SCTE·ISBE CABLE-TEC EXPO 2017
DENVER, CO
OCTOBER 17-20

2017 Fall Technical Forum
SCTE·ISBE • NCTA • CABLELABS

Assuring Security in the IoT

Implementing a Behavioral Analysis Approach to Thwart IoT Attacks

A Technical Paper prepared for SCTE/ISBE by

David Yates
VP Product Line Management
Guavus, A Thales Company
1800 Gateway Drive, Ste. 160
San Mateo, CA 94404
650-823-0674
David.yates@guavus.com

Table of Contents

Introduction

The “Internet of Things” (IoT) is here. Manufacturers across industries are reinventing consumer products—from refrigerators to thermostats—by incorporating smart, connected capabilities to capitalize on the global IoT market. IoT is growing exponentially; Experts forecast upwards of 50 billion connected devices by 2020. The industry estimates that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016. Total spending on endpoints and services will reach almost $2 trillion in 2017. While consumers purchase more devices, businesses spend more. In 2017, in terms of hardware spending, the use of connected things among businesses will drive $964 billion.

These businesses hope to ride the IoT wave to achieve competitive differentiation, cultivate additional revenue streams, deliver new monitoring capabilities that will transform maintenance services, and/or enhance and personalize the customer experience. Yet in the race to accelerate time-to-market for these next-generation products, many companies are giving short shrift to IoT-specific security challenges. IoT security concerns are comparable to enterprise IT concerns but complicated by scale, given the sheer number and variety of endpoints. Too often, organizations fail to account for security considerations during initial product development and test cycles. Alternatively, they opt to release IoT-enabled products quickly, only to address security issues after the fact. Both scenarios set the stage for possible breaches that can impact a company’s brand reputation and bottom line.

Concerns about IoT security are escalating as the number of IoT-enabled products multiplies. Experts have raised the possibility that any device connected to the Internet is at risk for hijacking. They underscore the unique security challenges of IoT, specifically that the small size and limited processing power of connected devices could impede encryption and other robust security measures.

It’s not just about the “things” under ownership or allowed to connect to the network. Imagine a situation where a flaw in a common network connected device was used to launch a Distributed Denial of Service (DDoS) attack—there have already been cases of home cable modems being used in botnets. This means systems may be affected by the insecurity of “things” in general. Similarly, if “things” are designed insecurely and have no mechanism for patching, they can act as a pool of malware capable of attacking other systems. So, the security of IoT is a concern for the entire Internet community, not just device owners. Those devices can affect the entire community, making for a common interest in the fundamental security of them.

Experts advise organizations to start building consumer trust in IoT devices by prioritizing security and by adopting “security by design” practices that integrate security capabilities at the earliest stages of product design. However, companies are still a long way from instituting security-by-design best practices. Most firms in the planning stages of IoT product development remain focused on connectivity, although organizations that have already released IoT-enabled products are grappling with more complex issues, including security.

Given the scope of possible issues, it’s increasingly clear that any business entering the IoT fray needs to consider security at the outset, not after the journey is underway.

Content

I. Business Trends and Pressures

At a high level, there are many business trends and pressures that will impact IoT security in the enterprise. IoT will represent a significantly complex system with low-capability users, creating a rich and evolving risk environment. Consumer and industrial ecosystems are different, in terms of technology, development, and priorities. There will be differing threats, actors, and reasons for targeting IoT. And, there will be additional considerations because of the technology's scale, adoption rates, and regulatory environment.

Cyber and physical worlds converge

The industrial product lifecycle encompasses cyber-physical systems where security equals personal safety. While there are complex governance and management processes, industrial systems often have long-lived and out-of-date information management systems due to underlying hardware. This represents a significant operational impact and financial investment. And includes a concern about connecting industrial systems: The industry may fail to learn lessons from the PC world about the importance of patching, upgrade lifecycle, and built-in security.

The consumer product lifecycle has a faster lifespan—focused on new features and quick time to market with minimal cost, which ultimately causes rapid obsolescence. The short support and upgrade periods means large numbers of devices will be left out there unpatched and forgotten. Some new business entrants won't even survive the length of time their products are in use. Also there will be a low bar to entry for IoT creators, which means there will be less experienced developers who aren't necessarily knowledgeable about security and privacy. The consumer environment makes use of crowd-sourced product development and common libraries; this results in systemic homogeneity that may increase the severity of widespread compromises like Shellshock and HeartBleed.

Different threats, actors, and reasons

The New Style of Business means there are new models to protect. Unfortunately, the criminals are smart and always seemingly one step ahead. With the changing landscape of technology and applications in the connected world, threat actors and attack vectors are expected to morph as well. In the beginning, threat actors will most likely be motivated by fame, focused on the newly interesting, novel technology. They'll want to showcase their hacking expertise and expose vulnerabilities.

But as IoT adoption spreads, the technology will be attacked or compromised based on the value to the attacker—monetary, ideology, or business disruption. Since real-time interactions are key to IoT value, actors may use jamming and interference of communications. This may include misrouting of information, impersonation, or flooding and draining of resources, which could cause a distributed denial of service (DDoS) or at least confusion. Many legacy industrial security controls assume the "protected" perimeter with walled environments. The connectivity into broader networks may inadvertently impact the physical security.

II. IoT Security Pain Points

IoT is ushering in whole new categories of products and services, but it is also creating novel opportunities for cybercriminals and other malicious actors to infiltrate networks and gain unauthorized access to data and systems. IoT hardware has access to sensitive information via a network connection—meaning it must be safeguarded just like any other enterprise endpoint. Unlike standard IT equipment, however, IoT products typically lack the processing power and memory to run antivirus software, firewalls, or other widely used enterprise IT safeguards. Similar to enterprise IT security, threats to IoT-enabled devices come in many forms and flavors. Following are some additional critical areas to consider as IoT evolves:

Outdated security model

Traditional IT security policies and controls will be untenable. The security model for it will need to transform to support all of the new aspects of operational technology security and transition to a data-centric aspect. Security will need to be automated, distributed, context aware, and real time.

Unauthorized Access and Control

By far the most pressing concern among companies that are building IoT products surrounds unauthorized access to an IoT device and/or restricting an unknown entity from taking control of its functions. Consider an early IoT product as a case in point. A smart refrigerator, which supported email and social networking applications, lacked the appropriate security features. As a result, it was compromised as part of a security scam that leveraged 100,000 consumer devices to send 750,000 malicious emails and online attacks. Researchers from the security firm Proofpoint discovered that the refrigerator's email capability served as a conduit for an attacker. Why? Despite its similarity to traditional endpoints, the fridge lacked the antivirus software and firewalls used to protect desktops, laptops, and servers.

Other common methods for hacking into IoT devices include spoofing, when a device pretends to be something or someone it's not, and identity forgery, when an unauthorized or unauthenticated user takes control over a device, or stolen credentials are used to gain access to data.

Also in this category are: **DDoS attacks**, which block a system from providing service by making it unusably slow, consuming available storage, or crashing. As with enterprise IT breaches, denial-of-service attacks in the IoT world are far-reaching, potentially impacting individual devices, vendor device accounts, third-party partners, and even end-user applications.

Compromised Data

A major point of IoT is to collect a treasure trove of data—about the product's physical state, how it's used, and environmental conditions, for example—which can later be mined for insights. If hackers gain unauthorized access to an IoT product, they can alter or maliciously damage the collected data. At best, this mitigates the usefulness of the data; at worst, it puts the company at risk for lost revenue opportunities, unhappy customers, and/or brand damage.

Man-in-the Middle Attacks

As in the enterprise IT world, an unauthorized entity can intercept communication and gain unintended control over an IoT product, such as a smart thermostat or home security system. The intruder could then

engineer a malicious action, such as a home invasion, or turn an IoT device into a vector for stealing payment information.

III. IoT Security Guiding Principles

As the security landscape continues to evolve, so will the threat actors. Currently, there are highly capable threat actors, capitalizing on the prolific black market to buy and sell capabilities and information. This will only continue to grow as additional devices and data sources come online. The growing volume and exchange of data require new technology to protect the user device and data entity. And, the expanding threat landscape and sheer number of devices— some smart, some not—will require adaptive, self-defending, autonomous capabilities.

In the future, there will still be fundamental quality and security requirements for solutions, systems, and devices. This isn't so different from current solutions, but there will be greater emphasis on beginning with the end in mind, because mitigating at the end becomes impossible with the distributed, massive scale of IoT. So, "things" on the Internet need to be designed for security, upgradability, and resiliency. IoT systems need to be safe and reliable with the following underlying attributes:

- **Secure access management**—The things and systems in the IoT ecosystem need to be identified and managed in the same way traditional enterprise systems are controlled. Key processes, which include identification, authentication, and authorization, will become more important because of the sheer quantity and variety of IoT systems. Trust mechanisms will be based on context and value scales, not simply a binary choice.

- **Self-protection**—IoT also needs self-protecting and self-healing systems. These attributes are important since systems will no longer have the advantages of a defined perimeter or enterprise-class managed environment. Some devices may also be specialized gateways or intermediaries that provide additional services and protections that can't be included in low power or small form-factor "things." Security solutions will need to leverage the added value of crowd-sourcing and peer intelligence to help form a self-protecting mechanism. These mechanisms will be the basis for resiliency at the device level.

- **Privacy controls**— Because data will be created in increasing quantities and situated everywhere, it's imperative that solutions give clear control of the data to the owner or source. Ownership will be complicated due to the distributed nature of the systems and complexities of the governing environments. Security and privacy will need to be addressed directly at each device and interaction—transaction and communication.

- **Embedded security**—Security will need to be deeply integrated in hardware and application software layers. The diverse functionality and small form factors won't be able to withstand generalized, bolted-on security mechanisms. The technical designs will need to use contextual awareness, adaptive security that senses and responds to a range of trust mechanisms.

- **Real-time information processes**—Information will be pervasive, seamless, and integrated across the whole IoT ecosystem. Solutions will need mechanisms to process and leverage the enormous sets of data into information for safe and reliable operations. Information analytics in

IoT will need to be predictive, proactive, and near real time to operate with resiliency. Always-on operations require continuous security features and controls.

IV. Information Analytics in IoT Security

A major consideration in assessing the model of analytics needed for IoT is the various types of analytics and sources of data used in an application. In a traditional model, descriptive and diagnostic analytics (sometimes grouped as historical analytics) are often developed independently and have multiple connection points to the various sources of data. The structured, semi-structured, and unstructured data that is often stored in different data warehouses and logical locations is connected independently and requires multiple connectors to consolidate all the relevant information. This is time and cost prohibitive and makes it difficult to build IoT Analytics applications quickly and meet business imperatives for timely action. It also significantly delays time to value and is not scalable from an economic point of view.

The first step in designing a new approach is to simplify the process by integrating all the data for an IoT application. That includes all the structured, unstructured, and semi-structured data in the picture. This range of data must be integrated for the analytics that will be run on the data. Better business outcomes are achieved when these silos are removed and analytics are used across a broad spectrum of valuable data.

The second key step in the streamlining process is to unify the analytics layer. In the traditional model, descriptive and diagnostic analytics made the problem challenging because of the “siloed” approach to data access. This issue will multiply rapidly in scale and become much more serious with the addition of predictive and prescriptive analytics. The problem is more acute and unworkable for IoT applications. This traditional heterogeneous and one-off approach to types of analytics will not suffice for IoT because it will take significant time and effort for data management vs. focusing on delivering outcomes based on the analytics. The explosion of data in all forms in IoT requires a more robust and broader lens in order to enable smarter timely actions and better outcomes.

All the types of analytics must be unified into a single engine to ensure scalability and real-time performance. This includes historical analytics (descriptive & diagnostic), real-time streaming analytics, predictive analytics, and prescriptive analytics. In addition, a design philosophy of openness and unification is needed to help customers get results rapidly. Businesses looking to deploy IoT applications cannot be expected to “rip and replace” their existing investments, and need approaches to leverage their existing analytics and data investments and migrate them into a larger unified framework. The payoff is that users will now be able to spend more time on insights and business outcomes that matter most and avoid the time and distraction of creating or managing a complex infrastructure.

The approach to analytics outlined above is a good first step for IoT. However, it is the ability to execute analytics (real-time, on-demand, streaming, historical, predictive, and prescriptive) with relevant contextual and situational data that addresses the critical “last mile” for timely outcomes. This is then combined with the ability to take the steps below in any particular scenario that creates the greatest value.

- Ingesting data at speed and volume sets the stage for additional processing.
- Real-time Analytics processes incoming streams of data from IoT sensors and devices.
- This refined data is then correlated with contextual and historical data to provide a baseline for advanced analytics.

- The next step is to predict failures, anomalies, or patterns using predictive analytics that are based on machine learning over historical and situational data such as external events like weather.
- The final step is to apply prescriptive analytics to determine the next best action to take.

The important point is that specific actions based on a rich understanding of history and context must be taken NOW in order to capture that value. New tools are needed to achieve this ambitious goal for IoT.

V. An Example of a Modern Security Analytics Platform

Through behavior modeling, contextualization, machine learning and reasoning, at big data scale, Guavus' security analytics platform is designed to empower business operations to effectively deliver business outcomes that address IoT business imperatives.

This new platform offers a novel conceptual, machine intelligence approach to analytics and its associated software architecture. It provides 360° visibility across data silos (L3 (network), L7 (application), Threat Intelligence, Data Lakes, Cloud, BYOD and IoT) and opens up data models for threat hunting through its Security Analytics toolkit and modules built ground up for security (on-demand, streaming, real-time).

The focus of the platform is on addressing the challenge of rapidly delivering better business outcomes and value in IoT initiatives and projects. It accomplishes this goal by providing a platform that:

- Delivers faster analytics in real-time with a unique methodology that ingests data (streaming, historical, predictive, and prescriptive) with relevant contextual and situational data to improve the quality of actions that lead to better business outcomes and results.
- Accelerates application development via a set modules and automation that empowers analysts to create faster analytics in minutes vs. months. The platform's faster analytics provide a rapid path to insights and actions that empower organizations to take smarter actions that lead to faster and better business outcomes.

Another important capability is an integrated graph-relational view of identity-asset-network-adversary model which enables persistence, retrieval, search, analytics and visualization across all data sets and data. This powerful capability with pattern and anomaly detection enables analysts to rapidly detect threats which significantly accelerates time-to value for IoT projects. These capabilities empower analysts to be nimble to react to business challenges and create solutions with the platform that enables timely action, implementing complex analytics faster in minutes, not months, and thereby improve business outcomes faster.

By unifying ingestion, all types of analytics, real-time contextual and situational awareness, with behavioral modeling and threat intelligence, Guavus' security analytics platform enables organizations to build applications that will meet the challenges of IoT scenarios. This unification is important not only for performance reasons, but also because the unification between each of the layers requires careful design and engineering to meet the demands of real-time business. Guavus' security analytics platform was built with these imperatives in mind.

Conclusion

For IT security leaders, it's a brave, new world—where it's necessary to step out of the traditional role of compliance and embrace the risk-reward of new IoT business models. This includes building bridges to and skills in the consumer ecosystem and operational technology domains of the organization. Leaders should seek to collaborate with manufacturing and physical security leaders. They should expand more deeply with enterprise risk management, which goes beyond IT systems. Security leaders should also take the lead in raising board-level visibility and protecting the brand. Now, more than ever, information technology is the business, so information security is tied to the brand.

Existing process standards for managing, monitoring, and upgrading should be leveraged. However, this needs to be balanced with a risk/reward approach, not in a universal manner. Details about operational technology will matter in terms of technology and process. Especially in security and risk management, there will be expert shortages, aging assets, and the need for automation and capital discipline. All these should be considered while running the security capability like any other business.

Future-proofing security operations is about getting away from "prevent," and moving past "detect and respond" to security foresight. The key is to: Focus on people, process, and reporting and close integration points between software and tools.

The futures for security in terms of security intelligence and insight include three areas of focus:

1. Advanced protection platforms: information-centric protections, endpoint activity monitoring and self-healing, advanced forensic capabilities
2. Predictive intelligence: advanced sharing capabilities, scalable threat intelligence vetting, feed-based to adversary-centric intelligence
3. Security analytics: detect the unknown with Big Data analytics, create advanced visualizations, establish proactive, counter-intelligence capabilities—hunt teams.

A new Security Intelligence Platform is needed to address this IoT world that demands rapid implementation time-frames and systems that enable intelligent real-time actions that deliver business outcomes quickly. It offers a careful and intelligent balance of unique and powerful security and Data and Analytics Engines that are the core of a broader and Intelligence platform that will work with a wide range of software and databases in place today. It provides powerful module-driven environment with visualization that accelerates time-to-value for even the most complex IoT applications.

This platform offers much more than just new technical approaches or faster "speeds and feeds." It is a new kind of platform for business operation managers that accelerates projects through analytics, behavior modeling, contextualization, machine learning and reasoning and delivers better business outcomes faster for IoT initiatives and applications.

To keep your enterprise safe and secure, adopt a proactive approach that enables you to secure your information while improving its flow throughout the enterprise—enabling innovation, improving collaboration, and increasing competitiveness.

Abbreviations

IoT	internet of things
DDOS	distributed denial of service
IT	Information technology

Bibliography & References

Gartner (2017*). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. [Press Release]. Retrieved from http://www.gartner.com/newsroom/id/3598917.

Russell, Brian and Van Duren, Drew (2016). *Practical Internet of Things Security*. Birmingham, B3 2PB, UK: Packet Publishing Ltd.

