Ubiquitous Computing asks for Ubiquitous Line of Defense

Oliver Stecklina, Peter Langendörfer
IHP
Im Technologiepark 25, 15236 Frankfurt (Oder), Germany
Email: {stecklina,langend}@ihp-microelectronics.com

Abstract: This paper gives an overview of security challenges and approaches for Cyber-Physical Systems (CPS). CPSs are systems, e.g. in industrial or medical environments, which connect physical elements to a public accessible network. By using a wireless communication or internet routes physical fences are not longer a sufficient barrier against malicious users or attackers. Classical approaches like IP-based firewall or Intrusion Detection Systems (IDS) can not be used one-to-one for this class of networks. The limited resources of sensors and actuators as well as real-time requirements ask for new approaches. Furthermore the approaches must run on the node itself due to its unattended operation. This paper discusses very recent approaches towards security in CPSs.

1 Cyber-Physical Systems and their Security Challenges

Sensor nodes used in modern industrial automation, medical systems, critical infrastructure protection or smart grid systems do more than collecting and processing data locally. They forward their information to other nodes as well as to local or central monitoring systems and cooperate in a complex and distributed network. These systems consist of sensors, actuators, wireless and wired computing and communication devices. They link the real world to the cyber world, in most cases to the Internet, and are called a *Cyber-Physical System (CPS)*. A major benefit of CPS is that its parts can be connected and controlled from any place in the world, which helps to reduce cost, e.g. in the area of automation control systems. The combination of cyber and real world is the prerequisite for new applications, e.g. telemedical systems. The positive effects of CPS are unfortunately tightly coupled with serious security challenges. By using wireless connections and attaching small systems to the Internet, which have been run isolated in the past, formerly physically protected systems can be attacked from anywhere. In the following we will discuss new threats, present potential countermeasures and new research fields focused on low power as well as wireless sensor nodes as the most vulnerable part of CPSs.

1.1 Design Constraints of CPS applications

The design of sensor nodes for industrial automation systems is mainly driven by the cost factor, properitary protocols and availability, safety as well as dependability requirements.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4

By connecting these systems to the cyberspace the integration of security schemes becomes indispensable. Nevertheless, their classic limitation are still unchanged. For an acceptable form factor Printed Circuit Board (PCB) antennas will be used, which limits the range of the radio modules and complicates the implementation, so that it is embossed by properitary protocols and standards. In the last decade a migration to standardized ethernet-based protocols like Modbus-TCP, Profinet, EtherNet/IP or DNP3+TCP/UDP, was accomplished. But classic approaches for analyzing network traffic are still not suitable here. Common problems of low power applications and sensor networks like node's mobility, low duty cycling, self-organization, self-healing, multi-hop routing and supporting a large number of devices in a network are not covered by these approaches.

Although the minimization of electronic structures reduces the power consumption in a significant manner MCU's ultra low power capabilities are payed by a minimization of functionality. Therefore, complex mathematic functions as floating point units or multipliers are not implemented in hardware and a secure address space separation is not available. In addition to this the clock speed is often less than 20 MHz. Table 1 compares the processing power of a typical sensor node Micro Controller Unit (MCU), for example a MSP430, with classic and common desktop processors. The MSP430 is orders of magnitudes slower than an Intel Core i7. A 15 years old Pentium Pro processor is still 34 times faster. In addition to its poor computing power a MCU is equipped with few kilobytes of memory and up to 64 kB of non-volatile memory for static and dynamic program data, only.

Table 1: Performance, power consumption and efficiency as well as life time comparison of the MSP430 MCU versus classic and common desktop processors. The power source for the shown life-time is a standard battery cell with 1440 mAh.

Processor	Speed	MIPS	Power Consump. (Watt)	MIPS / Watt	Life-time (min)
Intel 386	33 MHz	11	2	6	54
MSP430	16 MHz	16	0.0009	17,778	12,000
Pentium Pro	200 MHz	547	34	16	3
Intel Core i7	3,200 MHz	76,383	130	587	0.82

Due to the fact that replacement and maintenance of sensor nodes in industrial automation systems are difficult and expensive the aimed life time of a battery powered node should be up to ten years. In contrast to the sensor node's low computing power its power efficiency is very high. As shown in Table 1 a MSP430 has an efficiency of 17 kMIPS/W, which is two orders of magnitudes higher than the one of a desktop CPU. A battery powered system can run continuously more than eight days with one cell with an capacity of 1440 mWh. For achieving the aimed life time low duty cycling is a key technique. The active periods will be as short as possible, while in the rest of the time the node runs in an ultra low power sleep mode. But low duty cycling causes new problems to solve. Changes of temperature, air pressure or electric supply voltage and oscillator aging cause variations of time sources. Thus, clocks of sensor nodes run at different speeds and the nodes may wake up out of time [BSL10].

ISBN 978-3-88579-286-4

1.2 Security threats in CPSs

The nature of the applications served by CPS leads to the fact that devices exposed to potential attackers physically and logically. This has an extremely strong impact on protection means. Physical accessibility immediately requires tamper resistant if not tamper proof devices in area in which we never have thought about such protection means and in which as already said cost is an important design factor. But in order to make CPS dependable at least a minimal physical protection is necessary in such a way that an attack or malicious users can not gain important information or that the effort is higher as the benefit. In unprotected devices the firmware and the sensitive data can be read with a minimal expertise and effort.

The wireless communication allows anybody to directly contact the devices. This means there is no way to force attackers to trick out a highly secure well managed IDS and firewall system at a well known entry point into the system to be protected. In particular protocols for low power applications like IEEE802.15.4 are not part of commercial Intrusion Detection System (IDS)s or firewalls. Wireless Sensor Node (WSN)s are vulnerable for wormhole and sybil attacks [YCT08], [NABT08]. The real-time constrains make the systems more frail for this kind of attacks. In order to provide a level of security similar to todays wired systems, complex protection means need to be integrated into the resource constraint wireless sensor nodes. Otherwise they need to be considered equivalent dangerous as unprotected ports in a wired system. We call the idea of empowering individual sensor nodes with complex protection means the Ubiquitous Line of Defense (ULoD). We are aware of the fact that the implementation of appropriate defense mechanisms is by far more difficult than for powered, wired systems. But we want to highlight that the risk resulting from unprotected or not properly protected CPS is significant. *Stuxnet* has impressively demonstrated that CPS have already been identified as a prime target for professional attackers. The worm was active in over 30 percent of all systems of the power supply sector, caused by the fact that all these systems use a central unit from one vendor. Ongoing efforts towards standardization of communication protocols, and SCADA systems will aggravate the security risk. It makes the design and accomplishment of an attack more attractive for a malicious user, since it can be run against more individual systems.

2 Ubiquitous line of defense

Individual subsystems of CPSs such as sensor nodes need to become self-protected i.e. the line of defense has to become part of the nodes themselves. Furthermore cooperation between individual systems is needed to provide kind of a global protection. We are considering the following aspects to be key when researching and building the ubiquitous line of defense:

1. design issues,
2. physical protection of sensor nodes,

3. sensor node integrity,
4. support of cryptographic operations as a basic means and
5. inspection of network traffic.

In Figure 1 we illustrate the idea of the ubiquitous line of defense, by showing protection walls indicating specific protection means around the individual systems. In the following subsections we will introduce different approaches for these domains.

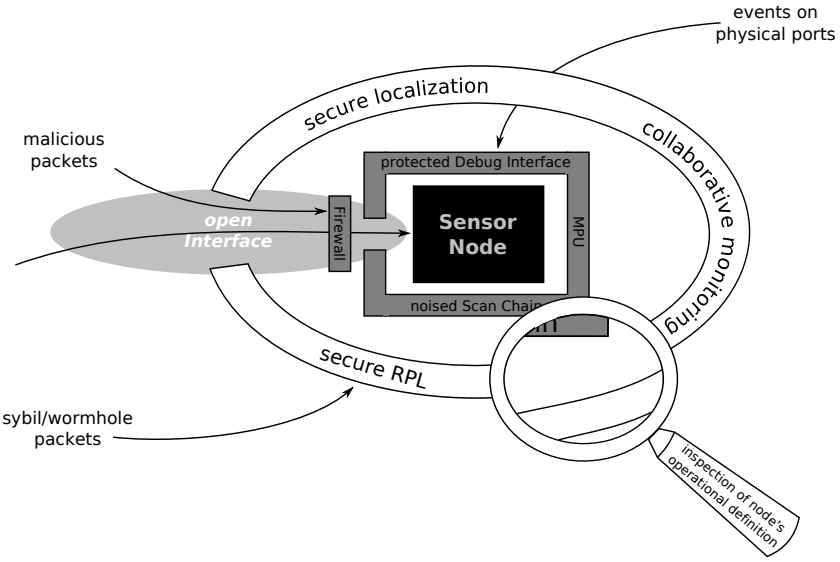

Figure 1: The ubiquitous line of defense of a CPS's sensor node must include various domains of security protection schemes.

2.1 Designing secure CPS

The span of CPS applications is very broad. In some areas real-time constraints and tight latency requirements are of utmost importance, whereas in process automation – even though somewhat belonging to the same class of applications – latency can be handled by far more relaxed. Also security goals may differ extremely. In some systems confidentiality is key to protect know how, whereas in other secrecy is negligible but integrity is key. In [PSL09] the idea of semi-automatic security design flow for industrial application scenarios was introduced. Such an approach is essentially needed when designing the ULoD since it needs to be adapted to the system under development.

ISBN 978-3-88579-286-4

2.2 Physical protection schemes

To increase the effort that an attacker has to invest the node's components can be sealed or the node itself can be placed at locations hard to reach. But these kind of approaches make maintenance more difficult or infeasible. Therefore, several interface protection and anti tamper mechanisms are invented in the last years. Sensor node's debugging interfaces can be protected by cryptographic authentication schemes in an energy neutral manner [SKB10] and chip scan chains can be disabled or noised after fabrication tests. Temperature, humidity, light as well as accelerator sensors can be used to detect environmental changes. But the main difficult of sensor-based anti tamper mechanisms is to determine suitable threshold values to differentiate between a normal condition change and an attacker action. Very often sensors have to be calibrated and tested in the final application scenario and threshold values are not usable for multiple nodes. This increases the cost for deploying and is currently a significant barrier for acceptance. All the approaches are merely embryonic and more research is needed in this area.

2.3 Cryptographic Operations

Due to the constrains of industrial applications in particular timing constrains of automation systems software based common symmetric and asymmetric cryptographic systems are not practical. To ensure integrity and confidentiality of services as well as meeting given timing requirements modified algorithms as described in [SPL10], [JEP11] can be used. Another option is to extend MCUs with hardware accelerators for cryptographic operations, which is a feasible solution from a cost as well as from an energy point of view [PLP08].

2.4 Node Integrity

The sensor node's operational definition includes its program code, measurement sources as well as its configuration data. For a dependable and secure operation of a CPS it must be ensured that this definition is unscathed all the time. Physical protection schemes can block physical attack but are ineffective in case of dynamic changes of the operational definition of a node, e.g. if the node was infected via wireless connection. Thus, for setting up a trustworthy and highly reliable sensor network it is essential that the node's operation definition is regularly tested. Here it is essential to differentiate between intentional attacks and system malfunction. While malfunction can be easily detected by using CRC sums, the detection of an attack is still infeasible. Code attestation by software-based methods in a successful manner is a non-trivial problem. In [CFPS09] it was shown that methods based on timing behavior examinations of the target device or on the lack of free memory to store malicious code [SPDK04], [YWZC07] can be broken. This clearly shows that the realization of pure software-based approaches is difficult and currently unsolved. Propos-

ISBN 978-3-88579-286-4

als with hardware support for code attestation are more effective and promising. But this requires specialized processor or MCU, so that an implementation with currently available components is impossible.

2.5 Network traffic and layout inspection

The behavior of a sensor node cannot only be influenced by malicious code but also by malicious data, e.g. bogus routing paths. This means that even though essentially needed code attestation is not sufficient to ensure proper node behavior. Thus, firewalls and IDS have to run on the node to be protected. But the missing of address spaces or privilege levels make an implementation of a physically separated demilitarized zone infeasible. Local errors or vulnerabilities will have a direct impact on the systems's availability, dependability and security. In other words even though these means are essential they are not yet the silver bullet, and need to be accompanied by additional means that help to keep impact of malicious packets minimal. First proposals for low power sensor node specific memory protection units - providing isolation on sensor nodes have been introduced in [FPC09] and [SLM11].

Even if a well functioning IDS is in place on individual sensor nodes, attacks build on malicious network information, such as wormhole and sybill attacks are still feasible. To counter such threats a firewall for packet inspection is needed. It can filter packets that stem from untrusted sources, could start verification means such as plausibility checks to validate a packet source. Such validation means will most probably require secure localization and/or secure time synchronization, which are currently also under research. Another means to empower firewalls to detect malicious packets is the use of secure protocols such as the recently proposed security extension of RPL [DHDB11]. But it requires to run cryptographic operations on the sensor node, which is a challenge concerning energy consumption if not supported by hardware. In order to reduce computational effort, the firewall can use information of malicious or at least suspicious nodes to filter out messages at the earliest point in time i.e. already when processing MAC and LLC headers [LPPL07].

3 Towards collaborative sensor network security framework

We assume that the protection of CPSs will be an important challenge in the next years. Several approaches were already presented but an ubiquitous and global protection that takes the broad requirements of industrial automation systems into account is not presented yet. We propose a framework that combines the node's security, a cooperative monitoring as well as system and security management for CPS.

A significant subset individual nodes of a CPS must be equipped with an attack detection unit, response capabilities and a self-protect module, where reduced functionality of a node and the real-time requirements have to be heeded. We assume that this is realizable

ISBN 978-3-88579-286-4

by focusing the security mechanisms on the node's data and activities. The standard approaches for detecting attacks - ongoing or completed - are based on detecting predefined attack signatures. Especially for small sensor nodes it seems to be infeasible to store a significantly large number of rules on an individual node. Various research results have shown that anomaly detection is extremely tricky and memory intensive in normal systems since expected behavior cannot be clearly predefined and learning approaches are very error prone. But especially in small systems in the area of industrial automation or critical infrastructure the behavior of a node is strictly predefined and regular - even more the behavior definition is the basis for setting up such systems. Exploiting features of this type of applications allows us to provide a clear definition of the expected system behavior in a small ruleset. By that any deviation can be considered an anomaly, which indicates that something goes wrong. Thus, we assume that an anomaly detection based on a node's behavior ruleset is feasible and more suiteable.

For detecting cross-node attacks a cooperative and distributed monitoring has to be implemented. Therefore, nodes will operate in a peer-to-peer overlay network with self-organization capabilities to be robust against non-predictable influences as well as malicious attacks. For setting up a reliable and distributed monitoring system of integrity trust among the nodes has to be established by using information security schemes.

To cope with the various security and safety requirements and broad constraints of CPSs a semi-automatic development flow is essential. Each security platform to install has to be adapted to the target environment. This includes the placement of sensors, the preparation of signatures and the definition of possible response and self-protection actions. All these activities should be combined in system and security management.

4 Conclusion

In this paper we sketched the security challenges of CPS and introduced the term Ubiquitous Line of Defense (ULoD), which denotes the fact that each individual node needs to be empowered to defend itself. The most important ingredients of the ULoD are tailor made IDSs and firewalls as well as reliable secure code attestation means. Cooperation between the individual nodes will help to significantly strengthen the security of the overall system. In addition we propose to research tools for supporting the realization of application specific ULoDs.

References

[BSL10] Marcin Brzozowski, Hendrik Salomon, and Peter Langendörfer. On Efficient Clock Drift Prediction Means and their Applicability to IEEE 802.15.4. *Embedded and Ubiquitous Computing, IEEE/IFIP International Conference on*, 2010.

[CFPS09] Claude Castelluccia, Aurélien Francillon, Daniele Perito, and Claudio Soriente. On the difficulty of software-based attestation of embedded devices. In *Proceedings of the*

ISBN 978-3-88579-286-4

16th ACM conference on Computer and communications security, CCS '09, New York, NY, USA, 2009. ACM.

[DHDB11] A. Dvir, T. Holczer, L. Dora, and L. Buttyan. Version Number Authentication and Local Key Agreement. Website, Januar 2011.

[FPC09] Aurélien Francillon, Daniele Perito, and Claude Castelluccia. Defending embedded systems against control flow attacks. In *SecuCode '09: Proceedings of the first ACM workshop on Secure execution of untrusted code*, New York, NY, USA, 2009. ACM.

[JEP11] Ke Jiang, Petru Eles, and Zebo Peng. Optimization of message encryption for distributed embedded systems with real-time constrains. In *Proceedings of the 14th IEEE Symposion on Design and Diagnostics of Electronic Circuits and Systems*, DDECS '11, Cottbus, Germany, April 2011.

[LPPL07] Peter Langendörfer, Krzysztof Piotrowski, Steffen Peter, and Martin Lehmann. Cross-layer firewall interaction as a means to provide effective and efficient protection at mobile devices. *Comput. Commun.*, 30, May 2007.

[NABT08] Farid Nait-Abdesselam, Brahim Bensaou, and Tarik Taleb. Detecting and avoiding wormhole attacks in wireless ad hoc networks. *Communications Magazine, IEEE*, 46(4), April 2008.

[PLP08] Steffen Peter, Peter Langendörfer, and Krzysztof Piotrowski. Public key cryptography empowered smart dust is affordable. *Int. J. Sen. Netw.*, 4, July 2008.

[PSL09] Steffen Peter, Oliver Stecklina, and Peter Langendoerfer. An engineering approach for secure and safe wireless sensor and actuator networks for industrial automation systems. In *Proceedings of the 14th IEEE international conference on Emerging technologies & factory automation*, ETFA'09, Piscataway, NJ, USA, 2009. IEEE Press.

[SKB10] Oliver Stecklina, Olaf Krause, and Thomas Basmer. Systemdesign einer sicheren und drahtlosen Debug-Schnittstelle für Sensorknoten unter Verwendung von RFID- und SoC-Technologien. In *Tagungsband 12. Wireless Technologies Kongress*, Bochum, Germany, September 2010.

[SLM11] Oliver Stecklina, Peter Langendörfer, and Hannes Menzel. Towards a Secure Address Space Separation for Low Power Sensor Nodes. In *In Proceedings of the 1st International Conference on Pervasive and Embedded Computing and Communication Systems*, PECCS'11, Algarve, Portugal, March 2011.

[SPDK04] Arvind Seshadri, Adrian Perrig, Leendert Van Doorn, and Pradeep Khosla. SWATT: SoftWare-based ATTestation for Embedded Devices. In *In Proceedings of the IEEE Symposium on Security and Privacy*, 2004.

[SPL10] Anna Sojka, Krzysztof Piotrowski, and Peter Langendörfer. Short ECC - A Lightweight Security Approach for Wireless Sensor Networks. In *Proceedings of the International Conference on Security and Cryptography*, SECRYPT '10, Athens, Greece, July 2010. SciTePress.

[YCT08] Jie Yang, Yingying Chen, and Wade Trappe. Detecting Sybil Attacks in Wireless and Sensor Networks Using Cluster Analysis. *4th IEEE International Workshop on Wireless and Sensor Networks Security IEEE WSNS 2008*, 2008.

[YWZC07] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao. Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks. In *Proceedings of the 26th IEEE International Symposium on Reliable Distributed Systems*, SRDS '07, Washington, DC, USA, 2007. IEEE Computer Society.

ISBN 978-3-88579-286-4