MOCANA

Standardizing Security Across Your Industrial Internet of Things

In this White Paper:

Mocana Corporation
710 Sansome Street
San Francisco, CA 94111
www.mocana.com/iot-security

866-213-1273
iotsales@mocana.com

Revised June 12, 2015

:: Security and The Internet of Things

In our modern world, the Internet invades and pervades every element of our society. As the Internet of Things (IoT), it connects everything and everybody. Responding to this unprecedented embrace of connectivity, the market is solving problems both old and new, as well as enriching our lives with seemingly simple apps that provide entertainment, knowledge, and connections with people worldwide. In short, it's good bye to unconnected, unmanaged devices. The Internet of Things is taking over .

Unfortunately, the platform of choice from which users want to manage such devices is by way of mobile apps that run on untrusted mobile devices, with the result that these mobile devices are joining the vast and ever-growing Internet's horizontal platform. This opens the previously closed and secure Industrial Internet of Things (IIoT) to all sorts of unsanctioned and unsavory activities. Indeed, debauchery has an IP address, and so Enterprises must scramble to secure their IIoT networks. This evolution mirrors the earlier Enterprise network security challenges that forced the change from protocols such as Netware to protocols such as TCP/IP. Now Enterprises must transform the formerly gated IIoT by moving from closed protocols such as MODBUS to open protocols such as TCP/IP.

More and more enterprises are experiencing security breaches, and the highest-level executives are being held accountable.

It is a tremendous challenge, as well as a tremendous opportunity, to enact this transformation and bridge the worlds of unfettered open internet and Enterprise closed communities. And while it's readily acknowledged that the security and apps industries should be doing more to lock down systems, very few companies have the technical expertise, the market credibility, and the business relationships to successfully bridge the untrusted and secure worlds. But Mocana does, and can secure your IIoT environment and devices, and save you time and money in the process.

:: Without Expertise, Security is Expensive

When security is not your core business, it's expensive and can seem a daunting process to implement. Open source security libraries are notoriously vulnerable and difficult to use for many reasons, including:

- Large and complex codebases
- Lack of coding guidelines
- Lack of documentation
- Lack of focus as features and patches are added
- Lack of security-conscious, defensive programming
- Under-resourced and under-funded

Securing your devices requires a design focus on negative requirements, threat modeling, fuzz testing, and more—none of which relate to your core business focus.

But if your engineering team lacks security expertise, they must rely on open source solutions or take the time to add security to their design and coding workloads.

As well, if product teams adopt different approaches to security and incorporate diverse vendors' solutions, the cost of reacting to a security breach increases. Each product team must evaluate whether they've been affected by the security problems, and if so, research and implement a solution, separately from other teams.

:: Skipping Security is Even More Expensive

Given the difficulty and expense of ensuring the security of the IIoT, it can be tempting to skip some security measures and just hope for the best. But even a limited security issue can cause immediate and long-lasting damage to your brand.

In 2013, IBM attempted to estimate the cost of an IT disruption to a business and its operations over the 24 months following the actual disruptive event [1]. The following table shows how costs can multiply exponentially if the disruption is severe.

Severity of Disruption	Estimated Cost over 24 Months After Disruption
Minor	$20,929
Moderate	$468,309
Substantial	$5,274,523

Security breaches are not limited to any specific industry or class of applications or devices. The number of reported cases increased by 30% from 2013 to 2014, and the number of organizations reporting financial hits of $20M or more increased by 92% [2].

:: Mocana Secures the IIoT

Whatever you call it—the Internet of Things, the Industrial Internet, the Internet of Everything, or some other phrase—Mocana secures it!

The Mocana Security of Things Platform™ is an enhanced version of the Mocana Device Security Framework. The Security of Things Platform provides services for:

- Tamper resistance
- App/device authentication
- File and system protection
- Secure network connectivity
- Remote diagnostics
- Secure cloud connectivity
- Secure firmware update

No matter what industry you're in—industrial automation, automotive, governmental agencies, military, healthcare, and so on—you can gain tremendous benefits by integrating the Security of Things Platform into your products and services:

- Faster time to market—Reduce development time and remove the security integration bottleneck.
- Reduced TCO—Easily standardize your security implementation across all your devices, products, platforms, services, and departments. The Security of Things Platform can be used across 35 operating systems and 70+ CPUs: more than 2450 combinations!

- Enhanced reputation as a trusted provider—Join the more than 200 major globally-recognized OEMs who have integrated Mocana security into their offerings.
- Reduced risk—Enjoy the peace of mind that comes with knowing that your IoT devices are secure. In sharp contrast to the frequent exploits of vulnerabilities of open source products such as OpenSSL, Mocana has NEVER experienced a documented remote exploit attack.

:: Case Study I: 60% TCO Reduction

Recently, an OEM vendor of IIoT devices, who is ranked in the top 10 of the list of Fortune 500 companies, approached the Mocana Internet of Things (IoT) division for help with standardizing their security effort across all the products in a department. The department had released 25 new devices, worked with five (5) different vendors, and individual project managers had purchased 17 security products at an average cost of $30K each (and some were 2-4 times as expensive).

Standardizing on the Mocana Security of Things Platform across products significantly reduces the cost of security.

This company understood that not only was it costly to maintain multiple security solutions, it was almost impossible to evaluate which products were at risk when a security issue surfaced. As well, if they could standardize on a solution that included better metrics gathering and incident logging, they could increase their analyses to discover trends.

By standardizing their 25 devices to all use the Mocana Security of Things Platform, this one department alone saved more than 60% of the TCO when compared to the original cost of $510K (17 products x $30K).

:: Case Study II: 93% Reduction in Security Effort for Faster Time-to-Market

An industrial manufacturing and services conglomerate with annual revenues close to $40B is working with Mocana IoT to standardize their security implementation. The company currently employs 132,000 people, and plans to hire an additional 10,000 software developers in the coming year to support a flurry of device development.

However, they were becoming increasingly concerned with the growing cost of the security component of their development efforts. Not only was it a drain on resources that were needed for their core business products, it was slowing their time to market. On a recent device development project:

- Three engineers formed the security team. They were dedicated to designing, writing, and testing the security code for three months, for a total of nine people months
- Total engineering hours equals 1440:

  9 months x 20 work days/month x 8 hours/work day = 1440

Even including training time for the Security of Things Platform, engineers took engineers just 7% of the time to implement security as compared to creating and integrating their own security framework.

After licensing the Mocana Security of Things Platform™, the same security team embarked on another project:

- The three security engineers attended our training webinar mini-series of three, 1-hour sessions, for a total of nine engineering hours.
- It then took the security team only four days to integrate and implement the Mocana Security of things Platform™ This equals x engineering hours:

  4 work days x 8 hours/work day x 3 people = 96
- Total engineering hours, including each person's one-time training investment, were a mere 105.

Our customer was thrilled! With one simple purchase, they reduced the security development component from 1440 to 105 engineering hours, or 93%. Such a large reduction not only saves labor cost, it reduces the development time for a faster go-to-market, which in today's world is every company's goal.

:: Conclusion

In this white paper, we've discussed how security can be expensive if you go it alone, and that ignoring it is even costlier as well as risky. But when you join our successful case study customers who purchased the Mocana Security of Things Platform, you'll save money and reduce your time-to-market, and contribute to your business' success.

:: References

[1] http://www.forbes.com/sites/forbesinsights/2014/04/14/protecting-your-companys-reputation-in-a-heartbleed-world/

[2] http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

About Mocana Internet of Things. The Mocana Security of Things Platform software suite addresses assorted security issues across industries such as industrial automation, federal organizations, automotive, and healthcare. As a security specialist with over a decade of experience, Mocana provides a solution to security issues that are constantly evolving and presenting new challenges to all classes of organizations—public, private, and federal. All Mocana IoT security software is OS/Microcontroller independent, and this unique architecture allows customers to easily implement security in their existing infrastructure and across multiple projects. Mocana's market-leading platform offering helps large manufacturers and their suppliers standardize on security implementations, which saves development time and cost. 5 of the top 7 Android handset makers have implemented Mocana for Android Security solutions, which provide enhanced Android security functionality and advanced Android protected ROM. www.mocana.com/iot-security.