CyberTrends – Your Smart Fridge May Be Listening: Securing Home Internet-Enabled Devices

December 15, 2022

Speakers

Doug Davidson
Director of Information Technology Services
(614) 947-5340
ddavidson@gbq.com

Ray Tefft
Manager of Information Technology Services
(614) 947-5341
rtefft@gbq.com

Agenda

Attacks, Risk, Privacy, and Scale → What is IoT? → IoT Challenges → Securing IoT Best Practices → Conclusion

Attacking an Organization vs. Attacking an Individual

- Attacking an organization is much more difficult than attacking an unarmed individual.
- Organizations - endless amount of security tools to select and at their disposal
- Entire teams dedicated to security
- Personal devices/networks - the same protection does not exist

Home Networks Pose a Major Risk

Again, why attack an organization when you can walk right through the open door?

- Home networks WIDE OPEN
- Out-the-box settings
- Generic admin username/passwords
- Open ports
- IoT devices

Privacy is Imperative

People share personal details on social media sites

Password security is poor

Data breaches occur every day

The Scale of the Problem

39% of compromised devices have malware, or their home has open cameras or IT networks

69% of exposed passwords are freely available on the Darkweb

75% leaking data due to improper privacy settings on devices

87% no security on cell phones or tablets

What is IoT?

The Internet Of Things (IoT) is a network of smart devices that connect to each other in order to exchange data via the internet without any human intervention. Simply put, Alexa, Google Assistant, Smart light switches, smart refrigerators, etc.

- The architecture of IoT systems usually consists of wireless networks, cloud databases for communication, sensors, data processing programs, and smart devices that interact closely with each other. IoT systems use the following components to exchange and process data

IoT Examples

Different Types of IoT?

- **Home automation** systems monitor and control home attributes like temperature, lighting, entertainment systems, appliances, and alarm systems. Common smart devices for home automation include assistant speakers, thermostats, refrigerators, plugs, and bulbs.

- **Healthcare** Medical IoT (MIoT) provides lots of opportunities for healthcare professionals to monitor patients, as well as for patients to monitor themselves. Smart devices for MIoT include wirelessly connected fitness bands, blood pressure and heart rate monitoring cuffs, and glucometers.

IoT Cybersecurity Challenges

- Software and firmware vulnerabilities
- Insecure communications
- Data leaks from IoT systems
- Malware risks
- Cyberattacks

Best Practices for Ensuring the Security of IoT Systems

Secure mobile devices

- Uses a passcode or bio-metrics to secure your smart devices
- Update your smart devices when a patch is available.
- When downloading an application, be aware of how your personal data is being used
- Don’t leave your devices out in the open unattended

Secure IoT devices

- Do your research, and make sure the IoT that you are using has security
- Update your IoT devices when a patch is available.
- If there is security protection available like multifactor authentication, use it

Best Practices for Ensuring the Security of IoT Systems

Secure networks

- Strong encryption for your home network WPA2 or WPA3 with a strong password
- If your cable modem/router, or wireless mesh (Google, eero, etc.) has a firewall option, use it.
- If you have the ability to group your devices on your network, do it
- If you have the ability to limit the bandwidth that each device uses for the Internet, do it

Secure data

- Protect sensitive information: each IoT device should have a unique password
- Collect only necessary data: ensure that your IoT is only collecting necessary data
- Secure network communication: for better security restrict what the IoT can talk to

Questions You Might Have

- If I don't know how to do some of this are there places or people I can go to for help?
- What if I'm buying something technical but I'm not sure if it is IoT? Where do I look to know?
- I'm about to buy a house that seems to be pretty wired with this stuff ... should I ask for a listing of what's there? the product names? manuals? what should I know to understand what I'm buying?
- My kids are online so much I think they are Internet of Things ... are there things I can do to help protect my family members, especially my kids?
- What if I’m buying second-hand IOT, what should I look out for?

Conclusion

- Your home IoT could be developing analytics on what you are doing in your day-to-day life.
- If you are purchasing that new IoT device (Alexa, Google Assistant, light switch, smart refrigerator, etc.) be aware of what data it is monitoring and collecting
- Do your research before purchasing, see if the IoT is secure or if others have had issues
- Keep your IoT firmware and software up to date
- Secure your home network (firewall, groups, limited bandwidth to the internet)
- If you plug it in and throw caution to the wind, you giving strangers insight into your personal life, be careful!

Resources

- Visit us online to view our Information Technology **webinar recordings** and **articles**.

Contact Information

Doug Davidson
Director of Information Technology Services
(614) 947-5340
ddavidson@gbq.com

Ray Tefft
Manager of Information Technology Services
(614) 947-5341
rtefft@gbq.com