SUMMARY: IoT Security Report

Introduction

"Smart" devices in the home are proliferating rapidly, from voice-controlled speakers to interactive doorbells to internet-connected refrigerators to remote-controlled light bulbs and electrical outlets. And while consumers know that Internet of Things (IoT) devices are useful and fun, it has become increasingly evident that consumers don't know much about what these smart devices are doing behind the scenes. What are they connected to, what information are they capturing, and who can see that information? And most importantly, can that information be misused by malicious actors?

Motivated to prove what many industry technologists feared, Dark Cubed analyzed a dozen consumer-grade connected devices that are broadly available through mass market and on-line retailers in the U.S. The findings raise the awareness of the security and privacy epidemic that exists today in consumer IoT devices that are currently installed and in use in tens of millions of U.S. households.

Summary of Findings from *The State of IoT Security* Report

The report highlights six findings related to consumer IoT security:

1. Several of the devices we tested were painfully insecure.
2. A few of the associated smartphone applications that control these devices were terrifying in the extent to which they can access our personal data.
3. There are a large number of IoT companies and startups, but many appear not to care about security, and neither, apparently, do the retailers who sell these devices to consumers.
4. There is cause for concern about China's role in IoT.
5. Using cloud infrastructure does not mitigate security threats.
6. Patching will not fix the systemic issues we uncovered.

These findings can be consolidated and summarized as follows.

Economics is driving insecurity: Given the explosive market growth, we are seeing a race to the bottom with IoT device pricing that prioritizes winning market share over making a profit. This approach is a key reason we see such disregard for security best practices on many products; the economics don't justify spending time on an appropriate level of security.

Additionally, the increasing volume of device communications to advertising services, including services in China, suggest that user data is being sold to subsidize low device prices.

A holistic approach is required: While much of the reporting on IoT security focuses on the hardware, this is only one small part of the equation. The security of the entire IoT communications stack must be considered, including device firmware, data encryption to and from the device, the communications infrastructure governing (and securing) the communications, the associated Android and iOS applications, and the platforms that store consumer data. Much like your cell phone carrier has built and manages a network to control your smartphone communications, the IoT requires a similar platform. While cell phone carriers are regulated to ensure consumer privacy and safety, a similar regulatory environment has not caught up with IoT. Most of the consumer devices we tested are managed on China-based or China-owned platforms. This is like a U.S. cell phone subscriber using the Chinese government's carrier, China Mobile, for your smartphone services.

The good news is that privacy and security solutions to the larger IoT problem do exist. There are platform providers who are uniquely positioned to solve issues like integrating security reviews into the IoT product lifecycle, integrating trusted computing and encryption technologies, and implementing continuous monitoring to protect against unauthorized changes after deployment. But these solutions need to become the rule rather than the exception.

Lack of visibility into privacy and security is a clear and present danger: Our testing found that there is no easy way for a consumer to know whether his or her device is safe, or if its communications platform is trustworthy. Worse, we saw examples of established brands being adopted by companies with strong ties to foreign counties including China. We believe that the distributers and retailers of these devices must conduct technical due diligence to ensure that communications are managed by a trusted and soon-to-be regulated U.S. company for the best chance at user security and data privacy, but this is clearly not being done by major retailers today.

This report is the first in a series produced through the collaboration between Dark Cubed, a cybersecurity company, and Pepper IoT, a platform provider focused on securing the future of IoT.

Pepper's Approach:

According to the report's findings, device security and data privacy are often overlooked by device manufacturers. Fortunately, there are more options today than there have been historically for IoT device manufacturers, retailers and service providers looking to manage connected consumer devices easily and securely.

Pepper's state-of-the-art full-stack IoT platform-as-a-service approach delivers end-to-end security of user's private information and data. Pepper utilizes a holistic suite of features and methods to protect connected IoT devices and the information they generate against unauthorized access. The platform is hardened against hackers and third parties attempting unauthorized access, which has been observed with many unsecured devices exfiltrating user data to IP addresses based in China.

Pepper IoT management brings decades of operational experience within large US wireless/telecom carriers. The team carries a principled approach that begins with the integrity of the core communications network that must be constructed with quality, security, and scalability as foundational imperatives – innovation can then flourish with this robust foundation. Pepper delivers advanced usability features that draw best in market app ratings for the enterprise partners who have customized their unique services on the Pepper platform. The company is venture-backed, Kansas City-based, and powers devices and services available globally. Pepper-powered solutions can be trusted by OEMs and service providers to protect customer privacy and personal data while delivering highly engaging and customized end-user experiences.