embeddedworld 2014
Exhibition&Conference
... it´s a smarter world

Security in Cyber Physical Systems CPS

Michael Wagner
Networked Systems and Applications
Fraunhofer IIS
Nürnberg, Germany
michael.wagner@iis.fraunhofer.de

***Abstract*ð Today security is seen an integral part of personal computing. There is always a talk about huge libraries containing numerous crypto algorithms, key agreement mechanisms, hash algorithms and many more, which leads to accumulation of software resources needed to establish a secure connection between any two PCs on the planet. Since the Embedded systems (at least the top level ones) use the PCôs operating system they end up having the same software packages. Still there remains a reasonable doubt while updating the system using the monthly security Bug-fixes: How can it be proven that a system is secure? The proof for a standard PC system should involve all the modules and components, accessible to an attacker. These include not only the network stacks from the hardware till the communication sockets (TCP/IP) but also the OS, its process separation, DMAs, Interrupts and other modules. And security does not only mean the threat of internet hackers and viruses. Threats like plagiarism or license violations by accessing the local debug features are foreseeable for an embedded system, but are a totally unheard of in the PC-world. It will be shown how the necessary security level can be reached by dividing the system into three parts: first the stacks connected to the outer world (black), second a security bridge as the line of defense and third the protected world of secrets (red) with its local interfaces. The proof of security now concentrates on the line of defense inside the security bridge and the separation of the red and black sectors. The bridge software can be concentrated to a few hundred lines of code, enabling a clear proof of security in a short duration. Implementation of the algorithms in hardware will reduce the overall compatibility but also the amount of software in the bridge. The higher parallelism is advantageous against side channel attacks. Starting from this basic system several goals can be reached. For CPS the three important aspects are: machine to machine communication (m2m), protection against local manipulation/IP extraction, and internet based hacker attacks. These scenarios will be discussed in the second part of the talk. Still advanced security is not allowed to produce higher costs. The third part of the talk will deal with a way to integrate these three systems to a security enabled multicore CPU. It is imperative to keep red, black and the bridge clearly separated by the security architecture. Techniques are shown to fulfil the requirements of the second part by using the mechanisms of specialized security processors. In the end an architecture is described, that combines cost efficiency, high security level and m2m features to form a new Cyber Physical Systems platform.**

I. INTRODUCTION

Currently there are three branches of security architectures. They differ in their application, the risks of a successful attack, and in the priorities of the customers. All three use different system designs, algorithms, measures, and sometimes even a different vocabulary to describe common concepts.

The three branches are military security, embedded security (mainly used for mobile phones) and PC security.

Cyber physical systems (CPS) are seen as the backbone of the future industry. They act without permanent human control, communicate with other CPS, order material, sell products world-wide and control locally connected machinery.

In the smart grid energy will be traded while generation, distribution, consumption and storage are controlled. The wide field of applications in this scenario includes high volume products like smart meter gateways but also cost sensitive low volume products like building specific energy management gateways.

On CPS the currently used approach is the PC security architecture, because platforms are enough powerful to run PC operating systems (OS). Still the complexity of those systems makes it difficult to run them unattended for extended periods ï for maintenance and security reasons. A second important aspect is the impact of an attack to a large number of nearly identical platforms, which manage critical infrastructure e.g. the smart grid. To grant a sufficient amount of security, evaluation procedures have been defined. Such procedures are expensive and slow down further platform development. These issues have already been solved by the other two branches in different ways.

A new CPS security branch could include the knowhow of all three existing branches resulting in a low cost and highly secure system.

II. STATE OF THE ART

A. Military security architecture

Military security protects communication. An attacker typically tries to break the algorithm, use any side channel or get hands on the equipment to extract algorithm and keys. The crypto device is typically located at the border between the protected and the open area.

Military security started to use multiple embedded processors in the middle of the 70ies and continued to evolve until in the 90ies more powerful processors led to a three module design: The red module processes the secret data. The security bridge module transforms the secret data (red) by encryption to black data and passes it on. The black module communicates the encrypted (black) data to the outer world. Examples can be found in [1].

This structure is optimized for several challenges. Customers usually want to evaluate a product for hidden bypasses (side channels) from the red side to the black side. A clear and easily provable separation of the red and the black modules will move them out of the focus of the evaluation. The security bridge ï the border line between red and black ï can be optimized for evaluation similar to safety systems: code of low complexity (no OS), core functionality and simple well documented interfaces grant short review times. Thus the security bridge can be easily customized, leading to an individual security solution for each customer.

The three module architecture reduces the level of trust necessary of the customer in the manufacturer.

B. Mobile phone security architecture

In the end of the 90ies mobile phones had their break through. Identification to the network was done by the SIM card. Business models like SIM locked sponsored phones enabled new deception scenarios: The value of such a mobile phone could be increased by reprogramming it to the original version. To prevent that, hardware platforms were designed, that allowed a control of the software image. The most popular representative is the ARM trust zone [2], which does not only provide a secure boot but also a secure operation mode for a limited part of the application software. The secure operation mode uses chip internal memory to hide the protected code and data from open mode software and debug tools.

Intrusion detection, temperature control, or data integrity control are added by some integrators, increasing the resistance against local attacks. [2]

Digital rights management and multicore processors triggered new mechanisms like virtualization extensions [4] and the trustZone controller 400 (TZC-400) [5] to control the memory access of virtualized applications and bus masters by hardware mechanisms.

C. PC security architecture

Also in the end of the 90ies home banking caused the need for security on the PC platform. Differing from the first two branches, the PC platform is defined by compatibility and flexibility. It is seen as a feature of the platform to be changeable within seconds. The process separation by the memory management unit (MMU) is the most important hardware security mechanism. Cryptography was introduced for the TCP/IP Communication as a software layer. The PC platform offers already broken algorithms for backward compatibility. Attacking such a system means not defeating the crypto algorithm but instead trying to execute code in supervisor mode.

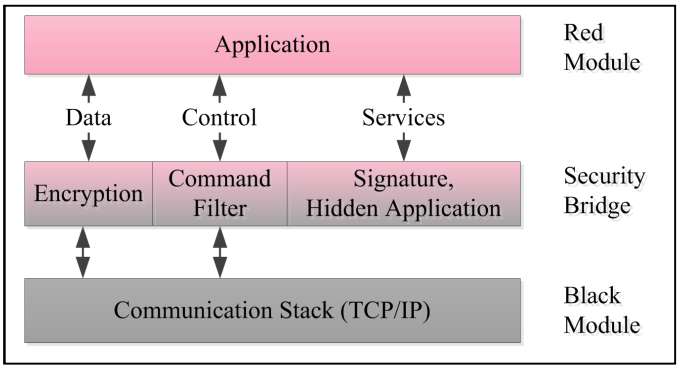

Fig. 1. Basic system for CPS as a three module design

III. CYBER PHYSICAL SYSTEMS

A. The security challenge for CPS

As described earlier CPS control the smart grid or buy and sell goods worldwide by machine to machine communication (m2m). The main issue here from a security perspective is trust: The identity of the communication partner, the integrity of the systems, the security and integrity of the communication and the certification of contracts can be solved by security mechanisms.

The application will be complex and highly flexible. Software modules may be downloaded on demand from third parties, introducing further need for trust or control. The operating systems will most probably be derivates of current PC OS. Due to their high complexity an evaluation process will raise high costs at medium security. This process must be repeated after any change, as a certificate is dedicated to a version, e.g. Common Criteria in one of its evaluation assurance levels (EAL) [6].

B. Basic system proposal

The success of such systems depends on a concept that allows a deep and easy evaluation while keeping the flexibility. So a partition into three modules as in military systems is an option. The black module contains the TCP/IP stack and the black OS. The red module contains the application software, the local communication stacks and the red OS. It is important to concentrate the security relevant control mechanisms in the security bridge. These are identification and access control of communication partners, resistance against attacks from both sides, and data encryption (today: transport layer security TLS). The socket methods called from the red side for socket control are inspected and forwarded by the security bridge. Digital signature generation can be offered to the application. Also protection against

reengineering can be offered by hiding a central part of the application.

As the complexity of the security bridge and its interfaces should be kept low, it would not distinguish between applications of the red side like a firewall. The proposal is to use in the red module an environment that allows internal rights management like Java and OSGi.

The black module could be successfully attacked via the internet. This is not an issue as long as the security bridge is not vulnerable for actions performed by an overtaken black module. The security bridge may react to unexpected behavior of the black side by restarting it from an intact boot image. As a result, the vulnerability to attacks from the internet is now defined only by the vulnerability of the security bridge.
This system is referred to as ñbasic systemò. It is already specialized for the internet communication, but it is still open concerning the operating systems, the application, the cryptography and the implementation. Depending on the tradeoff between security, development costs and system costs, some implementations are possible.

C. *Cost optimised system*

Minimizing the system costs will be the first target of the following discussion.

The modules can be integrated into a processor with security architecture as used in smart phones. For the explanation the syntax of the ARM trust zone is used. The red module and the security bridge share one core, the security bridge running in secure mode. The program and the memory of the security bridge have to reside in the internal secure memory. The black module can be implemented in three ways:

- Placed to a second core, the memory space can be separated from the red module by the TSC-400 or simply by the coreôs MMUs ï putting the MMU access on both modules under security bridgeôs control.
- Placed to the same core the separation can be done by virtualization extensions.
- An external microcontroller could carry the black module, resulting in a higher bill of material but significantly lower amount of software in the security bridge. The check for side channels is obviously easier. The evaluation costs are reduced.

The system will start in secure mode, which gives control to the security bridge. Configuration and the boot preparation of the red and black modules and their resources are done in the secure mode. Communication can be done by shared memory under the control of the security bridge (for an external black module serial communication is proposed). Some simple checks allow stable data and control information transfer. Additional security features can be used to detect changes in the security bridgeôs program.

Key storage is an important aspect for security. Two mechanisms are offered, both only accessible in secure mode:

- Flash cells store a factory programmed key and allow a permanent entrance.
- Buffered RAM in combination with intrusion detection allows storage of key material but also volatile information about the system status, e.g. to prevent roll back attacks.

D. *Security gain*

The secure memory space is limited thus limiting the security bridgeôs program and data size. Processors with up to 1,5 megabyte internal securable RAM are available.

The amount of bridge software depends on the integration of the black module, the number and kind of Control commands to be filtered (e.g. DNS), offered additional services and the specialization grade of the application.

Compared to a solution, build with three discrete modules, the separation of the modules will now be an additional aspect for the evaluation. The electromagnetic interference (EMI) between red and black depends on the integration of the black module. Due to the chip internal operation of the secure mode, its electromagnetic emission (EME) will be reduced. Software techniques avoiding compromising patterns in the EME should be used.

Compared to a PC solution, the amount of software participating in the red/black separation is strongly reduced. Also the complexity of this software can be held low. The described security bridge combines key storage and the crypto algorithms with the control of the communication between the application and the outer world. The encapsulation in the secure mode in combination with hardware intrusion detection eliminates the chance of key extraction in the field. Attacking the system from the internet now means attacking the security bridge from a conquered black module. As the security bridge will never execute external code and no internal buffering may cause overflows, no mechanisms exist for an attack from the wide area network. Only trusted partners, due to their connection across the security module, have the chance to interfere directly with the application.

[1] Dr. Boyd Buchin, ñSVFuA ï Grundlage für NetOpFü auf der taktischen Ebeneñ, Fachveranstaltung ÄTaktische Kommunikationñ Streitkräfteunterstützungskommando, Rheinbach, 14. December 2010, http://www.afcea.de/fileadmin/downloads/Fachausstellung/23._Fachausstellung_2009/Anmeldung/8%20-%202010-12-14%20SVFuA%20ZVEI-AFCEA%20Grundlage%20f%C3%BCr%20NetOpF%C3%BC%20.pdf (January 14th 2014).

[2] ARM, ñBuilding a Secure System using TrustZone Technologyò, http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.prd29-genc-009492c/index.html (January 14th 2014).

[3] Freescale, ñVF6xx: Vybrid family with ARM® CortexÊ -A5 + Cortex-M4ò, http://www.freescale.com (January 14th 2014).

[4] Prashant Varanasi and Gernot Heiser, ÄHardware-Supported Virtualization on ARMò, APSys 2011, Shanghai, China (July 11-12th 2011), http://apsys11.ucsd.edu/papers/apsys11-varanasi.pdf

[5] Rob Coombs and Simon Moore, ñGlobalPlatform TEE* &ARM TrustZone technology: Building security into your platformò, ETISS 2013, Graz University of Technology, Austria (December 1-5th 2013), http://www.iaik.tugraz.at/content/about_iaik/events/ETISS_INTRUST_2013/ETISS/slides/GPTEE_Public.pdf

[6] ñCommon Criteriaò, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/ITSicherheitskriterien/CommonCriteria/commoncriteria_node.html (January 14th 2014)