PREEMPTIVE

PREventivE Methodology and Tools to protect utilitIEs

Alessia Valentini
System Engineer & Business Developer
Vitrociset S.p.a.
Rome
a.valentini@vitrociset.it

Giorgio Sinibaldi
Project Manager
Vitrociset S.p.a.
Rome
g.sinibaldi@vitrociset.it

***Abstract*—This paper discuss the PREEMPTIVE research, an Fp7 project to provide an innovative solution for existing procedures enhancement, risk methods optimization and tools suitable to operate in prevention activity against cyber-attacks targeted on industrial networks and automated control systems of utility companies.**

Keywords—Cyber security, scada protection, Risk analysis.

I. INTRODUCTION

In recent years, we have witnessed an increase in the number and impact of cyber-attacks against industrial control networks. A successful attack might affect, or even endanger, daily human activities. Multiple and diverse countermeasures have been put in place to prevent Advanced Persistent Threat (APT) attacks, but they failed, allowing the latest generation of APT. PREEMPTIVE addresses, prevention of cyber-attacks against hardware and software systems such as DCS, SCADA, PLC, networked electronic sensing, and monitoring and diagnostic systems used by the utilities networks. Moreover, the research aims to implement detection tools based on a dual approach comprising low direct detection (e.g. network traffic and system calls) and process misbehavior detection (e.g. automatic industrial processes to control water distribution). The work is based on electricity, water and gas utilities.

II. MAIN GOALS

PREEMPTIVE aims to:

A. Enhance existing methodological security and prevention frameworks with the aim of harmonizing Risk and Vulnerability Assessment methods, standard policies, procedures and applicable regulations or recommendations to prevent cyber-attacks.

B. Design and develop prevention and detection tools complaint to the dual approach that takes into account both the industrial process misbehavior analysis (physical domain) and the communication & software anomalies (cyber domain):

1. Industrial process misbehavior detection tools.
2. communication & software related threats prevention and detection tools.

C. Define a taxonomy for classifying the utilities networks taking into account:

1. The utility network type and communication technology used
2. The utility network exposure to Cyber threats
3. The impact to the citizens of services disruption caused by a cyber-attack through the utility network.

D. Define guidelines for improving Critical Infrastructure (CI) surveillance.

E. Validate the PREEMPTIVE framework and innovative technologies in real scenarios with the support of the utility companies involved.

Utility companies will take advantage of PREEMPTIVE results to demonstrate compliance with high-level security requirements that originate from mandates, standards, and guidelines.

III. PREEMPTIVE MAIN OUTCOMES

A. **Taxonomy – report:** classifying the utility networks taking into account type and communication technology, sensibility to Cyber threats

B. **Modelling – software:** models and virtual environment for simulating and gathering data on cyber attacks

C. **Software detection (network, host and process based) and event correlation tools - software:** prevention and detection tools to improves security on SCADA utility networks.

D. **Cyber Defence Methodology Framework – guidelines:** Risk and Vulnerability Assessment methods and standard policies, procedures and guidelines to prevent cyber attacks.

E. **Privacy and Data Protection – guidelines:** Legal and Ethical aspects and impact of Preemptive

Taxonomy

The objective of Taxonomy is to gain a comprehensive understanding of the utility operational technology infrastructure to be protected. A taxonomy has been defined to structure the collected information in a consistent way across different utility sectors focusing on three sectors: electricity, gas and water

For each domain some critical processes has been considered:

- electricity (generation, transmission, distribution and distributed energy resources),
- gas (production, storage, transmission and distribution)
- water (drinking water treatment, waste water treatment and water distribution).

- metering cross-sector domain that includes the common end-user metering infrastructure for electricity, gas and water.

Knowledge has been organized by different types of utilities in order to provide a reference for assessing and studying their cyber-security properties. In particular, taxonomy should capture the types and characteristics of industrial processes, the different systems used to control such processes, the use cases implemented by the systems, and the devices and network communication protocols used by these systems. Taxonomy then describe the cyber-security-related properties of all these components in such a way that cyber-attack scenarios can be built for different types of utilities, and that different security solutions can be evaluated according to the applicability and coverage they offer with regards to the technology in use at different utilities.

Results of our analysis indicate that different domains share common vulnerabilities, which could be exploited by attackers. Despite the heterogeneous nature of utility networks, there are common components and protocols across the different domains. These components and protocols share similar vulnerabilities, which could allow resourceful and motivated attackers to subvert critical parts of the physical processes run by utilities. These common vulnerabilities include:

- Poor networking stack implementations make components vulnerable to denial of service and buffer overflow attacks.
- Components exposing interfaces (with default or no credentials required) that allow reconfiguring or taking control of process automation functionalities.
- Protocols do not define authentication or message integrity features, allowing attackers with network access to manipulate process control information

High-impact attacks are possible in all domains. In each of the domains taken into account there we identify use cases (functionalities) that (a) could be disabled by a cyber-attack and (b) whose disruption would have a high impact on society.

Modelling–software

To understand consequences of cyber-attack in different components and elements of the networks and to support the testing and validation of the detection tools to develop, a simulation tool has been developed because represent a safe approach to test the effectiveness of detection tools that does not require actual deployment into the operational environment; hence it reduces the associated costs as well as the risks of potential loss of service, achieving two main goals:

- produce synthetic datasets of typical behavior in different domains that can be used by detection tool to gain insight about typical processes and important variables
- verify the effectiveness of the detection tools developed to detect attacks that attempt to disrupt Industrial Control Systems

The virtual environments are composed of virtual images of basic components (work stations, servers, HMIs, SCADA/DCS servers and PLCs) that can be easily distributed to partners. We also provide realistic malware samples that attack Industrial Control networks from different entry points (both at system and process level). The environment constitute a useful toolkit for verify the effectiveness of the PREEMPTIVE tools against complex attack conditions and threats.

Software detection (network, host and process based) and event correlation tools-software

This Software is composed by 3 main components:

A. **The detection tools** which check *network traffic* (payload and flow), *host* (PLC and workstation) ,*process state* of the SCADA system. One detection tool makes *vulnerability assessment* of the whole network to automatically detect hosts main information (IP address, Operating System, version, open sockets…) and related vulnerabilities. These detection tools are independent each other and generate alarm/warnings in case of anomalous situation like a wrong packet, an anomalous traffic flow, an abnormal state of process… All these information are sent to central Database by secure SSL connection

B. **A correlation engine** which correlates all alarm/warning generated by the different detection tools. An historical detection and prediction tool analyzes all the events to check possible attacks and APT which could not be detected by a single tool. The process send also the events with high severity value to the graphical interface

C. **A graphical interface** where operator have a global view of all elements and in case of a warning/alarm the affected element is highlighted and operator may check information about the event

Cyber Defence Methodology Framework

A methodology framework is a catalogues of countermeasures, which may be organizational or technical.

- Organizational countermeasures are best practices related to the organization of work flows and the distribution of responsibilities
- Technical countermeasures are related to the deployment of devices and software components and their appropriate configuration and settings

In order to reach this target, we evaluate the state of the art within this field. Based on that, we look for gaps that could be filled up with the new methodology.

The final result is the development of a Risk Assessment methodology including Asset Identification, Threat Characterization and Vulnerability Assessment for securing utility networks from cyber-attacks

Privacy and Data Protection

Guidance is provided concerning the practical implementation of the legal requirements identified. The implementation guidelines cover key legal areas such as, critical infrastructure protection and security, privacy and data protection. The guidelines aim to assist project partners during the development of the PREEMPTIVE tools, as well as end-users in their implementation of the tools into the production environment.