WHITE PAPER

The Need for IoT Advanced Security: Why Do-It-Yourself Isn't Enough for IoT

CENTRI

Advanced Security for IoT

Introduction:
The Critical Need for Effective IoT Security

The Internet of Things (IoT) is growing massively, as is the need for effective IoT security.

Securing the billions of IoT devices already deployed is a top concern – everything from home appliances, to insulin pumps, to implanted pacemakers, to sensors deployed throughout manufacturing, to the spectrum of devices out in the wild controlling the power grid, water supply, and other utilities and services essential to daily life.

The U.S. Department of Homeland Security in a recent report noted: **while the benefits of the IoT are undeniable, so too is the reality that security is not keeping up with the pace of innovation.**[2]

*Some **5.5 million** new IoT devices come online every day —*

Gartner estimates that by 2020 the IoT will include more than **20 billion** devices.[1]

IoT Security: No Place for Do-it-Yourself

IoT security is no place for do-it-yourself (DIY). Even well-seasoned developers – including well-seasoned security developers – should turn to solid third-party expertise when approaching the critically important task of securing an IoT device or network.

"DIY is a bad idea..."

This is the message that Roopinder Tara, writing on Engineering.com, emerged with after covering the IoT Tech Expo North America 2016 in Santa Clara, in the heart of the Silicon Valley.

"You have to pick an expert to take on IoT, if you are not one already... there are too many fast-moving pieces, each requiring a certain expertise."[3]

How IoT Security Differs from Traditional Security

The challenge of securing IoT, and the inadequacy of traditional IT security measures, is captured in a recent quote from R. Danes, writing in Silicon Angel:

> *"The idea of a single monolithic firewall to provide protection from cyber threats is becoming a bit quaint. The data center is breaking up and moving to multiple environments – this is true for most companies moving to the cloud and doubly true for those involved in the Internet of Things (IoT). This is putting demands on these data outposts to do more and raising uncomfortable questions about how they will be secured."*[4]

Why Securing IoT is So Difficult

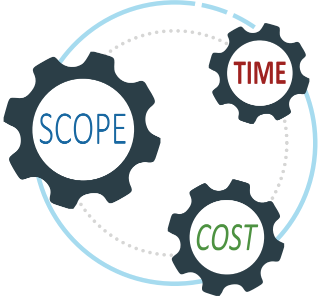
Securing IoT components – devices, data, and the cloud presents a complex and critically important challenge because they nearly always live beyond the protective firewalls and layers of security found in normal enterprise and mobile computing.

IoT devices can be minimal in size and in what they do, but their functions can be critically important – whether regulating dosage from an insulin pump, to detecting temperature changes in a nuclear power plant. This means that many IoT devices have minimal system resources, and because many are battery operated, it is essential to implement security that has minimum impact on storage, computing, and power needs.

To secure an IoT environment you must provide a *complete* solution because hackers can now look for and exploit gaps and seams from many more attack surfaces. Completeness includes support for device authentication, encryption for data while in transport, in use on the device *and* at rest in the cloud, visibility and insight to what is happening across the IoT security environment (including the ability to search your own encrypted data), and a number of other functions such as network bandwidth efficiency, and removing dependence on traditional and unscalable centralized key management for protecting data in use and at rest. Add to this the flexibility needed to work within an unlimited variation of IoT hardware and software architecture, while requiring only a minimal footprint from the standpoint of both storage and computational needs – the demands for a resilient IoT security solution are daunting.

While the above is just a glimpse of what is needed, remember that all of this must be accomplished in a completely secure and integrated fashion.

Shortcomings of DIY



In order to develop an IoT security solution in-house, development teams must make trade-offs in the project between scope, time and cost.

The typical pieces to build such a solution are borrowed from internal development and the open source community such as SSL/TLS, OpenSSH, OpenVAS, AES, Truecrypt and many others. However, these DIY pieces were developed years before the IoT even existed.

Gartner estimates that 2017 will see **up to 50%** of malware delivered via routinely compromised SSL/TLS.[5]

The IoT exists beyond firewalls, and in many cases beyond *all* walls as they hang from utility poles and other structures out in the wild. Because IoT devices are meant to be *everywhere*, they need to be designed to be small and inexpensive, and to require minimal compute power and energy consumption. All of these things work against home grown and legacy security solutions.

Vulnerabilities within the standard transport protocols have been exploited by cyber criminals and other bad actors. While there are now open source platforms emerging with components that developers can use to build their own IoT security solution, it is extremely risky to attempt this approach versus implementing a supported, tightly integrated and secure commercial-grade solution.

Protecting Developers from Their DIY Spirit

Generally speaking, developers are a creative class with a strong can-do attitude. This is heroic, but it may not be fair to the developer, your project, or company reputation when someone is appointed to (or volunteers to) become your IoT security expert. The challenge of creating tightly integrated IoT security solutions is measured in man *years*, not man hours.

Yes, they can swiftly download some open source transport and encryption code and wire it into the application. But the problem comes with the gaps and seams that are left open as attack surfaces for hackers. Doing it yourself simply isn't worth the vast commitment of human resources required to get it right, nor the bigger risks of getting it wrong.

What to Look for in IoT Security

IoT security should be a top priority for product, engineering and security leaders, developers, and all other stakeholders. IoT security should have a flexible design so you can incorporate it into your solution stack, complete security *including encryption of data in motion, in use and at rest*, and data intelligence to monitor and react to IoT security incidents across your IoT ecosystem.

Purpose-built, not cobbled together

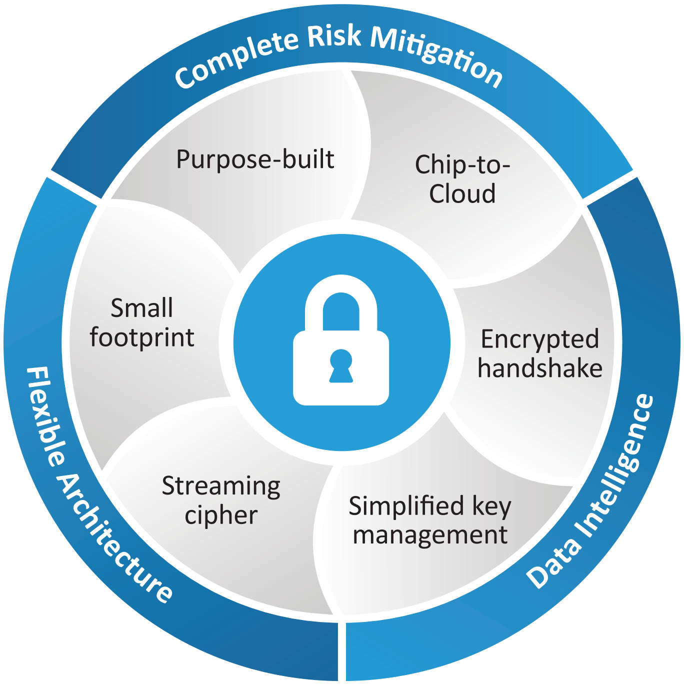
All stakeholders benefit from a purpose-built IoT security solution. The concept of purpose-built is important because so many IoT solutions are merely re-packaged enterprise solutions, scaled down in an attempt to fit clunky agents into a footprint that attempts to fit onto an IoT device.

Chip-to-Cloud data encryption

Your IoT security solution should ensure that data remains encrypted as it moves throughout the Cloud ecosystem – as well as when it is at rest, either on the IoT device or midpoint gateway, or being stored within the Cloud or in on-premises infrastructure.

Small footprint & flexibility

The ideal IoT security solution is measured in kilobytes, not megabytes, and is designed to minimize CPU and memory resources. For product managers and solution architects, such purpose-built solutions help minimize cost by enabling IoT devices to be built with less expensive CPU and memory components. And for developers, such small, efficient code libraries help reduce the total size of the application code they need to deploy on the IoT device.



Encrypted handshake for safer, faster, connection

Traditional transport protocols require a multi-step, time-consuming, handshake process that begins with an unencrypted exchange to establish trust and decide which protocols will be used. A purpose-built IoT security solution should provide components to allow devices to communicate securely, with uniquely identifiable end points and with all communication encrypted.

Streaming cipher for faster performance

You can gain faster performance – while preserving device resources – by using a streaming cipher rather than a block cipher solution, which can result in data blocks stacking up in queues, while also demanding more from onboard IoT device memory – especially when minimum block lengths exceed IoT data packets.

Data encryption with simplified key management

The ideal IoT security design provides encryption for data in use and at rest, without requiring complicated or non-scalable key management. Ideally, this is done by appending key-creation information to the encrypted data, and using this to dynamically create unique keys to secure the data.

Securing IoT with CENTRI IoTAS

The CENTRI **Internet of Things Advanced Security—IoTAS** platform provides a suite of purpose-built, standards-based, advanced security components *including leading-edge cipher technology* that enables IoT developers to deliver a complete IoT security platform with device integrity, data protection (in motion, in use at the edge, and at rest in the cloud), bandwidth and data storage optimization, IoT device management and insight into all IoT ecosystem data activity.

You can use CENTRI IoTAS to secure your entire IoT ecosystem – from IoT devices, mobile applications, gateways, Cloud infrastructure, and any network connection. Looking at just some of the CENTRI IoTAS components, here’s how you can put them to work:

IoTAS

Internet of Things **Advanced Security**

✓ **CENTRI Secure Communications Endpoint**
Developers provide security on the device side through incorporating our lightweight CENTRI Secure Communications library into their IoT application or the Proxy client within the device software stack.

✓ **CENTRI Secure Communications Service**
Developers provide security on your Cloud infrastructure side through use of our CENTRI Secure Communications Service running on your existing application servers.

✓ **CENTRI Data Protection**
Developers use the powerful but lightweight CENTRI Data Protection library, called from their IoT application, to encrypt data before placing it into your device or on-premise storage.

✓ **CENTRI Secure Manager**
Device management which enables users to manage and control all aspects of the CENTRI solution offerings. It offers endpoint management and server administration for registered security administrators.

✓ **CENTRI Secure Insights**
Insights dashboard provides visibility into security across your IoT environment. Secure Insights can be coupled with CENTRI Secure Communications, and CENTRI Data Protection.

✓ **CENTRI Service Layer**
Developers can use the CENTRI Service Layer to integrate with third-party solutions, including their own internally developed applications.

CENTRI IoTAS Platform benefits include:

COMPLETE AND PURPOSE-BUILT

CENTRI IoT Advanced Security was purpose-built from conception to provide a complete solution to meet the unique needs of the IoT environment, including securing data while in transit and at rest, providing device authentication, and giving you visibility into your IoT security operations.

FLEXIBLE

The CENTRI IoTAS platform, with its small footprint, standards-based architecture, and ability to work across device platforms and operating systems, provides the flexibility you need to extend security across your entire IoT environment, and flexibility to integrate into your own custom code and existing infrastructure. Flexibility is extremely important because of the lack of standardization within IoT.

INTELLIGENCE WITH MANAGEMENT ANALYTICS

The CENTRI IoTAS platform gives you dashboards providing the visibility and data intelligence you need to help you manage your IoT environment, and provide performance metrics, audit features, and forensics to help you ensure IoT security across your environment. Visibility into events across your IoT deployment is essential to ensuring full security.

EASY TO DEPLOY

In a single day, an experienced team of developers can completely deploy all components from the CENTRI IoTAS platform, integrating them into your own application code to provide a complete IoT security solution.

SMALL FOOTPRINT

The CENTRI IoTAS platform has a small 50 kB footprint, making it easy to embed the code into your application, providing you with a completely integrated solution for data security. IoTAS only requires about 100 kB of RAM for efficient performance.

DEVICE AND OS AGNOSTIC

Developers can use the C-based libraries and tools across a spectrum of operating systems, including Android, iOS, Windows, Linux, RTOS, and custom network stacks and other code you might want to use in creating your IoT solutions.

FAST, SECURE AUTHENTICATION WITHOUT CERTIFICATES

CENTRI IoTAS has a patented process for assigning secure device identifications upon registering a new device into an IoT environment. This allows for immediate, and encrypted, single-stage handshake communication between an IoT device using the CENTRI Secure Communications library, and the Cloud infrastructure side using the CENTRI Secure Communications Service. With CENTRI IoTAS, there's no need to exchange certificates or employ a third-party certificate authority solution.

STANDARDS-BASED, LEADING EDGE CRYPTOGRAPHY

The CENTRI IoTAS platform protects your data during transport, in use and at rest through standards-based, leading edge cryptography – the same crypto technologies as many of the leading technology companies and government agencies, including Apple, Google, the U.S. National Security Agency, and the European Union.

SIMPLIFIED KEY MANAGEMENT

CENTRI developed "vault-less" technology – a patented process to embed key seed information within the data, to eliminate the need for hardware appliances such as HSMs or other third-party key storage systems for data at rest (although CENTRI has the flexibility to be used with HSMs, if desired.) The seed data used to generate each one-time key is protected with asymmetric encryption. The result is unlimited key management, which is essential for IoT security to scale.

ENCRYPTED SEARCH OF BIG DATA

CENTRI IoTAS solves the problem of searching and accessing encrypted Big Data without having to decrypt the data.

DATA COMPRESSION

CENTRI IoTAS platform automatically performs data optimization, providing about 80% compression to save bandwidth and Cloud storage space. Data compression provides efficiencies and cost savings across the network layer, Cloud transport and data storage.

SMART CACHE TECHNOLOGY

CENTRI uses smart cache mapping technology and efficient algorithms to enhance data optimization, resulting in only 1% CPU utilization. The optimization algorithm utilizes a novel cache memory algorithm and can operate at a byte level of granularity. All of this is done with a single pass so optimization-protection ties the compression state directly to the encryption, strengthening security further and hindering any potential cryptanalysis.

DESIGNED BY AND FOR DEVELOPERS

The CENTRI IoTAS platform was designed by and for developers to speed your time-to-market and greatly reduce all security risks. The best way to experience this is to simply download a fully functional trial version of IoTAS, which is easily upgraded to the commercial version so none of your prototyping work is lost.

CUSTOM SOLUTIONS

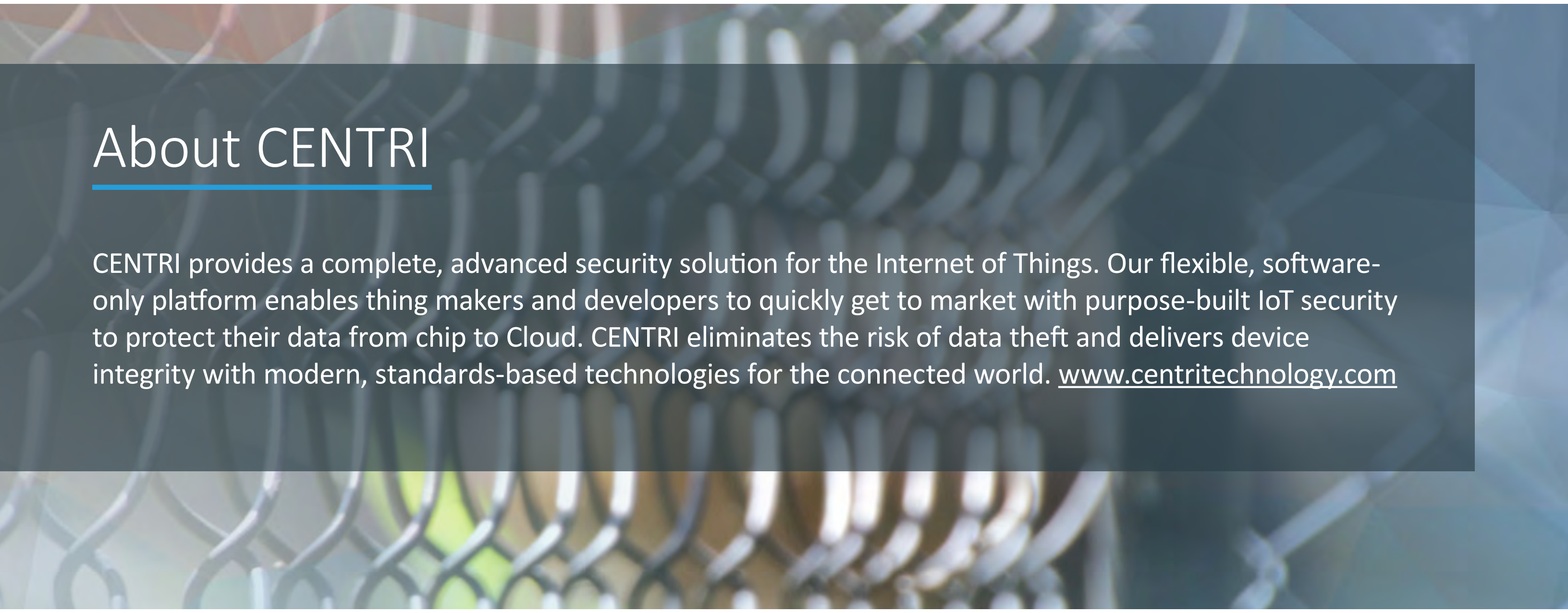
CENTRI can work with you to create custom applications if your solution uses a customized operating system or network stack. Even if you've already created a custom environment to reduce attack surfaces, you can still take advantage of the IoTAS security platform.

IoTAS

Internet of Things **Advanced Security**

Summary

CENTRI IoTAS meets the needs of stakeholders across your organization – from product leaders seeking a faster time-to-market with secure IoT devices and data, to engineers and developers looking for the best way to secure new and existing products with seamless integration with peace-of-mind and without the DIY risks, to the security leaders tasked with providing air-tight, standards-based security for IoT to minimize risks for the company. **No other commercially available platform or internally developed solution can provide a better platform for securing your IoT data.**



About CENTRI

CENTRI provides a complete, advanced security solution for the Internet of Things. Our flexible, software-only platform enables thing makers and developers to quickly get to market with purpose-built IoT security to protect their data from chip to Cloud. CENTRI eliminates the risk of data theft and delivers device integrity with modern, standards-based technologies for the connected world. www.centritechnology.com

CENTRI
Advanced Security for IoT
701 5th Avenue, Suite 550, Seattle WA 98104 | 206-395-2793 | www.centritechnology.com

[1] Gartner. http://www.gartner.com/newsroom/id/3165317

[2] Strategic Principles for Securing the Internet of Things. https://www.dhs.gov/sites/default/files/publications/IOT%20fact%20sheet_11162016.pdf

[3] Don’t Do IoT Yourself, Say Experts. http://www.engineering.com/IOT/ArticleID/13856/Dont-Do-IoT-Yourself-Say-Experts.aspx

[4] Living on the edge: Security threats loom as IoT decentralizes the data center. R. Danes. http://siliconangle.com/blog/2016/09/13/living-on-the-edge-security-threats-loom-as-iot-decentralizes-the-data-center-ioconversation/

[5] When Encryption Becomes the Enemy’s Best Friend. By Jai Vijayan, Darkreading. http://www.darkreading.com/attacks-breaches/when-encryption-becomes-the-enemys-best-friend/d/d-id/1324580