DEVICE AUTHORITY™
IoT Security Simplified

HOW TO CHOOSE A SECURITY SOLUTION FOR THE INTERNET OF THINGS:

A GUIDE FOR EVERYONE

By Bruce Judson [1]

Introduction

Providing security users can trust has become an increasingly important phrase in the development of applications designed to take advantage of the huge business opportunities associated with the Internet of Things (IoT). Jeep[2], Talking Barbie[3], Nissan[4], baby monitors[5], and medical devices[6] have all received widespread attention in the consumer, and trade press, for security vulnerabilities. While Gartner, a leading industry analyst, has placed the need for organizations to focus on solutions for "IoT security" at the top of its recently released list of "The Top 10 Internet of Things Technologies for 2017 and 2018.[7]"

Many papers and analyses have addressed corporate practices for providing security in the emerging era of the IoT. [8] In general, these analyses focus on the security-related best practices companies should adopt for the IoT. Unfortunately, these papers do not provide corporate executives with a compelling framework for the most critical aspect of ensuring IoT security: A detailed discussion of the elements that robust Internet of Things security solutions should incorporate. This paper is designed to remedy this knowledge deficit.

What is a Security Solution and Why is it Important?

Security and privacy are often used interchangeably. They are related, but they are different. Companies and institutions adopt privacy policies. These are the rules that govern how they intend to use, share, and maintain the confidentiality of valuable corporate or personally identifiable information. Privacy policies are what companies intend to do with potentially sensitive information they legitimately obtain from users of their products and services.

Security solutions are the way in which companies protect valuable and private information. Security solutions are the practices, services and technologies that companies use to ensure continuous compliance with their privacy policies, whether such policies are reflected in user agreements or are mandated by laws, such as HIPAA in the United States.

Trust is pivotal to the success of the Internet of Things. The need for a robust security solution operates on two distinct levels:

- **First, reliable security solutions are essential to prevent the harm caused by a security failure.** As detailed in press articles on connected cars[9], healthcare devices[10], and many others, the inadequacies inherent in traditional security solutions can permit hackers to remotely control vital systems, ultimately endangering the lives of users. Security breaches can also harm the privacy of consumers and endanger their financial wellbeing, by allowing malicious hackers to obtain confidential information, such as credit card data.

  As a means of illustrating the discussion in these pages, this paper will repeatedly reference the example of a connected insulin pump, worn by a diabetic. As shown in Figure 1, an insulin pump continuously monitors a diabetic individual's glucose level, and intravenously injects glucose into the individual's bloodstream on the basis of such readings. Such pumps may include wireless connections, that allow authorized individuals, such as doctors, to remotely monitor glucose levels, and to remotely adjust the level of insulin injected into the patient's blood. For such a device, a security breach, by a malicious hacker, could cause grievous, perhaps fatal injuries. In the absence of adequate security, a malicious individual could conceivably take control of the insulin pump without the patient's knowledge, and direct the device to flood the patient's body with a lethal volume of insulin.

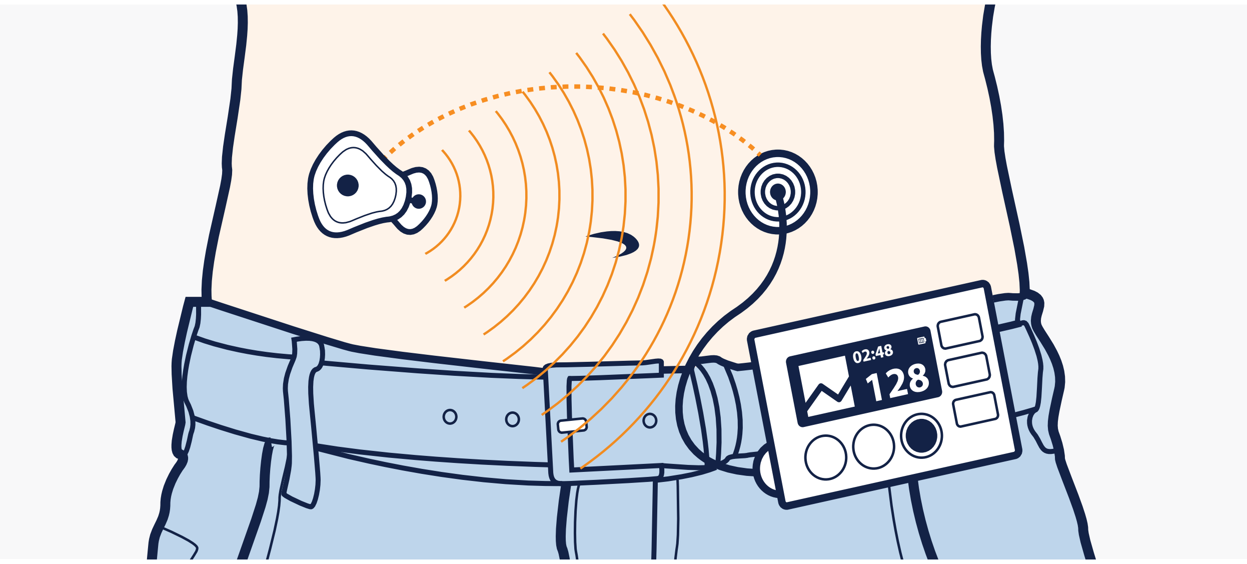


Figure 1 - Connected Insulin Pump

- **Second, IoT service providers and manufacturers must inspire trust in order to attract customers and build successful businesses.** Over the past year, the discussion of potential security vulnerabilities in IoT devices has amplified in the media, in analyst reports, at industry conferences, and led to a clear consensus: Prospective users of IoT products and services now view reliable security as a prerequisite to purchase and use. Indeed, a recent survey by Accenture, encompassing 28,000 consumers in 20 countries found that 47%[11], or almost one-half of those polled, cited privacy risk/security concerns' as a barrier to adoption. To succeed, IoT businesses must earn the trust of buyers.

What's Different About the Internet of Things

The Internet of Things creates fundamentally new security challenges for companies, and ultimately requires product manufacturers to adopt a new security paradigm. Here's why:

- **First, a central aspect of Internet of Things products and services is the frequent, or continuous, transmission of extraordinary amounts of information:** The sheer volume of personally identifiable information being collected, analyzed and (as appropriate) stored, by IoT services creates new challenges for companies.

- **Second, the Internet of Things involves the management of potentially millions of devices connected to the Internet.** Companies have never before needed to manage and protect information generated by so many devices, which may be located in far-off, potentially hostile locations.

For example, every time an insulin pump administers insulin into a patient, the volume injected and the accompanying glucose level are logged to a central monitoring service. Over the lifespan of the device, for each patient, this equates to an extraordinary volume of private information that must be securely transmitted to a central monitoring hub, securely stored and analyzed, and securely routed to authorized devices, operated by patients and doctors, to examine patient-specific activity.

- **Third, the connectivity of "smart" devices offers the potential for malicious exploitation through remote capture and control.** A "dumb" device, which is not connected to the Internet, cannot be remotely controlled by an unauthorized user. Indeed, a device with no connectivity cannot be remotely controlled by anyone. In contrast, "smart" Internet of Things devices, which are connected to the Internet and designed to accept remote commands, inherently create a security risk that must be addressed: Connected devices must ensure they are only accepting commands from an authorized user or system.

The insulin pump may, for example, be designed to allow doctors to remotely adjust the volume of insulin injected into a patient's blood stream. This connected health solution offers tremendous benefits as compared to requiring patients to visit their doctor or healthcare practitioner each time an adjustment is required. However, the benefits of connected "command and control" also creates an "attack surface", allowing the security of the device to be compromised by a malicious individual.

- **Fourth, the IoT has no clearly defined perimeter to defend from malicious attackers.** Cloud-based information has many access points, may flow through many devices, and often-shared physical storage locations. As a consequence, it presents a new security paradigm, where the data itself is defining the perimeter. This evolution of the data-at-the-perimeter contrasts sharply with earlier approaches to security systems, which could rely on a firewall, the software equivalent of a moat, to protect the perimeter when data was stored in a dedicated corporate controlled facility, with few access points. With data continuously moving among locations in the IoT, the defense perimeter formerly defined by the firewall no longer exists.

- **Finally, a large part of the value of the IoT results from the ability of consumers and businesses to maintain privacy, while sharing the data with third parties for specific uses and benefits.** A primary care doctor might, for example, want to share the information associated with a specific patient's insulin injections, from the insulin pump, with a doctor who specializes in disorders associated with diabetes. Success in the IoT requires that companies have the capability to securely share specific data elements with third parties.

Internet of Things Security Solutions: The Elements of the New Paradigm

In the era of the Internet of Things, a reliable security solution must adopt a fundamentally new approach, which focuses on four central elements as shown in the list below. These elements must combine both a new way of thinking about security and new technologies.

The Four Elements of a Reliable Internet of Things Security Solution

1. **Ensure the security of the devices themselves.**
2. **Protect the data with persistent encryption so it is secure both in transit and at rest.**
3. **Enable lifecycle management of IoT devices.**
4. **Implement a security solution that is device and workflow agnostic.**

Element #1: Ensure the Security of the Devices in The Network

To achieve reliable security for devices, means ensuring that only authorized devices can transmit or receive data associated with an IoT service.

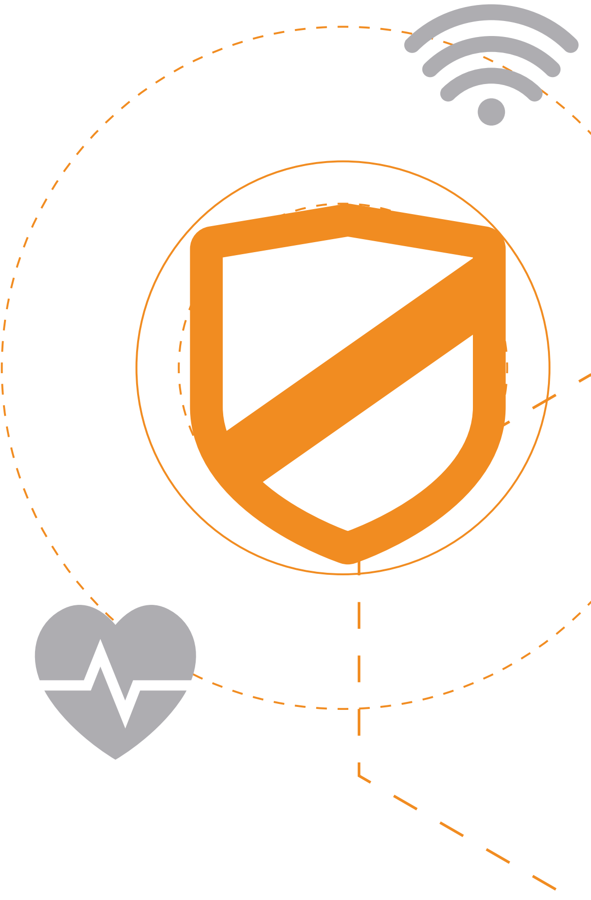
The necessary attributes of this device-focused security are:

- **Strong authentication (access control) for new and legacy network devices**, which ensures data actually originates from a legitimate device and not a fraudulent substitute.; and
- **The ability to scale**, so IoT service providers can efficiently and cost-effectively work with millions of devices.

Understanding strong device access controls: Strong controls, which ensure access is limited to authorized individuals or systems, are made up of two key elements:

- **Identity Assertion or Authentication:** Ensuring "you are who you say you are," and
- **Authorization:** Validating "you are permitted to do what you are trying to do." Authorization normally presupposes Authentication.

In traditional security solutions, authentication is managed through the use of static certificates which are issued by Certificate Authorities (CA's), these are installed onto devices to help assert their identity. The digital twin of the certificate installed on the device is mathematically linked to a counterpart certificate stored within a PKI. "Public Key Infrastructure" refers to the entire ecosystem devoted to digital certificates and encryption.
This ecosystem encompasses, not just the software and hardware, but all of the people involved with the digital certificates.
PKI certificates are issued from a CA (certificate authority), which creates and manages them. Once issued, the creation and management of the PKI can be handled in-house or via a management company.



Then, the communication between the data (which has a certificate attached to it) and the device (which has the counterpart certificate) verifies the matching pair enables the device to assert its identity for Authorization and Authentication .

For the Internet of Things, this traditional approach is ineffective.

- **Certificates don't identify devices:** The relationship between a digital certificate file (that can be verified by the issuing CA) that just is placed on a specific physical device is actually a loosely coupled relationship. As a result, there are many examples of certificates that have been forged, duplicated and even issued by compromised CA's, which have led to the unauthorized breach of critical systems.

- **PKI's are costly to manage and do not scale:** Research has shown that the full cost of managing an internal PKI can cost as much as $400,000 per 5000 devices per year including the capital cost of solution acquisition and the ongoing management of the system[12].

In fact, as the number of PKI managed devices increases into the millions, the complexity and cost of maintaining this system leads to the opposite of scale economies: Maintaining the security of every device on the network actually increases in cost, and the entire security model becomes difficult, if not impossible, to operate.

- **IoT devices have a life expectancy up to 15-20 years.** With traditional methods, managing static certificates across this lifespan is extremely challenging, inefficient, and costly.

Element #2: Protect the Data Itself with Persistent Encryption

The central principle in a security solution that protects the data is strong encryption, which turns data into a randomized string of numbers and letters (Ciphertext) that is meaningless to anyone except users who have the right key to unlock the code. In an Internet of Things environment large volumes of data are in transit (moving between millions of devices) and at rest (in storage). **A data-at-perimeter security solution must use strong encryption for data that is persistent, and ensures the data is encrypted both in-transit and at-rest.**

With encryption, data is transformed into meaningless code, which can literally travel anywhere and be stored anywhere, without fear of compromised security: To borrow a popular phrase, with encryption the information is hidden in plain sight.

Each data stream traveling to and from the potentially millions of insulin pumps operated by an IoT medical device service provider is encrypted throughout its entire lifecycle. In addition, it's worth noting that while a traditional firewall protects a large mass of data (making the security of all of the data rely on this single barrier), each of the millions of individual data elements potentially gathered by the pump is protected by its own distinct encryption key.

Element #3:
Enable Life-Cycle Management

IoT security solutions need to be highly adaptable, from the moment they are launched. Over time, the protected IoT services will inevitably be enhanced with new capabilities, as these services evolve. Hence, a security solution must, from the start, embody a mechanism for adapting throughout the lifecycle of an IoT product or service. A life-cycle approach is achieved when:

- **The software for all of an IoT service's devices can be centrally, securely upgraded; and**

- **The IoT security solution works seamlessly with legacy devices as well as new devices.**

Element #4: Implement a Solution that is Device and Workflow Agnostic

Security solutions will be most effective when they are device and work-flow agnostic: They work with any type of device; they are a functional add-on to any data work-flow.

The Internet of Things is a huge opportunity that is in its infancy. As it matures, manufacturers will modify devices, and the flow of data, associated with services will inevitably change to accommodate new opportunities and an enhanced understanding of customer needs. The most effective security solutions will consider these unpredictable, but inevitable, changes irrelevant.

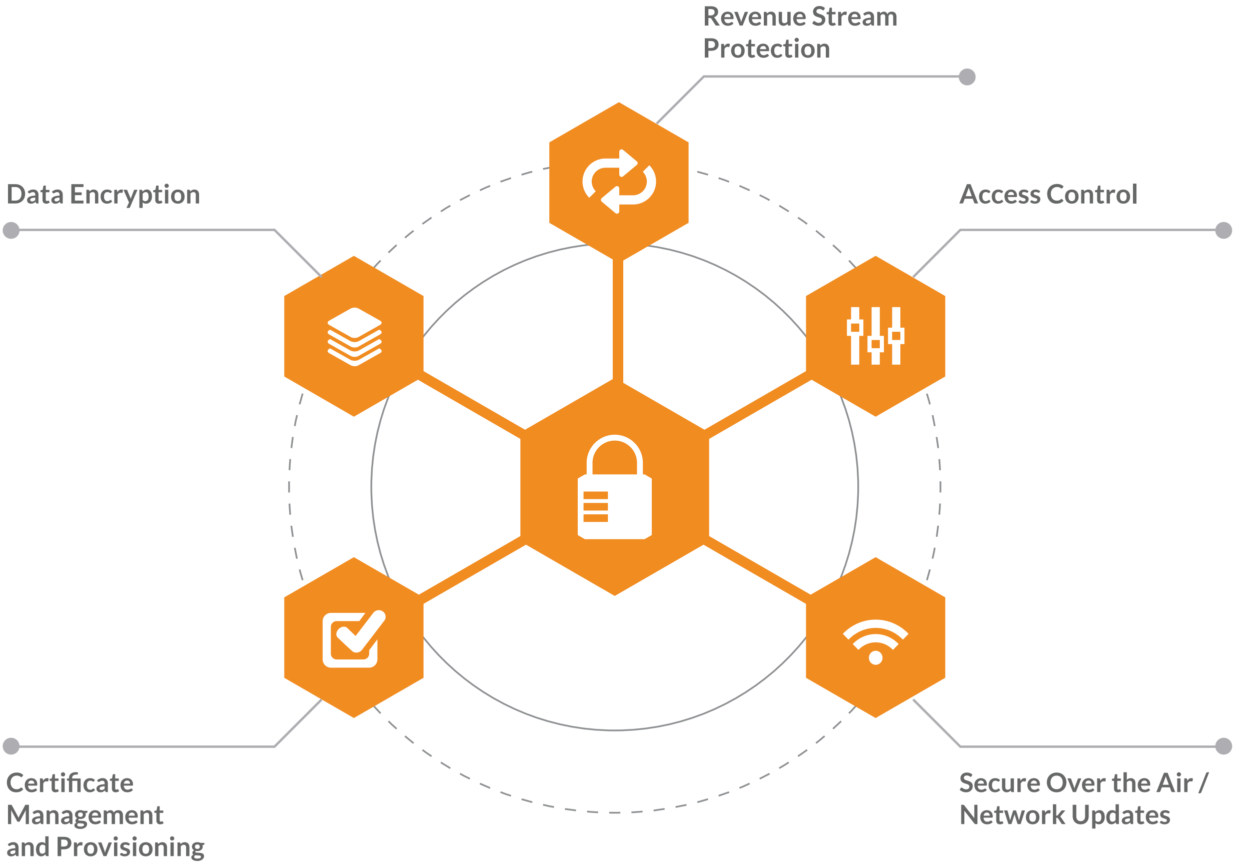
Internet of Things manufacturers and service providers want security solutions that simply work. When these solutions are limited to specific devices, or interfere with data work-flows, significant problems will be inevitable.

Device Authority: A Security Solution Created for the Unique Requirements of the Internet of Things

Security solutions developed for earlier eras are inadequate for the unique challenges posed by the era of the Internet of Things. As a consequence, manufacturers and service providers creating IoT offerings will benefit by learning more about the solutions offered by Device Authority, who sponsored this paper.

Device Authority was created to meet the specific security needs of the Internet of Things. The company's unique, patented software offerings are based on the fundamentally new approach to security solutions required by the IoT. For additional information, please visit our website: www.deviceauthority.com

Device Authority's IoT Security Solutions


Revenue Stream Protection
Data Encryption
Access Control
Certificate Management and Provisioning
Secure Over the Air / Network Updates

References

1. Bruce Judson, a former Senior Faculty Fellow at the Yale School of Management is the bestselling author of several books on achieving business success in the rapidly evolving digital economy. He is a Senior Adviser to Tern Plc., the majority owner of Device Authority,
2. Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired, July 21, 2015; http://www.wired.com/2015/07/hackers- remotely-kill-jeep-highway
3. How the Internet of Things Got Hacked, Wired, Dec. 28, 2015; http://www.wired.com/2015/12/2015-the-year-the-internet-of- things-got-hacked
4. Nissan Leaf electric cars hack vulnerability disclosed, BBC.com, Feb. 24, 2016; http://www.bbc.com/news/technology-35642749
5. 9 baby monitors wide open to hacks that expose users' most private moments, Ars Technica, Sept. 2, 2015; http://arstechnica.com/security/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments
6. How The Internet of Things Could Be Fatal, CNBC.com (March 4, 2016) http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html
7. Gartner, Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018, Feb. 23, 2016, http://www.gartner.com/newsroom/id/3221818
8. See, for example, AT&T Insights, Volume II, The CEO's Guide to Securing The Internet of Things; https://www.corp.att.com/cybersecurity
9. Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired, July 21, 2015; http://www.wired.com/2015/07/hackers-emotely-kill-jeep-highway
10. How The Internet of Things Could Be Fatal, CNBC.com (March 4, 2016) http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html
11. Accenture, Igniting Growth in Consumer Technology, released January 5, 2016.
12. In one study, Symantec found, for example, that the cost to manage just 1,000 devices using an on premise PKI-based system required one-time costs of $280,000, with annual recurring costs of $89,000. Over three years, this equated to a cost in excess of $500,000, while The costs to manage 5,000 devices (or five times as many devices) would be far higher. See Symantec, Comparing Cost of Ownership: Symantec™ Managed PKI Service vs. On-Premise Software.

Seamless end-to-end Security for every IoT Ecosystem

Device Authority is simplifying the security challenges that organisations face when protecting access to services and data for the Internet of Things.

Our patented dynamic key generation technology provides a strong, device-based trust anchor for automated, scalable IoT identity and secure data delivery.

We solve mission-critical IoT security problems, including provisioning and authorization, device-based access control, software and firmware updates, credential management and data delivery over third party networks and services.

DEVICE AUTHORITY™
IoT Security Simplified

Email
sales@deviceauthority.com

www.deviceauthority.com