INDUSTRIAL DEVICES ROBUSTNESS ASSESSMENT AND TESTING AGAINST CYBER SECURITY ATTACKS

F. Tilaro, B. Copy (CERN, Geneva, Switzerland)

ABSTRACT

CERN (European Organization for Nuclear Research),like any organization, needs to achieve the conflicting objectives of connecting its operational network to Internet while at the same time keeping its industrial control systems secure from external and internal cyber attacks. With this in mind, the ISA-99 international cyber security standard has been adopted at CERN as a reference model to define a set of guidelines and security robustness criteria applicable to any network device. Devices robustness represents a key link in the defense-in-depth concept as some attacks will inevitably penetrate security boundaries and thus require further protection measures. When assessing the cyber security robustness of devices we have singled out control system-relevant attack patterns derived from the well-known CAPEC classification. Once a vulnerability is identified, it needs to be documented, prioritized and reproduced at will in a dedicated test environment for debugging purposes. CERN - in collaboration with SIEMENS - has designed and implemented a dedicated working environment, the Test-bench for Robustness of Industrial Equipments ("TRoIE"). Such tests attempt to detect possible anomalies by exploiting corrupt communication channels and manipulating the normal behavior of the communication protocols, in the same way as a cyber attacker would proceed. This document provides an inventory of security guidelines relevant to the CERN industrial environment and describes how we have automated the collection and classification of identified vulnerabilities into a test-bench..

Industrial plants under risk

Industrial disasters are uniquely a human creation, which have started appearing since the beginning of the industrial revolution. Many of them were avoidable because caused by careless disregard for safety, but sometimes unforeseen and accidental. Industrial accidents have always been followed by different types of major impacts in terms of environmental damage, health condition and economic loss. As far as cyber security is concerned, it is essential to develop a strategy and methodology to secure any process control system (PCS) from internal or external cyber attacks. Although PCSs are now frequently based on standard IT technologies, their operational environments differ significantly from the generic IT environment; sometimes IT standard security measures result completely inappropriate or even not available for use in a control environment. So it is necessary to adapt and tailor the IT standard security tools and techniques in order to protect PCSs.

ISA Security Compliance Institute (ISCI) Communication Robustness Testing (CRT) implementation

Relevant attack patterns

An attack pattern is expressed as a series of repeatable steps simulating an attack against a system. Such patterns are useful to identify the cause of a vulnerability and a potentially related well-known solution.

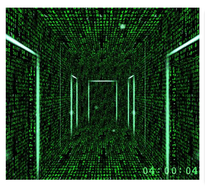
Scans represent the first step to gather information about a system by identify running services, opened ports and enabled protocol levels in the specific host.

Fuzzing attacks inject semi-random automatically generated data into various interfaces, with various levels of human intervention to specify the format of the data. They test a specific protocol implementation or function of the protocol stack, which should be able to handle invalid packets correctly.

Peach Framework

Storms attempt to make the devices' resource unavailable through an overload of communication; this will prevent the service from functioning efficiently or at all, temporary or indefinitely.

Syntax tests generate a wide range of legal and illegal input values, usually with some knowledge of the protocols and data formats used by the device.

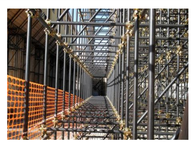


In **exploratory tests** there is no specific expectation about test outcomes, and generally not even a precise test plan. The idea is that the tester will spot anomalies that eventually lead to the discovery of new issues or at least refocus some of the remaining test effort.

Security stress testing creates extreme environmental conditions which could lead to some application anomalies or race conditions easier to exploit.

Data analysis focuses on the application data, especially in the cryptography context; but it also refers to the process of trying to understand a program's internals by examining the data it generates. This might be followed by an attempt to go beyond mere observation and influence the program's behavior as well.

Test scaffolding pattern provides testers with support tools they need in order to carry out their own black box tests.



Industrial device under test

Attack

Observe

Store

Security Vulnerability Report

Standards based format to report vulnerabilities for effective analysis and sharing of information:

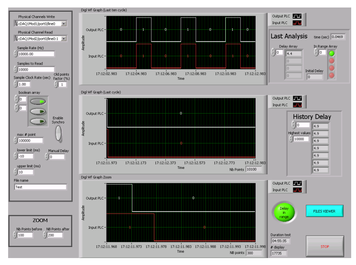
- **System characterization & reproducibility**
- **Threat identification**
- **Impact analysis and likelihood**
- **Risk reduction**
- **Threat search engine**

Monitoring

System observability is an essential part of any testing process to determine the test outcome. Usually it means examining the behavior of the device under test to establish whether it is symptomatic of vulnerability in the software or in the hardware. This examination can be harder in security testing than it is in traditional testing, because the tester is not necessarily comparing actual program behavior to expectations derived from specifications. Rather, the tester is often looking for unspecified symptoms that indicate the presence of unsuspected vulnerabilities.

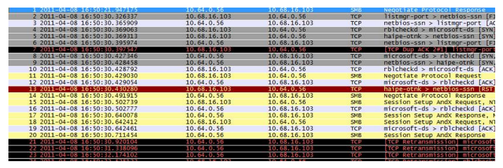
Process I/O Tracking

Detection of any anomaly in the I/O signals of the device under test.



Network Analysis

Traffic analysis coming IN/OUT of the device under test.



Internal Status Performances

Monitoring the internal resources of the PLC under test: scan-cycle ad execution time, memory usage, CPU status, I/O signals memory, communication modules conditions.

CONCLUSIONS

The current strategy has already proven to be effective at detecting device robustness issues. Thanks to the performed testing analysis, it was possible to detect critical anomalies in the devices' software protocol stack implementations. These research findings have been directly reported to their proper industrial vendors in order to be patched and incorporated in subsequent firmware releases. These initial encouraging results have motivated the team to continue following and expanding this approach for the future of the collaboration between CERN and the automation industry. It should be remembered that security analysis must be seen as a dynamic process which should be adapted according to new requirements, constraints and technological changes. So the testing techniques and methodologies defined in this document should be adapted and modified to fit incoming features and evaluate new functionality.

In the future, we will extend the scope of our analysis to the industrial supervision layer: the targets of our tests will not only be the individual devices but also SCADA systems in order to estimate the potential impact of malicious PDUs within the entire industrial network architecture.

CERN EN Engineering Department