Universidade de São Paulo
Instituto de Matemática e Estatística
Bachalerado em Ciência da Computação

Gabriel Capella

Título da monografia
se for longo ocupa esta linha também

São Paulo
Dezembro de 2018

Título da monografia
se for longo ocupa esta linha também

Monografia final da disciplina
MAC0499 – Trabalho de Formatura Supervisionado.

Supervisor: Prof. Dr. Alfredo Goldman vel Lejbman

São Paulo
Dezembro de 2018

Resumo

Elemento obrigatório, constituído de uma sequência de frases concisas e objetivas, em forma de texto. Deve apresentar os objetivos, métodos empregados, resultados e conclusões. O resumo deve ser redigido em parágrafo único, conter no máximo 500 palavras e ser seguido dos termos representativos do conteúdo do trabalho (palavras-chave).

Palavras-chave: palavra-chave1, palavra-chave2, palavra-chave3.

Abstract

Elemento obrigatório, elaborado com as mesmas características do resumo em língua portuguesa.

Keywords: keyword1, keyword2, keyword3.

Contents

Chapter 1

Introdução

falar que atuamente varios sao vulneráveis
pegamos uma solucao, melhoramos, testamos e vimos que eh possivel

Chapter 2

Key Concepts

Nowadays the term IoT (Internet of Things) is turning a buzzword. People, government, and industry have learned that connect simple devices to the internet, can produce a lot of useful data. This data can be used to improve production, make houses more smart e save money and time. Some studies show that by 2020 will be more than 20 billion IoT devices connected to the internet [].

This massive number of devices create new safety and security challenges. However, the vast number of known attacks in the lasts years show the responsible for this devices is not taking this challenge seriously. Some of this attacks can be in seen in the article X. Some of this attacks occur inside critical infrastructures, like nuclear plants, health, and transportation system.

Software, network, and hardware are layers of this devices that can be attack and damage. Study technics to verify if one device is attacked is the main object of this work. Attacks will ever occur, but if it occurs must have a way to identify than.

2.1 Embedded Devices

One embedded device is a system build to make a specific task. The main difference from normal circuits is the fact that this hardware is programmable, making possible the changes of it functionality only change the program inside it. Normal this devices are low cost, against failures and build work in real time situations. Because they aren't built for general propose, in the most cases they don't have a full operating system running inside it.

Nowadays these devices are changing, they are being connected to the to the internet and making part of the Internet of Things. This makes them vulnerable to attacks and invasions. Make them safe without increasing their cost is one big challenge.

There are embedded system based in processor and microcontrollers. The microcontrollers (or MCUs from microcontroller unit) are a chip with computational capabilities. In most cases, it is a single integrated circuit (IC) that has inside it the processor, memory, and digital I/O ports. This makes possible the use of same IC in different situations only changing its program.

This work the focus will be the low-cost embedded system that uses microcontrollers. Because of its low cost and main objective, this device as limited storage capability and, usually, as a single thread.

2.2 Trust Anchor and Root of Trust

REESCREVER

One of the principal themes related to security is the Root of Trust. Suppose Alice wants to talk with Bob using an encrypted channel. They can use a symmetric or an asymmetric encryption algorithm to do that. If they choose a symmetric algorithm, they will need to share passphrase before start talking. If they choose an asymmetric algorithm, they need to share their public key in a safe channel. If they share their public keys in an insecure channel, will not be possible to prove the identity of the other. There is a need for a reliable channel to start the conversation, and this idea is similar to the Root of Trust idea.

Another example of Root of Trust can be seen in the TLS (Transport Layer Security) use. When an encrypted connection is made, they need to use previous saved public keys (certificates). These certificates are provided during the operating system installation. There is a belief that the system is not corrupted during the installation and because of that, the certificates are not modified. The root of trust, in this case, are made by the installation moment.

Besides cryptography, the idea of the root of trust can be used in software verification. Suppose you want to know if a specific software is running on a device, you can verify the software before the run and, if it is the original one, you run with. On practical example is a computer manufacturer who wants their machines to run a specific version of an operational system. They can program the bootloader to verify the executable before running it. The root of trust, in this case, is made when the bootloader is written.

In field software verification are two roots of trust types[9]: dynamic and static. In the static one, the verification is only made before the software execution. In the dynamic, it is made during the software execution.

2.3 Remote Attestation

Remote attestation is a term used to design the capability to provide attestation cross a network [9]. Attestation is the ability to serve clear evidence of something. In the area of security, the evidence is the state of the device. The state is formed by what is present in the device memory in a particular moment.

Remote attestation techniques already have been developed for computers and high-end devices. The Trusted Computing Group (TCG[1]), a computer industry consortium, created a standard, the Trusted Platform Module (TPM[13]), to describe architectural elements needed to build a hardware module that provides security capabilities. Among this capabilities is remote attestation.

TPM is in its second version. Figure 2.1 shows all components that make part of this module. One use of this module can be to encrypt messages. It has a full encrypt engine inside it and a key stored securely. Commonly, this module is connected with the processor, making possible the exchange of information.

Within several uses, another interesting is the hardware and software verification. Assume one company do not want modifications in it computers hardware and software. The TMP can make a hash of the bootloader memory and all modules connected with the processor, after that it can sign this information and send to the company. If it suffers any modification, the company will see divergent in the expected data and the receive information. From this, she can stop providing system update or cancel the warranty, for example.

[1] https://trustedcomputinggroup.org/

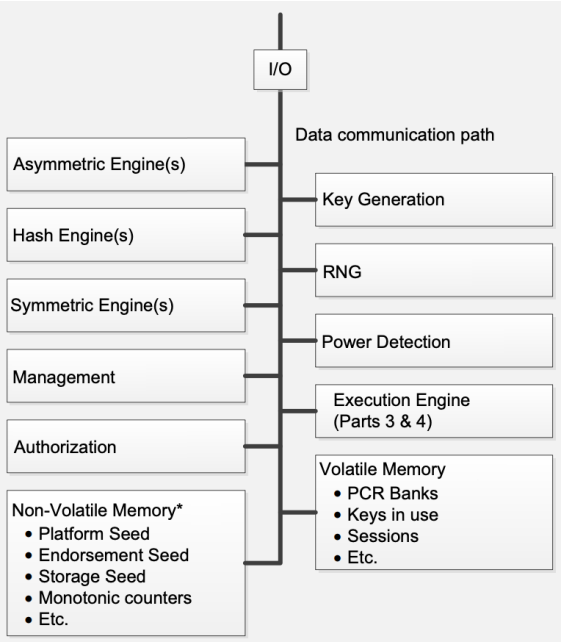

Figure 2.1: *Architectural Overview of TPM. Image from its manual [13].*

TPM is only one specification of secure cryptoprocessor. Intel and other brand have developed other technics to optimize the secure in its core processors. However, the cost of this coprocessors is not huge but significant when talking about embed systems. Usually, microcontrollers that driver the embed system costs a few dollars and the secure cryptoprocessor has practically the same price, making the price almost double. This provides an incentive to study and determine the minimum requirements need to provide a remote attestation.

The article [9] shows the essential elements and function to produce a secure remote attestation protocol. Using the language of this article, in a remote attestation, we have the **challenger** and the **prover**. The **challenger** his the device or computer that verifies the internal state of the **prover** across the network. The primary objective of the protocol is to allow a not compromised **prover** to provide an authentication token to the challenger, where it can to find out if the **prover** is in one expected state. In case the **prover** has been modified, the **challenger** needs to notice that.

To this protocol works there is a need for tree function:

- `Setup()`: needs to produce a long key k in a probabilistic way. This function will only be called once. The **challenger** saves that key and the **prover** have it, but it can only access it in certain circumstances.

- `Attest`(k, s): a deterministic algorithm that given one state s of the **prover** and key k, outputs an attestation token α. The **prover** computed this function.

- `Verify`(k, s, α): given a key k, a device state, and an attestation token a. The function returns `True` if `Attest`(k, s) is equal α. Otherwise, returns `False`. The **challenger** computed this function.

In a remote attestation verification, the challenger ask for the authentication token to the **prover**. The **prover** produces it using `Attest` function, creating the attestation token (in an indirect manner the information of its state). When the **challenger** receives α, it verifies if it can produce the same token, using the `Verify` function.

To this protocol works there is a need to share the key k between the **challenger** and the **prover**. We will suppose that this k will be shared in a safe way when the device is

manufactory. That is, the key will be write in the device during before it can suffer any attack. The company that produces the device is responsible for generating k and saving it securely. They will use this key after to make the attestation.

During the protocol is transmitted the attestation token. This transmission occurs over a network and is successive to attacks. If this occurs, the **prover** will send a token α and the **challenger** will receives a α'. In this case, the **challenger** will attest the **prover** as a violated device (in not know state). Some technologies, like the Transport Layer Security, can be used to prevent attacks in this connection. One interesting fact to note is that an attacker can save one old authentication token and send this token in a later connection. To prevent this type of attack, when the **challenger** ask for the authentication token, with the request it will send a nonce n. This nonce will modify the state of the **prover** providing a unique state. This nonce is randomly generated in each authentication token request. The n is not specified in the above function, to make clear the basic idea of the protocol, but in the future, it will be used.

Suppose the **prover** suffer an attack, when this happens the state s of the device becomes known by the attacker. With this information he can produce to types of attacks: simulate the `Attest` function a return a correctly α; returns a α that is not the real state of the device. To prevent the attacks mentioned the `Attest` function in the **prover** has to have the following properties:

- **Exclusive Access**: only the `Attest` function can have access to key k. This makes impossible to forge the token α without running the `Attest` function.
- **No Leaks**: after de execution of `Attest` no information of the key k can leak. Otherwise, the key k will become known by the attacker. Cleaning all memory after the function execution can solve this problem.
- **Immutability**: if the `Attest` can be changed, the attacker can change it to leak the key k.
- **Uninterruptibility**: if during the computation of `|Attest|`the device suffer one interruption, the key k information can leak.
- **Controlled Invocation**: the `Attest` function can only be called by its beginning. Otherwise, the attacker jumps important parts in the `Attest` code, like the code that disable all interrupts.

The way all these properties will be provided varies according to the device. Some approaches try to provide all these properties using a software implementation. Unfortunately, the remote attestation using only software has been proved that not work in the internet context.

2.4 Works in Remote Attestation for Embedded Devices

This section has the primary objective to show and discuss the mains works in Remote Attestation for Embedded Devices. It fist subsection will contemplate software remote attestation technics and show why they have been proven to be insecure on the internet. The others subsections focus on some hardware implementations.

One of the main remote attestation projects using the software approach is Piooner.

Currently the main works done in this area are: SMART [7], TrustLite [10] and SANCUS [12].

2.4.1 Software Protection Modules

[16]
[15]
poruqe nao funciona no geral e problemas [11]
porque nao funciona para embed devices [6]
One of the main remote attestation projects using the software approach is Piooner.
mudanca ipv6 para satisfazer.... [14]

2.4.2 SMART

TEM FALHAS, [8] [7]

2.4.3 TrustLite

TrustLite [10]

2.4.4 SANCUS

[12]

2.5 FPGA

FPGA is an abbreviation for "field-programmable gate array". This is a special type of integrated circuit created in the 80s, the main difference of others integrates circuits is the possibility to reprogram the circuit using an HDL (hardware description language).

The major benefits are that you can test new hardware and circuits without the need to produce a new integrated circuit. One of the tasks in this work is to change the memory backbone of on microcontroller and test the results. Using the FPGA the assignment to test the modification became easy because changing it is like reprogram.

There are two principal HDL languages used in the market: Verilog and VHDL. This language is totally differences from normal programming languages. The principal difference from normal programming languages is the fact that everything is happening in parallel. In this languages, variables are replaced by registers and connected with wires. There are some attempts to convert sequential programming languages, like C, in hardware description languages, like the LegUp High-Level Synthesis project [3]. But transforming sequential code to hardware normally require big circuit.

An approach used in used in most FPGA projects is to program a small processor inside it. This processor can be programmed using a sequential programming language. The good thing about this designer is the possibility to connect an hardware in the processor to make specifics tasks. Some companies that produce FPGA's are build processor optimized for their products. One of the most famous projects is MicroBlaze, a 32-bit RISC microprocessor, designed by Xilinx. A Linux kernel implementation has been made for this processor, making possible to run a Linux inside an FPGA.

2.6 Layers Contemplated

This work will build a device and program it, involves a different abstraction layer. The first layer, already explained, is the FPGA. It will run a hardware description code and

will build this hardware inside it. This hardware will run an assembly code generated by a compiler from the C language.

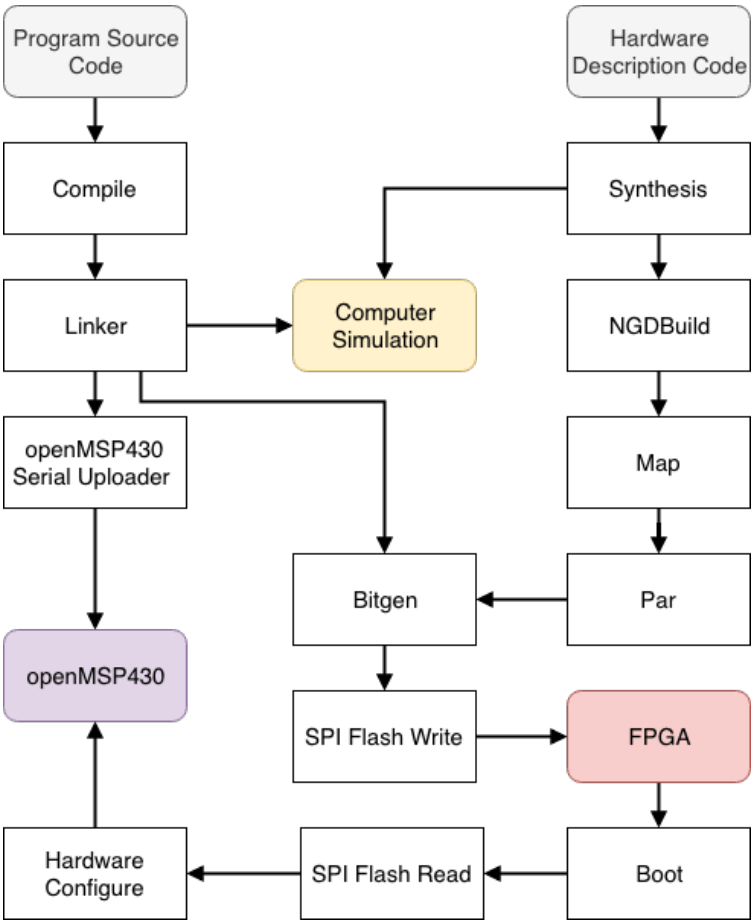

Figure 2.2: *Development building and load steps.*

Chapter 3

Implementing SMART

3.1 Premises

In the main article is presented few assertions to ake an informal proof of the SMART security. They are:

- A1: is impossible to forge the hash value. One significant difference from the main article is the fact that the hash is computed using special hardware and not software code. This hardware is designed to receive a data chunk and digest it to make the hash value. There is a guarantee on a hardware level to make impossible to recover the data sent to the hash computation.
- A2: the device with SMART will not suffer any hardware attack, only software.
- A3: only the SMART code can access the SMART key.
- A4: only the SMART code can change itself. This assertion is different from the original article but will provide additional features.
- A5: SMART code can only be called from the first memory address.
- A6: if the SMART code moves the instruction pointer from outside its region, it is impossible to return to the previous code. This assertion is a little different from the original but provides the same guarantees.
- A7: all interrupts are turned off during the SMART code execution.
- A8: after the SMART code execution the SMART key cannot be recovered. The hash hardware and software clean in all memory used in the SMART code guarantee this.
- A9: the SMART code compute the hash correctly after receiving a challenge.
- A10: after a reset, erase all memory data segment. This procedure prevents the leak of any information remaining in the memory.
- A11: none information from the SMART key can be a leak.

3.2 Implementation Details

One of the main objectives of this work is to implement the SMART as described in the article. The authors made two implementations of SMART, one in a Atmel AVR microcontroller and other in a Texas Instruments MSP430. Both are described

3.2.1 MSP430

falar sobre ele, como a memoria Ã© inicializada.... mostrar organizaÃ§ao de memoria....

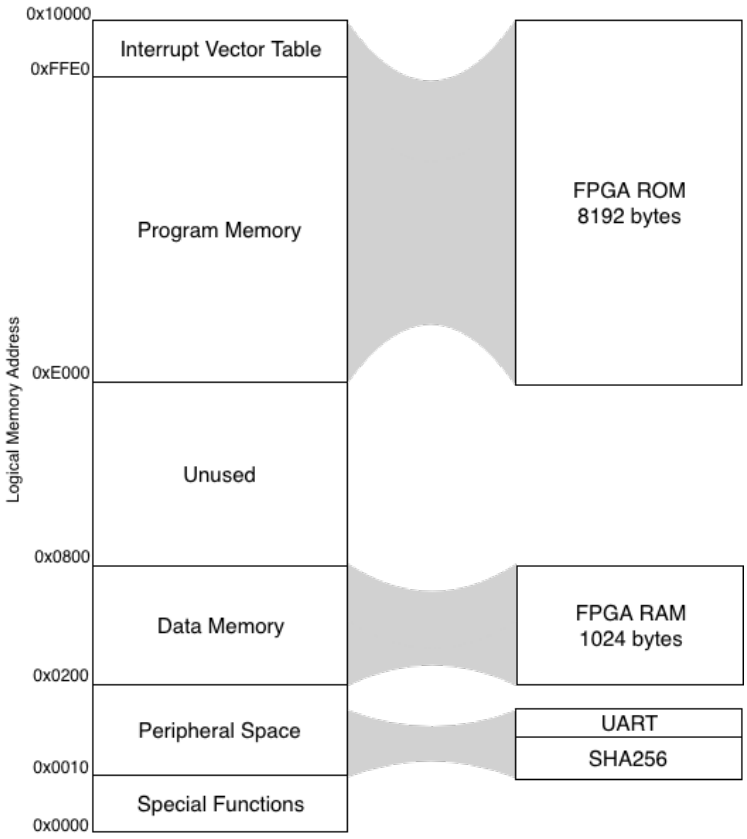

Figure 3.1: *a nice plot*

3.2.2 SPARTAN 6

3.2.3 Time Constants

One important thing when working with FPGA is the time constants. These values are essential for testing, and the dispose of the connections inside the FPGA.

For Verilog simulations, the time constants are set using a reserved macro named `timescale`. This macro receives two values: the time unit and time precision. The simulations delays and any time value use the time unit. And the time precision is used by the simulator to know how they can round the summation values. In the tests are used $1ns$ for time unit and $100ps$ for precision.

```
1 initial
    begin
3       CLK_100MHz = 1'b0;
        forever #5 CLK_100MHz <= ~CLK_100MHz; // 100 MHz
5   end
```

Listing 3.1: *Simulation clock signal generator.*

Code 3.1 is used in simulation to generate the clock signal. It changes the value of wire `CLK_100MHz` in intervals of $5ns$ (5 units of time), making an output signal of $100MHz$. Is chosen the frequency of $100MHz$ because the testing FPGA has a clock of this frequency.

These values are calculated using the frequency formula $F = \frac{1}{T}$, where $F = 100MHz$ is the desired frequency and T is the period. After solving this equation $T = 10^{-8}s$, this is equal to 10 units of time (10ns). The FPGA clock uses a duty cycle of 50%, that is that the clock will need to be 50% of their time active and the other part inactive (the signal will change to high to low or vice-versa in an interval of 5 units of time).

The communication with the simulator in testing or the computer in a real FPGA is made using the RS-232 standard. This standard is a serial protocol, the bits are sent one by time. A direct consequence is that the protocol use time constraints to send the information. In all test is used the 19200 bit/s baud rate, making each bit transmission time be $52100ns$.

To reduce the timing conflicts and problems inside the openMP430 [4] the microcontroller will receive a clock input of $20000MHz$. To change from $100000MHz$ to the desired input speed, a Digital Clock Manager (DCM) [1] will be used. The DCM is a dedicated hardware inside the FPGA for clock frequency conversion. To this module works it needs several configuration parameters, to simplify it a module named `clock.v` was created with all configurations inside it.

The microcontroller uses one hardware peripheral to interface with the RS-232 serial port. This hardware need to know the bit transmission time, in all software that uses serial has the `UART_BAUD = BAUD;` line. This line is responsible for setting a unique memory address to the correct bit transmission time.

3.2.4 SHA256

One improvement in this implementation compared to the original article has using a hardware SHA2 (Secure Hash Algorithm 2) to hash the memory. The original implementation uses a software SHA1. Different from SHA1, SHA2 is a family of hash function, in implementation use the SHA256 function.

The SHA256 has some improvements compared to the SHA1. The first one has the input size, SHA1 needs to receive only 160 bits to produce a hash, the SHA256 needs 256 bits. SHA1 was deprecated by NIST (National Institute of Standards and Technology) in 2011. There also some articles, like [17], to show how an attacker can forge two distinct PDF documents with the same SHA-1 hash.

It is important to notice that exist a new version of the secure hash algorithm, the SHA3. This version made some improvements and NIST advise to use it. There was the attempt to implement the SHA3 in the FPGA, but it exceeds the number of available LUTs in the FPGA, making the implementation impossible with the openMSP430 core. However, SHA256 is still considered segure, and it fit inside the FPGA.

A SHA3 implementation written by Joachim Strombergson [2] has used. A peripheral adaptor was built to communicate with the openMSP430 core. This adaptor is responsible for interfacing the SHA3 implementation with the peripherals pins in the microcontroller. The file `SMART/rtl/verilog/sha256/sha256per.v` contains this interface.

Another change is the use of a hardware hash function and not a software one. This change makes the hash timing faster and saves several bytes in ROM. However, it uses hardware approximately 2000 LUTs.

3.2.5 Linker Script

When building the binary to a microcontroller the compiler needs to know where place the code, data and other pieces of information in the memory. Linker script (or linker command file) is a particular file that describes to the compiler this attributes. Original the MSP430

mapped all memory using 16 bits addresses, making the maximum available space to be 65536 bytes.

However, the majority of microcontrollers compatible with the MSP430 architecture don't use all this memory.

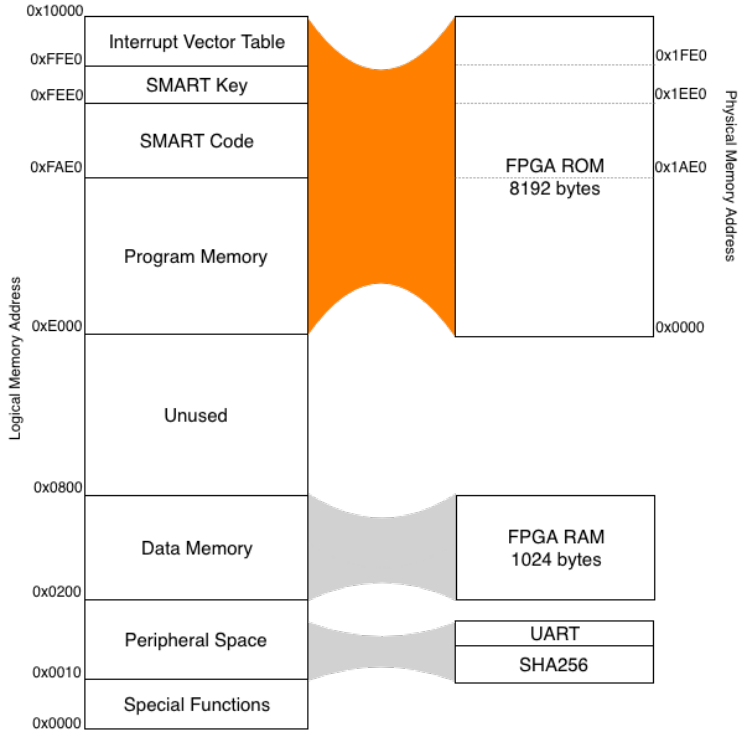

Figure 3.2: *a nice plot*

falar do original e da diferenÃ§a do que foi feito

3.2.6 MCAM

3.3 Tests

3.3.1 Light Remote Control

3.3.2 Light Remote Control

3.3.3 Continuous integration

A continuous integration system is used to prevent and identify any code error or change that affected the correct work of the microcontroller. A GitHub project is set to track the code changes and versioning the code. On every push, a server receives a notification, run all test in the project and build the FPGA files.

Jenkins[1] is used to build the continues integration. Other systems, like Travis or Gitlab CI, are not used because they have restrictions on the maximum size of their builds. To test and build the code the Xilinx ISE WebPACK Design Software is used, this software has approximately 6 GBytes. Jenkins makes possible install this software on the tester machine only one time and uses it when needed.

[1] https://jenkins.io/

Are used two software to simulate the behavior of the hardware: the Icarus Verilog[2] (an open-source project) and the Xilinx ISE (a property software). For every test are tested using this two softwares, this decision is made because during the development are notice that some errors only occur in one of them.

3.4 Results

[2]http://iverilog.icarus.com/

Chapter 4

Improving SMART

The opemMSP430 memory backbone is changed, allowing writing in the program memory. This change makes possible remote device updates, but also introduces several security breaches. However, the SMART implementation can identify if any breach occurs.

A system is built to control, verify and make a remote update using the SMART as the final example.

The article *ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices*[5] has the base of this system.

Chapter 5

Conclusion

Texto texto[1].

[1]Exemplo de referência para página Web: www.vision.ime.usp.br/~jmena/stuff/tese-exemplo

Appendix A

Módulo de Controle de Acesso à Memória

O objetivo desse apêndice é descrever o funcionamento do módulo o módulo de controle de acesso a memória (MCAM) implementado nesse trabalho.

Esse módulo permite que uma região da memória seja lida somente se uma função for executada. Ele verifica se o ponteiro de instrução é igual a um valor específico. Caso seja, habilita que uma região protegida da memória seja lida. Ao sair dessa função ele inibe o acesso à essa região. Caso haja a tentativa de acessar uma região sem autorização, o módulo reinicia o dispositivo.

A descrição de cada entrada e saída está presente na tabela a seguir:

Nome do Parâmetro	**Tipo**	**Tamanho (bits)**	**Descrição**
`in_safe_area`	Saída	1	Quando ativado (ligado) simboliza que o acesso à região da memória protegia está liberado. Ou seja, a função que terá acesso a essa região está sendo executada.
`reset`	Saída	1	Quando ativado o dispositivo tem que ser reiniciado.
`mem_dout`	Saída	16	Saída dos dados da memória.
`mem_addr`	Entrada		Endereço da memória à ser acessada. O seu tamanho pode ser configurada via parâmetros.
`mem_din`	Entrada	16	Entrada dos dados da memória.
`mclk`	Entrada	1	Relógio da memória.
`ins_addr`	Entrada	16	Endereço que o ponteiro de instruções está usando.
`disable_debug`	Entrada	1	Quando ativado, desabilita o módulo. Útil para depuração.

Além das entradas e saídas, é possível entrar com alguns parâmetros na confecção do módulo. A tabela abaixo mostra quais são esses parâmetros e suas funcionalidades.

Nome do Parâmetro	**Descrição**
SIZE_MEM_ADDR	Valor que representa o número de bits presente no endereço de memória (`mem_addr`) menos um.
LOW_SAFE	O menor endereço físico na memória da região à ser protegida.
HIGH_SAFE	O maior endereço físico na memória da região à ser protegida.
LOW_CODE	Onde começa a função que terá acesso a região protegida na memória. Endereço virtual.
HIGH_CODE	Onde termina a função que terá acesso a região protegida na memória. Endereço virtual.

Note que para o endereçamento das funções que tem acesso a parte protegida é utilizado o endereço virtual. A descrição do espaço de memória protegida utiliza o endereço físico. O endereço virtual é o utilizado na pelo programa e mantido pelo compilador. Já o endereço físico provém do virtual adaptado para o tipo de memória conectado ao dispositivo. Aqui utilizamos dois tipos de endereçamento diferente, pois o ponteiro de instruções utiliza o endereço virtual. Em contrapartida, o acesso de memória utiliza o físico nativamente. Uma descrição mais detalhada sobre as diferenças de endereçamento e como realizar a conversão de um para outro pode ser vista na página do openMP430 [4].

No artigo é citado que para criação do controle de acesso a memória é necessária poucas modificações. Essa afirmação ;e verídica, no entanto as modificações devem ser feitas de forma precisa. Em nenhum momento no artigo é citado que o controle da memória deve ser sincronizado com o relógio de acesso a mesma. Apesar dessa premissa ser óbvia ela é relevante, pois se somente observamos o endereço da memória, sem levar em conta o relógio, haverá momentos em que o dispositivo será reiniciado sem a necessidade.

A implementação do módulo pode ser separada em duas partes principais. A primeira verifica se o ponteiro de instruções entrou corretamente no bloco de código que tem direito ao acesso à região protegida. Essa verificação é efetuada comprando o ponteiro de instruções do microcontrolador com os parâmetros do módulo. Caso o valor do ponteiro `ins_addr` seja igual a LOW_CODE, temos que valor dentro do hardware se torna positivo, habilitando o acesso. Quando o `ins_addr` $\geq$ HIGH_CODE ou `ins_addr` $\leq$ LOW_CODE-1, esse valor se torna 0, impedindo o acesso.

A segunda parte é responsável por verificar se o endereço de memória está tentando ler uma região protegida. Ela verifica se LOW_CODE $\leq$ `mem_addr` $\leq$ HIGH_CODE. Caso essa condição seja verdade, mas o dispositivo não tenha executado a função da primeira parte, ele é reiniciado.

A implementação completa desse módulo pode ser vista no repositório Github desse trabalho [1].

[1] https://github.com/capellaresumo/MAC0499/blob/master/SMART/rtl/verilog/mcam.v

Bibliography

[1] *Spartan-6 FPGA Clocking Resources*, 2018. https://www.xilinx.com/support/documentation/user_guides/ug382.pdf [Accessed: September 2018]. 10

[2] *Hardware implementation of the SHA-256 cryptographic hash function*, 2018. https://github.com/secworks/sha256 [Accessed: September 2018]. 10

[3] *LegUp High-Level Synthesis*, 2018. http://legup.eecg.utoronto.ca/ [Accessed: September 2018]. 6

[4] *openMSP430*, 2018. https://opencores.org/project/openmsp430 [Accessed: August 2018]. 10, 16

[5] N. Asokan, T. Nyman, N. Rattanavipanon, A.-R. Sadeghi, and G. Tsudik. Assured: Architecture for secure software update of realistic embedded devices. 07 2018. 13

[6] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente. On the difficulty of software-based attestation of embedded devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 400–409, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-894-0. doi: 10.1145/1653662.1653711. URL http://doi.acm.org/10.1145/1653662.1653711. 6

[7] K. Eldefrawy, D. Perito, and G. Tsudik. Smart: Secure and minimal architecture for (establishing a dynamic) root of trust. 01 2012. 5, 6

[8] A. Francillon, Q. Nguyen, K. B. Rasmussen, and G. Tsudik. Systematic treatment of remote attestation. *IACR Cryptology ePrint Archive*, 2012:713, 2012. 6

[9] A. Francillon, Q. Nguyen, K. B. Rasmussen, and G. Tsudik. A minimalist approach to remote attestation. pages 1–6, 01 2014. 3, 4

[10] P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan. Trustlite: A security architecture for tiny embedded devices. In *Proceedings of the Ninth European Conference on Computer Systems*, EuroSys '14, pages 10:1–10:14, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2704-6. doi: 10.1145/2592798.2592824. URL http://doi.acm.org/10.1145/2592798.2592824. 5, 6

[11] X. Kovah, C. Kallenberg, C. Weathers, A. Herzog, M. Albin, and J. Butterworth. New results for timing-based attestation. In *2012 IEEE Symposium on Security and Privacy*, pages 239–253, May 2012. doi: 10.1109/SP.2012.45. 6

[12] J. Noorman, J. V. Bulck, J. T. Mühlberg, F. Piessens, P. Maene, B. Preneel, I. Verbauwhede, J. Götzfried, T. Müller, and F. Freiling. Sancus 2.0: A low-cost security architecture for iot devices. *ACM Trans. Priv. Secur.*, 20(3):7:1–7:33, July 2017. ISSN 2471-2566. doi: 10.1145/3079763. URL http://doi.acm.org/10.1145/3079763. 5, 6

[13] T. Published. Trusted platform module library - family 2.0 - revision 01.38, 09 2018. 3, 4

[14] A.-R. Sadeghi and S. Schulz. Extending ipsec for efficient remote attestation, 01 2010. 6

[15] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. Swatt: Software-based attestation for embedded devices. 04 2004. 6

[16] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla. Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems. *SIGOPS Oper. Syst. Rev.*, 39(5):1–16, Oct. 2005. ISSN 0163-5980. doi: 10.1145/1095809.1095812. URL http://doi.acm.org/10.1145/1095809.1095812. 6

[17] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov. The first collision for full sha-1. pages 570–596, 07 2017. 10