Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Smart Home Devices Open New Vulnerabilities

By: Brad Russell

Key value propositions for consumers around the smart home are noted as more security, more safety, and easy management of home solutions for communication and controls in the home. Really, the promise of the connected home hinges on the security, safety, and simplicity of protecting this advanced technology from being exploited to harm households.

In 2017, the connected home market has experience an expansion of the kinds of attacks that have been increasing in recent years.

Attacks include:

- **Distributed Denial of Service (DDoS) attacks**—like the largest-ever October 2016 Mirai botnet attack—will target devices where default password usage provides easy unauthorized access. Ransom attacks, using DDoS as a threat to an organization or ransomware targeting individual consumers, are predicted to continue seeking to extort payment by hijacking control of devices.
- **Permanent Denial of Service (PDoS) attacks**, as known as phlashing, seek to destroy the firmware and permanently render IoT devices inoperable. Malicious impact without particular rewards has been enough motive for some hackers.
- **Man-in-the-middle attacks** often exploit router or device setup vulnerabilities to gain access to data traffic moving to and from devices on the home network.
- **Phishing scams**, increasingly difficult to identify, lure consumers onto fake websites that solicit their login credentials to fix an imaginary problem. According to The Anti-Phishing Workgroup, almost 100,000 email phishing attacks are reported each month. Thousands of people fall for them, divulging sensitive personal and business information in the process.

Investment in data privacy and security by stakeholders in the consumer IoT ecosystem has never been greater. However, vulnerabilities still exist and are highlighted in the news regularly. Parks Associates research finds that nearly one-half of consumers cite strong data security and privacy concerns related to Internet-connected devices.

Inhibiting Adoption

Security concerns can inhibit adoption for the mass of consumers who need more confidence in connected products Whether security solutions are provided at the level of hardware, communication networks, control hubs, routers and gateways, or cloud platforms, these protections are vitally important to the success of IoT providers throughout the ecosystem.

Securing the connected home today is not as much a technological challenge as a product development, product management, and consumer behavior challenge. Current attacks largely focus on the low-hanging fruit of known vulnerabilities. Reliable security technologies and procedures are well-established for ensuring home network security, including best practices for securing routers and gateways, access management, data transport, and data storage at the local and cloud levels.

Many enterprise-grade processes that have been worked out over the years are being deployed in the home. Having product manufacturers and consumers adhere to recommended best practices

appears hit-or-miss and future attack strategies require new solutions within IoT security architecture that is flexible and scalable.

Product Development Challenges

Security and privacy planning is critical to the product development process. Tough decisions abound around the degree of investment into security-related strategy, hardware design, application design, networking protocol selection, platform build-or-buy strategy, integration with third-parties, cloud transfer and storage, and product testing.

Ultimately, the business model and company culture of the manufacturer serve as the foundation for these decisions. A focus on one-off sales of value-tiered devices produces minimally viable products that are a security threat to both the homeowner and the broader IoT ecosystem. On the other hand, deep investment in security by design and comprehensive support throughout the product lifecycle requires a business model that can offset these costs and still provide sufficient return on investment. A trade-off between cost and time-to-market also challenges companies throughout security planning and product testing. The consumer IoT market has seen startups and established manufacturers rush to ship connected products without sufficient knowledge of security threats or adequate plans for how long the product will live.

Another challenge resides in planning for the relationship map of a device and its data to an end customer. The enterprise segment typically has clear management of the user relationship to data, while the connected home provides complex challenges regarding mapping multiple users and their data to devices. This creates access problems and work streams with which many product manufacturers have little experience. These challenges are compounded by increasing interactions with other devices and third-party services. The Babel of protocols and procedures without any generally accepted standards leaves product developers with no clear definition of what a secure product actually is. At worst, this confusion reduces security to a marketing challenge preoccupied simply with, “How much security does a product need to satisfy the consumer?”

Parks Associates data indicate that almost half of U.S. broadband households are “very concerned” (rating 6-7 on a 7-point scale) about hackers gaining control of connected devices. Consumers are equally concerned about hackers getting access to historical data from those devices.

Product Management Challenges

Beyond product development, product management for connected products faces security challenges that require a level of product support that pre-connected products have not. Product managers must take a long-term view of supporting connected devices that may have replacement cycles as long as 10-15 years. Over the lifecycle of a product, product managers need to continually evaluate the need for firmware and software updates to incorporate issues like Wi-Fi standards, data ownership and usage policies, response to new regulatory compliance requirements, and more.

Development of updates requires continual monitoring of the device, expanding knowledge in all security-related fields, solutions development, quality assurance testing of all firmware and software updates before rolling out, and feedback monitoring and analysis after each update. For some products, this process needs to be conducted every 3–6 months.

In mid-September, Fitbit sent out security updates after learning about vulnerabilities in two popular models where hackers could access data from consumers’ devices. These updates are prime examples of responsible product management.

Given the complexity and costs related to supporting connected products throughout the product lifecycle, one major challenge to securing the connected home results from manufacturers’ inability or unwillingness to provide the support needed to secure the product. Instances have already occurred, for example with routers, where security patches for well-documented threats have been available for years without being adequately installed in firmware updates on products in the field.

Whether this happens as a result of consumer inattention or a manufacturer's dereliction of duty to ensure updates are created and installed, the continuing vulnerability is evidence of poor product management.

Consumer Education Challenges

Consumers trust vendors to provide a secure experience. Where service providers control product selection, installation, and take responsibility for the platform delivering their services, consumer education is less of a challenge. However, a growing share of connected products are self-installed and self-monitored, including almost half of all networked cameras installed by owners, family, or friends.

The task of securing the connected home is challenged by a customer base largely uninformed about how home networking functions. In the absence of security standards, some consumers are easily attracted to lower-cost, minimally viable products from vendors with cheap, often open source solutions designed merely for a quick one-off sale. Consumers often choose the path of least resistance, preferring ease of setup with default passwords over changing login credentials regularly or mastering security settings offered for device configuration. They may assume that vendors are providing a secure experience with no practical means of evaluating whether that is true or not.

Consumers continue using routers or other devices past their recommended life cycle or after product support stops, security patches are needed, or encryption standards change. Generally, if a router is four to five years old it needs replacement. Part of the consumer challenge also derives from the lack of visibility into what is actually happening in the home network. Traditional router applications have been relatively simple, leading to the primary consumer interaction with a router being restarting it when a problem is observed.

While the best remedy for a lack of education is education, some vendors express reluctance to bring up security concerns with consumers. They believe addressing the issue undermines overall consumer confidence in connected products. A more positive approach takes a proactive position to add value by providing security education, emphasizing all the steps the vendor is taking to secure the connected home. In the end, relieving consumers of as much responsibility for security as possible is the most productive path.

New security gateway products like Bitdefender Box, Dojo by Bullguard, and Cujo are on the market for less than $200 and focused on providing additional security at the router level as well as educating consumers about additional security options to secure the home network and all devices on them.