Security in IEC 62351 for GOOSE and MMS

Roland Fiat
TÜV SÜD AG
Embedded Systems
Barthstr. 16
D-80339 Munich

Phone: +49 89 5791-3627
roland.fiat@tuev-sued.de

Abstract
To cope with an increasing amount of power from renewable energy sources being fed into the grid these need to become smarter which essentially means to improve the accuracy and availability of data within the power grid. To accompany this evolution IEC 61850 was introduced to streamline the communication within substations. Some security features and extensions for those communications protocols which were added in IEC 62351 are presented in this paper. A discussion about the challenges of real time systems and key management that comes with the use of cryptographic algorithms follows.

Introduction
Smart Grids are a relatively new technological concept currently in development. They are designed to help handling the increasing complexity of future power grids where in addition to more traditional power sources like coal power plants energy is also generated at a multitude of lesser sources like photovoltaic panels and wind turbines.
An essential aspect to make the power grid smarter is to have a sufficiently fast access to data like the amount of energy being produced and the consumption at any given time. This also applies to the communication going on in substations which are important building blocks of power grids. In the past a lot of proprietary protocols were used to implement this communication, but the current evolution is clearly showing a growing acceptance of an international standard developed specifically to promote more interoperability within substations: IEC 61850 [1]. While this standard does a good job at streamlining the communication it was developed with a focus on usability, unfortunately completely ignoring any security aspects. However, as recent high profile attacks like Stuxnet have shown security in industrial environments is not an option any more, it has become mandatory.
Based on the work done in IEC 61850 and other communication standards, IEC introduced another standard, namely IEC 62351 [2], with a focus on improving the security of said communication protocols.
In the following section I will present IEC 62351 in general, before presenting the proposed security features for Manufacturing Message Specification (MMS) and Generic Object Oriented Substation Event (GOOSE) in the sections 2 and 3. The last section will concentrate on the challenges of implementing those features and raise some questions that need to be answered before IEC 62351 can be used on a large scale.
1 General presentation of IEC 62351

IEC 62351 currently consists of eight published parts (1 to 8) as shown in fig. 1. These are:

- 1: Introduction
- 2: Glossary
- 3: Security for profiles including TCP/IP
- 4: Security for profiles including MMS
- 5: Security for IEC 60870-5 and derivatives
- 6: Security for IEC 61850 profiles
- 7: Objects for Network Management
- 8: Role-Based Access Control

In addition to the parts that are already available, three more parts to further enhance the standard are either just accepted as ‘new work in progress’ (9) or in discussion (10 and 11):

- 9: Key Management
- 10: Security Architecture
- 11: Security for XML Files

![Fig. 1: Interrelationships between the IEC TC57 Standards and the IEC 62351 Security Standards](source: IEC TC57 WG15 Security Standards ver 14)

I decided to focus my analysis on MMS and GOOSE because these are prominent protocols that IEC 61850 maps to: fig. 2 illustrates typical communication channels both within a substation and with external elements such as a SCADA system.

Because MMS and GOOSE work very differently from a network communication point of view and don’t have the same constraints the technologies to secure these protocols also differ greatly. The most relevant parts for MMS in IEC 62351 are part 3 and 4 while GOOSE security is treated in part 6. Note that due to similar timing constraints a lot of challenges that occur in securing GOOSE also apply to Sampled Values (SV).
Although IEC 62351 covers different aspects of securing various communication protocols the recommended solutions concentrate on two topics: integrity and confidentiality. How to fend off Denial of Service (DoS) attacks to guarantee a certain degree of availability is not addressed in the same detailed manner. In “Security Authentication for Smart Substation Communication based on IEC 62351” [3] the authors propose an enhanced version of the Secure Remote Password (SRP) [4] to get some DoS protection. Measures to prevent DoS attacks should be considered very carefully given the fact that an overzealous protection could potentially lock out a legitimate operator from accessing resources at a critical time.

2 Securing MMS

Part 3 of IEC 62351 is quite generic and, therefore, applies to all protocols built on top of TCP/IP, not only MMS. Because it is readily available and mature TLS [5] is the solution of choice to secure MMS traffic on the transport layer. That protocol’s main features are authentication and encryption which are paramount to attain integrity and confidentiality of data. Indeed, TLS protects against the following common attack types:

- eavesdropping through encryption
- replay attacks through the use of counters
- man-in-the-middle attacks through message authentication
- spoofing through certificates (node authentication)
These measures greatly improve the security of MMS on the transport layer. Further enhancements are presented in part 4 of IEC 62351 to secure higher layers in the OSI reference model:

- MMS association profiles define whether non-secure communication is allowed or not
- Association Control Service Element (ACSE) extensions allow for a more secure configuration of ASN.1 encoding

Part 4 also recommends parameters for key management aspects (Certificate Revocation List check interval) and specifies the required supported cryptographic algorithms to claim compliance to the standard amongst others.

3 Securing GOOSE

The approach for securing GOOSE messages is different for the following two reasons: first of all, GOOSE is a multicast protocol based on UDP. This means a publisher sends a GOOSE message and all subscribers get it. Secondly, GOOSE just like SV must adhere to very strict timing constraints in the order of 3-4 ms. This leaves no time for encryption mechanisms like TLS. Therefore, part 6 of IEC 62351 specifies that GOOSE packet data units shall be extended to support digital signatures: each message should first be hashed with SHA256 to generate a Message Authentication Code (MAC) and then cryptographically signed with RSA’s Signature Scheme with Appendix - Probabilistic Signature Scheme (RSASSA-PSS). Such an implementation guarantees the integrity of data. Any changes like tampering or spoofing will be detected.

To additionally protect against replay attacks the standard recommends checking both the status number of GOOSE messages stNum and their timestamp. It is assumed that the confidentiality is given by the fact that the GOOSE communication takes place within a substation’s LAN.

4 Challenges

According to [6], the only way to achieve the 4 ms mark is to use a dedicated crypto-chip for the computationally demanding Rivest Shamir Adleman (RSA) signature. It is unclear why this is not feasible now given the fact that these results were already reported in October 2009. I would also like to point out that progress has been made in the field of lightweight cryptography [7] and that Elliptic Curve Cryptography (ECC) for example could help reduce the computational burden of signing.

The proposed solution at that time was to use Hashed Message Authentication Codes (HMAC) instead of the RSA signature. Some details can be found in IEC 61850-90-5 [8] and should be incorporated to IEC 62351-6. Based on the results published in [9], it appears that even HMACs that require two consecutive hashing steps would still be well within a 3 ms threshold. However, it is unclear whether an AES encryption should follow as described in [8] and whether this can be done given the strict timing constraints.

Another major issue that needs to be addressed before a fully fledged implementation of IEC 62351 regarding MMS and GOOSE can be rolled out is the key management process. The standard will eventually provide some guidance when part 9 is published but the work on it has unfortunately just begun.
TLS and the current version of GOOSE security with RSA signatures both require some form of process to handle public key cryptography. This is best solved by using X.509 certificates. However, steps like:

- certificate generation and rollout
- certificate revocation and renewal
- validity check

have to be carefully thought through in the planning phase. In larger countries with tens or hundreds of thousands substations, a manual rollout of certificates is absolutely unfeasible. So this step would have to be largely automated. The same goes for the renewal of certificates after a few years in production. Checking the validity of a given certificate can either be done through the use of Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP) servers. In both cases additional questions about the security of the required connections for these services arise. What happens when a CRL cannot be refreshed or an OCSP server is momentarily unavailable?

Although the big players have built up Public Key Infrastructures (PKI) that can cope with tens of millions of certificates, this certainly isn’t a trivial task. It should be checked whether a filtering mechanism to handle CRLs locally, i.e. on a substation level, to significantly reduce their size isn’t an improvement worthwhile.

Unfortunately, replacing asymmetric cryptography by symmetric algorithms doesn’t help much when it comes to key management. No matter whether the proposed revision of IEC 62351-6 includes an Advanced Encryption Standard (AES) signature or not, to verify an HMAC computed by a publisher a subscriber requires access to that publisher’s secret key. In typical setups where we encounter 1-1 communication, the number of required secret keys is $n(n - 1)/2$ where $n$ is the number of communication partners. Here, fortunately, the number of required secret keys increases only linearly: a single key per publisher suffices for all subscribers to check the origin of the GOOSE message. However, this still implies that a secret key should not only be adequately protected on its owner, a given publisher, but also on all its subscribers.

Questions about secret key rollouts, revocations and renewals are open issues.

**Conclusion**

Although IEC 62351 is still in its early stages there is no denying that it already offers significant improvements regarding the security of protocols found in IEC 61850 which is solely focused on increasing the conformity and interoperability of communication devices within substations. Nonetheless, crucial parts of IEC 62351 like part 9 are still missing and existing parts might need an overhaul as the suggested security measures were impractical at the time they were published. It is important to keep in mind that security cannot come at the cost of safety.

A brief look at key management processes either for PKIs or secret keys showed there is no easy solution to these problems. We are actually facing similar issues in the office IT. However, the real time constraints of industrial environments make it even more challenging and the remote location of unmanned substations demand a high degree of automation.
Even though IEC 62351 covers important aspects of securing the communication in substations it is only a small portion of the big picture. As described in details in IEC 62443 [10] which is a standard for the security of Industrial Automation and Control Systems (IACS) the goal should be to implement a defense-in-depth security concept. Such a holistic approach does not only consider the security of the communication channels but also integrates aspects of physical security, zoning, etc. to reach a total protection that is more than the sum of its parts.

References