EXPERIMENTAL EVALUATION OF CYBER INTRUSIONS INTO HIGHLY CRITICAL POWER CONTROL SYSTEMS

Giovanna DONDOSSOLA
RSE – Italy
dondossola@rse-web.it

Fabrizio GARRONE
RSE – Italy
garrone@rse-web.it

Judit SZANTO
RSE - Italy
szanto@rse-web.it

ABSTRACT

This paper analyses complex intrusion experiments carried out in the Power Control System - Resilience Testing Laboratory of RSE. The paper focuses on sneaky intrusion scenarios where the attacker forces the protective barriers implemented at different layers of the architecture thus gaining access to sensitive connections in order to arbitrarily modify the state of the power system.

INTRODUCTION

This paper addresses the assessment of cyber threats to communication networks and systems having a critical role in power grid operation. The probability of cyber threats to critical infrastructures has been increasing with the deployment of advanced automation and communication technologies relying on standardized protocols. Information and Communication Technology (ICT) security is even more emphasized in the upcoming smart grid model as a huge network of interconnected, heterogeneous sub-networks needed for controlling new generation power systems, e.g. active distribution grids [1].

This paper analyses complex intrusion experiments carried out in the laboratory test bed following the experimental activity on Denial of Service (DoS) attacks published in the 20th CIRED Conference [2]. The paper focuses on sneaky intrusion scenarios where the attacker forces the protective barriers implemented at different layers of the ICT architecture thus compromising the process networks where malware arbitrarily modify the state of the power system. The Stuxnet work [3], recently affecting Siemens controllers, is a real intrusion case confirming the occurrence of similarly complex attacks.

The rest of the paper presents i) the test bed deployed for experimenting intrusions; ii) the reference attack model; iii) the details about intrusion experiments and iv) conclusions .

INTRUSION PROCESSES INTO THE TESTBED

The test bed of interconnected high to medium voltage distribution networks includes a set of security mechanisms positioned at different layers of the ICT architecture, such as redundant systems and channels, firewalls, virtual private networks, intrusion detection systems, secure application protocols, antivirus, communication monitoring. The experiments concern cyber threats to those ICT network components, such as gateways and SCADA (Supervisory Control And Data Acquisition) systems, having a critical role in the power grid operation. The experimented scenarios are related to the violation of the authenticity property of information flows consisting of streams of process status data, events and commands used for the execution of acquisition and actuation sequences. In these scenarios the attacker is assumed to have a detailed knowledge of the target systems and their communications.

The test bed platform for the intrusion experiments (Fig. 1) is an extension of the platform used for the DoS experiments [2] including:

+ DSO (Distribution System Operator) substation automation networks;
+ DSO control centre networks remotely controlling a partition of the distribution substations;
+ TSO (Transmission System Operator) centre and substation networks supervising critical regions of a transmission grid and triggering defence actions;
+ ICT management centre networks remotely controlling ICT components of DSO/TSO networks;
+ DSO/TSO process networks;
+ ICT management networks.

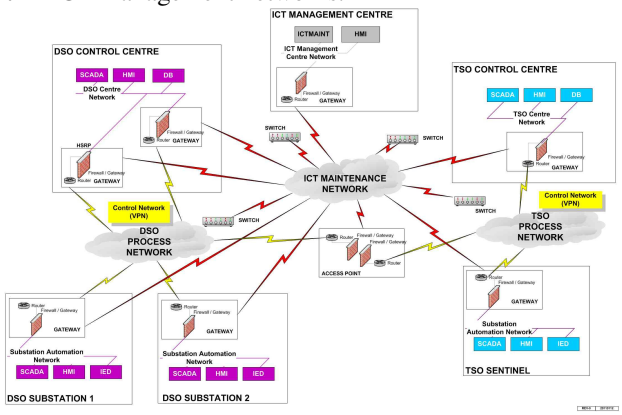

Fig. 1. Test bed architecture.

Besides its primary use as support to the remote control of substation automation systems and the interconnection of SCADA systems, the IP (Internet Protocol) connectivity of the intrusion test bed supports also the activities related to the remote monitoring and control of the ICT infrastructures through the ICT management centre. Following the current trend [4], in the test bed the ICT management centre is in charge of the management of both automation and communication applications in the process networks, including cyber security monitoring and control. In the real world each power utility is responsible of the ICT and cyber security management of their respective control infrastructures. Clear security policies have to be

established for the management of inter-operator wide area connections, such as lines leased by third party telecommunication service providers, secure tunnels cross-connecting TSO and DSO networks or virtual private networks supporting third party management services [5].
The workstations in the ICT management centre are endowed of appropriate applications providing the following functionality:

- monitoring of the ICT devices status and event management through Syslog messages;
- remote access to the ICT devices through SSH, HTTPS, SFTP or SSVNC sessions over the management network;
- remote configuration of the ICT devices through configuration commands and files;
- monitoring of the communications through appropriate sensors.

In the intrusion experiments a malicious insider, in the ICT management network, compromises a workstation for gaining unauthorized remote access to critical nodes in the process networks, then intrudes them with malware code interfering with TCP/IP centre-substation and UDP/IP inter-substation communications, causing the arbitrary trip of power substations. The experimental results allowed assessing the residual vulnerabilities of protected IEC 60870-5-104 [6] TCP/IP based communications of process networks in presence of intrusion processes.

ATTACK MODELS

The possible intrusion scenarios disturbing the communications of power control networks vary depending on the intruder's access point and the, intermediate and target, compromised nodes. By focussing on the intrusions from outside the DSO/TSO networks, 40 compromise paths may be enumerated from the network topology in the Fig. 2.
A compromise path is a sub path of the network topology defined by the list of nodes that are modified by the intrusion process. For instance, assuming that the attacker is inside the ICT management centre and that s/he intends to intrude into the DSO substation networks, six compromise paths are possible, of whom only three are able to comprise the most critical communications.
An intrusion process consists of a sequence of intrusion steps along a compromise path in the network topology. All the intrusion possibilities may be characterised by an intrusion process composed by five intrusion steps, represented in the state diagram of Fig. 3 that is the horizontal explosion of an ordered goal-tree representation [7], where:

+ the state transitions n. 1-5 are all timed transitions whose durations vary significantly on a step and technique base. Considering the topological extension of real scale power control networks, network scanning of transitions n. 1 and n. 3 may be in the order of hours;
+ gaining a valid access to a process network node (transition n. 2) may have different durations depending on the technique used to get the valid access. For instance in the case of password-based accesses, a combination of guessing, sniffing, logging, infecting or social engineering techniques may be used, each assuming different vulnerabilities and taking from hours to days to succeed;
+ the malware development (transition n. 4) may last from hours to months, while its installation and execution is a relatively fast operation in the order of minutes.

The whole intrusion process may take from several days to months for reaching the final state of intrusion successfulness. It is worth mentioning that malware developed by organized skilled teams, like Stuxnet [3], may take over a year to succeed.

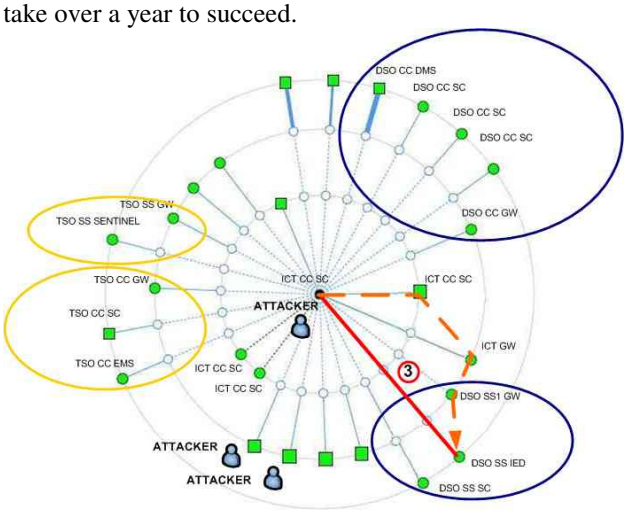

Fig. 2. Compromise paths in the network topology.

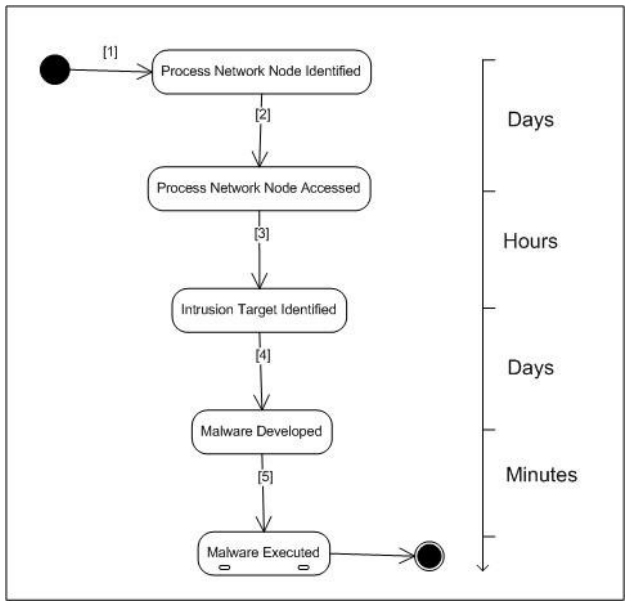

Fig. 3. Intrusion Process - State Diagram.

INTRUSION EXPERIMENTS

The test bed intrusions target the information exchange originated by an emergency control station whose implementation in the test bed is compliant with profile of the load shedding peripheral units specified in the Italian grid code. This target procedure belongs to the national defense plan and deploys both standard IEC 60870-5-104/TCP-based communications and UDP-based multicast communications for the fast and simultaneous transmission of trip commands to multiple geographically distributed substations. The details about the information flows targeted by the intrusion experiments are reported in [2].

In order to analyse the cyber risk of the above defence procedure, three intrusion processes have been implemented by assuming the presence of the intruder in the ICT management network and by selecting the compromise paths targeting the systems able to provoke a relevant impact on the power network, namely

1. DSO substation networks;
2. DSO centre networks;
3. TSO centre/substation networks.

As will be explained in the next section, each intrusion process differs in the complexity and the transition times of some intrusion steps, thus resulting in different risk values. The risk evaluation will analyse the impact of the three intrusion processes on a real scale power control network, considering the effort needed for each intrusion process to achieve the highest impact on the power grid, i.e. the disconnection of all the substations involved in the defence procedure.

Intrusions into the DSO substation networks

The intrusion experiment instantiates the model of an intrusion process onto the tele-control architecture as detailed in the following steps:

1. network scanning from the ICT management network to identify the process networks, their interconnection gateways, nodes and services: the scanning process discovers open ssh services on Cisco IOS routers, Linux gateways and SCADA components;
2. gaining highly privileged accesses to the process network nodes: the intruder compromises a workstation in the ICT management network by means of a malware activated through a faked e-mail or a USB driver. The malware disables the antivirus barrier, then installs and activates a key logger for registering the input data of log-on sessions;
3. accessing the process network nodes to identify the DSO substation gateways and the SCADA systems: substation routers are recognised by redundant IEC 104/TCP tunnels towards the control centres, whilst SCADA systems are identified by their IEC 104 servers;
4. developing the malware: given that the defence procedure adopts both TCP and UDP based information flows, a couple of malware have been developed. Trip Attack implements the intrusion into the UDP flows, whilst Arm Attack compromises the TCP flows. Trip Attack causes the unexpected disconnection of substations that have been preventively armed due to some pre-emergency condition on the transmission grid. Arm Attack is much more dangerous, causing the extemporaneous disconnection of substations even in the normal operation of the transmission grid;
5. loading the malware on nodes of the DSO substation networks and activating the malware: the malware may be loaded either on the Cisco routers or on the SCADA systems. After sending the faked arm request, the TCP connection takes 4 seconds to close, then trying repeated reconnection attempts. From the supervision workstation, the power operator is informed of the Substation disconnection, whilst the tool analysing the communication behaviour highlights the extemporaneous loss of a couple of tele-control packets and an IEC 104 reconnection (Fig. 4).

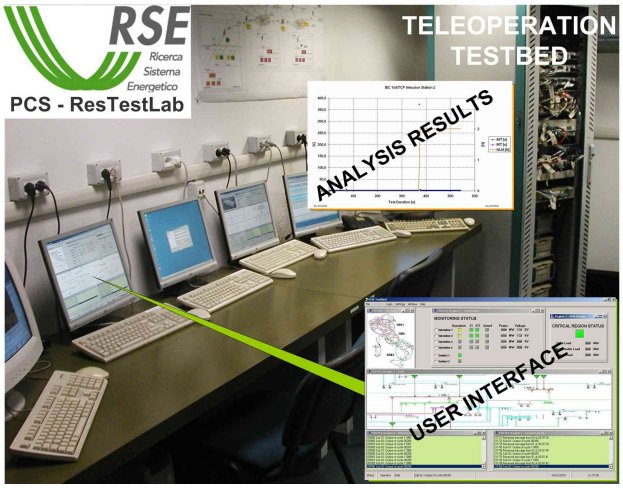

Fig. 4. Intrusion Effects - measurements.

In a real scale power control network, the highest intrusion impact requires compromising hundreds of substation nodes. As a power control network connects thousands of substations, the time needed to acquire logo-on data and to identify all the substations involved in the defence procedure may span over several days. In a real application the malware implementation requires a preparation phase for building the critical event matrix to be used by the next intruding phase for sending arm requests and trip commands. The preparation phase from the DSO substation networks is most convenient thanks to the complete visibility of required data. Once finished collecting the needed information, the malware code may be developed by a skilled programmer able to exploit the communication knowledge for manipulating data traffic and inserting un-authorised arm request and trip commands into the regular

information flows. The malware implementation is more complex in the Arm Attack malware than in the Trip Attack, requiring to overcome the reliable mechanisms (sequence numbering, acknowledge numbering and checksum) implemented by the TCP protocol.

Intrusions into the DSO centre networks

This intrusion process differs from the previous one in the steps n. 3 and n. 4. The DSO centre routers are recognised by numerous IEC 104/TCP tunnels towards the substation networks, whilst SCADA systems are recognised by their IEC 104 clients. For developing the malware here the intruder needs to collect a set of arm requests for mapping critical events with corresponding substations. In a real scale power control network, the highest intrusion impact requires compromising decades of centre nodes, decreasing the total time needed to complete the identification step n. 3.

Intrusions into the TSO centre/substation networks

The intrusion process consists of a coordinated attack where the faked arm requests sent from the TSO centre network has to be synchronised with the trip commands sent from the TSO substation networks. Also the malware preparation phase is more onerous in this case because it is distributed into the TSO centre and substation networks.

Intrusions through the Cisco routers

In order to execute a malware on a Cisco IOS router (step n. 4) the router architecture has to be extended with an AXP (Application eXtension Platform) module that allows to the IOS executing third party software. Instead of the AXP hardware module, in the test bed the AXP Emulator image has been deployed virtualising the AXP platform on a Vmware virtual machine. The availability of the AXP platform represents a source of vulnerability for the communication cyber security.

CONCLUSIONS

The coexistence of ICT management and tele-control accesses on a same power network device exposes the control infrastructure to residual vulnerabilities of the management network, even in presence of architectures deploying secure remote access protocols, access filtering and intrusion prevention functionalities. A lot of first hand information is needed for an attacker to be able to interfere with the communications of the real time devices in the power control networks. This decreases the probability of successful intrusions during critical functions. The robustness of the communication protocols at the application and transport layers influences the complexity of an effective malware implementation. Special effort is recommended in the development/deployment of security mechanisms at the different layers of the communication stack as a preventive measure to intrusion successfulness.
The performed experiments demonstrate that an intrusion is successful if the network access controls and the user authentication mechanisms can be bypassed or circumvented. The countermeasure configurations influence the probability of success of each intrusion step toward the intrusion objective. In the ongoing RSE research activity the information on the difficulties/weaknesses encountered in the realisation of the intrusion processes are being given in input to the cyber-power risk assessment framework to estimate the vulnerability and threat probabilities conditioning the successfulness of a given attack. The risk index instantiated over the experimental results allows identifying the tuning points of the mitigation measures in the test bed architecture. The test bed experiments may be exploited by industry to accelerate the deployment of security technologies in their control architectures and to increase the security analysis and risk assessment capabilities during power system operation.
The results presented in the paper intend to provide the power utilities with cyber security methods, tools and practices useful in their own selection of security measures for the protection of control infrastructures, as appropriate for their specific regulatory regime and assessment of business risks.

Acknowledgments

This work has been financed by the Research Fund for the Italian Electrical System under the Contract Agreement between RSE and the Ministry of Economic Development - General Directorate for Energy and Mining Resources stipulated on July 29, 2009 in compliance with the Decree n. 117 of May 22, 2009.

REFERENCES

[1] IEC Smart Grid Standardization RoadMap, 2010, SMB Smart Grid Strategic Group SG3, Edition 1.0.

[2] G. Dondossola, F. Garrone, J. Szanto, G. Fiorenza, 2009, "Assessment of power control systems communications through testbed experiments", *Proceedings CIRED 2009*, paper no. 0650.

[3] N. Falliere, L.O. Murchu, E. Chien, 2010, "W32.Stuxnet Dossier".

[4] Cigré WG D2.17, 2008, "Integrated Management Information in Utilities", *Technical Brochure no. 341*.

[5] Cigré Task Force D2.10, 2007, "Operational services using IP Virtual private Networks", *Technical Brochure no. 321*.

[6] International Standard IEC 60870-5, 2006, "Telecontrol equipment and systems - Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles", *International Standard*, Second Edition, Reference Number IEC 60870-5-104(E).

[7] M.-Y. Huang, T. M. Wicks, "A large–scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis", The Boeing Company, Seattle.