EXECUTIVE BRIEF

INTERNET OF THINGS (IoT) SECURITY IN SMART HOME DEVICES

- Insights for busy professionals
- Read in less than 10 mins
- Knowledge without the fluff

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

Symantec™

THIS EXECUTIVE BRIEF IS A SUMMARY OF THE WHITE PAPER:

Insecurity in the Internet of Things

CLICK TO ACCESS THE WHITE PAPER

DEFINITION

- The Internet of Things (IoT) refers to a network of devices that have an assigned IP address and send and receive data without human interaction or influence.

INTRODUCTION

- The IoT market is growing by leaps and bounds. Yet security for these devices contains many vulnerabilities, leaving users open to hacking.
- Examples of IoT smart home devices include smart thermostats, smart locks, smart light bulbs, smart smoke detectors, smart energy management devices, smart hubs, security alarms, IP cameras, entertainment systems, routers and network storage devices.

KEY POINTS

- The most common entry point into the IoT is through a web browser or smartphone app.
- Although users find it difficult to secure their IoT devices due to a lack of secure modes of operation, there are a number of ways to mitigate the risk of attacks.
- IoT attacks include sniffing network traffic, injection, tampering/forging, jamming, battery exhaustion, collision and unfairness (link layer), greed, homing, black holes (network layer), misdirection, flooding and desynchronization.
- Weak passwords on IoT devices are a serious security issue as many manufacturers do not offer users the chance to change the default password to an individualized stronger one. In cases where it is possible, it is difficult to use a long, complex password, as it requires remote access to change because many IoT devices do not have keyboards.
- Cloud systems allow owners the ability to control devices while away, like thermostats in their home, but without strong passwords and robust encryption, attackers can do the same.
- There is no single standard network protocol in IoT so devices can use networks other than the home's Wi-Fi broadband connection, like Z-Wave, Zigbee, Powerline, Bluetooth 4.0 and radio frequencies.
- Most devices use the broadband Wi-Fi connection, like computers and tablets. IoT devices can use these as well, giving limited protection through the network's basic firewall filtering technology.
- If "smart" devices - those capable of sending and receiving information - rely on the home network, users can use their Wi-Fi to control them.
- Wireless networks at home get hacked easily due to prevalence of weak Wi-Fi passwords. Symantec's 'test' attack easily took over a smart hub by piggybacking on its programmed update search.

KEY POINTS (cont.)

- Currently, IoT devices do not offer many direct profit opportunities for hackers, such as stealing credit card numbers. Right now, hackers hack them as a "proof of concept", or just because they can, to take control of the climate in the home or the actions of a Smart TV, for example.
- Manufacturers need to secure the devices against the weak points that come with cloud control interfaces.
- Attackers or hackers can intercept or change the behavior of IoT devices through physical access to the device, over Wi-Fi/Ethernet, through the cloud infrastructure or malware.
- The Top 10 IoT vulnerabilities are: insecure web interface, insufficient authentication/authorization, insecure network services, lack of transport encryption, privacy concern, insecure cloud interface, insecure mobile interface, insufficient security configuration, insecure software/firmware and poor physical security.
- Researchers' efforts have helped discover potential vulnerabilities in IoT devices which vendors have subsequently fixed.
- Having physical access to a device allows an attacker to alter configuration settings, tamper with the power source, disable for intended activity or take control of the device itself.
- There are two types of local attacks over Wi-Fi/Ethernet: cloud polling and direction connection.
- In cloud polling, when a device connects to the cloud for firmware checks, attackers use the connection to access the device.
- A direct connection attack is possible because of the use of unencrypted network communications that leave the backend and critical personal data open to viewing.
- Malware, or malicious software, also can leave a smart home device open to attack a hacker.

TAKEAWAYS

- The best a user can do is follow these tips: use strong passwords on device accounts and Wi-Fi networks; change default passwords if you can; stay away from used IoT devices, disable features not being used, and install updates as they are available.
- It is crucial that smart home and IoT devices in general use mutual authentication and encryption to secure the use for the intended party only.
- Smart home device manufacturers should use encryption on their devices, require password changes, provide standalone options that work offline and provide security analytics.

Click or scan to access the full white paper

CLICK TO ACCESS
THE WHITE PAPER

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers.

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

Our team produces short documents for busy professionals, summarising longer reports and research papers so that readers can swiftly become acquainted with a large body of knowledge and decide whether or not to read the full source document(s).

We vet and qualify reports for relevancy and value to its intended audience before creating an InsightBrief document. Our editorial team is independent from the originator of the report, ensuring that the insights exclude sales or vendor centric messaging, thereby creating real value for our time-poor readers.