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

A Network is Only as Secure as its Weakest Device

By: Yossi Atias

The Internet of Things (IoT) is growing exponentially and, unless you have been hiding under a rock, it's hard not to notice the proliferation of connected devices we're utilizing in our daily lives. According to Gartner, as of the end of 2017, there were 6.3 billion smart devices already connected to networks, and it is predicted this number will grow to **20.4 billion by 2020.** Gartner's estimates tend to be more conservative than others, some of whom predicted 50 billion devices by 2020. However, Gartner's figures are collated from an installed base of smart TVs, fridges, security cameras, speakers and other devices.

Other analysts and consultancy firms offer similar predictions. McKinsey even said that IoT could generate up to $11.1 trillion a year in economic value by 2025, provided businesses and policymakers throw their weight behind it.

Security—or the lack of it—is increasingly a pressing concern with IoT devices. However, this is an area in which CSPs can thrive. They can protect their customers' network's weakest point. By leveraging their network connectivity services, CSPs can build sustainable, cost-effective and revenue-generating cybersecurity services.

But before we dive into the detail, let's look at the specific security issues that are opening up opportunities for CSPs.

Profit, not security

IoT device manufacturers have—by and large—simply not prioritized security. They are driven by tight margins and rely on high-volume scales to generate revenue and profit.

Radisys
Getting Edgy
Optimizing performance and user experience with edge computing
intel
ERICSSON
vasona networks
FierceWireless

Embedding good levels of security into IoT devices requires significant investment and security expertise. If device manufacturers are to ensure robust security, they must ensure security-by-design at the planning stage. From a manufacturer's perspective, however, this often means a product redesign to accommodate, for example, larger processors that power security features.

In turn, this makes devices more expensive and larger, eating into what are often slender profit margins. The fact is that many device manufacturers are simply not equipped to manage security;

how many security architects, security-certified software engineers, or network experts do they employ?

The specific security concerns around IoT are:

1. Default login credentials: There are already tens of million manufacturers only use a small number of default password a de use the default passwords after pur ha e quite challenging for consumers t the password and username, and as a result, many people ke

2. Software updates: Many smart device manufacturers don't r devices. If a software vulnerability is discovered, there's little t exploited without the manufacturer stepping in.

3. Insecure user interfaces: A well-designed product will lock brute force attacks. However, many IoT devices are not well-designed and persistent hackers can manipulate them.

4. Unencrypted communications: Some devices lack basic encryption. For instance, data that is sent between the device and server is unencrypted, potentially exposing personal information such as names and addresses to hackers. Of course, this is just an open invitation if someone is listening in on the device.

5. Poor privacy protection: There are smart devices that amass a mountain of data, such as location information, usage patterns, names, addresses, conversations if it includes voice technology, and more. Often it isn't clear what privacy protections are in place to safeguard data.

6. Malware: Malicious code that targets smart devices has begun to surface, with a notable example in the Mirai botnet. This is simply because some IoT devices are poorly designed and exposed to cyber attacks. We've also already seen additional IoT botnets created from Mirai that target IoT devices.

7. Hacker attacks: Given the growing number of devices in play, it's hardly surprising that hackers are turning their attention to IoT. Common hacking techniques such as buffer overflows, code injection, and spoofing have already been detected. These and other attacks are going to become increasingly commonplace.

8. Unsecured ports: Many smart connected devices use unsecured ports. This is another major flaw. It allows hackers easy access to a device for exploiting its existing vulnerabilities.

Consumer awareness

Clearly many consumers are aware of the security issues. They may not know or understand the details, but there is a growing consensus that, by and large, smart connected devices can be vulnerable. In short, there's a growing awareness that smart devices can be a hacker's dream and a cybersecurity nightmare.

This is driven by widespread media coverage of IoT hacks—whether it's the Mirai botnet taking down some of the biggest web operations in the U.S., a parent and baby being stalked by a hacker who has taken control of a baby cam or hackers remotely controlling utility services in a building.

CSPs can step in to provide security

The variety of devices comprising IoT is staggering—while standardization of security is most blatantly lacking. These devices need to be supported and users need to be updated on every vulnerability. And, if manufacturers don't update them, then patching is not an option. Unfortunately, protecting these vulnerable devices is well beyond the ability of most consumers.

CSPs, however, are perfectly positioned to successfully address these issues. They already own

Inquiry Form

First Name*: ____ Last Name*: ____ Company*: ____ Title*: ____ Email*: ____ Message ____

Submit

1

Web Links

- The Future Starts at the Edge White Paper
- MobilityEngine™ 5G RAN Software Datasheet
- The Journey to 5G
- Accelerating Commercialization of Open Telecom Innovation

2

About Radisys

Radisys, a global leader in open telecom solutions, enables service providers to drive disruption with new open architecture business models. Radisys' innovative disaggregated and virtualized enabling technology solutions leverage open reference architectures and standards, combined with open software and hardware to power business transformation for the telecom industry, while its world-class services organization delivers systems integration expertise necessary to solve communications and content providers' complex deployment challenges. For more information, visit www.Radisys.com

3

the network and provide connectivity and Internet services. CSPs already offer some network security services, provide content such as TV, and have established billing relationships. Moreover, bundling services is second nature. Most importantly, they are also trusted brands.

IoT devices already use a CSP's existing infrastructure for network connectivity, hence CSPs are in a perfect position to serve as gatekeepers. The residential gateway is typically the weakest point of a home network. Yet from a CSP's perspective, it is the ideal point from which to deploy advanced cybersecurity. A range of advanced and scalable security technologies can be deployed at the network edge to effectively address all the vulnerabilities mentioned above.

Advanced security at the network edge

Automatic device discovery detects all devices on a wi-fi network and assigns them to appropriate security groups, and then tailors specific profiles for each device to enforce security and privacy policies.

The network edge security needs to include a continuous vulnerability scanning, smart firewall, enterprise-grade intrusion detection and prevention, and URL filtering engine securing all devices from malicious activity. This system must be constantly updated by advanced threat detection tailored to identify IoT-related vulnerabilities and threats.

Artificial intelligence delivers intelligent security

Importantly, advanced behavioral analysis based on cutting-edge artificial intelligence and machine learning technology can use sophisticated algorithms for detecting threats, and even regarding already compromised devices.

When anomalies are detected, a cloud-based platform distributes updated policies to all the residential gateways protected by the CSP, ensuring each home network is constantly updated to meet the latest threats.

Cost-effective for CSPs

This approach provides a raft of benefits for CSPs. First of all, it provides an additional subscription-based revenue stream from a large percentage of existing subscribers. This user base is only going to grow as more IoT devices come online. A wide range of manufacturers are certainly pushing in this direction, including Amazon and Google with their smart home hubs and speakers. This alone explicitly acknowledges that IoT is going to be much bigger than it already is.

A 2016 **Ericsson mobility report** claims that IoT sensors and devices are expected to exceed mobile phones as the largest category of connected devices in 2018, growing at a 23 percent compound annual growth rate (CAGR) from 2015 to 2021. This is close to what we are already witnessing; more IoT devices already connected in 2018 than there are people on the planet (and the year isn't up yet).

But the issue is not just about providing IoT security alone. Security is also a key enabler for IoT adoption when customers understand comprehensive security is available. Further, it doesn't require huge investment; it's simply a question of leveraging the residential gateway for value-added services. It also safeguards CSP's weakest link—that is, CPEs and residential gateways.

CSPs can offer different cybersecurity offerings such as basic, standard, and premium packages. Further, they gain full visibility into customers' home networks, including device inventory. The insight gained into customers' device vulnerabilities also provides a raft of information that can be used for targeted marketing.

Managed cybersecurity services increases operational efficiency—such as customer support and customer service—thanks to the increased insight into residential networks and IoT devices in use. This will most certainly strengthen brands, too. Overall, providing this deep level of IoT device security delivers a compelling advantage in a fiercely competitive and saturated market.