BLUESKYTEC

WWW.BLUESKYTEC.COM

ZOMBIE BOTNETS!
Eight good reasons to use Module12

ABSTRACT

What problem are we trying to solve? There are number of issues that are currently in the news: IP being stolen by organised crime and state sponsored actors. A Mirai botnet zombie attack to launch a Distributed Denial of Service at Dyn. The power outage in Ukraine. Hacking of Tesla and other vehicles. All of these attacks are similar in that they attacked the embedded systems housed in equipment not personal computers, company IT systems or banks.

The botnet zombie attack is particularly disturbing because, this attacked embedded systems such as CCTV cameras and home hubs etc. The zombies are small segments of code inserted into the embedded operating system of devices that are used on the Internet – CCTV cameras or digital video recorders for example. Once they are installed in the equipment they lie dormant until they are activated and thus the equipment starts to generate IP packets that target other systems on the network. These zombies could be there at the time of manufacturing, or could be introduced at a later stage.

At its heart the power outage in Ukraine was caused by an attack on a part of the fabric of the control system - the RS232 to Ethernet converters. These devices were re-programmed over the network to allow a classic Man-in-the-middle attack and enabled the whole power grid to be taken off-line.

Module12 technology can help secure embedded systems connected to the Internet.

ANALYSIS OF THE ZOMBIE PROBLEM:

This extract is from The Guardian on the 26th of October entitled “DDoS attack that disrupted Internet was largest of its kind in history”

“*On the 21st October 2016 Dyn, a company that controls much of the Internet's Domain Name System (DNS) infrastructure was attacked. It was hit and remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.*

The cause of the outage was a distributed denial of service (DDoS) attack, in which a network of computers infected with special malware, known as a “botnet”, are coordinated into bombarding a server with traffic until it collapses under the strain.

What makes it interesting is that the attack was orchestrated using a weapon called the MIRAI BOTNET. Unlike other botnets, which are typically made up of computers, the Mirai botnet is largely made up of so-called "internet of things" (IoT) devices such as digital cameras and DVR players.

Because it has so many Internet-connected devices to choose from, attacks from Mirai are much larger than from what most DdoS attacks could previously achieve. Dyn estimated that the attack had involved "100,000 malicious endpoints", and the company, which is still investigating the attack, said that there had been reports of an extraordinary attack strength of 1.2Tpbs.

To put that into perspective, if those reports are true, that would make the 21st October attack roughly twice as powerful as any similar attack on record"

With an on-line botnet zombie attack – like Mirai - a remote agent takes over the embedded system - usually a Linux operating system - and controls it. How, you might ask, can they take over a Linux machine? Well, there are a number of ways...

All IoT mass-produced consumer products contain embedded systems and there is no incentive for the sub-contractor to install proper security measures – for example, unique and randomly generated passwords. They are usually shipped with "**username**: *admin*, **password**: *password*", and crucially cannot be altered. Mirai contained a dictionary of around 65 common passwords used by industry to protect the embedded system. All it had to do to gain entry to the device was to successively try the password until it found the correct one.

Linux is a very good operating system – it's used by the majority of phones, computers and embedded devices on the planet. However, all Linux builds that are done for embedded systems are based upon a standard version of the Linux kernel, and the boot loader. If the company that is doing the development have other priorities, they may leave lots of standard code in the build that's not needed for their application. For example, support for a keyboard when used in an IP camera, or display when used in an engine management system.

This spare code can be used by malicious agents as a way into a Linux system - for example Telnet, Rlogin or FTP. If they are not disabled or removed at the build time of the product, then they could be potential ways into the system.

There are a number of ways to mitigate this problem:

1. The simplest is to ensure that the manufacturers produce randomly generated passwords for the IoT products.

2. Use an RTOS like VxWorks, GreenHills, FreeRTOS etc. All military equipment will use an RTOS like GreenHills that is passed by the security agencies as safe and secure for use in the device.

3. Use the services of a company that will take a Linux build and make sure it is secure for your application.

So, to recap – zombie attacks and man-in-the-middle attacks have started targeting embedded systems. They are either used to launch attacks at other systems on the net, or are used for classic denial-of-service – which is critical to a physical device connected to the web.

SO HOW CAN MODULE 12 TECHNOLOGY HELP?

1. ZOMBIE ATTACKS

Module12 technology has a secure boot system that does not contain standard Linux. It utilities a Real- Time Operating System and an embedded IP stack (freeRTOS+TCP/IP), that has been tailored to this application and hence contains no redundant ports that an adversary can mount an attack onto. Additionally, the on-chip flash cannot be updated, so malicious code cannot be inserted into the device. Although it does contain external SDRAM, it cannot be forced to crash and produce a core dump to external memory, where it could be analysed. The on-board flash is encrypted so an adversary cannot intercept the code in the supply chin and analyse it for weaknesses.

Module12wt does not contain IP thus it could never be used in Zombie attacks.

2. MANUFACTURING ATTACKS

M12 technology is based around the Microsemi M2S Smartfusion 2 chip (see Ref and Ref), that offers industry leading security features. These include the ability to program the chip with an AES256 encrypted boot and application code so that at no stage is the original code exposed to a potential adversary in the manufacturing supply chain.

The chip includes an ARM processor for running the RTOS and IP stack, and an area of programmable hardware for the security enforcing functions (SEF's) and additional processing.

The SEF's that Blueskytec provide allow a very secure boot process that allows encrypted and authenticated boot with no user code, keys or data exposed to the supply chain at any stage.

No-one can stop the manufacturing of additional boards by the supply chain, but without the original 256bit key (unique per board) the boards are useless. The bare boards could be programmed by a different engineer to do a different job, but no circuit diagram information is available to the supply chain, and the boards have been designed to use Blind and Buried vias to make it as difficult as possible to do trace analysis. The process is designed to stop the application IP being altered or falling into the wrong hands.

NOTE – Many commercial TPM's do not allow the use of encrypted boot and applications – only authentication. This means that an adversary could potentially copy the code – either at programme time at the production facility or post production by snooping the boot process – for the express purpose of copying the IP and/or analysing it for weaknesses. Module12s are designed to specifically protect against unauthorized analysis of customer IP by encrypting with AES256 the boot and application code.

Physically Unclonable Function

This is an extract from Reference - "Overview_Supply_Chain_WP" on the Microsemi website...

"To provide true device binding, an intrinsic physical property with a high degree of repeatability and individuality can be used. Such a behavior is known as a physically unclonable function (PUF). In an electronic circuit, any internal SRAM memories, when powered up but before being written to, will contain a random collection of 1s and 0s. These are largely due to the nano-scale individual manufacturing differences of each memory cell (plus some noise), and are replicable to a high degree from power-up to power-up (typically more than 80% repeatability over all test conditions). This unique pattern of 1s and 0s, specific to an individual device, can be used to identify that particular device, analogous to the way fingerprints can provide biometric identification of people. Cryptographically binding this "silicon biometric" with the digitally-signed device certificate provides the strongest, most tamper-resistant, and difficult to forge method known today for assuring the pedigree of intelligent devices".

3. PHYSICAL ATTACKS ON THE CIRCUIT BOARDS

Any attempt to tamper with any item within the security boundary results in a tamper alarm and a range of actions result (full erasure of everything – to a remote alarm being raised). The boards use a layered approach to security with the outer layer being an external tamper switch. Then there is a secure enclosure on the circuit board, protected by a number of anti-tamper measures. Finally, there are chip level measures developed by Microsemi for the SmartFustion2 device that will erase the chip upon tamper. If an adversary removes any memory component from the board to try to mound a decryption attack (see the attack on Apple iPhone NAND flash - Ref "NAND mirroring attack on iPhone") the memory is AES256 encrypted with a 256bit key. This renders the flash all but useless.

4. MAN-IN-THE-MIDDLE ATTACKS

A remote application can connect to the Module12 technology over any of the communications channels. However, we do not trust this application, because the laptop/smart phone/tablet may be compromised with malware that may record and replay commands - REPLAY or MAN-IN-

THE-MIDDLE attack. These attacks could be performed at any point from the operator through to the actuator.

Because we do not trust this application, all commands issued by the operator are subject to a time-bound authentication token. This token must be used within a few Milli-seconds before it expires. The token is generated by the M12 wearable technology in the operators pocket. The application connects to the wearable technology via low energy Bluetooth. The operator must bond the M12wt with the application before use. The bonding process uses a unique number that the operator knows so that if the M12wt is stolen it cannot be used by adversary in the time duration it takes the operator to report the theft/loss of their M12wt.

Any commands captured by the MAN-IN-THE-MIDDLE could be replayed and/or altered but the token will not be valid so the Module12 technology will not respond. This token is unique and will not repeat, ever. (actually 2^256 possible codes over 10-100 mS gives many 100's of years before the possibility of a BIRTHDAY ATTACK).

5. BIRTHDAY ATTACK

A birthday attack is one where the possibility of 2 codes are generated that are the same. If AES256 is used in CBC mode, this could occur with 2^128 bytes of information. If 2 codes are recorded that are the same in CBC mode, then a simple XOR can be used to get the original key. Using IP where high bit rates are available with large transfers of data, we must be careful to change the key regularly, to avoid the birthday attack. There is no possibility of a birthday attack on the RS232/RS485 embedded network as this does not use CBC mode, and the data rates are exceptionally low – 9600 bps (not enough data to analyse).

5. ATTACKING THE CYPHER AND IMPLEMENTATION

AES256 has been accredited by all the major agencies as the default security standard. There is no evidence to suggest that AES256 can be attacked by the standard techniques (BRUTE FORCE, NON-LINER, HIGH ORDER etc). The implementation of the AES256 standard on the SmartFusion2 chip has been passed by a number of US and UK agencies for use in both military and commercial applications.

Module12 can use a variety of methods for authentication – from Symmetrical techniques using pre-placed keys and One Time Pads (OTP) to asymmetrical techniques using Elliptical Curve Cryptography (ECC) and other methods.

Module12 and Blueskytec also offer a number of custom algorithms for further security and additional tradeoffs/benefits.

6. ATTACK THE RANDOM NUMBER GENERATOR

The SmartFustion2 processor contains patented technology that generates a set of user keys from the state of the internal SRAM at start up – see the Physically Unclonable Function example above. This has been certified by various US and UK agencies for the purpose of generating keys for AES256.

In addition to this Module12ECU has a separate random number generator that is guaranteed to produce continuous random numbers. Again, this cannot be influenced by standard techniques, and is proprietary technology.

7. WHY NOT USE A TPM CHIP IN THE DESIGN?

In essence the Microsemi SmartFusion2 has a TPM integrated into the fabric of the FPGA, thus it is secure at chip level. A TMP that is housed on the same PCB or on a module attached to the PCB is always more vulnerable from snooping of the bus, than if it is integrated into the FPGA fabric.

Thus, there are 3 main reasons why the SmartFusion2 device (and hence Module12) is better than a separate TPM: (1) it is more secure by virtue of having security integrated into the silicon of the chip – not bolted on afterwards. (2) it requires less board space because of the high level of integration of the system-on-a-chip. (3) using the internal security features allows custom hardware extensions to the process to add unique features not found in TMP modules.

8. WHY NOT USE AN ARM PROCESSOR WITH BUILT-IN TPM?

The solution developed by ARM for their new range of processors has an integrated TPM. This will be well thought out and well designed to give designers using the chip a high degree of confidence of security. However, sometimes there are situations where a processor only solution, is not the best solution, and we need to turn to a system-on-a-chip from vendors like Altera, Xilinx or Microsemi.

Module12 is designed around the Microsemi SmartFusion2 processor. This is unique in the industry in offering a mix of programmable Flash based hardware (tiles) with a full Micro Controller in the fabric (ARM cortex M3), and an integrated TPM. Why is this important? In typical applications a software approach is usually taken – which can be very effective. But ideally Digital Signal Processing tasks such as FIR filters, FFT, Polar to Cartesian conversion, running average, Matrix manipulation and transformations are usually more effective when programmed in distributed hardware (more effective = higher throughput for lower power), leaving the processor to tackle the more complex tasks – such as IP stack manipulation or communications.

The SmartFusion2 provides the systems integrator with the ability to trade the cost, speed, power consumption and time to market. The processor is available from 5,000 to 90,000 programming elements (tiles) allowing the end customer or systems integrator to choose the device most appropriate for their application.

A typical ARM processor does not have this flexibility. The choice between the two approaches must be down to the systems integrator but with Module12 there is at least that choice.

SUMMARY

What problems are we trying to solve? These are outlined below:

Zombie attacks - in the paragraphs above, we have highlighted the issues around zombie attacks, and have suggested a number of methods to counteract this. Module12 uses a number of methods to eliminate this potential problem.

Supply chain attacks are very difficult to detect – especially if the production is off-shore and the quality procedures are subcontracted. The opportunity for organized crime, or governments to copy and analyse expensive software IP is widely available in far-east production facilities. The SmartFusion2 chip used in Module12 technology has been specifically designed to allow expensive IP to be protected and these have been cleared by various US/UK government organizations for use in this type of application.

The security of the system is of prime importance. If we cannot rely on the safety of the process we are controlling (a chemical or pharmaceutical plant for example), then the possibility of loss of life becomes important. The attacks on the controller come in many forms – from local physical attacks on the equipment to attacks on the operators laptop. It is essential that a Root-of-trust is established at both ends of the communication channel to avoid compromising the system.

Blueskytec believes it has some useful technology that can help in securing embedded systems, and we have a system and equipment view of that market.

REFERENCES

1. Microsemi: “Overview_Supply_Chain_WP”, http://www.microsemi.com/products/fpga-soc/security/security-concepts

2. Dr Sergei Skorobogatov: “demonstrated NAND mirroring attack on iPhone”, http://www.bbc.co.uk/news/technology-37407047

3. Microsemi: “security overiew page”,
http://www.microsemi.com/products/fpga-soc/security

4. Microsemi: “Extract from data security”
http://www.microsemi.com/products/fpga-soc/security#data-security

Microsemi FPGAs deliver key data security capabilities to protect applications data at rest or in transit:

- Root of Trust- the immutable secure starting point for your design Tamper Protection and Detection- deterring and detecting physical attacks on a device
- Zeroization- used to erase all sensitive data when a tamper event is detected
- Pass-through license- for CRI patented DPA protection for securing data in transit or at rest

Building on a Secure Root of Trust

Once a secure Hardware Root of Trust is established, higher level security functions can be utilised safely.

- Secure Algorithms and Protocols
    - Suite B algorithms such as: AES, SHA, HMAC, ECDH, ECDSA
    - Protocols such as: IPSEC, SSL, TLS, SSH, WEP, WPA2, HAIPE
    - Other algorithms and protocols benefiting from a secure execution environment
- Data Protection for:
    - Financial transactions
    - Medical records
    - Military applications
    - Trade secrets
    - Personal Communication
- Secure Boot
    - Protects the start-up code for processors and MCUs from attack
    - The Microsemi Secure Boot reference design can be used as a starting point for your embedded system design