IoT Security Demands a Multi-Layered Approach

With IoT Devices Operating Anywhere, Visibility and Control Must Exist Within IoT-connecting Networks

FROST & SULLIVAN

An Executive Brief Sponsored by
Allot Communications

Michael Suby
VP of Research, Stratecast | Frost & Sullivan

October 2018

INTRODUCTION

For years now, enterprises have been preparing for and acting on digital transformations; key to which is the Internet-of-Things (IoT). IoT describes the practice of embedding processors and communications capabilities in all types of devices, from consumer goods to manufacturing devices, control systems, and sensors. By transforming these common devices into "smart devices," businesses will be able to unlock tremendous benefits such as optimization and automation of business processes and production systems.

According to Frost & Sullivan, the number of deployed IoT devices is expected to reach 45.4 billion by 2023.[1] As the world is now firmly entrenched in the IoT age, enterprises are finding that they have become highly dependent on IoT devices for critical business functions. IoT dependence is now commonplace in enterprises of all sizes, and includes organizations in traditionally less information technology (IT) savvy industries such as manufacturing, retail, healthcare, and automotive.

Unfortunately, enterprises are discovering that IoT devices present unique challenges that defy traditional perimeter-based and bolted-on endpoint-security tools and practices. Enterprises require a new and broader reaching model for mitigating cyber risk introduced by the unavoidable IoT trend. Most likely, a secure IoT landscape will require a combination of network-based protections, such as behavior analysis and anomaly detection; and built-in security controls such as a Trusted Execution Environment (TEE), trusted boot, and other root of trust mechanisms.

The pressing need to secure the IoT presents new opportunities for the telecommunications industry, including mobile network operators that provide connectivity for millions of IoT devices operating remotely via cellular connections. The IoT trend has already presented opportunities for network operators to deliver enhanced customer value through IoT connectivity and value adding services. Yet, telecommunications companies are increasingly expected to deliver IoT connectivity that is secure. The CTIA Cybersecurity Certification Test Plan for IoT devices represents an organized industry-led initiative to combat IoT-related risk, and highlights the importance of IoT security in the wireless industry.[2]

IOT CHALLENGES AND THREATS ESCALATE CYBER RISK

While IoT presents new opportunities for massive business benefits, it also entices enterprises to deploy new and untested IoT devices rapidly and in far-flung locations—too often in locations where they lack essential visibility and the means to enforce security controls. The end result is that new vulnerabilities and uncontemplated cyber risks are present and ripe for abuse by malicious actors. To wrap one's hands around this IoT cyber risk and how to address it, two categories of challenges must first be understood: device-related and organization-specific.

IoT Device-Related Challenges

With little regulation in place defining a minimum level of security, consumers and businesses alike are exposed to IoT devices with gaping vulnerabilities. This is the root problem that led to the infamous massive Mirai distributed denial-of-service (DDoS) attacks in 2016. The Mirai botnet relied on a simple vulnerability: devices shipped with factory default administrator credentials; and most disconcerting is that the vulnerability was publicly reported months earlier.

[1] *Securing the Connected Ecosystem—Leading Security Solutions and Approaches for IoT*, Frost & Sullivan, Jan. 12, 2018, available on Frost.com

[2] *Wireless Industry Announces New Cybersecurity Certification Program for Cellular-Connected IoT Devices*, CTIA, Aug. 21, 2018 accessed here

When IoT devices do function properly and with minimal vulnerabilities, these devices continue to represent "unusual" and unique characteristics compared to traditional devices that IT organizations oversee. IoT devices have limited processing power and storage, and may have proprietary operating systems, real-time operating systems (RTOS), or may use a pared down version of Windows or Linux, such as Windows IoT or Android Things. As a result, IoT devices are unable to support a client-based security software model. Additionally, these devices may be transient, connecting briefly or at certain times of day; and may be mobile, crossing multiple network boundaries. Many enterprises have found that traditional IT security controls are inadequate when it comes to IoT security. Simply, these security controls were not designed for IoT.

This category of connected, smart, but limited IoT devices includes distant and remote devices that typically connect to a cellular network. For these "off-network/beyond the perimeter" devices, enterprise IT organizations have limited options for enforcing security controls, and almost zero visibility on the performance and behavior of these devices. The enterprise may attempt to use specialized gateways or other methods to ensure secure connections to the central IT organization. However, in many cases, these IoT devices are subject to conditions and activities on CSP-owned networks that complicate, operationally and economically, the placement of gateways owned and operated by enterprises.

Organizational Challenges with IoT

The nature of IoT devices also creates challenges within traditional organizational processes and practices. Most notably, IoT devices may operate on Operational Technology (OT) networks, but pass data and receive control information from the IT environment. As such, IoT crosses the gap between the traditionally segregated OT and IT groups. These groups operate differently, at drastically different tempos, and each with unique processes. A primary difference: OT networks are designed for performance and function, and are not typically connected to the internet or IT networks. As a result, OT organizations are accustomed to rapid project initiation and deployment to achieve rapid results, with traditionally limited exposure to and concern for the myriad online threats today. By comparison, IT network planning includes accommodations for security risk mitigation strategies and practices.

A specific organizational risk is that remote and mobile IoT devices are becoming integral to business processes. Businesses are more reliant on IoT than ever, using IoT devices to track assets, manage fleets, monitor patients, ensure proper functioning of production systems, and much more. These IoT-derived capabilities are the building blocks that will enable enterprises to achieve greater optimization, and even automation, of key business processes. However, a heavy reliance on remotely deployed and mobile IoT devices represents a vast virtual expansion of the enterprise network perimeter, and exposes a broader attack surface to threat actors.

IOT CYBER RISK IN ESSENTIAL INDUSTRIES

IoT-specific cybersecurity challenges open the possibility of data theft, network intrusion, business disruption, and loss of control over devices. In August 2018, the FBI issued a public service announcement warning that threat actors were compromising IoT devices for malicious purposes, such as creating proxies from which to hide their activities and theft of sensitive data.[3] These types of malicious activities can lead to costly and embarrassing data breaches, as are so often reported in the media. However, loss of control over IoT devices can lead to catastrophic consequences in vital industries such as Digital Health and Fleet Management.

[3] *Cyber Actors Use Internet Of Things Devices As Proxies For Anonymity And Pursuit Of Malicious Cyber Activities*, Public Service Announcement, Federal Bureau of Investigation, August 2, 2018, accessed here

Digital Health

The healthcare industry is undergoing extensive technological change as part of the digital transformation era. Digital Health allows health clinics to adopt practices that improve efficiency, and ultimately, treatment efficacy. For example, doctors can utilize mobile applications that allow them to perform visual inspections, remote health assessments, and patient monitoring services. Digital Health organizations, including hospitals and clinics, are increasingly embracing "connected" and "smart" medical devices as they modernize their systems. Cutting-edge care providers are able to monitor IoT-based health sensors and control devices such as pacemakers remotely, to detect problems before they arise.

Unfortunately, Digital Health organizations have become a popular target for cyber attacks, as hackers recognize the black market value of health data—Electronic Health Records (EHR) include extensive patient personally identifiable information (PII) and financial data such as family names, work history, residence information, credit card numbers, and social security numbers. Additionally, these records may also include patient health data that may be sensitive and could be used for targeted harassment or extortion.

Threat actors are now targeting Digital Health IoT devices as vulnerable points of network entry and as footholds to use as potential launch points for follow-up attacks. Advanced threat actors now understand the value of patience, as they engage in carefully calculated efforts to compromise network defenses, establish a foothold, and carefully explore the internal network for sensitive and high value data stores worth stealing, such as EHRs.

But Digital Health IoT devices are also moving beyond the walls of clinics and hospitals. IoT Digital Health devices such as biometric sensors and health monitors may be extremely sensitive to tampering, and disruption may cause possible physical injury. A recent proof-of-concept revealed in a 2018 Black Hat Conference presentation demonstrated the ability to deploy malware on pacemaker devices.[4] Over the course of the Black Hat presentations, many dangerous vulnerabilities in Digital Health IoT devices were announced, including the ability to hack insulin pumps, remote patient health monitors, and pacemakers.[5]

Hacking proof-of-concepts targeting pacemakers were first revealed over 10 years ago, but were considered unrealistic as they required an ability to modify radio signals. More recent research demonstrated the ability for hackers to remotely gain control of pacemakers to manipulate the pace of operation or drain the battery. Little imagination is required to understand the potential real-world impact a hacker could create if able to compromise Digital Health IoT devices.

An additional consequence of IoT adoption in Digital Health organizations is a greater reliance on internet connectivity. Forward-thinking enterprises that recognize the value of IoT may also adopt cloud services such as Amazon AWS, to support IoT deployments with scalable, on-demand storage and compute power. According to the Frost & Sullivan *Global Digital Health Outlook 2018* market study, "all healthcare stakeholders will need to utilize the cloud to manage increasingly complex data generated from a mix of patient- and hospital-based monitoring systems…the economics of digital healthcare will require cloud-based services."[6]

Fleet Management / Asset Tracking

Fleet Management and asset tracking companies rely on steady streams of information regarding asset location, operational status, and other factors, to keep a high degree of productivity and ensure timely deliveries and arrivals.

[4] *A New Pacemaker Hack Puts Malware Directly On The Device*, Lily Hay Newman, Wired, August 9, 2018, accessible here

[5] *Hacking Pacemakers, Insulin Pumps And Patients' Vital Signs In Real Time*, CSO Online, August 12, 2018, accessible here

[6] *Global Digital Health Outlook 2018*, Frost & Sullivan, July 2018, accessible at http://www.frost.com/k262

Connected Fleet Management technologies can help to prevent or reduce collisions, which will help to minimize lawsuits, repair costs, and insurance rates. As an example of value-adding connected Fleet Management strategies, IoT functionality and internet connectivity will enable shipping companies to pursue "platooning" techniques. Platooning uses wireless connectivity to allow individual drivers to create convoys of multiple vehicles, delivering benefits such as reduced road congestion, fuel consumption, and driver downtime.

Fleet Management companies are extremely motivated to guarantee safe, timely, and complete deliveries, as well as to safeguard information about these operations. Any disruption of connectivity can block important over-the-air updates, telematics data and control data; leading to various problems ranging from downtime, fines or penalties, to real world damages.

Connected Fleet Management vehicles have multiple sensors and data systems including telematics, wireless connections, diagnostic ports and sensors, which are all exposed to the possibility of data breaches through the connection to the IoT. Vulnerabilities in connected consumer cars provide an example of potential exploits: in 2016, a security researcher discovered a vulnerability in the APIs of remote vehicle access applications for Nissan Leafs. The exploit granted the researcher control over in-cabin climate systems, and disclosed GPS data.[7]

Critical automotive systems such as steering, braking, and safety controls are extremely sensitive to tampering, and are thought to be equally well protected. However, security researchers have demonstrated a remote exploit in Chrysler Jeep vehicles that allowed attackers to remotely seize control of both vital and non-vital systems ranging from climate control to windshield wipers to braking controls. Attackers were able to control steering functions when driving in reverse as well. Traditionally, access to these critical driving functions has been protected by separating these vital control functions onto a specialized computer circuit called a Controller Area Network (CAN) bus. But the researchers were able to reach this system by first exploiting a vulnerability in the in-vehicle infotainment (IVI) system—a severe breach of an expected security control in any vehicle.[8]

A similar vulnerability in IoT connected Fleet Management vehicles could cause devastating effects, including costly and embarrassing damages to the fleet owner, as well as real-world damages to property, injury, maiming, and loss of human life. In another example, compromised GPS information could be used by malicious actors to disclose cargo information, or track shipments. This type of data theft could be more innocuous in nature, such as an attempt to embarrass a targeted company by publishing routes or cargo manifests. However, if sold to a criminal organization, stolen IoT data could possibly be used to coordinate and improve efforts at theft or hijacking.

Moreover, every vehicle sold in the United States since 1996 must have an on-board diagnostic (OBD) interface. Today, anyone can purchase a cellular ODB2 plug-in (offered also by some CSPs) to remotely monitor car performance and track its location. They are offered and used extensively in the auto insurance industry, to collect driver behaviors to support premium discounts and encourage safer driving. Thus, cyber risks are not limited to the latest vehicles; even relatively old vehicles can be connected to the internet and, subsequently, become vulnerable to cyber attacks.

[7] *Nissan Car Hack Allowed Remote Access*, Tom Spring, Threatpost, Feb. 25, 2016, accessible here

[8] *Hackers Remotely Kill A Jeep On The Highway—With Me In It,* Andy Greenberg, Wired, July 1, 2015, accessible here

IOT SECURITY REQUIREMENTS

There is no one silver bullet that can address IoT cyber risk in its entirety. Instead, IoT security is best approached as a combination of layered best practices and technologies. For example, use of TLS for mutual authentication between IoT devices, and deployment of IoT-aware firewalls on the corporate network are useful in ensuring communications integrity and access control, but they are just starting points in addressing IoT cyber risk.

To place this multi-layered approach into perspective, consider remotely deployed IoT devices. These devices, whether climate sensors in fields, patient monitoring devices, or sensors tracking fleet movements and operations connect via service provider networks that are not under the enterprise IT domain of control. These IoT devices require low bandwidth or even ephemeral or transient connections to third-party networks well beyond the ownership or control of the central enterprise IT organization. Moreover, while some IoT devices might support the use of security controls on the device itself, enterprise IT organizations must operate under the assumption that, like any other compute system, there will be vulnerabilities. Hence, the need for a multi-layered approach.

With these requirements in mind, and given the unique challenges presented by remote and/or mobile IoT devices, a crucial point of visibility and control is the network to which these devices connect. Frost & Sullivan recommends that IoT includes a network-based layer with capabilities built and offered by the network service provider that deliver on the following:

- **Policy-based Protections** – IoT devices are typically designed for a specific purpose with a pre-defined set of functions, and have well known behavioral patterns. Most service provider IoT solutions should provide a well-defined set of communication parameters for robust policy definition and enforcement for connecting IoT devices. These policies can be defined based on IoT asset identification, device visibility (ports, protocols, etc.), and profiling within its asset class. Such policies define minimal security requirements for connecting and controlling access to and from IoT devices, much like a firewall provides a foundation of allowing only approved, "known good" connections to the local network, and blocking all other connections. Additionally, a complete solution will include a means to enforce these policies, and generate risk alerts for non-compliant devices.
- **Proactive Protections** – IoT solutions must provide a means to deliver more advanced protections that are granular and asset-specific. Most likely, this would require the use of behavioral monitoring and advanced analytics to identify and alert or block abnormal and suspicious activities. This is the vital counterpart to the policy enforcement component, deploying active measures to identify malicious or suspicious activities. Proactive protections would provide intrusion detection and prevention capabilities, anti-malware and bot protection, in addition to behavioral analysis and anomaly detection.

Comprehensive Security Deployment Necessitates Partnership

A mixture of tools and partnerships will be required to design, implement, and execute on an effective IoT security strategy. Risk mitigation, such as quarantining, is a vitally important capability because simply detecting threats or security exposures is not enough—protective action must be taken. Similarly, remediation capabilities, such as modifying network-enforced acceptable use policies, are another important capability that may require integration across multiple technologies.

Importantly, policies must have a hybrid IT application attribute, as IoT devices are likely to connect and rely on a wide range of access points. Whether asset origination or the resources the IoT asset is communicating with are in on-premises, co-location facilities, private clouds, public clouds, or Software-as-a-Service applications, risk management is feasible and must be maintained through a single administrative console.

IoT Security Presents Opportunity for Service Provider Leadership and Enhanced Customer Value

Enterprises no longer have well defined network boundaries, and likely have many devices exposed to internet threats. This challenge is becoming widespread, especially with the proliferation of low bandwidth IoT devices, such as sensors that typically access a radio access network (RAN) owned and managed by CSPs. IoT data must then cross over multiple networks, and may transit through multiple peering points before reaching the enterprise network. As a result, these devices primarily operate beyond the reach of the cyber security defenses protecting the enterprise network.

Service providers operate multiple networks that likely have varying quantities of IoT devices accessing the network, or passing critical data over these networks. Service providers, as the "all seeing" entity of IoT communication flows (and communication flows of other assets) are strategically positioned to identify, assess risk, and facilitate risk mitigation and remediation.

Enterprises increasingly rely on the connectivity provided by a host of service providers to maintain connection with IoT devices that they rely on—whether owned or otherwise. As a result, the critical role of the service provider as first line of defense is crystallizing as digital transformation, including IoT adoption, becomes a global phenomenon. IoT presents a set of unique challenges that require visibility and controls not only in the enterprise network, but ingrained in the fabric of all the networks that IoT devices depend upon. Service providers that can meet these growing expectations will be considered industry leaders with a differentiated value offering.

THE LAST WORD

The digital revolution is here, and IoT is proving to be a particularly unique security challenge. Cyber attacks are increasingly popular tools of nation-states that seek opportunities to cause financial and even real world harm, while hiding behind the anonymity and deniability afforded by the internet. Digital Health and Connected Fleet Management industries represent two vital segments of critical national infrastructure, and are potential targets for cyber criminals, hacktivists, and hostile nation-states.

However, the technologies and practices required to secure IoT devices are different than conventional enterprise network security tools. This resulting challenge is not limited to Digital Health and Connected Fleet Management, but affects all industries. To combat, a multi-layered security approach is essential. Favorably, network service providers are strategically positioned to offer a crucial layer of visibility and security control suitable across countless IoT use cases and industries. Our advice is to investigate with your network service provider what it can do for you in not only connecting your IoT devices but in systematically mitigating the cyber risks those IoT connections create.

Michael Suby

VP of Research
Stratecast | Frost & Sullivan
mike.suby@frost.com

Silicon Valley
3211 Scott Blvd
Santa Clara CA, 95054
Tel: 650.475.4500
Fax: 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion