CYBER SECURITY IN SMART GRID STATIONS

Per Erik Nordbø
Norway
per.erik.nordbo@bkk.no

ABSTRACT

We are currently faced with the need of modernization of the electrical energy system, which means that an Monitor and Control (M&C) information network eventually will overlay the entire electric power network (generation, transmission, distribution and customer).

Smart Grid environments like SCADA have historically focused on physical isolation and protection of equipment, and less focus on hardening the system with the best ICT security technology available. The Stuxnet virus was a reminder that physical isolation is not a guarantee against unauthorized access to SCADA equipment.

This paper describes some of the technology and standards that are available and that should be applied in Smart Grid networks, and a migration strategy for reaching those goals is described.

I. INTRODUCTION

In this paper the Smart Grid Station is defined as any transformer or power electronics node that from 1) an energy supply point of view can be considered flexible, efficient and reliable, 2) a cyber security point of view robust against inside and outside attacks.

In order to secure the Smart Grid, the Smart Grid must be designed in such a way that it can fulfill its role and the same time being able to handle the security threats. That means we should implement security by segmenting network resources into virtual private networks, use application firewalls between security zones, encrypt network traffic between sited, and make sure we have proper methods for authorization and authentication. Further, network traffic should be analyzed and inspected in order to detect malicious activities and shut down components in order to prevent damage due to unauthorized access to M&C functions.

Currently electrical grids which can be described as "smart" are capable of M&C functions of HV and MV lines and processing nodes. These facilities most often are well shielded and have locked gates, surveillance cameras, fences, intrusion alarms etc. In addition, the SCADA system is typically isolated by firewall from the rest of the corporate network, with minimal data exchange between the two.

However, we are now faced with two new trends:

- Increased demand for information exchange with the corporate network and the Smart Grid zones
- Increasing level of M&C equipment in MV, LV and Customer Premises locations (including smart meters) where shielding is difficult or even controlled by the customer

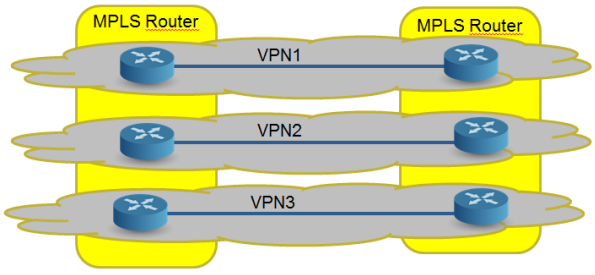
As a result, more focus must be addressed using advanced ICT tools and standards in order to accomplish a secure Smart Grid.

Segmenting the Smart Grid into security zones

In order to control exchange of data between Smart Grid domains, we need to define security zones and move M&C ICT functions within each zone into the corresponding virtual private network (VPN) for that zone.

A practical way to segment the network into security zones into virtual private networks is by using routers capable of MPLS (Multiple Protocol Label Switching). By using MPLS, you can define and run virtual routers inside one physical router. By having a set of MPLS routers, you can define virtual private networks on one physical network.

Initially these routers are not interconnected and are isolated as shown in the figure below.



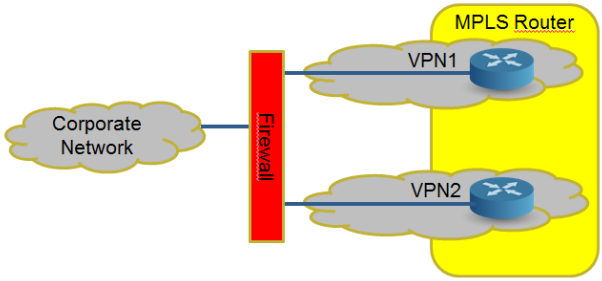
Data Exchange between security zones

Data exchange between security level N and N-1 should only be carried out via firewalls. As a default rule, assuming that security level N is higher than N-1, data exchange between N and N-1 should only be possible if *initiated* from level N. However, *exchange* of data between N and N-1 can

be allowed in both directions, as long as it has been initiated from level N and according to the security policy defined by the organization.

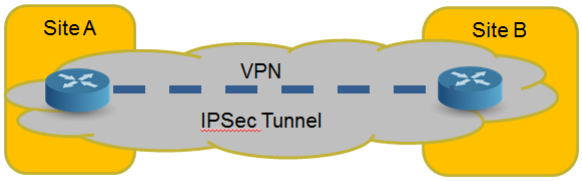
If the traffic is encrypted, application layer filtering may not be possible. As a minimum, traffic filtering should be based on IP-source/destination, transport layer protocol (TCP/UDP) and port numbers. If needed, encrypted protocols should be terminated and inspected in proxy firewalls. This may require certificate spoofing in the application proxy firewall.

Unencrypted traffic exchanged between zones should go via proxy firewalls for maximum security, since unencrypted traffic may have been tampered.



Securing the VPN with IPSec encryption

Historically Smart Grid systems like SCADA have exchanged data with little or no encryption and poor authentication. If this is the case and if lines between sites are "easily" accessible, we must make sure that traffic between sites can handle "man-in-the-middle-attack". If we lack end-to-end application layer encryption between decices, a suitable solution is to use network layer encryption (IPSec) between sites (site border routers), which prevents an intruder to monitor inter site communication links, inject or replay packets between devices like the SCADA head-end and RTUs.



Implementing IEC 62351 security protocols

IPSec solves the problem with man-in-the-middle-attack (eavesdropping) for unencrypted traffic between sites, but inside the site the traffic is still unencrypted and does not prevent an intruder (i.e. human, virus, worm) having local access to lines or devices - to monitor, inject or replay illegal M&C traffic.

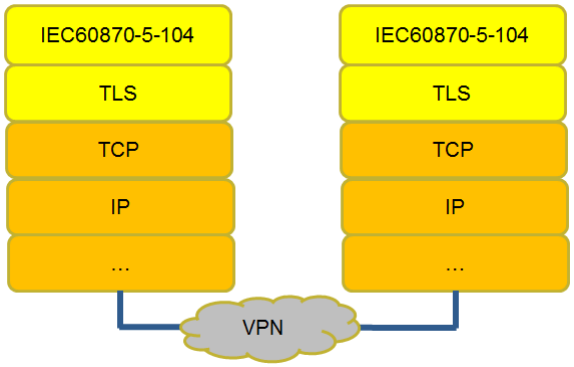
The solution to this problem is to implement the functionality in IEC 62351, which specifies how to secure/encrypt Smart Grid protocols which was not designed with security in mind.

The IEC62351 defines an extra layer of security for protocols such as IEC 60870-5-104 and the IEC 61850 protocol suite through encryption, certificates, authentication, roles and digitally signed messages. Some of these protocols have been designed with compatibility in mind, such that secure devices can coexist with unsecure devices which allow a gradual transition to a secure smart grid environment.

Below is listed the core IEC62351 [1] security profiles:

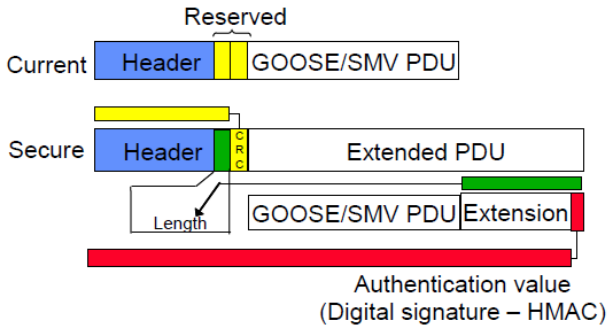
- IEC62351-3: Security Profiles for TCP/IP
  - TLS – Transport Layer Security
  - Used by
    - IEC 60870-6 ICCP
    - IEC 61850-8 MMS
    - IEC 60870-5-104
- IEC 62351-4: Security Profiles for MMS
  - Used by
    - IEC 60870-6 ICCP
    - IEC 61850-8 MMS
- IEC 62351-6: Security for IEC 61850 profiles
  - Used by
    - IEC 61850 SMV & GOOSE
    - IEC 61850-8 MMS
- IEC 62351-8: Role Based Access Control
  - For IEC 61968

IEC62351-3 has adopted TLS (Transport Layer Security) for end-end security over TCP, such that unencrypted application protocols can exchange data without risk of being eavesdropped and tampered. The most common use of TLS today is HTTPS, but the protocol is independent of the actual application protocol, and is therefore suitable for securing protocols such as the RTU protocol IEC61870-5-104. This is show in the figure below.



For multicast applications in IEC61850, classical public-key

is not used, since this requires that all the receivers share a private key. This was not the intention with private/public key technology. By design, the "secure" payload for IEC 61850 multicast is not encrypted, but the messages are digitally "signed" with a hash. This means that GOOSE and SMV applications supporting IEC62351-6 are able to detect spoofed messages and reject them. IEDs that do not support IEC62351-6 are able to receive but not verify "signed" messages, which means they are compatible, but are running in unsecure mode. The unsecure (current) and secure versions is shown in the figure below and described in detail in [2].



Role based authorization and user id authentication

ICS (Industrial Control Systems) such as SCADA has often lacked advanced authentication and authorization tools. Often security has been solved by having a group of employees share a secrets consisting of a user name and a password. This is a huge risk, because shared passwords have to be changed each time a trusted employee leave or shall no longer have access to the system. Even worse, it is difficult to track "who is doing what" because they are using the same username/password, which can be time consuming and dangerous if operator actions quickly must be reversed.

A proper solution to this is to use role based authentication and authorization. By registering users in a directory service, each user can be assigned roles, and is authenticated via the normal user login mechanism. Operator activities than can be tracked down to user id. If an employee no long shall carry out a role, the user id is removed from role in the directory service, and no further action must be done to maintain security. In order to provide this service to ICS, a directory server such as LDAP is needed, and access to the service must be secured by using TLS and certificates.

Intrusion Detection Systems

We must assume that an attacker primarily is trying to penetrate the border of the VPN, but we must also assume that the attacker already is inside the VPN, like the Stuxnet virus. In order to detect these threats, an Intrusion Detection System (IDS) is needed. The IDS should detect malicious activities at both exchange points between VPNs and inside VPNs. The IDS should analyze trends and warn IDS operators about incidents or abnormal traffic pattern. Whereas an application firewall will function as IDS at the exchange points, the IDS should also be able to detect malicious activity also *within* the security zone, i.e. inspect and analyze the "trusted" traffic in a VPN zone.

The IDS must be able to "tap" traffic from router interfaces independent of their physical location. This often requires that network equipment can duplicate traffic on ports and forward this traffic to the IDS location for inspection. Apart from introducing extra "listener" traffic in the network, the IDS should not interfere with rerouting within the VPN, thereby degrading robustness of the network.

II. MIGRATION STRATEGY

New Sites / Systems

1) All devices should be based on IP for flexibility and security. Running RTUs over serial interfaces is not a valid argument when it comes to implementing security. Using IP encryption from IEC 62351 over IP provides extra security not available for serial protocols.

2) Substation Automation shall be based on IEC 61850. Make sure that all components supports or will support IEC62351 and that equipment passes vendor interoperability tests if available. Only allow IEDs in unsecure mode if no other option is available, and in this case only for a limited time until the vendor fully supports IEC62351.

3) Plan your next generation SCADA system based on IEC 61850. Data exchange with other control centers shall be based on IEC 60870-6 TASE.2 and the TLS security from IEC 62351.

Existing Sites

1) Plan for software upgrade of the SCADA system such that TLS can be enabled. The SCADA system should be able to run in mixed mode, capable of running with or without TLS depending on whether the RTUs or gateways support IEC62351 or not.

2) Front end machines and SCADA gateways shall support IEC 62351, if possible. Enable secure mode if supported by the SCADA system.

3) RTUs (IEC61870-5-104) and IEC 61850 IEDs should support IEC 62351. IEDs running GOOSE and SMV shall be able to running in both secure and unsecure mode.

4) If the communication network between cannot be fully trusted against eavesdropping and tampering, consider running IPSec tunneling between these sites/routers.

5) Protect your head-end SCADA system with an application proxy firewall that can analyze unencrypted SCADA messages and make sure that only well-defined SCADA messages as defined in the site specific SCADA configuration can reach the SCADA system.

6) For Smart Grid protocols using TLS, consider using dedicated servers located in a protected secure location for certificate verification and directory services. This makes it much harder for a "spoofed" device to be accepted as a "legal" device, since the intruder than must be able to "spoof" both the device and the certificate server without being detected/rejected by the peer device.

7) Use IDS for analyzing the traffic pattern. The IDS should detect changes in traffic pattern, both at zone interfaces (firewall/router ports) and inside a trusted network/zone. The IDS should not be visible to an intruder.

8) No data should be imported into security zones carried on physical media such as usb memory sticks. If data must be imported into security zones, the data should be imported via firewalls capable of advanced virus detection.

9) If low power Radio Mesh radio to Smart Grid Stations must be used, network equipment should be based on the forthcoming Smart Utility Network (SUN) / IEEE 802.15.4g standard, which allow the IEC 62351 security suite to be implemented on top of IPv6.

Summary

A modern Smart Grid / SCADA system should be able to withstand eavesdropping and tampering. By requiring that IEC62351 must be supported, configured and activated in all devices, our SCADA/DMS/EMS system will be hardened against attacks. This is not only critical for introducing Smart Grid functionality in the LV distribution network, but also for hardening the Smart Grid in the core MV/HV network where IEC62351 security too often is not implemented. In addition, by using IPSec, firewalls and IDS, the risk of being compromised at the network level should be significantly reduced.

III. ACRONYMS

DMS Distribution Management Systems
EMS Energy Management Systems
GOOSE Generic Object Oriented Substation Event (IEC 61850)
ICS Industrial Control System
IED Intelligent Electronic Device (IEC 61850)
IP Internet Protocol (RFC791)
IPSec IP Security
SCADA System Control And Data Acquisition
SMV Sampled Measured Values (IEC 61850)
SUN Smart Utility Network (SUN), IEEE 802.15.4g
TCP Transmission Control Protocol (RFC 793)
TLS Transport Layer Security

IV. BIOGRAPHY

Per Erik Nordbø – Project Manager / Smart Grid:
Per Erik Nordbø is involved in Smart Metering and Smart Grid projects in BKK Nett AS. He has earlier on been involved in distributed processing and networking, real time programming, automation, data acquisition. The Smart Grid and Smart Metering activities in BKK Nett are coordinated in the "Nett2020" program, where a major goal is to get synergy out of the Smart Metering rollout and new "smart" functionality in the Distribution Network.

REFERENCES

[1] IEC, 2012-10-12, "IEC 62351-SER ed. 1.0", IEC
[2] Herbert Falk, 2008, "Securing IEC 61850", IEEE