CERCES

CEnter for Resilient Critical infrastructurES

Mads Dam György Dán Henrik Sandberg Ragnar Thobaben
Andreas Lindner Jezdimir Milosevic Henrik Forssell

ACCESS Linnaeus Centre
KTH Royal Institute of Technology

Introduction

Cyber attacks and malfunctioning IT systems in critical infrastructures such as power networks, water supply systems and traffic systems, pose a serious threat on public health and safety. In response to this growing threat, the MSB (Swedish Civil Contingencies Agency) funded the Center for Resilient Critical Infrastructures (CERCES) project with the goal to improve the resilience of critical infrastructures. The project team consists of four research groups at the School of Electrical Engineering and at the School of Computer Science and Communication at KTH, all belonging to the ACCESS Linnaeus Centre. Each group will be working on one area vital for the critical infrastructure security, namely:

- A1: Highly Trustworthy Execution Platforms
- A2: Wireless Communication
- A3: Resilient Communication and Computing Infrastructures
- A4: Resilient Control of Cyber-Physical Systems

An illustration of the components of a critical infrastucture control system and how the project activities relate to them can be seen in Figure 1.

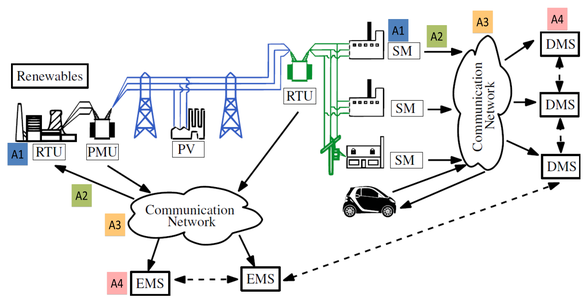

Figure 1: Illustration of a control system in a critical infranstructure.

The objective of CERCES is to develop algorithms, protocols and tools for the prevention, detection and mitigation of cyber attacks on industrial control system components and infrastructures. Emphasis will be given on SCADA systems (Supervisory Control and Data Acquisition systems). CERCES will also develop a testbed that will consist of wireless sensors, embedded computing devices and a virtualized control environment. The testbed will be used for the experimental validation of the algorithms and solutions developed and for demonstration of the results to industrial partners.

A1: Highly Trustworthy Execution Platforms

Using complex software stacks in critical infrastructure applications exposes them to potential faults and attacks. Therefore, fault contention and isolation among software components could be enforced by utilizing a provably correct hypervisor providing virtualization abstraction, see Figure 2.

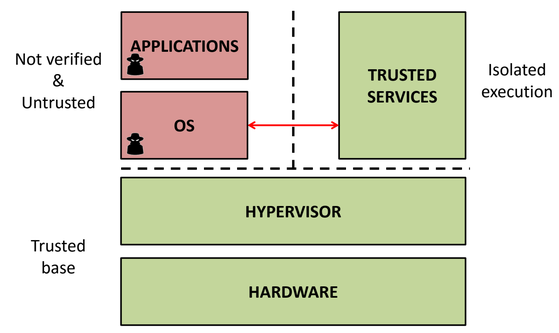

Figure 2: Isolated execution of trusted services.

Our focus lies on the exploration of virtualization-based techniques in terms of:

- demands of current and future SCADA/critical infrastructure platforms
- industry requirements concerning functionality, real-time performance, and cost
- transfer of know-how, designs and code

A2: Wireless Communication

Motivated by the benefits of wireless deployments, organizations are starting to replace parts of the SCADA infrastructure by wireless technologies. With this change, wireless security becomes a key issue for future SCADA system infrastructures.

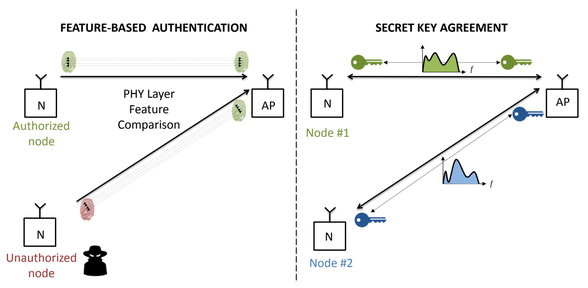

Figure 3: Illustration of feature based authentication and secret key agreement.

In this activity, our goal is to demonstrate that physical-layer security techniques that exploit the randomness of the wireless transmission medium to improve resilience against various types of attacks in the wireless domain, are a powerful means to complement conventional security features of wireless SCADA system infrastructures. See Figure 3 for illustration of two considered techniques. Focus will be on three aspects of physical layer security:

- Physical-layer authentication (feature- and tag-based)
- Secret key generation and distribution
- Jamming resilient wireless infrastructures.

A3: Resilient Communication and Computing Infrastructures

Current SCADA communication protocols, and security architectures pose several shortcomings and vulnerabilities. An overview of the threats covered by CERCES activity A3 can be seen in Figure 4.

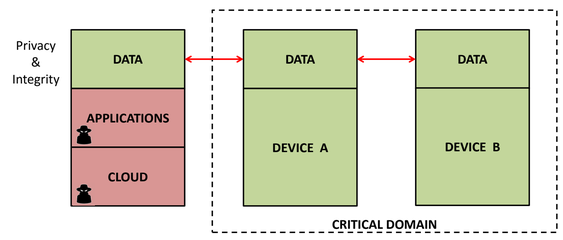

Figure 4: Threats to communication and computing.

In this activity, we develop secure and resilient algorithms and protocols for SCADA communication and computation in shared environments. We will focus on three areas:

- Secure communication protocols emerging SCADA application scenarios
- Resilience to denial of service attacks
- We secure computation on untrusted computing platforms

A4: Resilient Control of Cyber-Physical Systems

The closed-loop nature of control systems makes them particularly vulnerable since attacks can target any point in the loop, and yet result in harmful physical actuation on the controlled infrastructure, see Figure 5. Therefore, the main goal of this activity is development of control and monitoring algorithms which ensure resilient operation of critical infrastructures.

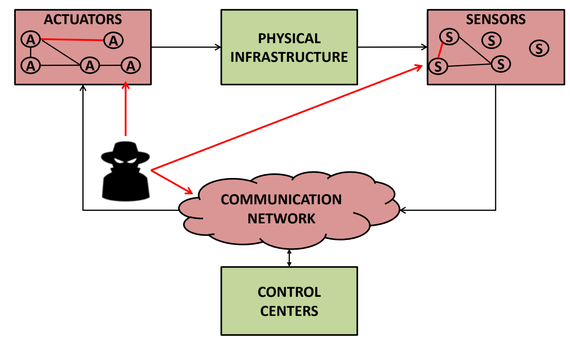

Figure 5: Cyber-physical system under attack.

To achieve this, models that capture the essential behavior of cyber and physical components first need to be developed. Vulnerability and impact analysis will be conducted on these models, which further enable us to identify critical areas in the infrastructure, and then to design application layer intrusion detection systems. These systems will be incorporated in novel resilient control architectures, which will serve to encapsulate and attenuate malicious actions.