 2016. Web. 1 December 2016. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[15]"Strategic Principles for Security the Internet of Things," U.S. Department of Homeland Security, November 15, 2016. Web. 1 December 2016. https://www.dhs.gov/securingtheIoT.

©2017 UL LLC. All rights reserved. This white paper may not be copied or distributed without permission.
It is provided for general information purposes only and is not intended to convey legal or other professional advice.