IEC-61850 INDUSTRIAL COMMUNICATION STANDARDS UNDER TEST

F. Tilaro, B. Copy, M. Gonzalez-Berges, CERN, Geneva, Switzerland

Abstract

IEC-61850, as part of the International Electro-technical Commission's (IEC) Technical Committee 57 (TC57), defines an international and standardized methodology to design electric power automation substations. It specifies a common way of communicating and integrating heterogeneous systems based on multivendor Intelligent Electronic Devices (IEDs); these devices play a fundamental role in the control architecture of these electric power systems. IEDs are connected to Ethernet network and according to IEC-61850 their abstract data models have been mapped to the following communication protocols: MMS (Manufacturing Message Specification), GOOSE (Generic Object-Oriented Substation Event), SV (Sampled Values), and possible in the future Web Services. All of these protocols can run over TCP/IP networks, so they can be easily deployed and integrated with Enterprise Resource Planning (ERP) network; if this continuous integration on one hand provides economical and functional benefits for the companies, on the other hand it exposes the industrial infrastructure to the external existing cyber-attacks; so it is necessary to face with the changing threats and vulnerabilities of the entire cyber world. Within the OpenLab collaboration between CERN and Siemens, a test-bench has been developed specifically to evaluate the robustness of industrial equipment [1] (TRoIE). This paper describes the design and the implementation of the testing framework and in particular of that part used to evaluate the robustness of the IEC-61850 [2] previously mentioned protocols implementations.

INTRODUCTION

Smart grids are electrical power systems that are more efficient, more resilient, more advanced - hence "smarter" - than old, electromechanical power grids. Unlike the latter, smart grids use digitized information and communication technology to drive the industrial process operations on the base of consumers' needs; they are also capable of integrating diverse energy resources and emerging technologies. As Smart Grid technology progresses, the information technology (IT) and telecommunications infrastructures have gained more and more importance at ensuring the reliability and security of the entire electric system. Therefore, the security of IT systems plays a fundamental role in the evolution of any safe power smart-grid. As pointed out by several historical events like the North America blackout in 2003 [3], cyber security must address not only deliberate attacks, but also inadvertent compromising of the information infrastructure due to user errors, possible equipment failures, and even natural disasters. Any vulnerability might allow an attacker to penetrate any network boundary, gain access to the control software, and alter the industrial process data to destabilize the grid in unpredictable ways.

At the lower level of a typical power system architecture, two main parts can be detected: the power system infrastructure, which represents all the physical equipment and industrial field devices, and its control infrastructure which is responsible to automate and control the former. This means that the latter does not only retrieve and monitor the information from electrical equipment, but also takes actions to control the physical process. Furthermore, we are observing a growing trend of replacing proprietary industrial control networks (like PROFIBUS or Modbus) with open and standardized TCP/IP based Ethernet networks. This solution allows an easier and cost-effective integration of all industrial control system levels, but at the same time it exposes the entire infrastructure to internal and external cyber-attacks. This requires a proper design in order to face not only the typical functional aspects of an industrial power system, but also the growing number of cyber-security threats [4]; this actually represents the proof that hackers are more and more getting interest in exploiting common industrial control systems vulnerabilities by developing new viruses, worms and malicious applications.

The next chapters offer a brief description of the cyber security model used to drive the testing activities at CERN, based on the international ISA-99 [5] standards; nevertheless the entire pattern focuses on evaluating the security robustness of IEC-61850 protocols implementations.

OVERVIEW OF RECENT SECURITY STANDARDS AND OUR GOAL

Among the latest activities which have been carried out with the objective of regulating and standardizing security aspects in smart-grid systems, we could mention:

- The North America Electric Reliability Corporation (NERC) reliability standards define the requirements for planning an operation on the base of risk-analysis results. In particular the NERC [6] Critical Infrastructure Protection (CIP) Cyber Security Standards CIP-002 through CIP-009 [NERC, North American Reliability Corporation, Standards, Critical Infrastructure Protection] provides a list of guidelines to identify and protect critical cyber asses to support the reliability of the Bulk Electric System.

ISBN 978-3-95450-139-7

- The National Institute of Standards and Technology (NIST) published a three-volume document: the NISTIR 7628 [7] presents an analytical framework for the development of effective cyber security strategies tailored to the specific combinations of smart-grid-related characteristics.
- The technical specification IEC-62351 [8] represents another effort to secure the IEC - 61850 communication in the substations real-time environment. This document does not want to cover the smart-grid security topic in its generality or any of its security policy; but, keeping an eye on the current international security regulations, we will present a solution to evaluate the robustness of the IEC-61850 communication model implementations. Our evaluation strategy is mainly based on the ISA Security Compliance Institute [9] (ISCI) Communication Robustness Testing [10] (CRT) program, which has been produced on the basis of ISA-99 security standards specifications.

EVALUATION OF THE IEC-61850 COMMUNICATION MODEL

The concept of grid computing is essential to fully understand how smart-grids work. In general terms a grid is a distributed system able to deal with complicated and heavy computation problems that, once split into smaller tasks, are submitted to a network of computing resources; in this case the main objective is the computation efficiency coming out from the interconnection of high performance computers. Similarly, in a smart grid the power efficiency is the main objective: it is optimized by retrieving and analysing the real energy consumptions of each substation and driving the process in order to reduce the amount of power usage. So it is evident how important is the communication among the subsystems within a smart-grid and the necessity to secure it from possible cyber security threats.

IEC-61850 standards define strict rules to map specific functions into control industrial devices independently from the device manufacturers; this provides the vendors with a common and clear interface to implement in order to reach a full interoperability with other vendors systems. A key feature of IEC-61850 standards is the separation of the application-layer from the specific communication protocols through a generic abstract interface. Therefore any domain-specific model describes both the device functional aspects and the application data for all the supported services. As shown in the following figure, the standards foresee different types of communication load according to the specific service level: this goes from MMS (Manufacturing Message Specification) over TCP/IP to Ethernet protocols. It could be summarized saying that the application object model is mapped to the MMS application layer, but time-critical data messages make direct use of the Ethernet layer. All these protocol specifications are written in natural - not mathematically deterministic - language, so they cannot enumerate how to handle all the possible faulty situations; this means that, in the latter cases, the developer has to take some decisions on how to implement the protocol specifications. Hence distinct implementations of the same protocol will react and handle malicious traffic load in different ways. Because of that the security of the entire power-grid relies on the robustness of the specifically deployed protocol implementations: once a vulnerability has been discovered, it can be exploited by any attacker to jeopardize the entire industrial control system. Theoretically it should be the manufacturers' responsibility to detect all these defects and fix them during the industrial devices process lifecycle. The methodology presented in this paper allows automating the execution of security tests specifically conceived to assess the protocol implementation robustness of critical system like smart-grids. If we want to be more precise, our main objective is certifying that the individual IEDs are able to properly handle malicious and malformed packets (*i.e.* not compliant with the protocol standards definition) by keeping the normal operational behaviour. If all the deployed devices can pass this evaluation, the entire power-grid will in turn be more secure and stable against not only explicit attack attempts but also against involuntary mistakes.

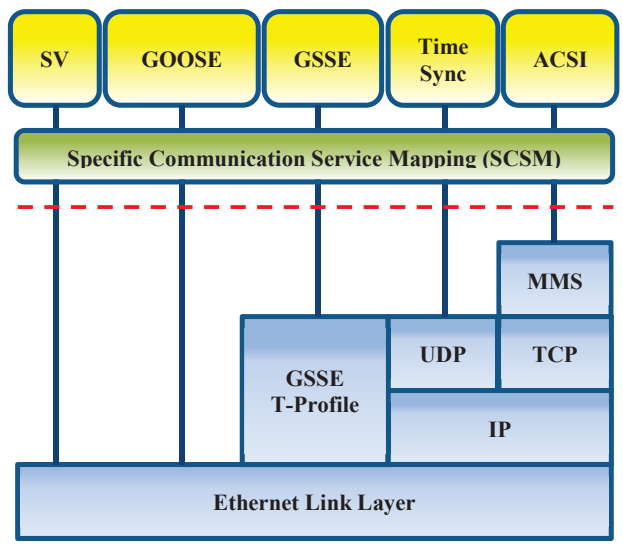

Figure 1: IEC-61850 Communication Protocols

Moreover the definition of several performance classes has been defined on the basis of the specific communication flow. So GOOSE (Generic Object Oriented Substation Event) messages – like trip, interlocks and low level signals - represent critical communication and therefore must be transmitted within a maximum delay of 10ms (Performance Class P1), or for some signals even within 3ms (Performance Class P2/3). The performance classes (M1, M2, M3) for Sampled Values (SV) messages are defined in IEC-61850-5, which are normally used for raw data messages. It is obvious, then, that our security evaluation has to take into account all of these performance requirements.

ISBN 978-3-95450-139-7

NETWORK PROTOCOL SECURITY TESTING BASED ON FUZZING AND GRAMMARS

Our approach to evaluate the robustness of the IEC-61850 communication model implementations is mainly based on fuzzing and grammar techniques. Protocol Fuzzing refers to the process of injecting valid and invalid sequence of packets, which can be generated randomly or pseudo-randomly – in the latter case we speak of "smart fuzzing" [11]. Fuzzing is known to be a very effective testing technique overall when the domain of analysis is so huge that it cannot be fully explored.

The enumeration of all possible faulty messages for each IEC-61850 protocol is exponential in the number of protocol fields; so it is necessary to devise a strategy to reduce the number of possible malformed messages to generate, but at the same time to increase the confidence that few vulnerabilities remain. To achieve that, the knowledge of communication experts has been translated into XML files, which define specific grammars to generate sequence of malformed messages into a systematic manner. Grammars consist of a set of syntactic and semantic rules to cover precise contexts that, in our case, are represented by protocol headers and their specifications. If the protocol implementation cannot properly handle invalid packets, anomalous behaviours may occur and possible security breaches could be detected. From this analysis, it has been possible not only to detect direct faults, but also expose race conditions [12], that can be easily exploited to compromise the entire system. These XML grammar-files are used as input of the Peach fuzzing framework [13], of which software components have been extended and chained together to generate customized IEC-61850 complex data flow. In our case, fuzzing is deployed to destabilize protocol implementations and specific functions of the protocol stack by injecting unexpectedly malformed input parameters values.

IMPLEMENTATION OF THE IEC-61850 PROTOCOLS FUZZING SYSTEM

The models - used to develop the traffic generator - are mainly based on the IEC-61850 standards definition; in particular: the part 9-2 describes the Sampled Value protocol structure over Ethernet; the part 8-1 defines the Specific Communication Service Mapping (SCSM) over MMS and the Generic Object-Oriented Substation Event over Ethernet protocol formats. As previously mentioned the Peach Fuzzing framework has been chosen out of many other available testing tools for two main reasons: 1) it is open-source, hence it is possible to verify and alter – whenever needed – even the core of the framework (code transparency is an essential feature in security context); 2) unlike other tools that are explicitly developed for and tied to specific protocols, Peach has proven to be a generic fuzzer, capable of testing any arbitrary communication protocols by performing simple, in principle non-protocol-aware, data mutations. In our analysis, a high level of customization is necessary to assess the robustness of IEC-61850 standards protocols implementations released by different vendors.

It is also worth mentioning that the Peach package contains a utility to convert Wireshark [14] captured network traffic files into its internal protocol model format. This capability has actually facilitated the definition and implementation of the Peach test-files for every analysed protocol.

Peach relies on specific software modules, referred to as "Agents", to detect any anomalous behaviours of the system under test; unfortunately these built-in agents could not be used to observe and monitor the behaviour of the IEDs. Nevertheless a custom "agent" has been developed in order react to any possible fault detection received from external systems (i.e. the SCADA monitoring all the smart-grid).

In this paper we cannot go through the complete list of the Peach software components that have been customized or entirely developed for the generation and injection of the fuzzed traffic. Anyway in the following, a brief description of the abstraction level of the Peach software architecture will be provided. One of the major actors responsible for the data transmission is the "Publisher". Three different Publishers have been implemented in order to support the IEC-61850 communication protocol formats. As Sampled Value and GOOSE headers are encapsulated directly on Ethernet frames, the Linux raw-sockets have been used to send raw-datagrams directly in the user-space. This choice has been necessary, since the TCP-IP kernel-space checks prevented us from injecting some malformed packets. The Peach fuzzing framework comprises several "Mutators" components, but we defined new ones in order to simplify the generation of data ranging values and types.

As described by the IEC-61850 standards, the byte structure of all the SV, GOOSE and SCSM Application Protocol Data Units (APDUs) is based on the Abstract Syntax Notation One (ASN.1) and the Basic Encoding Rules [15] (BER) Type-Length-Value (TLV) triplets. The Peach framework architecture supports this kind of task, so the data encoding has been delegated to a custom "transformer" class. It must also be said that the data encoding has been the fuzzing objective for some of the security tests, which try to poison the device under test through an incorrect encoding schema. In line with the ISCI Communication Robustness Testing (CRT) specifications, two different "mutation strategies" have been implemented: one that applies the fuzzing operations to the individual protocol header fields (Single Fuzzing Mutation); the other one that iterates through the combination of all them (Cross Fuzzing Mutation).

Another important characteristic of the security fuzzing system is its reproducibility, that is, the possibility to re-inject the same sequence of packets in a systematic way. It is essential to achieve the same results for debugging purposes. This is why each test has been numbered and in case of failure detection the current state is stored in order

ISBN 978-3-95450-139-7

to reproduce the security issue or restart it later from the last point.

Once the implementations of the previously described components was achieved, we started the definition of so called "PeachPit" files; they are XML files containing the grammars and the information necessary to run the fuzzing tests. Each of these files contains three main sections: the data model, the state model and a generic configuration. The first defines the data structure, the information type, the field values, and any possible intra-data relationship (i.e. length field, checksum) related to the individual IEC-61850 protocol header. The state model contains the finite state machine (FSM) that drives the execution of the fuzzing tests. Each state has an associated action aimed at sending or receiving a single packet or a sequence of them. Moreover the transaction of one state to another one depends on specific conditions (i.e. the reception of a precise frame or even a timer). The definition of a FSM is essential for stateful protocols, like TCP, where the two entities in communication must establish a connection and keep the current status of the communication. In these cases, the fuzzing tests make use of the FSM to jeopardize the protocol implementation by forcing it towards an unpredictable state, which is not even foreseen by the standards definition. Nevertheless, even if SV and GOOSE protocols are theoretically stateless, their implementations might not be.

The latest section consists of the configuration of publishers, agents, monitors and their initial parameters values to use for the specific test.

The PeachPit files definition is not totally arbitrary, but aims at fulfilling the ISCI Communication Robustness Testing (CRT) requirements. However it must be said that they do not cover the communication protocols described in the IEC-61850 standards yet; so, to overcome this limitation the main security testing concepts and principles have been extracted from the ISCI certification program and applied to the definition of the fuzzing tests. From this perspective, our testing activities could be seen as an effort to extend the ICSI CRT requirements, whose test-platform has been implemented through the use of the open-source Peach Fuzzing framework.

ACHIEVEMENTS AND CONCLUSIONS

In conclusion, the approach presented aims at discovering protocol implementation vulnerabilities by generating malicious non-standard traffic load on the basis of XML files. They contain the protocol specifications translation according to specific grammar rules. This testing methodology, making use of both fuzzing and grammar testing techniques, is so flexible that it could be used to generate any kind of communication traffic, therefore able to test any kind of network communication protocol. In our scenario the developed methodology has been indeed employed to evaluate the robustness of those IEDs, which provide an IEC-61850 protocols implementation; but, in principle, it could be adopted for any other industrial control devices.

The developed tools and extended testing framework can help any organization or control system manufacturer to assess and validate their own products; the result of these testing activities is an improvement of the security level, and then a better quality of the product itself.

The current strategy has already proven to be effective at detecting communication robustness issues, and at the same time generic enough to be adapted to any industrial protocol.

At last "Security-by-Obscurity" is not anymore a valid approach to secure any industrial system like power grids: it could work in the past when the industrial networks were totally isolated and disconnected by the external environments; today industrial systems are not immune against external threats, so they need to be provided with a more robust design, which takes care not only of the functional but also the security aspects.

REFERENCES

[1] F. Tilaro, "Test-bench for Robustness...", CERN, 2009
[2] International Electrotechnical Commission IEC-61850 http://www.iec.ch/smartgrid/standards/
[3] The Wikipedia article about North America Blackout http://en.wikipedia.org/wiki/Northeast_blackout_of_2003
[4] Stuxnet, Duqu http://www.langner.com/en/2011/08/04/stuxnet-and-beresford/
[5] ISA-99: Manufacturing and Control Systems Security http://www.isa.org
[6] North American Electric Reliability Corporation NERC Cyber Security Standards CIP http://www.nerc.com/pa/Stand/Pages/default.aspx
[7] The National Institute of Standards and Technology NIST Interagency or Internal Reports 7628 http://csrc.nist.gov/publications/PubsNISTIRs.html
[8] International Electrotechnical Commission IEC-62351 http://www.iec.ch/smartgrid/standards/
[9] ISA secure http://www.isasecure.org/
[10] The ISA Secure Communication Robustness Testing http://www.isasecure.org/ISASecure-Program.aspx
[11] C. Bekrar, R. Groz, L. Mounier "Finding Software Vulnerabilities by Smart Fuzzing", 2011 IEEE Fourth International Conference
[12] Race Condition Exploits http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/RaceConditions/index.html
[13] Peach Fuzzing Framework http://peachfuzzer.com/
[14] Wireshark http://www.wireshark.org/
[15] Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), ITU-T

ISBN 978-3-95450-139-7