BG NETWORKS

IoT Cybersecurity Simplified Using Security Automation Tools

Keep Threats and Hackers Out with BG Networks Cybersecurity Solutions

1 Overview

This paper provides an overview of how BG Networks Security Automation Tools (BGN-SAT) can be used to implement IoT cybersecurity in a very short amount of time, by any embedded developer, from those who are new to cybersecurity to those who are experts.

Topics also covered include:

- Why IoT cybersecurity is important
- A list of 15 types of IoT devices that have been hacked
- The reasons why most IoT devices ship without cybersecurity
- What constitutes a good IoT cybersecurity baseline feature set
- How to make an easy transition from the engineering team to the manufacturing team

2 Introduction

Advancements in CMOS manufacturing technologies have led to tremendous improvements in cost, power, feature integration, and performance for networking-capable microprocessors and microcontrollers. This, in turn, has led to a flourishing of Internet of Things systems and applications. IOT Analytics forecasts that there will be over 30 billion IoT devices deployed by 2025. However, IoT security remains years behind IT network security. This lack of cybersecurity is a significant problem because these devices are used everywhere, from our national infrastructure to vehicles to hospitals to our homes. Because they are network-connected, they are vulnerable. While connectivity is the key to enabling huge gains in productivity from IoT, it also gives remote adversaries, often located in other countries, the attack surface to compromise anything that relies on these devices.

Security in IoT devices is a must. However, it can be difficult to justify additional resources, extra development time, or product cost to add cybersecurity, especially for price-sensitive and schedule-constrained IoT developments. However, in an increasingly connected world, cybersecurity is growing in the public consciousness with every ransomware attack, data breach, and privacy invasion that headlines the evening news, destroys lives, and threatens the security of entire countries. At-risk stakeholders are demanding security to prevent these increasingly sophisticated attacks. Failing to deliver this security can represent a costly or even existential threat to IoT suppliers and their customers. To address these obstacles to

15 IoT Device Types Hacked

Enter the terms “Defcon” and “IoT” in a web search, and it does not take long to find a long list of IoT devices that have been hacked. Defcon presenters are ethical hackers and typically disclose the vulnerabilities they find responsibly. Below you will find a list of 15 types of IoT devices hacked, unfortunately not all by ethical hackers.

- Apple AirTags
- Building HVAC controller
- Cardiac pacemakers
- Cars: BMW, Jeep, Mercedes, Tesla
- Electric Grid
- Electric meters
- Home door locks (Bluetooth)
- Industrial control systems
- IP security cameras
- Light bulbs (Philips Hue)
- Printers (many models)
- Routers (many models)
- Traffic Lights
- TVs (many models)
- Water treatment systems

correctly implementing cybersecurity, BG Networks has developed security automation tools that make IoT security easy to add, without having special cybersecurity expertise, in a very short amount of time. BG Networks' goal is to make sure all devices ship with IoT security by eliminating the barriers of time and resource constraints to implement cybersecurity.

3 Why is IoT Cybersecurity Important

Like traditional enterprise IT networks, cybersecurity is critically important for the IoT because compromises can mean financial loss and the exposure of sensitive data. But IoT networks have additional cyber-risks to physical safety and critical infrastructure operation. The reason is that IoT systems control physical devices, and there is a real possibility of these risks being realized. IoT devices without cybersecurity, limited cybersecurity, or even cybersecurity that is not implemented correctly are all vulnerable. The evidence of this is the many types of IoT devices that have been compromised.

Correctly implementing cybersecurity is becoming a requirement and not an optional feature in the development of IoT products. The evidence shows that IoT devices are not being deployed with the security needed to prevent these attacks which continue to grow in frequency, sophistication, and consequence.

4 Are IoT Devices Shipping with The Cybersecurity They Need?

Unfortunately, the answer is no. Figure 1 shows data from a recent worldwide research study. While the data at first looks encouraging, given that 70% of the respondents had taken one measure of security, the problem is that one measure is not enough.

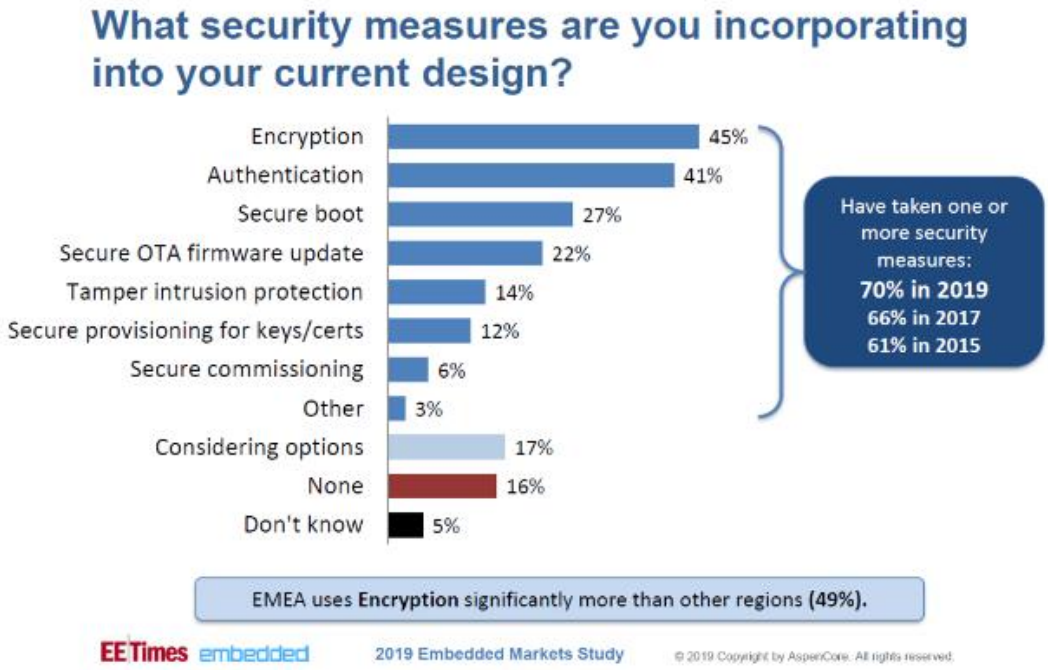

Figure 1

A set of cybersecurity features that would provide a good baseline of protection would include all of the top 4 in the referenced study:

- Encryption
- Authentication
- Secure boot
- Secure OTA firmware updates.

Encryption protects data and makes reverse engineering by hackers much more difficult. Authentication ensures that hackers cannot insert their code to take control of a device. Secure boot based on a hardware root of trust ensures the device is in a secure state after reset. Secure OTA firmware updates allow for bugs in code that cause security vulnerabilities to be fixed.

From the data above, we can safely conclude that over 80% of the respondents are not implementing these four security features and therefore are not including the basics of cybersecurity.

5 Simplifying IoT Cybersecurity with Security Automation Tools

BG Networks Security Automation Tools have been designed to simplify the addition of IoT cybersecurity and to make sure it is implemented correctly. These tools provide a solid security foundation that can be built upon and added to in the future. They take maximum advantage of security features built into the silicon in embedded processors and open-source software, and can be used with off-the-shelf hardware or your own custom hardware.

The security features supported are based on the National Institute of Standards and Technology's NISTIR 8259 recommendations for IoT cybersecurity. The security features supported include:

- Secure boot
- Encryption for data protection
- Secure interfaces
- Security state awareness
- Secure key storage
- Secure software updates
- Secure device identification

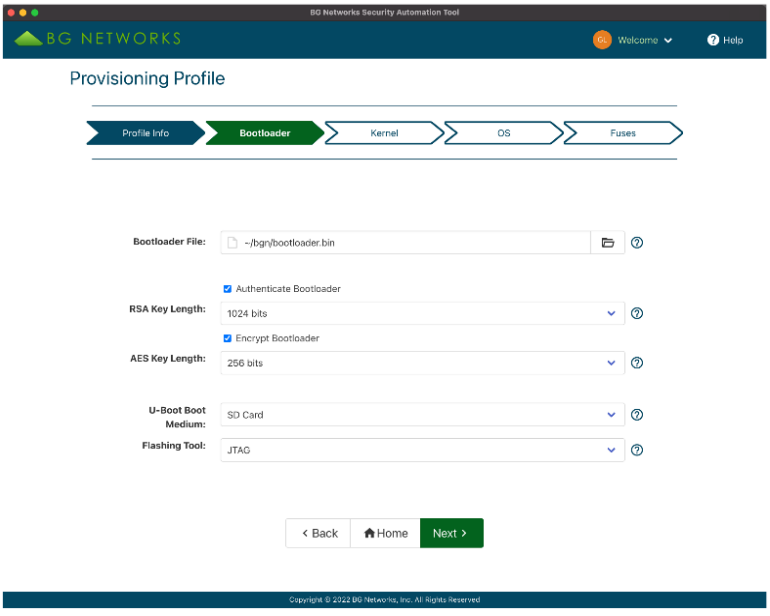

Figure 2

The BG Networks security automation tools offer an easy-to-use graphical interface that takes the user step by step through a series of questions with context help. The answers you provide to these questions select the security features to be included in your IoT device. Our goal is to make these tools as easy to use as other popular software in widespread consumer use but for IoT cybersecurity. Figure 2 shows a screenshot from the embedded developer view of the BG Networks security automation tools.

Figure 3 shows the security architecture supported by BG Networks security automation tools in terms of hardware and software. This is a complete security stack designed to be implemented in a very short amount of time.

The BG Networks security automation tools, BGN-SAT for short, are designed to leverage security features built into embedded processor silicon. This results in the most secure, low power, and highest throughput implementations for cybersecurity. Even ARM M class based, very low-cost embedded microcontrollers, now include excellent and comprehensive sets of security features. The hardware security features used are represented by the grey layers in the bottom of the security stack in Figure 3.

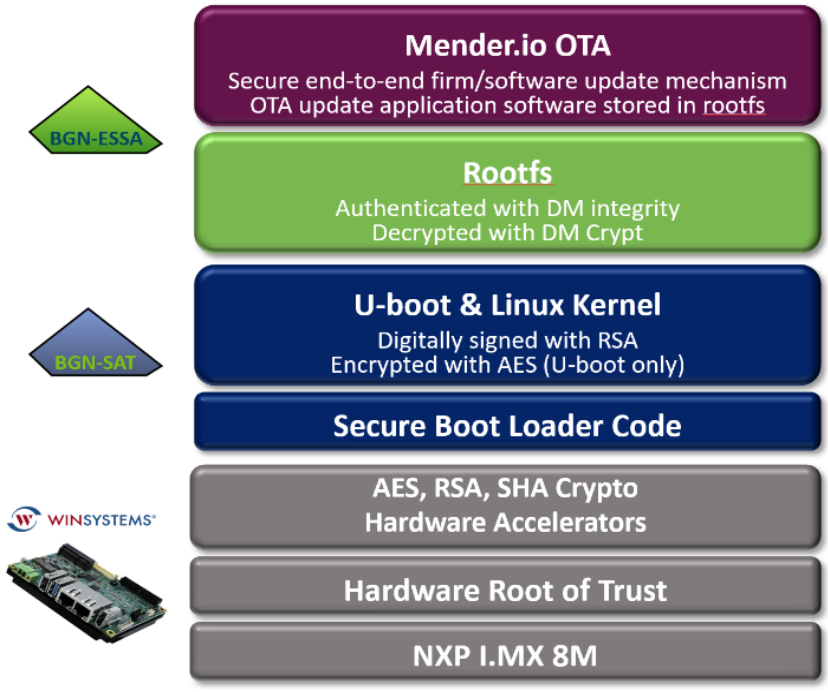

Figure 3

BGN-SAT is also designed to work with open-source code, represented by the two top layers of the stack, which yields a richer security feature set while saving costs. BG Networks ESSA open-source code takes advantage of security features built into Linux (authentication, encryption, decryption). In addition, Mender.IO is an open-source OTA software update application that offers an incredibly rich feature set that has been integrated into this security stack.

An RTOS version of our security stack will be available in an upcoming product release.

If you are looking to save time by using off-the-shelf hardware, a WINSYSTEMS Single Board Computer (SBC) is a great option. The WINSYSTEMS I.MX 8M SBC is designed with security in mind, is optimized for IoT applications, has a long production life, with an excellent set of I/O options for the edge and the processing power needed for AI applications.

6 Cybersecurity Considerations for Manufacturing

IoT cybersecurity is also a consideration for the manufacturing team. Concerns range from key generation to securely locking an embedded processor. An excellent IoT cybersecurity practice is having unique keys per IoT device. This avoids a "break one, break them all scenario". In other words, the situation to avoid is preventing an adversary from extracting a key from one IoT device, which would give access to the entire fleet. To support unique keys, the manufacturing team needs a fast and automated way to generate a unique set of keys for each device manufactured.

BGN-SAT supports unique key generation and a seamless handoff between the engineering and manufacturing teams. A security profile that BGN-SAT automatically generates makes this transition

easy. This profile represents the security features specified by the engineering team. With a one-step command to perform all security functions manufacturing times are kept as short as possible. The combination of this security profile and BGN-SAT enables the manufacturing teams to:

- Generate unique keys per device
- Store those keys securely
- Sign code binaries with those unique keys
- Encrypt binaries
- Configure security features on the embedded processor
- Download signed and encrypted code to flash memory on the IoT device

Figure 4 shows the one step command ("Program Board") to perform all the cybersecurity steps listed above for an IoT device being manufactured. Commands executed in this one step are based on a particular security profile that is selected.

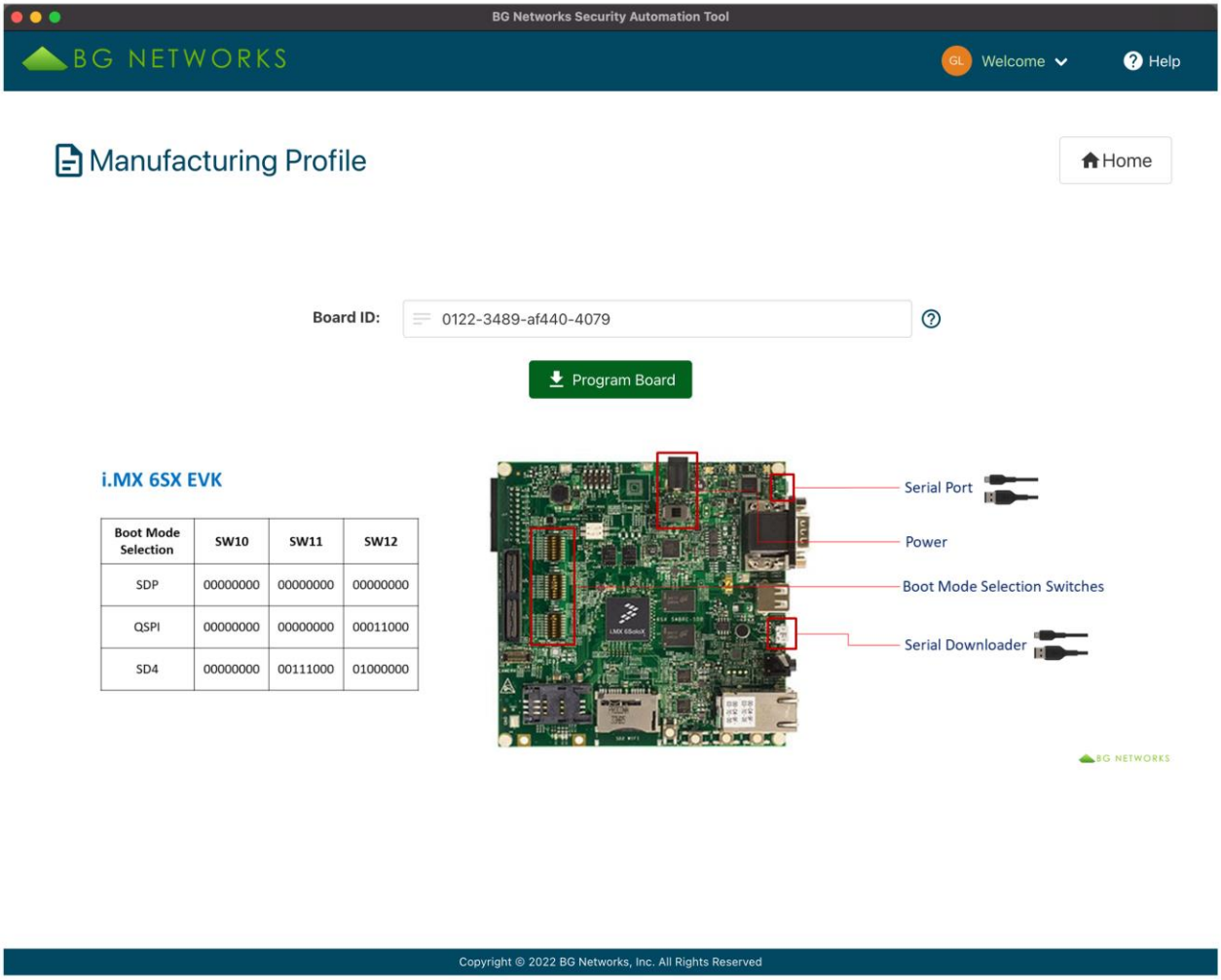

Figure 4

7 Conclusion

BG Networks security automation tools are designed to simplify and correctly implement IoT cybersecurity. These tools can be used by any embedded developer. BGN-SAT will guide those who are new to cybersecurity through all considerations, help those who are experienced to configure security very quickly, fully taking advantage of embedded processor security features. The goal is to remove barriers of time and resource limitations to adding security. With a set of security features based on NISTIR 8259 IoT security recommendations, these security automation tools provide the most important features of cybersecurity with a very efficient implementation. They also address the challenge of secure manufacturing by making it easy for a manufacturing team to generate and manage keys while very efficiently configuring and programming IoT devices as they are produced.

A free 60-day evaluation license is available so you can try them risk free. For more information contact us at info@bgnetworks.net or see our website at www.bgnetworks.net.