Myndigheten för samhällsskydd och beredskap

FAKTA

OKTOBER 2018

FORSKNINGSPROJEKT FINANSIERAT AV MSB

Infrastrukturer skyddas från cyberhot

Samhällets kritiska infrastrukturer, som elnät och andra distributionsnät, övervakas och regleras med hjälp av så kallade industriella informations- och styrsystem (ICS). Om dess komponenter utsätts för cyberattacker riskerar det att leda till stora samhällsstörningar. Forskare vid KTH har under tre år arbetat med att identifiera sårbarheter och utveckla nya säkra lösningar.

Ett allt mer oroande hot är att storskaliga övervaknings- och reglersystem utsätts för cyberattacker. I värsta fall kan det leda till att kritisk infrastruktur fallerar med stora samhällsskador som följd. Inom projektet CERCES studeras och motverkas sådana hot. Projektet har löpt tre år och här redovisas några delresultat från projektets fyra olika huvudspår.

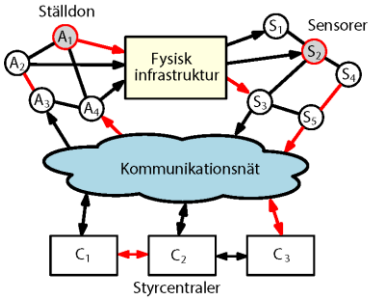
(A1) Säkerhet i inbyggda system
Forskarna har utvecklat nya verktyg för att automatiskt verifiera att mjukvara i inbyggda processorer exekverar korrekt och säkert. Verktygen, baserade på formell logik, kan i verifikationsprocessen också upptäcka nya sårbarheter, såsom tidigare okända informationsläckage via processorstacken.

(A2) Trådlös kommunikation
Forskarna har studerat nya typer av säkerhetslösningar för trådlös kommunikation mellan t.ex. sensorer och regulatorer. Tillgängliga lösningar baseras på kryptografi, men dessa kan i praktiken vara svåra att underhålla i ett ICS. Istället tittar forskarna på metoder som utnyttjar komponenters unika fysikaliska signatur för att verifieria att kommunikationen är autentisk.

(A3) Kommunikations- och beräkningsinfrastrukturer
Forskarna har utvecklat nya säkra algoritmer och protokoll för beräkning i, och kommunikation över, delade infrastrukturer som t.ex. molntjänster. Nya typer av angrepp mot, och försvar av, tidssynkroniseringsprotokoll har identifierats, med tillämpning inom t.ex. synkronmätningar i elnät. Vidare har resilient allokering av s.k. virtuella regulatorer för processstyrning studerats.

(A4) Resilent reglering av cyberfysiska system
Forskarna har utvecklat nya metoder för att effektivt lokalisera särskilt sårbara komponenter och kanaler i ett ICS (se figur ovan till höger). Komponenter anses vara känsliga om de vid ett angrepp kan resultera i stor fysisk skada. Vidare har metoder för kostnadseffektiv allokering av försvarsmekaniskmer och design av anomalidetektorer tagits fram.

Bilaga: Informationsblad för forskningsområde A1-A4 (på engelska).



Ett ICS för övervakning och styrning av kritisk infrastruktur kan ha många komponenter och kommunikationskanaler som är känsliga för angrepp (indikerade i rött). I CERCES utvecklas nya metoder för identifiera och skydda sådana känsliga systemelement.

Projekttitel
CERCES – Center för resilienta kritiska infrastrukturer

Projektperiod
September 2015 – Augusti 2020

Projektorganisation
Professor Mads Dam
(områdesansvarig A1)
Avd. för teoretisk datalogi, KTH
mfd@kth.se

Docent Ragnar Thobaben
(områdesansvarig A2)
Avd. för teknisk informationsvetenskap, KTH
ragnart@kth.se

Professor György Dán
(områdesansvarig A3)
Avd. för nätverk och systemteknik, KTH
gyuri@kth.se

Professor Henrik Sandberg
(projekt- och områdesansvarig A4)
Avd. för reglerteknik, KTH
hsan@kth.se

Svårbegripliga ord
ICS (Industrial control system): System för övervakning och reglering av industriella processer.

Resilient system: Ett system som har förmåga att stå emot eller återhämta sig efter stora störningar.

MSB-89.5

A1: Secure Embedded Software Platforms

Embedded software systems, controllers and actuators form the backbone of all societal critical infrastructure such as the power network, transportation, communication networks, etc. The security of these control networks relies heavily on the security of their underlying execution platforms and their sub-components. This reliance is greatly challenged by recent incidents and vulnerabilities such as Stuxnet, Rowhammer, Spectre, Meltdown and Foreshadow. In CERCES activity A1 "Highly trustworthy execution platforms", we work on formal modelling and verification to develop new generations of execution platforms for embedded systems and controllers with radically improved security guarantees applicable for critical infrastructure.

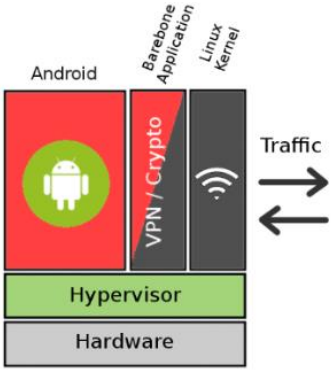


Figure 1

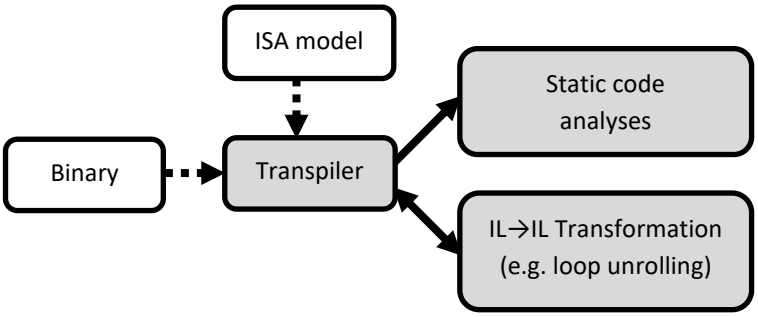


Figure 2

In our research, we are working towards demonstrators (e.g. Figure 1) for high assurance platforms and analysis tools (e.g. Figure 2) to achieve high assurance by providing computer checkable proofs.

Formal analysis of the HASPOC ARMv8 secure hypervisor

The HASPOC ARMv8 secure hypervisor was developed with SICS/RiSE, Ericsson, Tutus Data, T2Data, Atsec, and Sectra in the Vinnova funded project "High Assurance Security Products On COTS platforms" [1], see Figure 1 for an instantiation for red/black separation developed with Tutus Data. Within CERCES, we have worked on the modelling and verification of the HASPOC hypervisor. One notable result is a highly detailed case study [2] on the formal model and security analysis of virtualized interrupt processing in the ARMv8 based HiKey platform.

Tools for binary code analysis

A difficulty with modelling and verification at low level is the high churn of devices and variability of processor architectures. To address this, we are developing a tool framework, integrated with the HOL4 theorem prover, to provide an architecture-independent code analysis format (intermediate language IL) similar to LLVM (Figure 2).

Models and provable countermeasures against hardware level vulnerabilities

Over the recent years a number of microarchitectural vulnerabilities such as Spectre, Meltdown, etc. have emerged, which challenge the soundness of formal analyses performed at the Instruction Set Architecture (ISA) level. To address this, more fine-grained models are needed. Within CERCES we have started examining this type of complication and showed [3] how formal integrity can be reestablished in the presence of a certain type of cache misconfiguration attack identified earlier in the project.

Future Work

The key challenge is scalability and currently only small binary code fragments can be analyzed. At the same time, hardware platform models quickly become unwieldy and their relation to the real-world systems unclear. To overcome these problems, we are investigating new ways of automating the security analyses, including the use of modular techniques.

[1] HASPOC: *High Assurance Security Products On COTS platforms*. https://haspoc.sics.se. 2018.

[2] C. Baumann, O. Schwarz, M. Dam. Compositional Verification of Security Properties for Embedded Execution Platforms. *6th International Workshop on Security Proofs for Embedded Systems*. 2017.

[3] M. Dam. Formal Verification of Integrity-Preserving Countermeasures Against Cache Storage Side-Channels. *Principles of Security and Trust: 7th International Conference*. 2018.

A2: Wireless Communication

Wirelessly connected critical infrastructures pave the way for many new interesting and beneficial societal applications such as wireless sensing and actuation at remote locations, interconnected vehicles and road infrastructure, and wirelessly automated industries. However, communications through the open wireless medium immediately exposes systems to new types of attacks. Traditional security techniques based on cryptography are one approach to protect these systems. However, with improvements in computing power it is expected that today's cryptographic protocols might be broken in the future, not the least with the dawn of quantum computers. Furthermore, delay, reliability, and availability requirements on communications in cyber-physical systems that operate without humans in the loop differ in many ways from traditional human-oriented communications. For these reasons, we are in CERCES interested in studying and developing new reliable alternatives and complements for cryptographic security in wireless systems used for cyber-physical applications.

Physical Layer Authentication

Physical layer authentication has attracted a lot of attention recently. It is a technique for verifying that messages are coming from legitimate sources by utilizing the fact that the wireless channel and hardware possesses transmitter-specific properties that can be used for identifications. As part of the CERCES project, we have developed and investigated a new algorithm for physical layer authentication in multi-carrier systems with time varying channel conditions [1]. One issue of these protocols are rare but inevitable errors (i.e., false alarms and missed detections) that occur in physical layer authentication protocols and might have unintended consequences on communication delays. However, our results in [2] indicate that physical layer authentication can achieve appropriately low delays under certain conditions, and hence, it appears to be an appropriate low-complexity, low-latency authentication technique at the physical layer for delay sensitive applications, which can be used standalone or to complement existing security features.

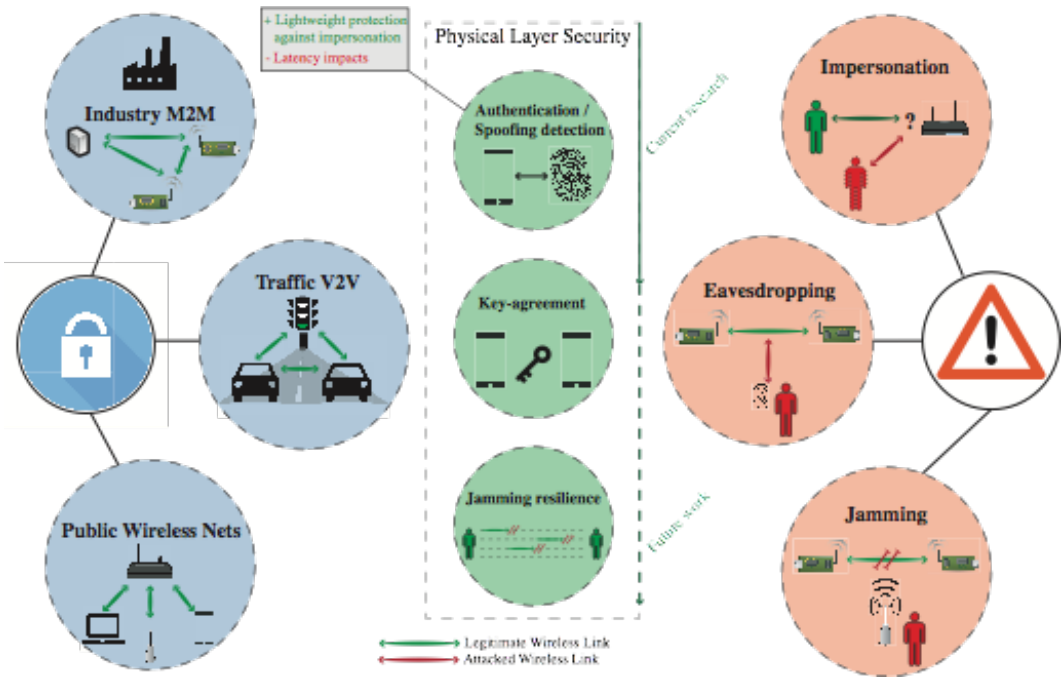
Future Research

Many theoretical and practical problems remain to be solved in order to utilize the benefits of physical layer security techniques in practice. In the future, we will study other techniques for physical layer authentication, in particular focusing on delay sensitive applications. Furthermore, we will approach physical layer security topics like key-agreement and jamming resilience and investigate their use for security in the context of wireless critical infrastructures.

[1] H. Forssell, R. Thobaben, J. Gross and M. Skoglund, "Feature-based multi-user authentication for parallel uplink transmissions,"*International Symposium on Turbo Codes and Iterative Information Processing (ISTC)*, Brest, 2016, pp. 355-359.

[2] H. Forssell, R. Thobaben, H. Al-Zubaidy, and J. Gross, "On the impact of feature-based physical layer authentication on
network delay performance," in IEEE Global Communications Conference, Dec 2017, pp. 1–6.

Figure: Critical wireless communication scenarios (left), potential threats (right) and three PHY-layer techniques studied in CERCES-A2 (center) .



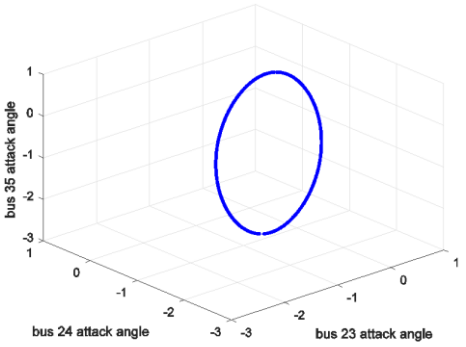
A3: Communication and Computation Infrastructures

CERCES is developing secure and resilient algorithms and protocols for communication and computation in critical infrastructures in shared environments. In this area we focus on:

- End-to-end security for time synchronization, with a specific focus on its use for Phasor measurement units (PMUs) in power grids.
- Resilient computation in process control. We develop algorithms for placement and migration of controllers in process control for resilient computation.

Secure Time Synchronization

Precise time synchronization between devices in the smart grid is a key requirement for secure and efficient operation. However, time synchronization sources, both space based (e.g. GPS) and network based (e.g. PTPv2), are known to have vulnerabilities that could be used for compromising time synchronization, with potentially severe consequences. Therefore, CERCES is investigating the security of time synchronization in power grids, with a focus on synchro-phasor measurements taken by PMUs. We have showed that it is possible to mount successful time synchronization attacks on PMUs that would bypass state-of-the-art detection techniques, such as PMU based linear state estimation and associated statistical bad data detection, while inflicting serious damage to grid stability.



A figure illustrating the feasible region of the attack angles (attack magnitudes) that need to be implemented in order to mount an undetectable time synchronization attack, manipulating the time references of three current measuring PMUs on three buses in the IEEE 39-bus benchmark network. The feasible region is a continuum allowing the attacker to choose an attack with maximum impact.

Resilient Computation

To reduce equipment cost for process control systems, hardware controllers can be replaced by low-cost and flexible software controllers, referred to as Virtual Process Control Functions (VPFs). VPFs can be placed and executed on commodity hardware, e.g., in emerging Mobile Edge Clouds. In CERCES we have addressed the problem of resilient placement of VPFs with the objective of minimizing the operational cost, and guaranteeing the availability of the VPFs under cyber attacks and failures. We developed a resilient VPF placement (RVP) algorithm based on Benders decomposition and linear relaxation. The proposed RVP algorithm reduces the operational cost significantly compared to reference algorithms. Furthermore, to dynamically adapt to the cyber attacks and failures, we addressed the problem of scheduling VPF migration with the objective of maximizing service availability, subject to a migration deadline. We developed a solution to generate migration schedules by building and decomposing dependency graphs. Our results show that our solution is computationally efficient and outperforms the state-of-art Wedelin heuristic for solving binary programming problems.

Future Work

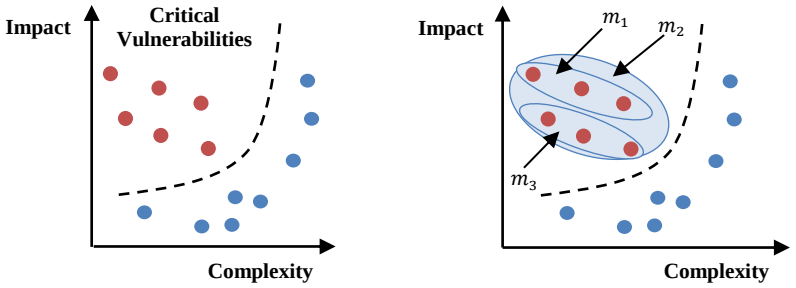
We plan to develop countermeasures for time synchronization attacks, including mitigation schemes that make it significantly harder or impossible to implement an attack, and detection techniques based on state of the art machine learning algorithms. For resilient computing, we plan to refine our models of computing and communication constraints and to include models of the physical processes in the considered problems.

[1] S. B. Andrade, J. Le Boudec, E. Shereen, G. Dán, M. Pignati and M. Paolone, "A continuum of undetectable timing-attacks on PMU-based linear state-estimation," *IEEE Intl. Conf. on Smart Grid Communications (SmartGridComm)*, Dresden, 2017, pp. 473-479.

[2] Peiyue Zhao, György Dán, "Time Constrained Service-aware Migration of Virtualized Services for Mobile Edge Computing," in Proc. of International Teletraffic Congress (ITC), Sep. 2018

A4: Resilient Control of Cyber-Physical Systems

Securing industrial control systems (ICSs) is challenging because of two reasons. Firstly, it is known that many security vulnerabilities can be found in ICSs. For instance, communication protocols commonly used in ICSs are often lacking basic security features, or the local area network in the control center may be connected to the Internet without adequate protection. Secondly, deployment of security measures in an ICS is costly. For example, due to the long life span of ICSs, support for some of the equipment found within ICSs may not exist anymore. Moreover, stopping an ICS can be expensive and complicated due to their real-time requirements. Therefore, preventing all of the vulnerabilities at once may impossible due to a limited budget. For this reason, in CERCES A4, we are interested in developing tools for finding the most dangerous vulnerabilities within the system, and preventing these critical vulnerabilities in a cost-efficient manner.



(a) (b)

Figure. In our research, we are interested in providing tools for: (a) finding the most critical vulnerabilities within the system (red dots in the figure); (b) finding a cost-efficient way to prevent these vulnerabilities by selecting the best combination of security measures (illustrated with m_1-m_3).

Cost-efficient Protection of ICSs

In [1], we have developed a modeling framework for finding critical vulnerabilities within the system. For this purpose, we use a physical model of the system to simulate impact of different attack strategies once the vulnerabilities are exploited. For each attack strategy, the *exact* value of the impact can be found *efficiently* using our framework. Once the high-risk vulnerabilities are determined, we tackle the problem of preventing these vulnerabilities in a cost efficient manner. This problem is combinatorial in nature, which means that once the number of security measures is large, the optimal solution is difficult to obtain in reasonable time. However, in [2], we show that the approximate solution to this problem with guarantees on performance can be found efficiently, using well-established algorithms.

Future Work

In the future, we plan to address the problem of analyzing and protecting very large scale ICSs such as power grids or water distribution networks. In the literature, a so-called security index was proposed for this purpose. In our work, we aim to extend this index to more realistic system models, make it more robust to modeling errors, and find an efficient way to calculate the index once the number of control components (sensors and actuators) in the system is very large.

[1] J. Milošević, D. Umsonst, H. Sandberg, K.H. Johansson, "Quantifying the Impact of Cyber-Attack Strategies for Control Systems Equipped with an Anomaly Detector," *European Control Conference, 2018*. **To appear.**

[2] J. Milošević, A. Teixeira, T. Tanaka, H. Sandberg, K.H. Johansson, "Security Measure Allocation for Industrial Control Systems: Exploiting Systematic Search Techniques and Submodularity," *International Journal of Robust and Nonlinear Control*. **To appear.**