SECURITY IN INTERNET OF THINGS SYSTEMS
# TABLE OF CONTENTS

1. INTRODUCTION ................................................................. 1
2. THE IOT PROBLEM: A NEW LANDSCAPE OF THREATS ................................................................. 1
3. SECURITY BUILDING BLOCKS ................................................................. 1
   3.1 Data at Rest ................................................................. 1
   3.2 Data in Motion ................................................................. 1
   3.3 Data in Use ................................................................. 2
   3.4 Exosite Platform Security Features ................................................................. 2
4. PRAGMATIC END-TO-END SECURITY SOLUTIONS ................................................................. 2
5. ABOUT EXOSITE ................................................................. 3
6. CONCLUSION ................................................................. 3
1. Introduction

Although it has been known under different names over many years, the Internet of Things (IoT) is suddenly the thing. The ability to connect, remotely manage, and monitor networked devices via the Internet is becoming pervasive. This phenomenon is taking place everywhere, from the factory floor to the residential living room to the hospital operating room.

The growth of IoT is occurring at an incredible rate, justly raising alarms about security and privacy issues as we become increasingly reliant on these intelligent, interconnected devices in our lives and businesses. How are we to protect billions of devices from attacks and intrusions that could compromise our personal privacy, public safety, or business viability?

As a global leader in IoT, Exosite is deeply involved in securing sensors, devices, networks, cloud platforms, web applications, and mobile applications for diverse industries. This white paper examines the landscape of security challenges posed by connected devices and outlines Exosite’s approach to address them.

2. The IoT Problem: A New Landscape of Threats

Every week, there are new hacking incidents in the media. Credit card data is stolen, identities are forged, services are overloaded, and private information is leaked. And the rate of security incidents is not going down. According to a recent report by PricewaterhouseCoopers (PwC) on the global state of information security, the rate of information security incidents has grown 48% in 2014 to 42.8 million, which is the equivalent of 117,339 attacks per day.1

As the cost of computation continues to decrease and the number of software-controlled systems that make up IoT continues to proliferate, this problem will only get worse. New devices, networks, cloud technologies, and users will all contribute to this phenomenon.

Devices used in IoT solutions have two major attributes that make them more susceptible to attacks than other personal computing applications:

1. RESOURCE CONSTRAINTS

IoT devices are often resource-constrained, making standard security mechanisms (e.g., TLS) difficult or impossible.

2. ACCESSIBILITY

IoT devices are becoming more accessible. If an attacker can open a device, disassemble the contents, add a USB drive, de-solder RAM chips, convince a user to gain access for them, or use other advanced side-channel attacks2 (e.g., timing information, power consumption, or acoustic signatures), the device can quickly become compromised.

Perfect security is not possible without disconnecting network interfaces. With so many devices, software packages, deployment configurations, and use cases, key tradeoff decisions must be made between ease of use and high security. How do we make these tradeoffs?

For instance, securing communications sent over the wire so that user information cannot be sniffed is of high importance to almost every application, and there are standard mechanisms for doing that. However, preventing a device from having its flash re-programmed, essentially re-purposing a device, may or may not be a problem, depending on the context, application, and sensitivity of the device and its data.

When designing an IoT security solution, the goal is to keep the required effort for attacks higher than the level of the hacker’s motivation.

3. Security Building Blocks

Data is the currency of IoT solutions. Data is the thing we collect, process, analyze, and use to identify and control users, behaviors, and environments. To secure data, it is useful to think about it in three contexts: data at rest, data in motion, and data in use. Exosite’s platform has a number of security building blocks to protect data at every point.

3.1 DATA AT REST

Data at rest is data that is stored on a hard drive, in a database, in flash memory, or in RAM. Data that is customer-private should always be encrypted so that if attackers gain access to the database, they cannot understand the information. Other data, like analog sensor data, may or may not be important to encrypt depending on the application. Of particular importance is the embedded system that may or may not have encrypted flash. Some microcontrollers also allow a fuse to be blown at manufacturing time to disable another user from reading the contents of flash or re-programming it with their own software. These are all mechanisms to protect data at rest.

Exosite encrypts customer-private data in the cloud and works with customers to make recommendations on the use of effective microprocessors, secure memory, and crypto engines that keep data safe on embedded devices.

3.2 DATA IN MOTION

Data in motion is data that is sent from a sensing device over a wired or wireless network, like Wi-Fi, public Internet, or cellular. For this mode, it is important to make sure that an attacker is not able to listen in on the communications and understand

---

2. Side-channel attacks are based on information gained from the physical implementation of a cryptosystem, rather than from brute-force attempts or by finding and exploiting theoretical weaknesses in algorithms.

All content copyright © EXOSITE 2015. All rights reserved.
what data is being sent. This is especially important for private customer data, but for many use cases, it is also important for machine data. Each delivery mode should be carefully analyzed for any IoT solution.

Exosite uses standard Internet security, secure sockets layer/transport security layer (SSL/TLS), on all application programming interface (API) end points to protect data in transit and works with customers to determine the application-specific security layers that are needed.

3.3 DATA IN USE

Data in use is data accessed by a user, machine, or web service with particular permissions that others do not have. For instance, a facilities engineer that is responsible for keeping an HVAC system up and running may have access to see data for their facility, but may not have permission to see another facility. Even more importantly, non-authorized personnel must not have access.

Exosite has a hierarchical security policy that is strictly enforced. It ensures that the right people have access to the right information at the right time for the duration of the product lifecycle, from manufacturing through activation, usage, and retirement.

3.4 EXOSITE PLATFORM SECURITY FEATURES

The Exosite platform has a number of cutting-edge security features that act as building blocks to protect data at rest, in motion, and in use.

1. SECURE TRANSMISSIONS

API end points are all available via SSL/TLS or Datagram Transport Layer Security (DTLS). TLS is standard best-of-class Internet security used in banking applications and most other online financial and health platforms. DTLS provides communications privacy for datagram protocols. Similarly to TLS, DTLS allows applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery, but does so over datagram protocols. DTLS is based on TLS and is intended to provide similar security guarantees.

2. SECURE STORAGE

Physical access to data stored on Exosite servers is restricted. Only staff with badged entry passes may access server rooms, which are monitored 24/7. In addition, the Exosite cloud is architected in a way that separates the data from the application entities that know how to access it. This architectural separation significantly reduces the chance that a would-be attacker can gain access to customer private information on Exosite servers.

3. DEVICE AUTHENTICATION

Device identities are protected via temporal API keys that Exosite calls Client Interface Keys (CIKs). When a device is provisioned in the field, a secure exchange of identity information takes place between the device and Exosite servers over SSL/TLS or DTLS via the Exosite provisioning API interface or through the Exosite Portals application. Once a device receives a CIK, indicating that the Exosite platform has provisioned the device and commissioned it for service, the device uses that CIK for subsequent interaction with the Exosite platform. If a CIK is ever compromised, a user or entity with proper permissions may securely regenerate it without disrupting the flow of data or the usage of the system.

4. USER ACCESS AND AUTHENTICATION

Users are authenticated via an email/password combination. Additionally, users may log in using OpenID credentials from providers such as Google and Yahoo. Once users are logged in, there are many user permission layers, including administrators, managers, and those responsible for billing. A number of custom-defined user groups can be tailored to any application. Temporary API keys can also be generated based on user-level permissions.

5. MANUFACTURING INTEGRATION

The Exosite provisioning system allows original equipment manufacturers (OEMs) to manage full product fleet deployments from manufacturing through usage and retirement. In addition to managing firmware over the air (FOTA) updates, the provisioning system allows manufacturers to integrate with their manufacturing processes to whitelist certain device types, models, and specific serial numbers. OEMs can securely ensure that only devices they produce are allowed to interact with cloud services powered by Exosite.

6. TIME-BOXED PROVISIONING WINDOWS

Once devices are in the field and ready to be used, a multi-factor provisioning method occurs that is orchestrated by the Exosite platform. This ensures that the device is provisioned only during a rolling window of time that coincides with an activation step initiated by an authorizing entity. All OEM customers of Exosite can take advantage of this feature that provides an additional layer of assurance that a device is not being impersonated.

4. Pragmatic End-to-End Security Solutions

Crafting an effective and appropriate IoT security strategy is one of the most important things an OEM must do. In addition to using the standard Exosite security features identified in the previous section, there are additional security aspects that should be considered:

1. SECURE KEY STORAGE

Exosite CIKs are used to identify devices within the Exosite cloud. Because of the way Exosite has designed its security instruments, if a device CIK is compromised, an attacker would only have access to that one device and not to other devices in the system. It is highly recommended that these CIKs be stored in a secure EEPROM or flash memory that ensures an attacker cannot gain access.

2. ENCRYPTED FLASH/MEMORY

Sensor data, customer private data, or anything else that is deemed to be private or secure data should be stored in a secure area of flash/memory.
3. TAMPER PROTECTION
For some applications, it is important to be able to identify when a user begins tampering with a system and disable the device or securely remove the security keys. Some microcontrollers/microprocessors on the market provide tamper protection, but not all IoT applications require it.

4. SECURE RF COMMUNICATIONS
IoT solutions often include short-range RF communications (e.g., Wi-Fi, Bluetooth, 802.15.4, or sub-GHz communications). Care should be taken to understand the security implications in this environment. What could a hacker sniff? What would the implications be if a security incident occurred?

Exosite recommends a comprehensive security review from a reputable third-party security firm as part of any serious IoT deployment.

5. About Exosite
Exosite is a leading developer of cloud-based solutions that enable customers to connect smart devices to the Internet for remote control, monitoring, and business analytics. Exosite’s software solutions are highly scalable, customizable, secure, and reliable. These tools accelerate the time to market for customers building IoT businesses.

Exosite’s cloud-based data exchange platform is a seamless solution to acquire, store, share, and analyze data from remote sources for a variety of end-market applications, including predictive maintenance analytics, SCADA replacement, asset monitoring and control, service-delivery optimization, and the creation of actionable business outputs. Figure 5.1 provides a high-level overview of the type of system Exosite enables.

Exosite has partnered with a number of leading semiconductor manufacturers, wireless communications IC vendors, companies that provide boxed gateway products, and other OEMs interested in Internet-enabling their products by embedding Exosite’s low-cost technologies. These secure, rugged, low-power, cost-effective products can transmit encrypted information from “in the field” systems over the Internet to the Exosite platform. Hosted on servers located strategically around the world, Exosite’s platform acts as a centralized clearing house that collects, curates, and analyzes real-world data in real time. The secure data is then made available to end users for a wide range of value-creating activities, including asset and process tracking, analytics, data aggregation, and command and control in the field. On request, Exosite can create custom user interfaces, including dashboards, graphs, filters, and controls on devices such as computers, tablets, and smartphones. By using Exosite, OEMs and systems integrators can deploy complete connected product solutions in just days.

Founded in 2009 and headquartered in Minneapolis, Minnesota, Exosite operates in the large, rapidly growing IoT market. IoT is the complex ecosystem of connected devices that exchange data with cloud-based platforms that control and monitor assets or processes. In its simplest form, IoT enables seemingly inanimate objects to communicate with end users through sensors, microcontrollers, cellular modules, and cloud-based software.

With the proliferation of connected devices worldwide and the emergence of cost-effective, ultra-low power wireless technologies, the IoT concept has matured and is expected to become a major technology growth theme over the next several years. In a recent report, Cisco projected that 50 to 75 billion devices will be connected by 2020. This is a sharp increase from the 15 billion connected today, equating to six to ten devices per person. As users continue to demand faster, more-reliable mobile data, IoT is poised for significant growth, and Exosite is well positioned to enable OEMs to participate and differentiate in this burgeoning market.

6. Conclusion
Exosite is committed to providing a world-class, end-to-end security foundation to build the future of connected products. This foundation includes solutions for networks, applications, users, devices, and data. In addition, Exosite’s Information Security Management System (ISMS) is modeled after ISO27001/2, so security, privacy, and the protection of sensitive assets and information is at the core of Exosite’s culture. Contact Exosite to discuss how we can help you navigate the security implications of your IoT solution.

FIGURE 5.1: HIGH-LEVEL DEPICTION OF EXOSITE-ENABLED SYSTEM
Exosite has partnered with a number of leading semiconductor manufacturers, wireless communications IC vendors, companies that provide boxed gateway products, and other OEMs interested in Internet-enabling their products by embedding Exosite’s low-cost technologies. These secure, rugged, low-power, cost-effective products can transmit encrypted information from “in the field” systems over the Internet to the Exosite platform. Hosted on servers located strategically around the world, Exosite’s platform acts as a centralized clearing house that collects, curates, and analyzes real-world data in real time. The secure data is then made available to end users for a wide range of value-creating activities, including asset and process tracking, analytics, data aggregation, and command and control in the field. On request, Exosite can create custom user interfaces, including dashboards, graphs, filters, and controls on devices such as computers, tablets, and smartphones. By using Exosite, OEMs and systems integrators can deploy complete connected product solutions in just days.

Founded in 2009 and headquartered in Minneapolis, Minnesota, Exosite operates in the large, rapidly growing IoT market. IoT is the complex ecosystem of connected devices that exchange data with cloud-based platforms that control and monitor assets or processes. In its simplest form, IoT enables seemingly inanimate objects to communicate with end users through sensors, microcontrollers, cellular modules, and cloud-based software.

With the proliferation of connected devices worldwide and the emergence of cost-effective, ultra-low power wireless technologies, the IoT concept has matured and is expected to become a major technology growth theme over the next several years. In a recent report, Cisco projected that 50 to 75 billion devices will be connected by 2020. This is a sharp increase from the 15 billion connected today, equating to six to ten devices per person. As users continue to demand faster, more-reliable mobile data, IoT is poised for significant growth, and Exosite is well positioned to enable OEMs to participate and differentiate in this burgeoning market.

6. Conclusion
Exosite is committed to providing a world-class, end-to-end security foundation to build the future of connected products. This foundation includes solutions for networks, applications, users, devices, and data. In addition, Exosite’s Information Security Management System (ISMS) is modeled after ISO27001/2, so security, privacy, and the protection of sensitive assets and information is at the core of Exosite’s culture. Contact Exosite to discuss how we can help you navigate the security implications of your IoT solution.

6 http://exosite.com

All content copyright © EXOSITE 2015. All rights reserved.
Exosite's cloud-based services provide companies with the technology needed to build and deploy next-generation IoT applications that leverage the expanding world of connected devices. Customers all over the world use Exosite to build custom remote monitoring and control solutions that meet the demands of their connected products, which in turn improves uptime, reduces maintenance costs, and increases value-added service offerings.