21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

D2_205_2010

CIGRE 2010

Identifying cyber security events in IEC 61850 substations by analysing different traffic patterns

R. URIBEETXEBERRIA (*) I. ARENAZA (*) I. GARITANO (*)
T. ARZUAGA (**)

(*) MONDRAGON UNIVERSITY
SPAIN

(**) ZIV – USYSCOM
SPAIN

SUMMARY

IEC 61850 faces the same security issues as any IP/Ethernet based automation system. Many initiatives have been started in order to add security to industrial automation systems. Some of them, such as IEC 62351, have a clear focus on IEC 61850.

CIGRE Study Committee B5 started a working group (B5.38) to analyze how these initiatives cope with the seven foundational requirements defined by ISA-99.01.01[1] to assess different cyber security solutions:

- AC: Access Control
- UC: Use Control
- DI: Data Integrity
- DC: Data Confidentiality
- RDF: Restricted Data Flow
- TRE: Timely Response Event
- NRA: Network Resource Availability

IEC 62351, as other standards, does not address all seven foundational requirements with sufficient detail to deploy a secure IEC 61850 system. Focusing on TRE and RDF, it is clear that more research is required [2] to detect traffic patterns anomalies and to decide how IEC 61850 traffic is restricted onto the areas it has to flow. This paper will propose an effective security architecture for IEC 61850 substations that can help to cope with RDF and TRE foundational requirements. To do so, it has been organized in four different paragraphs. First one will describe the different traffic patterns that can be found in IEC 61850 automation system. Second and third paragraph will briefly explain the state of the art for identifying cyber security breaches in IP/Ethernet networks. A final paragraph will propose a secure technical implementation to apply cyber security technologies to IEC 61850 systems without affecting its performance.

KEYWORDS

IEC 62351, cyber security, Restricted Data Flow, IDS – Intrusion Detection system, security breaches, data spoofing, packet filter, honeypot.

t.arzuaga@ziv.es

TRAFFIC PATTERNS FOUND IN IEC 61850 SUBSTATIONS

All of us are familiar with the different traffic patterns we can find in IEC 61850 automation systems. As depicted below, most traffic is based on TCP/IP/Ethernet.

In the station bus we will find:

- Control and monitoring traffic, reports and commands, which are based on MMS over TCP/IP
- Protection traffic based on GOOSE messages, which are multicast Ethernet frames.
- Synchronization information, based on SNTP/UDP/IP.
- Management information, being the most common used protocols, FTP for exchanging SCD files and HTTP for accessing IED's configuration parameters via their built –in web servers.

In the process bus we will find:

- Sample values, which are multicast Ethernet frames.

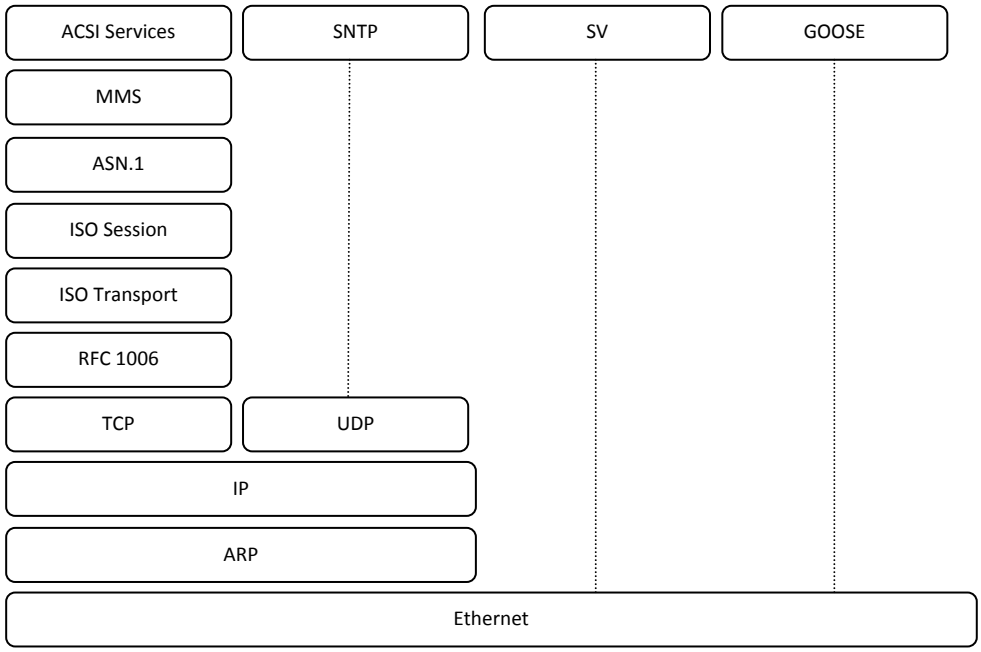

Figure 1: IEC 61850 protocol stack

From the above protocol stack it is clear that IEC 61850 will face the same security challenges as any TCP/IP/Ethernet based automation system. For that reason, we will now focus on understanding the main threats we will face for TCP/IP/Ethernet networks.

THREATS IN THE TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite was conceived in an environment that was quite different from the hostile environment they currently operate in. Many protocol specifications focus only on the operational aspects of the protocols they specify, and overlook their security implications. Some of vulnerabilities found during the last twenty years were based in flaws in the protocols themselves, affecting virtually every existing implementation. Researchers are still working on security problems in the core protocols.

Therefore attacks exploit characteristics of the protocols itself. An excellent review of possible TCP threats and countermeasures as well as many implementation flaws can be found in [3]. The following table lists most of those threats:

Exploited feature	Attack, threat
Connection-establishment mechanism	SYN flood
	Connection forgery
	Connection-flooding attack
	Firewall-bypassing techniques
	FIN-WAIT-2 flooding attack
Buffer management	TCP retransmission buffer
	TCP segment reassembly buffer
	Automatic buffer tuning mechanisms
TCP segment reassembly algorithm	Problems that arise from ambiguity in the reassembly process
TCP congestion control	Congestion control with misbehaving receivers
	Blind DupACK triggering attacks against TCP
	TCP Explicit Congestion Notification (ECN)
TCP API	Passive opens and binding sockets
	Active opens and binding sockets
Blind in-window attacks	Blind TCP-based connection-reset attacks
	Blind data-injection attacks
Information leaking	Remote Operating System detection via TCP/IP stack fingerprinting
	System uptime detection
Covert channels	Covert channels
TCP port scanning	Traditional connect() scan
	SYN scan
	FIN, NULL, and XMAS scans
	Maimon scan
	Window scan
	ACK scan
Processing of ICMP error messages by TCP	Blind connection-reset attack
	Blind throughput-reduction attack
	Blind performance-degrading attack
TCP interaction with the Internet Protocol (IP)	TCP-based traceroute
	Blind TCP data injection through fragmented IP traffic
	Broadcast and multicast IP addresses

Table 1: TCP threats

THREATS AT THE ETHERNET LINK LAYER

While certainly less complex and therefore less susceptible to design flaws than TCP/IP, Ethernet link layer protocols have had their share of security problems. Among those, the most severe and widely exploited are:

MAC flooding is a technique used to compromise the security of network switches. Switches maintain a table where they map the MAC addresses of all the hosts in a network to the physical port where they are connected to. This table is often called CAM table. A common attack may try to consume the memory available for CAM. Once run out of memory, the switch broadcasts all the incoming packets through all the ports making the switch work as a hub. Thus, an attacker can sniff all the traffic of the LAN. To protect the switches against this attack we can limit or hardwire one or some MAC addresses to a given port.

The concept of **VLAN attack** consists in gaining access to traffic on other VLANs that would normally not be accessible. This attack can be made in two different ways, double tagging and switch spoofing:

- **Double tagging** attack consists in prepending two VLANs tags to transmitted packets. The first switch strips off the first VLAN header and the packet is then forwarded. The second VLAN header is then visible to a second switch, so the attacker can bypass layer 3 security measures that are used to logically isolate hosts from one another.
- In a **switch spoofing** attack, the attacking host supports tagging and trunking protocols thus imitating a trunking switch. Multiple VLANs traffic is then available to the attacking host.

ARP attack also known as **ARP spoofing** or **ARP poisoning**, is an attack that allows an attacker to sniff, modify or interrupt data frames. This kind of attack can only be performed in networks that make use of ARP protocol to resolve MAC address. The attack consists in sending fake ARP response messages to a network and associate the attacker's MAC address with the IP address of another node. This way, all the traffic heading a legitimate destination IP address will have the attacker's MAC address. The attacker could now become an eavesdropper or perform DoS attacks. RARP protocol could be use to check the address mapping and detect this kind of attacks.

In a **spanning tree attack** Bridge Protocol Data Unit (BPDU) messages are sent by the attacker asking the switches to renegotiate the root switch identity. As this process usually takes around 30 seconds, a DoS attacks is possible. To avoid it, the "portfast" option should be deactivated on those ports that do not require it.

DHCP starvation attack is a DoS attack where the attacker requests all the available IP addresses to the DHCP server. Then the attacker itself offers the DHCP service and thus all man-in-the-middle attacks are feasible.

SECURITY TOOLS

Having sound TCP/IP protocol stack implementations is desirable to mitigate security problems. Unfortunately "known" security problems have not always been addressed by all vendors. In addition to it, in many cases vendors have implemented "quick fixes" to the identified vulnerabilities without a careful analysis of their effectiveness and their impact on interoperability. On the other hand there are tools that may help the administrator handle security issues. Some of these tools are briefly described in the following paragraphs:

Vulnerability scanners work at different layers of the OSI reference model. Many of them have a client-server structure. They scan all the ports of a system, searching for open ports and using known exploits to see how vulnerable the system is. This in fact is the same approach that attackers use. New vulnerabilities are found and their corresponding exploit developed almost every day. Therefore scanners will require updating their vulnerability databases, which is usually done via Internet (some tools require a subscription fee).

An **Intrusions detection system**, often called IDS, looks for intrusion attempts in the systems. An IDS can use different information sources, a network IDS analyses network traffic to detect intrusion attempts while a host based IDS uses the system logs of a host. An attack detection engine will process the data and will register, alert and/or react in accordance to a predefined strategy. Like vulnerability scanners, they keep a database with attack patterns that can be updated from the Internet.

Networks monitoring tools analyse and make reports of the captured data. They are composed by a set of modules and scripts that capture network activity data and format the information to be stored and displayed on screen or printed. They can generate graphs that can be used in web sites to show the network traffic in real time. There are several tools for network auditing and penetration testing. They can also facilitate the interception of network

traffic normally unavailable to an attacker. They may also perform man-in-the-middle attacks against redirected SSH and HTTPS sessions.

Layer 2 packet filters can act as layer 2 firewalls and also permit MAC address translation. They are included in the standard Linux kernel since version 2.4 and may be present in some "traditional" firewall systems too. There are also **ARP traffic filters** that set rule tables to filter ARP packets. These tables can be configured and modified in the Linux kernel.

There are many **layer 3 and 4 packet filters**. Some of them are software tools to be installed in PC like machines while others are special purpose devices. They usually perform Network Address Translation and have logging capabilities too. They can intercept and manipulate network packets.

Honeypots and **honeynets** are software pieces or devices that attract attackers as they pretend to be vulnerable systems. They are tools that allow administrators to gather information about the attackers and their techniques. They can also distract attackers from relevant real services and alert administrators about such situations.

It should be noted that many of these tools are often offered together as a single security bundle and include other additional features such as VPN, AAA, etc.

EFFECTIVE SECURITY ARCHITECTURE FOR IEC 61850 SUBSTATIONS

Working Group 15 of Technical Committee 57 of the International Electrotechnical Commission (IEC) develops standards for end-to-end cyber-security of the electric system, in particular for the communication protocols defined within TC 57. Security measures in IEC 62351 include SSL/TLS with specific parameters for TCP/IP profiles, electronic certificates for MMS profiles, challenge-response authentication for 60870-5 profiles, digital signatures for 61850 profiles.

The main impairment of the security measures proposed in IEC 62351 are the extra computing requirements for the devices in the network and especially key management requirements. The need for a X.509 PKI infrastructure and certificate management [4] may delay the deployment of IEC 62351 and increase its cost.

The following figure shows an alternative scheme, which presents a better cost/benefit ratio and can also, be applied to IEC 61850 legacy systems. The alternative scheme is based on having **measures in place to protect the physical access to the station and process bus networks**.

The presented scheme avoids implementing the IEC 62351 security requirements at Bay and Processes levels. There is no need to encrypt or sign messages at these levels.

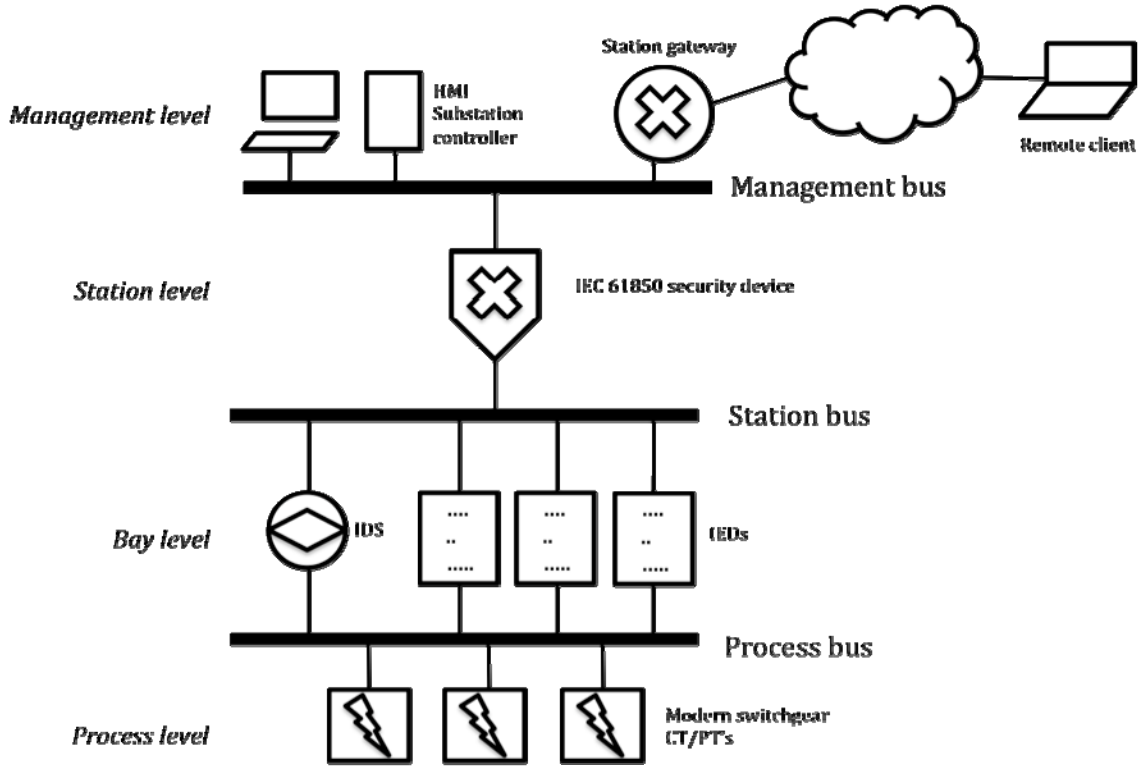

Figure 2: Security scheme for IEC 61850

In this scheme the main security provider is the **IEC 61850 Security Device,** 61850SD from now on. The 61850SD can implement several security functions and services. First, it can act as an IPSec server for the traffic coming from any subcontractor that plugs his computer onto the Management Bus to perform any type of configuration or maintenance task. It will establish the secure session with the management level and then 61850SD will decrypt the packets from the management bus before forwarding them to the other two buses. On the other way round, packets from the station and process buses heading the management network will be encrypted by the 61850SD. It should be noted that 61850SD will register all operations performed by this subcontractor computer (system log).

To further improve the security of the system, the 61850SD can also work as a firewall (level 2 and 3 packet filter) as well as anti-virus or authentication server. As the physical access to the station and process bus networks is protected, the 61850SD can filter layer 2 traffic coming from the management bus that does not comply with the security policy (e.g., non-digitally signed packets, IEC 61850 GOOSE type packets that should not originate on the management bus network, etc.) or filter layer 3 or 4 traffic that should not reach the station or process bus networks. 61850SD can also limit the traffic throughput exchanged between the management bus and the IEC 61850 automation system. In this way, we reserve the needed resources to avoid a possible IEC 61850 system unavailability.

The scheme also proposes to include an Intrusion Detection System that monitors the station and process buses. Security functionalities will thus be divided. This device will check the security in these two buses alerting the administrator in case the security of the 61850SD is compromised.

CONCLUSION

This paper proposes a security architecture for IEC 61850 that is based on:

i. Physical isolation of the IEC 61850 system.
ii. All IEC 61850 system management, configuration or maintenance tasks must be electronically controlled. Avoid that subcontractors plug their laptops directly onto the IEC 61850 ethernet switches. Instead, set up a unique secure access (via a 61850 SD) so that all accesses to an IEC 61850 system are authenticated and logged.
iii. Analyze continuously the IEC 61850 system traffic to detect possible traffic patterns anomalies.
iv. Minimize the security management requirements. Only one device, the 61850SD is to be managed (certificates, SW patches...) per IEC 61850 automation system.

BIBLIOGRAPHY

[1] ISA 99WG01, “Security for Industrial and Automation Control Systems – Terminology, Concepts and Models,” Standard ISA-99.01.01,2007.

[2] WG B5.38, “The Impact of Implementing Cyber Security Requirements using IEC 61850”.

[3] Security assessment of the transmission control protocol (TCP), CPNI technical note, February 2009.

[4] Cryptographic Key Management for SCADA Systems, Issues and Perspectives. L. Piètre-Cambacédè, P. Sitbon. International Journal of Security and Applications, July 2008.