Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Networking

Author(s): Elisa Costante (SM)

CC RG-22 - Improving integrity and confidentiality of heterogeneous utilities networks.
CC RG-23 and CT RG-23 – Improve trade-off between protocols security and latency.
CC RG-27 – Improve efficiency and security of communication protocols for wide area power systems.

ABSTRACT

The clear advantages in terms of cost reduction and efficiency gain that is offered by the adoption of new technologies such as the Internet of Things (IoT) and smart grids, is pushing many systems (including utilities) to move from closed environment to open IP-based communication networks. This trend opens up a new range of risks to data integrity and confidentiality that can be compromised by network attacks such as data injection, man-in-the-middle, spoofing, impersonation, or denial of service. Therefore, it is important to improve the security of communication networks such as those in use in systems such as utilities, smart grids and power systems and Advanced Metering Infrastructure (AMI).

RESEARCH ACTION #1

Monitoring and intrusions detection systems to identify network intrusions that can undermine data integrity (e.g. corrupt operational data with traffic injection) or confidentiality (e.g. with a man-in-the-middle attack).

DISTANCE TO THE MARKET: **TRL 5**
COST OF THE TOPIC: **3 STREPs + 0 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **Industry, Critical Infrastructures, Research Institute**

Monitoring and intrusion detection systems can identify intrusions and signs of possibly compromised devices before the threats they pose to utilities and critical infrastructure materialize, thus minimizing their negative consequences. In particular, it is important to design novel network intrusion detection technologies that, aware of the specific communication protocols adopted and aware of the possibly limited access to the data due to cryptographic schemes or legislation, can still be effective in detecting increasingly complex attacks. Specifically, monitoring solutions for critical infrastructures should meet the following requirements:

- Pose a minimal impact on utilities network that typically have limited resources.
- Capabilities of detecting new emerging complex targeted attacks.
- Capabilities of performing monitoring and detection even in the presence of encryption schemes.

RESEARCH ACTION #2

Protocols for utilities, smart grids and Advanced Metering Infrastructures (AMI) with embedded support for encryption, security, authentication and scalability

DISTANCE TO THE MARKET: **TRL 5**
COST OF THE TOPIC: **3 STREPs + 0 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **Industry, Standardization Body, Research Institute**

Industrial Control Systems (ICS) are typically used to regulate industrial processes (e.g. in utilities). ICS are exposed to the same security vulnerabilities associated with enterprise networks. To overcome these risks, cryptography can be used; however, applying cryptographic algorithms to ICS environment introduces communication latency that violates operational requirements. Thus, it is important to improve existing cryptography techniques (or device innovative methodology) that can support encryption by respecting real time constraints. Recently, IETF has standardized RPL (routing protocol for low power networks), which is expected to be the standard routing protocol for the majority of applications including advanced metering infrastructure (AMI) networks. Although the RPL protocol provides optimal routing performance, it does have numerous security flaws that should be addressed prior to its use in critical infrastructure. Especially, it is important that protocols in use in critical infrastructure exhibit the following features:

- Being robust to complex attacks aimed at disrupting functional operations or violating data integrity.
- Support encryption and authentication with a reduced latency, so that operational time constraints posed by critical environments can still be respected.

RESEARCH ACTION #3

Innovative solutions to guarantee data integrity without relying on encryption.

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **3 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **60 months**
ACTORS: **Industry, Research Institute**

Typically, encryption is adopted to guarantee data integrity. However, in critical environments, the extra latency required by cryptography techniques often makes it impossible to respect operational time constraints. This may lead to a situation where encryption cannot be adopted at all. To solve this issue, it is important to devise innovative techniques capable of data integrity verification without relying on encryption. For instance, an alternative to encryption could be to check data integrity by verifying that data is in line with process status and sensors' measurements.