CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

IN THIS EDITION

4 Industries Being Hurt by Counterfeit Materials (and How to Spot Them)

5 Most Disastrous Ransomware Attacks of the Last Decade

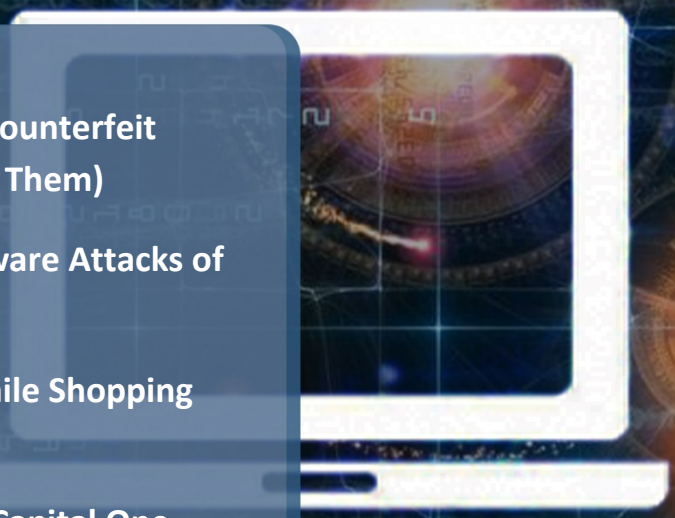
How to Protect Yourself While Shopping Online

Top 5 Questions about the Capital One Data Breach

Ways to Protect Sensitive Data Online

5 Key Differences between Software and Hardware Vulnerability Mitigations

...and much more...



SEPTEMBER 2019

MORE INSIDE!

Voice Commerce Calls for Built-in Security

By Julian Weinberger, NCP engineering

In the mid-1990s, retailers embraced the Internet to increase customers and to introduce new service offerings. A new breed of online-only merchants quickly emerged to challenge traditional brick and mortar stores for Internet-based transactions. Since then, successive advances from eCommerce to mCommerce to omnichannel have forced retailers to make their virtual presence every bit as strong as their physical one just to stay relevant. Today, the ever-evolving retail industry shows no signs of slowing down. The latest phenomenon taking merchants by storm is voice-assisted shopping.

Retail Talk

As voice-activated IoT devices such as the Amazon Echo, Apple Homekit, and Google Home grow in popularity, consumers are starting to use them to order goods using simple voice commands. A study by Adobe Analytics showed that 22 percent of digital assistant owners use their devices for shopping.

While the Artificial Intelligence (AI) powering these voice systems is presently limited to accessing automated customer services via voice-bots or repeat orders of items bought previously, the technology is quickly becoming more sophisticated and will soon be capable of delivering a highly personalized service. Walmart, for example, recently announced a new voice-ordering service available via Google's many smart devices.

Industry observers anticipate that, within a few years, consumers will be able to use voice-powered digital assistants to shop with the vast majority of retailers. Manufacturers are already designing everyday machines and appliances with built-in voice-powered technology. LG, for example, has demonstrated a

smart refrigerator that uses Alexa to order food items, while some car makers have integrated voice-technology into their vehicles to allow voice-shopping while driving.

Analysts forecast that voice-assisted shopping will grow by 500% over the next three years with more than 1.6 billion people regularly using the technology by 2021. OC&C reports that voice commerce spending will reach $40 billion by 2022 and that more than half (55%) of households will have at least one smart speaker.

Cybersecurity Threats

When it comes to security and data privacy, manufacturers of voice-assisted IoT devices still have a long way to go to reduce consumer fears. A 2018 Global Consumer Insights Survey by PwC found 13 % of study participants were concerned about the security of AI devices.

Recent data breaches do little to help build trust – Amazon sent 1,700 Alexa voice recordings to the wrong person by mistake following a data request in 2018. Without proper security measures in place, digital assistants make attractive targets for cyber criminals looking to harvest personally identifiable information (PII) to sell on the dark web.

Even though these devices are smart, they can still be triggered by random voices from TVs and radios and can be controlled by unknown users. For example, a prerecorded message on a random Spotify Playlist can easily say, “Alexa, buy me the new Mac Pro,” and the device will send orders to everyone who plays the playlist on a speaker. This is basically a formjacking attack on voice-controlled devices.

Data Privacy

To protect voice commerce, the makers of AI-powered voice-activated IoT equipment must first ensure that devices are designed with in-depth security and data privacy protection built-in.

While authentication is available on some smart devices already, it’s based on a biometric authentication which, unfortunately, always has a false acceptance and rejection rate. Adding a second layer of authentication to the smart device will make it more secure, e.g. smart devices can only order merchandise when the user/owner is in the same room.

Recommended layers of defense include certificate-based authentication plus a unique hardware identifier. Smart speakers should also feature multiple security mechanisms including authorization, virus protection, and remote access management for business environments.

Finally, the best way to preserve the privacy of voice data exchanges is with end-to-end encryption, a technique synonymous with remote virtual private network (VPN) services. End-to-end encryption protects data at every stage of the communications process – at device-level, while in transit, and when stored at its destination – by scrambling the content to render it unintelligible to outside observers.

In summary, smart speakers are quickly becoming a part of the average connected home. While the retail industry is responding by adding AI-powered voice technology to a multitude of machines and devices, manufacturers must ensure that security is built-in by design. Virtual private networks with end-to-end encryption will effectively protect the data privacy of consumers who purchase merchandise from their smart speakers.

About The Author

Julian Weinberger, CISSP, is Director of Systems Engineering for NCP engineering. He has over 10 years of experience in the networking and security industry, as well as expertise in SSL - VPN, IPsec, PKI, and firewalls. Based in Mountain View, CA, Julian is responsible for developing IT network security solutions and business strategies for NCP.