Threat Bulletin

Vulnerabilities of Digital Assistants

June 2019

Introduction

My girlfriend asked me why I'm speaking so quietly at home.
I said, "I'm afraid that Mark Zuckerberg is listening".
She laughed.
I laughed, too.
Then Siri laughed.

It's 7.00 am. Your digital assistant wakes you up and briefs you on your personal schedule while you're brushing your teeth. Now you're cooking breakfast, and the same assistant guides you through the new recipe it found online, tailored to your specific dietary needs. In the office, you have a slight fever and it books an appointment with your doctor, signing you up for the necessary tests to find out what is ailing you. It contacts your car and sends it the optimal route to the hospital, considering the current traffic situation.

Less than 20 years ago, this modern-day scenario where every command is at the tip of your tongue was considered science fiction. In 2014, Amazon marked a new era of home automation when they introduced the Echo, a smart speaker powered by Amazon's digital assistant, Alexa. Since then, digital assistants have been massively adopted and revolutionized the way we live our everyday lives – with about 3.25 billion assistants currently in use[1].

The rise in popularity indicates how helpful they can be but ignores the trade-off between privacy and convenience that this intimate integration carries. Digital assistants act as *"The Smart Home HQ"* which introduces additional cyber risks. They control a lot of IoT devices that can be potentially compromised by hackers and used to conduct various criminal activity including unlocking smart locks, accessing users' bank accounts, and stealing personal information.

Technology providers and ISPs should raise user awareness about privacy issues and the risks of owning a digital assistant. In addition, they can offer cyber security services for the connected home that would be mutually beneficial.

Digital Assistants In a Nutshell

Digital assistants use the power of the Internet of Things to browse the web, access the news and weather, shop, send emails, pay bills, order services, and more, all in response to voice commands. With machine learning advancements, digital assistants adapt to user's needs by learning their routines, preferences, favorite apps, and previous requests, so they become more helpful over time.

The digital assistants accessed by smartphones are dominant today, but smart TVs are the fastest growing segment at 121.3%, followed by smart speakers at 41.3% and wearables at 40.2%[2]. The key

[1] Juniper Research, 2019 study https://www.businesswire.com/news/home/20190212005064/en/Juniper-Research-Digital-Voice-Assistants-Triple-8

[2] Juniper Research

point here is that digital assistant access isn't limited to smartphones and smart speakers. Other connected devices ranging from microwaves to cars will increasingly serve as digital assistant access points in the future (maybe this year's Amazon Super Bowl Commercial isn't so far from reality?).

The most well-known and popular AI-powered digital assistants are Amazon's Alexa, Google Assistant, Apple's Siri and Microsoft's Cortana. Apart from them, there are numerous others available on the market today in different countries - Alice by Yandex, DuerOS by Baidu, Xiaowei by Tencent, Bixby by Samsung, Xiaoyi by Huawei, AliGenie by Alibaba, and Xiao AI by Xiaomi. According to rumors, Facebook too is currently working on its own voice assistant to compete with the main players.

Threat Vectors

So far nearly all possible attacks on digital assistants rely on the misuse of official commands and not on modifying the actual code running on the devices. Despite this, as they go mainstream, it is essential for users to really get to know how they work and learn about their vulnerabilities.

Generally, the risks can be divided into the following groups.

Privacy Concerns

According to a recent Microsoft survey, 41% of users report concerns around trust, privacy, and passive listening by smart speakers with built-in voice assistants. These devices are always listening for a command, and while this might seem harmless, once the device is awake, it will record everything that is said. So far, there is no evidence that these recordings are sold to external companies, but they are of course processed and archived by the service provider. Therefore, there's always a threat that if the servers were to be breached, users' voice files would be exposed and could be accessed by criminals.

In April 2019, Amazon admitted that thousands of its full-time workers listened to customer conversations with Alexa to help improve its grasp of human speech. Moreover, there have been numerous malfunction incidents when assistants accidentally recorded family conversations and sent it to a random contact, or when Alexa unexpectedly started laughing for no reason. Sounds creepy, right?

The microphone can be muted, but unless the device is switched off, it is always ready to listen.

IoT Hub

Digital assistants are designed to be the hub for the IoT ecosystem. Apart from allowing users to surf the internet, they can also communicate with and control all the other connected smart devices at home as well as integrate into them. It could be anything - smart TV, lights, baby monitors or toys, appliances, cars, thermostats, and even smart door locks. The convenience also means that if a single IoT device gets hacked, it becomes a backdoor which allows hackers to entirely control your smart home via the hub. This can result in all kinds of illegal actions including breaking into your house.

Digital Payments

Digital assistants are also changing the consumer purchasing experience in the retail industry. Voice shopping is a rapidly growing segment – shopping on Alexa alone could generate $5 billion per year in revenue by 2020. Surveys show that consumers are willing to make payments via their smart assistant, but many are wary about security.

26% of respondents[3] who own a smart assistant have used it to make a payment. However, 74% of respondents had security concerns that they said would stop them from making a hands-free payment.

Just as your assistant uses your bank details for seamless payments and your passwords for easy logins, criminals can hack it and do the same thing.

Accidental Commands

Most assistants typically require a specific voice command like “Ok Google” or “Hello Alexa”, that lets them know that the user is ready to ask something. As a result, anything said on the radio or TV can unintentionally trigger the assistant’s services. For instance, a 2017 Burger King TV commercial featured an actor asking ““OK Google, what is the Whopper burger?”. The loud prompt was inadvertently waking up Google Home devices in people’s homes. Accidental voice commands can cause devices to mistakenly place orders for unwanted products without their owners realizing. In February 2018, British Advertising Standards Authority (ASA) asked for a Purina cat food TV commercial to be taken off air, after it inadvertently caused one man’s Amazon Alexa to place an order for the product.

“Dolphin Attacks”

In 2017, Chinese researchers discovered that it’s possible to send secret high frequency audio commands through speakers. The method is dubbed a “dolphin attack” because the creatures can hear sounds that humans often cannot.

This vulnerability allows hackers to secretly communicate with your device through music or YouTube videos – letting them send text messages or open malicious websites without the owner’s knowledge. “Dolphin attacks” require the attacker to be within whisper distance of your phone or smart speaker. New studies conducted since its discovery suggest that ultrasonic attacks like these could be amplified and executed at a distance as far as 25 feet away.

[3] Transaction Network Services data

Conclusion

In the coming years our homes will be getting smarter, with digital assistants leading the trend of connecting more devices to the "Internet of Things". As security expert Bruce Schneier said, "Today, everything is becoming a computer. The more we connect things to each other, the more vulnerabilities in one thing affect other things". More connected devices at home, work, in cars and even on our bodies, mean more paths and opportunities for cybercriminals to target us. Anything connected to the internet can be hacked. Like any small business, smart homes need to be protected with a cybersecurity service – which CSPs are best positioned to provide.

Tips to Stay Protected

Despite popular smart assistant manufacturers building security protocols into their products, it is always best to take precautions and follow security guidelines:

- When using digital assistants or other IoT devices, make sure your home network is secure. Use WPA2 encryption and a strong account password to protect it. Many smart speakers blindly trust the local network, meaning any hacked device in the same network could compromise the assistant and change its settings. Smart thermostats, baby monitors, TV, and even baby toys have all been hacked.
- A strong password is particularly important considering anyone with access to your account can listen to old recordings or change the settings of the device over the internet.
- Consider switching off devices that are not in use.
- By keeping an eye on which personal information you share with the speaker and regularly deleting your saved files via the smart assistant app, you can minimize the risk of a security breach. Only store limited personal information on these devices.
- Do not connect your digital assistant to any critical things at home such as smart door locks.

Are you concerned about security of digital assistants?
Allot's HomeSecure can assist.
Contact Allot.