DOI: http://dx.doi.org/10.14236/ewic/ICS2015.2

Assessing the Security of IEC 62351

Roman Schlegel
ABB Corporate Research
Segelhofstr. 1K, Baden
Switzerland
roman.schlegel@ch.abb.com

Sebastian Obermeier
ABB Corporate Research
Segelhofstr. 1K, Baden
Switzerland
sebastian.obermeier@ch.abb.com

Johannes Schneider
ABB Corporate Research
Segelhofstr. 1K, Baden
Switzerland
johannes.schneider@ch.abb.com

IEC 62351 is an industry standard aimed at improving security in automation systems in the power system domain. It contains provisions to ensure the integrity, authenticity and confidentiality for different protocols used in power systems. In this paper we look at the different parts of IEC 62351 and assess to what extent the standard manages to improve security in automation systems. We also point out some incongruities in the algorithms or parameters chosen in parts of the standard. Overall, we conclude that the standard can significantly improve security in power systems if applied comprehensively, but we also note that the need to preserve (partial) backwards-compatibility has led to some design choices that provide less security than could have been achieved with a more ambitious approach.

Keywords: cyber security, IEC 62351, cyber security standard

1. INTRODUCTION

Automation systems are an important part of everyday life. They manage the distribution of energy (e.g., electricity, gas, etc.) and water, control transportation systems, run power stations and factories, and manage environmental aspects of large office buildings (e.g., heating/cooling, lighting, etc.), among many other things. A failure of critical infrastructure can cause significant economic damage within a short period of time (Anderson and Fuloria (2010); Guthrie and Konaris (2012)), and even endanger the lives and safety of a population. Failures of critical infrastructure can be caused by different events, such as natural catastrophes (e.g., flooding), equipment malfunction or also human error. However, another cause that has become more important in recent years are targeted attacks by hackers on the systems running critical infrastructure (Miller and Rowe (2012)). Because of society's dependence on automation systems it is therefore paramount to not only improve the resilience of such systems against equipment malfunction and human error, but also improve the security against targeted and malicious attacks of hackers. Unfortunately, many of these systems have been designed and built at a time when defending against malicious attackers was not a priority, because such attacks were rare and systems were much less interconnected than they are today. Furthermore, because of the typically long lifetime of automation systems of up to several decades, improvements can only be made gradually and over time. Nevertheless, in recent years efforts have been made to address these issues, for example by creating new standards that describe how to augment decades-old systems and protocols so that they can offer better protection against malicious attacks. There are a number of standards for automation systems in general, however, IEC 62351 (International Electrotechnical Commission (IEC) (2010b)) in particular addresses security in systems and protocols that are predominantly used in automation systems in the electricity distribution domain. Like many of these standards, it is not a revolution, but a careful evolution, to address security issues without completely breaking backwards-compatibility and interoperability with legacy systems. In this paper, we evaluate how IEC 62351 addresses security issues in existing systems, to what extent it can mitigate these issues, and whether there are remaining issues that are not mitigated by the standard.

This paper is organized as follows: In Section 2 we give an overview of IEC 62351 and its ten parts, followed by an evaluation of the standard in Section 3. Section 4 provides an overview of related work and standards, and Section 5 finally concludes.

2. IEC 62351 OVERVIEW

While the first parts of IEC 62351 (International Electrotechnical Commission (IEC) (2010b)) were published as early as 2007, more recent parts have been published in 2010, with some parts still being a work in progress and an expected stability date of around 2015. The standard addresses information security for power systems control operations, and the overall objective is to preserve the properties of confidentiality, integrity, availability and non-repudiation in a system, mainly through the introduction of authentication mechanisms.

The standard is split into ten different parts that address different areas, although at least one of the parts has not yet been released (part 9). In the following we give a brief overview of the different parts of the standard.

IEC 62351-1: The first part contains a general overview of the IEC 62351 standard, outlining the aim of the standard, as well as briefly introducing the different chapters. It also provides general information on security, an enumeration of security threats (both inadvertent and deliberate, e.g., equipment failures, cyber hackers, etc.), as well as a general overview of possible security countermeasures. The part also briefly describes concepts such as risk assessments, key management and security processes, among other things.

IEC 62351-2: The second part of the IEC 62351 standard is a glossary of terms, explaining terms such as Access Control, Data Security, etc.

IEC 62351-3: The third part of IEC 62351 addresses the security of protocols based on TCP/IP (Postel (1081a,b)) that are used for automation systems in the electricity distribution domain. Specifically, it prescribes the use of Transport Layer Security (TLS) (Dierks and Rescorla (2008)) with X.509 certificates (Cooper et al. (2008)) for TCP/IP-based protocols. The purpose is to ensure authenticity and integrity of data on the transport layer, and optionally also confidentiality by using the encryption mechanisms of TLS. The use of TLS also counters threats such as man-in-the-middle-attacks and replay attacks. This part of the standard also requires mutual authentication through certificates (i.e., client and server each present a certificate), and prescribes the algorithms and some minimum key lengths to be used, as well as how to handle certificate revocation.

IEC 62351-4: This part of the IEC 62351 standard addresses security for profiles such as Manufacturing Message Specification (MMS) (International Organization for Standardization (ISO) (2014)), which is used in other IEC standards (e.g., IEC 61850-8-1 and IEC 60870-6). Specifically, the part provides recommendations for the A-Profile as well as the T-Profile based on TCP/IP. For the A-Profile, IEC 62351-4 describes the use of X.509 certificates to authenticate applications, while for the TCP T-Profile the standard describes how to use TLS as a layer between TCP and the ISO Transport Service (Rose and Cass (1987)) using a different TCP port for secure connections. Further defined are the TLS cipher suites that must (or should) be supported.

IEC 62351-5: The fifth part of the IEC 62351 standard describes security for protocols related to IEC 60870-5 and derivatives such as DNP-3 (IEEE Standards Association (2012)). These protocols are message-based, and authentication therefore needs to be done on a per-message basis. In addition, any security mechanisms need to take into account the often limited processing power available in the affected devices. As keys used for authentication and / or encryption should be changed regularly, this part also proposes mechanisms that allow to update the keys in a device remotely.

IEC 62351-6: Part 6 of the IEC 62351 standard addresses security for protocols described in the related standard IEC 61850 (International Electrotechnical Commission (IEC) (2010a)). For protocols in IEC 61850 making use of TCP/IP and MMS, the provisions described in IEC 62351-4 shall be applied. Furthermore, this part proposes an extension to the IEC 61850 GOOSE and SMV PDUs (protocol data unit), adding a field to the PDU containing security-relevant information. The extension is intended to authenticate a PDU by containing a signed hash of the PDU. This part of the standard also adds extensions to the Substation Configuration Language (SCL) (International Electrotechnical Commission (IEC) (2010a)) that permit to include certificate definitions in the configuration.

IEC 62351-7: Power systems infrastructure makes heavy use of interconnected information systems to manage operations. This information systems infrastructure also needs to be securely managed, which is done using the Simple Network Management Protocol (SNMP) (Case et al. (1990, 1996); Harrington et al. (2002)). Part 7 of the IEC 62351 standard describes the data object models to be used that are specific to power systems.

IEC 62351-8: Part 8 of the IEC 62351 standard defines system-wide role-based access control for power systems infrastructure. It addresses different modes of access, such as direct and remote access, as well as access by human users and automated access by computer agents. To transport roles, this part proposes three different formats for access tokens, namely, X.509 ID certificates with extensions, X.509 attribute certificates and software tokens. Furthermore, the standard defines certain mandatory rights and roles.

IEC 62351-9: This part of the standard has not been released yet, but is intended to address certificate and / or key management.

IEC 62351-10: Part 10 of the IEC 62351 standard provides general guidelines for the security architecture of power systems. This includes an overview of security controls that can be applied in power systems, as well as system architecture advice on how to structure the communication infrastructure of power systems.

In the next section we will evaluate the different parts to determine to which extent they can address security issues in power systems.

3. ASSESSING IEC 62351

3.1. IEC 62351-1: Introduction to Security Issues

The information contained in this part of the standard provides an overview of security in power systems, listing the different threats to a system and the corresponding security requirements that can mitigate these threats. The enumeration is quite complete, ranging from inadvertent threats such as natural disasters to deliberate threats such as disgruntled employees, industrial espionage and hackers. The security requirements are also quite comprehensive, and the standard cross-references them with the appropriate security countermeasures (although not all countermeasures are part of the actual standard). Also mentioned are activities such as risk assessments, or security policies, as well as the challenges of security in power system operations, where availability is much more important than for example confidentiality.

Assessment. Overall, this section provides a comprehensive overview of the security issues that are relevant in a power system. However, the remaining parts of the standard do not address all of the issues mentioned in this part, but focus on the countermeasures that can realistically be implemented in an evolutionary manner.

3.2. IEC 62351-2: Glossary of Terms

The list of terms and abbreviations listed in this part of the standard is quite extensive, providing a short description of each term listed. The description is usually concise and accurate. The glossary is not entirely complete, there are some abbreviations or terms that are not contained, e.g., “MAC” for Message Authentication Code or the related “HMAC” (Hash-based Message Authentication Code).

Assessment. This part provides an extensive list of terms, together with a relatively detailed description for each item.

3.3. IEC 62351-3: Profiles including TCP/IP

Part 3 of the IEC 62351 standard is targeting power system automation protocols based on TCP/IP and aims to achieve the following security objectives:

- Message integrity protection, i.e., messages cannot be modified or inserted. This counteracts the threat of a man-in-the-middle attack.
- Confidentiality of messages (i.e., through encryption), although this is optional. This counteracts the threat of eavesdropping.

In addition, other mechanisms described in this part also counteract the threat of replay attacks, where a message is intercepted by an attacker and replayed at a later point in time.

The key part of IEC 62351-3 is to use TLS (Transport Layer Security, (Dierks and Rescorla (2008)) as the underlying protocol to provide end-to-end transport security for power system automation protocols, together with X.509 certificates for the authentication of devices. Because of the different requirements of OT (operational technology) compared to IT (information technology), the standard also provides information on how to address these differences. For example:

Session Duration. In power systems, connections are often much more long-lived than in regular computer networks. The standard therefore describes mechanisms how TLS connections should be renegotiated in regular intervals (e.g., depending on time or number of bytes transferred) to ensure the freshness of sessions. Furthermore, renegotiation provides an opportunity to re-check certificates, in case a certificate has been revoked in the meantime.

Certificate Handling. The standard supports the use of multiple certificate authorities (CAs) in a single IED, using a TLS extension (Eastlake (2011)). This can be useful where IEDs are accessed from different administrative domains. Also handled are certificate revocation and certificate expiry.

Cipher Suite. IEC 62351-3 does not provide a concrete list of TLS cipher suites that need to be supported. Instead, it mandates the support of RSA and DSS as the signature algorithms, while ECDSA or ECGDSA are optional signature algorithms. Furthermore, the use of RSA requires a key size of

2048 bit, with optional (albeit discouraged) support for 1024 bit keys. For key exchange, support for regular and ephemeral Diffie-Hellman key exchange are mandated, with a mandatory key length of 2048 bit, and an optional, backwards-compatible key length of 1024 bit.

General Requirements Additional requirements foresee the co-existence of secure and insecure communication by having TLS connections run through a different port of a device. An optional requirement is furthermore the use of certificate pinning / whitelisting.

Assessment. The proposed use of TLS for power system automation protocols based on TCP/IP is a suitable choice that makes use of a well-known and widely used protocol instead of trying to implement proprietary security protocols. However, the standard leaves the selection of acceptable cipher suites for TLS to other standards, risking incompatible implementations and the use of cipher suites that do not offer sufficient security (e.g., cipher suites using RC4, AlFardan et al. (2013)). Furthermore, the standard allows the use of NULL ciphers, e.g., TLS_RSA_WITH_NULL_SHA[1], within an administrative domain, i.e., ciphers that do not use encryption, although integrity and authenticity is still guaranteed. However, it can be argued that there are benefits of using encryption even within an administrative domain. If an attacker gets access to the local network, the use of encryption between devices in the local network will make it more difficult for the attacker to collect further information and continue his attack.

One attack that IEC 62351-3 does not defend against are IEDs that have been compromised by an attacker, as the compromised IEDs will still be recognized as legitimate by other devices in the system. The use of TLS and certificates, can, however, defend against the introduction of rogue devices within a power system, as such a rogue device would not have access to a valid X.509 certificate required for the secure communication with other devices.

An additional issue with IEC 62351-3 for secure communication within power systems that needs to be kept in mind is that backwards compatibility could be used by attackers to circumvent certain security features. If an IED offers both secure and insecure communication, an attacker could choose to make use of the insecure communication channel to get around authentication requirements. Likewise, offering backwards-compatibility (e.g., 1024 bit keys) will also reduce the security provided by the standard, although it is clear that backwards-compatibility is an important concern. However, this compatibility will always have an impact on security.

3.4. IEC 62351-4: Profiles Including MMS

Part 4 of the IEC 62351 standard describes measures for securing MMS (Manufacturing Message Specification, (International Organization for Standardization (ISO) (2014)). The standard proposes security for the A-Profile (i.e., application-level security) as well as for the TCP/IP-based T-Profile. The T-Profile based on OSI (i.e., ISO TP4 and ISO CLNP) is not covered by this standard. Depending on whether encryption is used, the mechanisms described in this part will achieve different security goals. If no encryption is used, only unauthorized access to information is prevented. If encryption is used (i.e., IEC 62351-3 is employed), then authentication, integrity and confidentiality can be achieved.

A-Profile Security. Security for the A-Profile (the application level) is achieved through certificate-based peer entity authentication during association setup. Specifically, a device will include an X.509 certificate, together with a timestamp and a signature on the timestamp using the given certificate in the association request. A receiving device will verify the timestamp, and accept it, if the timestamp does not differ by more than 10 minutes from the local time. In addition, a device will not accept a message with a timestamp that has already been seen within the last 10 minutes.

T-Profile Security. For TCP T-Profiles, the standard recommends the use of TLS between TCP and RFC 1006 (ISO Transport Service on top of TCP, Rose and Cass (1987)) on a separate port (3782). The standard also recommends a list of cipher suites for TLS, with one mandatory cipher prescribed (TLS_DH_DSS_WITH_AES_256_SHA).[2] However, TLS cannot be used for the T-Profile based on the OSI stack, as TCP is not part of the network stack. IEC 62351-4 therefore considers the T-Profile based on OSI as out of scope.

Assessment. The main issue of IEC 62351-4 security for the A-Profile is that it does not cover message integrity or confidentiality. It only covers the initial authentication, but the authentication does not extend to the subsequent messages within the session. Furthermore, the authentication only covers a timestamp included in the initial message, and the timestamp only has to be accurate to within

[1] This seems to be mistakenly designated as TLS_RSA_NULL_WITH_NULL_SHA in the IEC 62351-3 standards document.

[2] While the text of the IEC 62351-4 standard mentions TLS_DH_DSS_WITH_AES_256_SHA, a table of cipher suite combinations within the same document mentions TLS_DH_WITH_AES_256_SHA (i.e., without a signing algorithm). Presumably, TLS_DH_DSS_WITH_AES_256_SHA is the correct cipher suite designation.

10 minutes of the local clock of a device. This leaves the A-Profile open to at least three different attacks:

- an initial PDU can be modified (except the timestamp) without invalidating the signature
- the timestamp and authentication value can be extracted from a PDU and re-used in a forged PDU to a different device within 10 minutes of the original PDU being sent
- because intermediate messages are not authenticated or protected, after the initial authentication, an attacker can forge or modify PDUs exchanged between two devices

Therefore, unless transport-level security (i.e., TLS for the T-Profile) is also used, the security provided by A-Profile security mechanism is minimal, as it can neither guarantee integrity of messages, nor the authenticity of any intermediate messages.

Regarding the T-Profile security, the mandatory cipher defined in the standard does not use ephemeral Diffie-Hellman (*_DHE_* or *_EDH_*), but only uses regular Diffie-Hellman (*_DH_*), and hence does not support perfect forward secrecy (PFS). If perfect forward secrecy is a concern, then the standard should also prescribe cipher suites that support PFS. Among the optional cipher suites are also combinations that include RC4, the use of which has been discouraged (i.e., see RFC 7465, Popov (2015), based on results by AlFardan et al. (2013)), and 3DES, which has been estimated to be only secure until approximately 2030 by the National Institute of Standards and Technology (NIST) (2007). The standard also does not include recommendations for any cipher suites making use of elliptic curves, for example for the key exchange (i.e., ephemeral elliptic curve Diffie-Hellman). Cipher suites that support PFS using elliptic curve Diffie-Hellman instead of regular Diffie-Hellman are considerably faster, and only slightly more expensive than cipher suites without PFS (Vincent Bernat (2011)).

Furthermore, the same caveats apply for IEC 62351-4 as for IEC 62351-3, namely that systems will still support both secure and insecure communication (e.g., through different ports for the T-Profiles using TCP/IP), allowing an attacker to gain access by accessing the insecure mode. In addition, having the option of disabling TLS is also explicitly permitted by the standard.

Other concerns are that IEC 62351-4 permits 1024 bit RSA keys, which can no longer be considered secure (Lenstra (2004)). All cipher suites recommended in the IEC 62351-4 also make use of SHA-1, which has shown significant weaknesses, affording less than 80 bits of security (Stevens (2013)).

3.5. IEC 62351-5: Security for IEC 60870-5 and Derivatives

The core of this part of the standard is a challenge-response authentication mechanism using HMAC with pre-shared secret keys for integrity protection of data. Messages (ASDUs) that are critical can be protected by a challenge-response authentication mechanism, where the sending station has to reply to a challenge sent by the receiving station before processing the ASDU. Alternatively, the sending device can anticipate the challenge and include a response with the initial ASDU to eliminate one round-trip of data. There are also provisions for updating keys remotely, using both symmetric or asymmetric keys.

Assessment. The algorithms described in IEC 62351-5 address authentication and the integrity of critical messages, although they do not provide any confidentiality of messages (except key update messages). A detailed security analysis of all the mechanisms described in IEC 62351-5 is out of the scope of this paper, but the described mechanisms seem to achieve the stated goals.

However, there appears to be some potential for Denial-of-Service (DoS) attacks, as a device can be tricked into taking certain actions (e.g., invalidating session keys) if an attacker sends invalid messages. The state space of all possible interactions between devices (e.g., remotely updating keys, keeping track of counters, etc.) appears sufficiently large that there might be some concerns for a system to reach a “dead-end” state, for example, a state where controlling and controlled device are de-synchronized such that no mutually agreed keys can be established anymore. However, a conclusive evaluation of the possible state-space is outside of the scope of this paper.

There are also some constraints on choosing the initialization vector (IV) for the AES-GMAC message authentication code, and ensuring that these are met might not be trivial.

3.6. IEC 62351-6: Security for IEC 61850

Part 6 of the IEC 62351 standard defines security for protocols in IEC 61850 International Electrotechnical Commission (IEC) (2010a)), such as GOOSE (Generic Object Oriented Substation Events) and SV (Sampled Values). Some applications within IEC 61850 require response times of 4 ms, and IEC 62351-6 does not recommend encryption for these applications, as the cryptographic overhead might already incur delays of more than 4 ms. The standard does include recommendations for confidentiality in case of relaxed real-time requirements (i.e., more than 4 ms). For installations using IEC 61850 over MMS, the use of IEC 62351-4 is recommended to provide security. For installations using IEC 61850 with VLAN technologies, IEC 62351-6 provides an extension to the GOOSE and SV PDUs, adding an RSA-based signature to ensure the integrity of the PDU.[3]

IEC 62351-6 also defines how to extend the substation configuration language (SCL) to add information about certificates to the configuration of a substation, so that separate certificates for GOOSE and SV can be defined.

Assessment. The proposed extensions in IEC 62351-6 address some of the threats, for example the integrity of messages, and some protection against replay of messages. For MMS messages making use of IEC 62351-4 with TLS, authentication, confidentiality and integrity can be achieved. For protocols like GOOSE or SV, the extended PDU containing a signature should guarantee authenticity and integrity. No provisions are foreseen for traffic that requires a 4 ms response time.

The standard suggests the use of RSA signatures for providing authenticity and integrity of extended PDUs, which makes it unsuitable for applications where a 4 ms response time is required, as RSA signatures are relatively expensive in terms of computation power required. An HMAC (hash-based message authentication code) on the other hand can be implemented in hardware, requiring only around 10μs for generating an HMAC for a typical IP packet (Deepakumara et al. (2003)) in 2003. This is likely to have improved significantly nowadays. Even in software the calculation of an HMAC takes only around 30μs, which should be short enough to still allow a 4 ms overall response time.

The standard also does not define any details about the certificates related to the RSA keys used for signing extended PDUs.

3.7. IEC 62351-7: Network and System Management (NSM) Data Object Models

Parts 3 to 6 of the IEC 62351 standard try to address the security of communications and applications within a substation and also between substations. These considerations are mostly localized, but it is all part of larger communication and information infrastructure of a power system operator that needs to be monitored. Part 7 therefore defines network and system management (NSM) data objects that can be used together with the simple network management protocol (SNMP) to monitor and configure such an infrastructure. The scope is to monitor and control not only the communication networks, but also end devices (e.g., IEDs, RTUs, gateways, data concentrators, etc.).

Assessment. The impact of this part of the standard is mostly to provide a common framework to allow for managing and controlling a communication and information infrastructure as found in power systems. The list of possible objects is quite complete, covering a wide range from alarms, to status data, to measurements, etc.

The standard does not define how these objects are mapped to an underlying protocol (e.g., SNMP), leaving this to other standards. It also does not define in detail how access to these objects should be controlled.

3.8. IEC 62351-8: Role-based Access Control

Part 8 of the IEC 62351 standard defines the use of role-based access control (RBAC) in power systems. This is not a new concept, it is in fact part of best practices in many IT systems. The use of RBAC in power systems makes it possible to reduce the number of permissions that have to be assigned to certain users such that they only have the permissions they need to perform their duties. This reduces the risk to the power system as permissions are only assigned when they are actually needed, according to the principle of least privileges. The standard also defines a list of pre-defined roles (e.g., VIEWER, OPERATOR, etc.), and of pre-defined rights (e.g., View, Read, Control, etc.). In addition, the standard also defines two different models (i.e., push and pull) for authorization mechanisms, and provides more information on how to handle sessions.

Assessment. While the role-based access aspects of this part are similar to current best-practices in IT systems, some of the choices for the access token profiles are unusual. In particular, X.509 attribute certificates do not seem to be widely used nowadays, and are an unnecessarily complex choice for a token, potentially requiring an additional and separate certificate hierarchy. Even using X.509 ID certificates for carrying authorization information is not an obvious choice, as any changes in role affiliation require issuing a new certificate, making it quite inflexible. Because issuing

[3] The standard refers to this mechanism as a MAC (message authentication code). However, in cryptography, MAC has a specific meaning that is different from the mechanism described in this standard, i.e., a MAC combines hashing with a secret key, which is different from the signature-based mechanism described in the standard.

certificates is typically an expensive operation (in terms of management overhead), certificates are better suited for providing authentication of subjects, with a relatively long life-time of such certificates. Authorization information should then be carried in software tokens to allow for flexibility in assigning and changing roles.

Part 8 also seems to define its own protocol for secure session establishment. This is in general not recommended, as devising cryptographic protocols that are correct is extremely hard. Instead, peer-reviewed and well-tested algorithms should be used.

3.9. IEC 62351-9: Certificate Management

This part of the standard has not been published yet, but is expected to handle certificate management for the certificates needed in the other parts of this standard.

Assessment. As IEC 62351-9 has not been published yet at the time of writing this article, no assessment can be made.

3.10. IEC 62351-10: Security Architecture Guidelines

Part 10 of the IEC 62351 standard provides general guidance on power systems architecture with respect to security. It enumerates possible security controls (e.g., access control, firewalls, but also processes like incident response, etc.), and contains information on how to determine which security controls should be used. Furthermore, it illustrates the differences between security for power systems and regular IT security. It also provides several specific example architectures (e.g., an advanced metering infrastructure, or a substation automation system), with advice on the appropriate security controls that should be used to secure a system.

Assessment. This part of the standard gives a comprehensive overview over how the different standards address security in power and automation systems at different levels. There is also a detailed overview of possible security controls ranging from the technological security controls (e.g., authentication, access control, firewalls, etc.) to the procedural (e.g., incident response, coding guidelines, etc.), as well as regulatory and physical security controls. Together with the concrete architecture examples, this part of the standard provides detailed and applicable information on the security of power and automation systems.

4. RELATED WORK

There are a number of standards for security in industrial automation systems apart from IEC 62351. There is the ISA/IEC 62443 (The International Society of Automation (ISA) / International Electrotechnical Commission (IEC) (2014)) standard (formerly ISA-99) concerned with security for industrial automation and control systems. This standard seems to be more broadly applicable than IEC 62351, which focuses on power systems. In addition, ISA/IEC 62443 concerns itself more with procedures and management of security in ICS, and less with the actual technical implementation details. IEC 62351 on the other hand describes detailed and specific changes to protocols to improve security. Also a rather broad standard is NIST SP 800-82 (Stouffer et al. (2011)), which targets automation systems in general. Another standard that is relevant for the energy domain is NERC CIP (North American Electric Reliability Corporation (2015)), although it focuses rather on the operators of power systems, instead of on the engineering companies.

In terms of research papers related to IEC 62351, there are some papers examining IEC 62351 or aspects of it. The paper by Fuloria et al. (2010) examines in particular part 6 of the standard, which deals with security for IEC 61850. In the paper, they examine the impact of using RSA-based signatures for authenticating PDUs within IEC 61850. Their conclusion is that even hardware-based solutions will not be sufficiently fast to achieve 4 ms response time for reasonable RSA key sizes. They also show that elliptic curve cryptography achieves lower response times (e.g., below 1 ms), but it is not yet widely used in substation automation. In summary, the paper makes some valid points about IEC 62351-6, but does not really go into the other parts of the standard.

Two other papers examining IEC 62351 are papers by Fries et al. (2010, 2011). Fries et al. (2010) investigates IEC 62351 in the context of smart grid environments, and gives an overview of the standard as it existed in 2010. In particular, it examines part 4 of the standard, and how it applies to situations where connections are established over multiple hops. It also provides suggestions on how to improve the standard to allow for application-level end-to-end encryption using different technologies (e.g., H.235, XML security, etc.). Fries et al. (2011) examines similar situations, focusing on end-to-end security in new use-cases. However, both papers only focus on specific parts of IEC 62351, and do not give an overall assessment of IEC 62351.

5. CONCLUSIONS

The IEC 62351 standard addresses security concerns in power systems, providing in part authentication, integrity and confidentiality of data. The standard proposes both standardized technologies (e.g., TLS), and proprietary extensions to industrial protocols.

The standard contains some inaccuracies (e.g., cipher suite designations), and unconventional choices (e.g., RSA signatures for IEC 61850). It also does not consider newer cryptographic algorithms that could provide the same security guarantees at a lower performance cost (e.g., elliptic curve cryptography).

Nevertheless, the standard does provide a significant improvement in security, providing authenticity, integrity and at times confidentiality of data. However, it is clear that the standard is to some extent constrained by requirements related to backwards-compatibility, and hence does not always provide as much security as could be provided if backwards-compatibility was sacrificed. Overall, the standard provides a balanced approach that can be implemented with reasonable effort and that provides a reasonable amount of security if implemented comprehensively.

REFERENCES

AlFardan, N. et al. (2013) *On the security of RC4 in TLS. In: Presented as Part of the 22nd USENIX Security Symposium (USENIX Security 13).* Washington, D.C., 305–320.

Anderson, R. and Fuloria, S. (2010) security Economics and critical national infrastructure. In: *Economics of Information Security and Privacy*. T. Moore, D. Pym, and C. Ioannidis, Eds. Berlin, Germany: Springer. 55–66.

Case, J. et al. (1990, May) *Simple network management protocol (SNMP).* RFC 1157 (Historic).

Case, J. et al. (1996, Jan.) *Introduction to community-based SNMPv2*. RFC 1901 (Historic).

Cooper, D. et al. (2008, May) *Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile*. RFC 5280 (Proposed Standard). Updated by RFC 6818.

Deepakumara, J., Heys, H. M., and Venkatesan, R., (2003). Performance comparison of message authentication code (MAC) algorithms for Internet protocol security (IPSEC). In: *Proc. Newfoundland Electrical and Computer Engineering Conf.*

Dierks, T. and Rescorla, E., (2008, Aug.). *The transport layer security (TLS) protocol version 1.2. RFC 5246 (proposed standard)*. Updated by RFCs 5746, 5878, 6176, 7465.

Eastlake, D., (2011, Jan.) *Transport layer Security (TLS) Extensions: Extension Definitions*. RFC 6066 (Proposed Standard).

Fries, S., Hof, H., and Seewald, M., (2010, May) Enhancing IEC 62351 to Improve security for energy automation in smart grid environments. In: *Fifth International Conference Internet and Web Applications and Services (ICIW)*, 135–142.

Fries, S. et al. (2011, Apr.) Security for the smart grid - enhancing IEC 62351 to improve security in energy automation control. *Int. J. Adv. Security*, 3, 169–183.

Fuloria, S. et al. (2010) The protection of substation communications. In: *Proceedings of SCADA Security Scientific Symposium*.

Guthrie, P. and Konaris, T. (2012). *Infrastructure and resilience*. Government Office for Science. Tech. Rep.

Harrington, D., Presuhn, R., and Wijnen, B. (2002, Dec.) An *architecture for describing simple network management protocol (SNMP) management frameworks*. RFC 3411 (INTERNET STANDARD). Updated by RFCs 5343, 5590.

IEEE Standards Association 1815-2012 (2012) - *IEEE standard for electric power systems communications-distributed network protocol (DNP3)*. Available from http://standards.ieee.org/findstds/standard/1815-2012.html

International Electrotechnical Commission IEC 61850 (2010a)*Power utility automation*. Available from http://www.iec.ch/smartgrid/standards/

International Electrotechnical Commission IEC 62351 (2010b) Security. Availbale from http://www.iec.ch/smartgrid/standards/

International Organization for Standardization ISO 9506 (2014) *Industrial automation systems - manufacturing message specification*. Available from http://www.iso.org/iso/catalogue_detail. htm?csnumber=37079

Lenstra, A. K. (2004) Key length. In: *Contribution to The Handbook of Information Security*.

Miller, B. and Rowe D. (2012). A survey of SCADA and critical infrastructure incidents. In: *Proceedings of the 1st Annual Conference on Research in Information Technology, RIIT '12*. New York, NY, USA, 51–56.

National Institute of Standards and Technology (NIST) (2007, Mar.) Recommendation for key management - Part 1: general (revised). Available from http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

CIP (Critical Infrastructure Protection) Standards (2015) North American Electric Reliability Corporation Available from http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Popov, A. (2015, Feb.) *Prohibiting RC4 cipher suites*. RFC 7465 (Proposed Standard).

Postel, J. (1981a, Sept.) *Internet protocol. RFC 791 (INTERNET STANDARD)*. Updated by RFCs 1349, 2474, 6864.

Postel, J. (1981b, Sept.) *Transmission control protocol. RFC 793 (INTERNET STANDARD)*. Updated by RFCs 1122, 3168, 6093, 6528.

Rose, M. and Cass, D. (1987, May) *ISO transport service on top of the TCP version: 3. RFC 1006 (INTERNET STANDARD)*. Updated by RFC 2126.

Stevens, M. (2013). New collision attacks on SHA-1 based on optimal joint local-collision analysis. In:*Advances in Cryptology–EUROCRYPT*. New York: Springer, 245–261.

Stouffer, K. A., Falco, J. A., and Scarfone, K. A. (2011) SP 800-82. *Guide to Industrial control systems (ICS) security: Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)*. Gaithersburg, MD, USA. Tech. Rep.

ISA/IEC 62443 (2014) The International Society of Automation (ISA) / International Electrotechnical Commission (IEC). Available from http://isa99.isa.org/ISA99%20Wiki/Home.aspx

Bernat, V. (2011) *SSL/TLS & perfect forward secrecy.* Available from http://vincent.bernat.im/en/blog/2011-ssl-perfect-forward-secrecy.html