Securing Critical Infrastructure

Michael Schukat
OSNA Cyber Security Research Group
Discipline of IT
National University of Ireland, Galway
michael.schukat@nuigalway.ie

***Abstract*— Energy Systems are undergoing radical changes, driven by a combination of factors, including full economic cost, efficiency, environmental impact and security-of-supply, while being facilitated by increased deregulation. This complexity can only be dealt with effectively with the rollout of complex ICT systems that will play a significant role in managing, planning, and securing the energy infrastructure.**

However, this ever-increasing complexity of energy and support ICT systems greatly increases the potential for cyber attacks. Modern energy systems are becoming increasingly coupled and interdependent and the move/convergence from heterogeneous protocols and systems to all IP-based systems and open standards, whilst beneficial from many perspectives, increases the attack surface and scope, and thus raises many cyber-security challenges.

This paper will provide an overview of the cyber threat landscape in smart grid infrastructure from a Machine-to-Machine (M2M) communication perspective and discuss the role of PKI and authentication protocols for risk mitigation.

Keywords—smart grid; cyber security; PKI; M2M communication; authentication protocols

I. INTRODUCTION

Cyber-security is defined as information security - applied to computing systems, computer networks or the Internet as a whole - with the aim to avert cyber-attacks, e.g. malicious attempts to damage or destroy a computing system or network [1].

Cyber-attacks are seen as a major threat to society in the 21st century. They can be conducted by individuals or entire organisations; politically motivated attacks fall under the categories of cyber warfare and cyber terrorism. These threats are taken very serious by governments around the world, as for example seen in the recent establishment of cyber military units in various industrial nations (like USCYBERCOM, the United States Cyber Command) or the articulated fear of US experts and politicians of an impending “digital Pearl Harbor”.

Among all the worthwhile potential targets for a cyber attack, critical infrastructure has a very prominent position. This is for two reasons:

- Firstly critical infrastructure has traditionally not been designed or deployed with cyber security in mind. Potentially vulnerable ICT components were either non-existent or isolated with no network interface, therefore rendering external attacks impossible. However, this situation has changed in recent years, as more and more critical infrastructure systems have internet-connected ICT subsystems for management and control purposes. Furthermore, the appearance of advanced malware like Stuxnet [2] has shown that even physically isolated ICT infrastructure (e.g. the industrial control system of the Natanz uranium enrichment facility in Iran) can be targeted using out-of-band methods like infected removable drives.
- Secondly, a successful attack of critical infrastructure in a highly populated area will have an immediate, drastic, terrorising and potentially long-lasting effect on a population, as it deprives people from day-today essentials like energy, water, transport or communication.

This paper will address M2M-communication specific aspects of cyber security in smart grid, as such communication is of critical importance in this domain. This view is shared by the US-DOE (United States Department of Energy), who identified integrated, automated communication between components of the electric grid as being critical for the success of smart grid [3].

The following sections pursue a bottom-up approach by outlining how gold-plated internet security standards and methodologies (in particular public-key infrastructure, digital certificates and authentication protocols) can be adopted into smart grid. It follows loosely the recommendations of the IEC 62351 standard that is currently developed by WG15 of IEC TC57 [4], but also addresses other security-related aspects.

The paper is structured as follow:

- Section II gives an overview of critical infrastructure, smart grid and smart grid security standards.
- Section III provides an M2M perspective to smart grid cyber security.
- Section IV discusses in detail, how public key infrastructures, digital certificates and authentication protocols can be used to improve cyber security in smart grid.
- Section V completes with a summary and conclusions.

II. CRITICAL INFRSTRUCTURE AND SMART GRID

A. Overview

The term critical infrastructure describes assets that are essential for the functioning of a society and economy. It includes electricity generation, transmission and distribution, telecommunication, water supply and transportation.

Smart grid is a generic term for the application of computer intelligence and computer networking to electricity distribution systems [5]. Its development is driven by various factors:

- Utility companies have to adapt to a deregulated and more competitive market, which requires them to have better control and better data on full economic cost, efficiency, environmental impact, security-of-supply etc.
- The traditional simple one-way supply-demand relationship between large bulk energy producers (e.g. oil and coal-fired power plants) and consumers is being replaced by a more complex model consisting of distributed generation on demand (e.g. gas-fired power plants), unpredictable wind and solar generation capacities and micro-generation, which makes a consumer effectively a producer of electricity.
- Thirdly, new legislation requires utilities to provide their customers with new "smart" metering technology as for example happening in Europe.

The resulting 2-way information flow between producers and consumers can be seen in Figure 1.

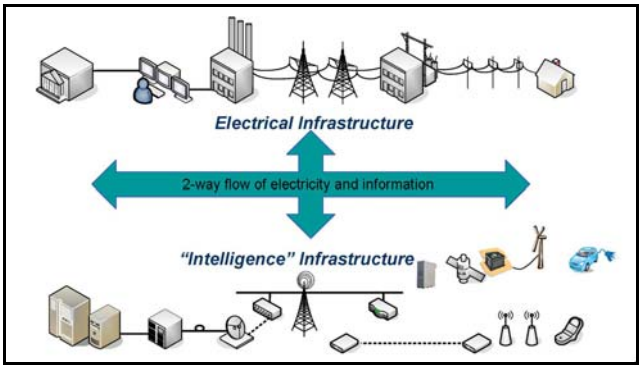

Figure 1: Information Flow in Smart Grid [21]

B. Cyber Security Standards in Smart Grid

Figure 2 shows the inherent complexity of an integrated smart grid with interfaces into other domains / ICT systems, which translate into many different potential cyber-attack surfaces.

According to the Electric Power Research Institute (EPRI) [6], one of the biggest challenges facing the smart grid development is related to cybersecurity of systems. According to the EPRI Report, "*Cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected…*".

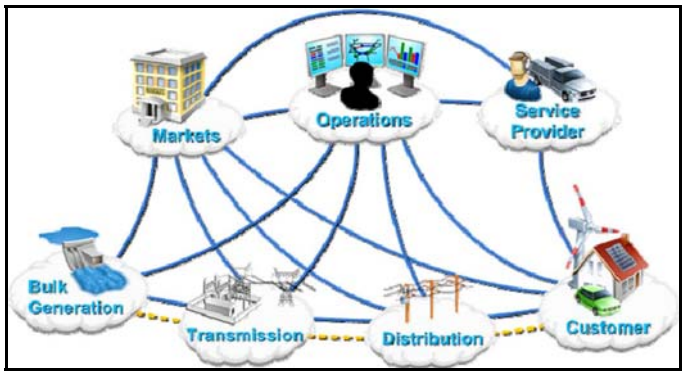

Figure 2: An integrated Smart Grid [18]

As a result there are many international organisations working on the development of smart grid security requirements and standards including the North American Electrical Reliability Corporation—Critical Infrastructure Protection (NERC CIP), the International Society of Automation (ISA), the National Infrastructure Protection Plan (NIPP) or the National Institute of Standards and Technology (NIST) in the US or ENISA in Europe.

Recently published smart grid security standards include NERC CIP and ISA/IEC-62443:

- The NERC CIP standard [7] consists of 9 parts covering the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning. It defines an electronic security perimeter (ESP) around any critical cyber-asset that aims to prevent any unauthorised access.
- ISA/IEC-62443 is a series of standards [8] that define procedures for implementing electronically secure industrial automation and control systems. On network level it promotes security levels for zones (e.g. groupings of logical or physical assets that share common security requirements) and conduits. The latter are interfaces that control access to zones, resist DoS attacks or the transfer of malware, shield other network systems and protect the integrity and confidentiality of network traffic.

However, providing comprehensive cyber security standards is an uphill battle as seen with the 2013 "Crain / Sistrunk" DNP3 vulnerability [9]. This vulnerability enables attackers to bring down control equipment in substations (see section III.A) that use the DNP3 communication protocol to communicate to slave devices (EP-1 to EP-3 in Figure 3) via a serial (i.e. RS485) link. The attack requires the injection of a single crafted packet addressed to the controlling master device (EP-M in Figure 3). The problem is that this attack falls outside the merits of NERC CIP cybersecurity regulations, as these specifically exclude serial communications and the equipment that uses serial communication from meeting any security requirements. Further on, remote slaves can be pole-mount devices outside the ESP of the substation (EP-3 in Figure 3). To be effective against these attacks, NERC's ESP now has to include the entire country [9].

III. SECURE M2M COMMUNICATION AND PKI

A. *Smart Grid Security from an M2M Communication Perspective*

As outlined before a smart grid infrastructure is abstracted into a complex machine-to-machine (M2M) network consisting of a number of interconnected and communicating end points (EP). These EPs are based on (deeply) embedded systems with often very limited computational resources that have a long operational lifespan (up to 15 years) and that operate autonomously with very little or no user / operator intervention.

EPs are for example deployed, either individually or as networked groups of devices, in grid substations as shown in Figure 3. Substations are placed between the high-voltage transmission system and the low voltage distribution system.

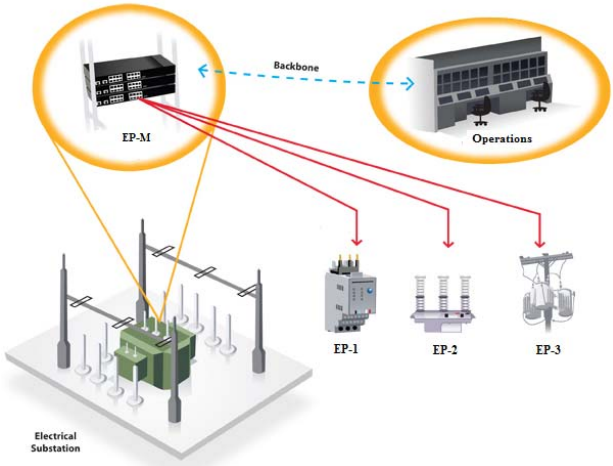

Figure 3: Electrical Substation linked to Operations

Inter-EP communication (either within a substation or back to operations via Supervisory Control and Data Acquisition (SCADA)) is provided via a range of protocols including the already mentioned Distributed Network Protocol (DNP3), Generic Object Oriented Substations Events (GOOSE), IEC 61850, IEC 60870-5, or Modbus.

Since EPs can only be accessed / attacked via their network interface, cyber security as defined in the introduction will be interpreted as information security for computer networks, e.g. network security.

In information security terms, any network protocol used in smart grid should fulfill the following requirements (Figure 4):

- Message confidentiality
- Message integrity
- End-point authentication
- End-point authorisation

Used in tandem these features alleviate the risk of common network cyber-attack strategies, which are based on (a combination of) network eavesdropping, packet injection and packet modification (as for example seen in the DNP3 vulnerability). Denial of Service (DoS) attacks do require other means of security (e.g. firewalling).

However, message confidentiality, e.g. the encryption of messages using symmetric or asymmetric keys, is not being applied in the above protocols. This is for a number of reasons; firstly confidentiality was traditionally not deemed to be an essential requirement for EP communication; secondly EP-encryption requires additional hardware resources; thirdly message encryption / decryption does impose latencies, which are unacceptable for real-time protocols like GOOSE [10]. Likewise message integrity is in the majority of all protocols only provided via CRCs, which can be easily tampered for message modification attacks. End-point authentication and authorisation are broadly not considered at all.

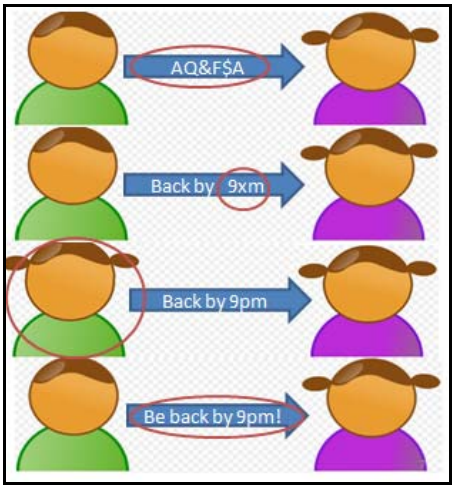

Figure 4: Message Confidentiality & Integrity, End Point Authentication & Authorisation

B. *Public Key Infrastructures*

In a public key infrastructure (PKI) a certificate authority (CA) binds a public key to an end-entity identity (i.e. a user name or server DNS name) by issuing a digital certificate. The required steps to issue a digital certificate can be seen in Figure 5: An end-entity sends a certificate request to a registration authority (RA), which validates the request (i.e. the end-entity details) before sending it to the CA for signing. The CA returns the created digital certificate back to the end entity. This certificate can be independently validated by a 3rd party to which the end-entity wants to interact with. The 3rd party can also request the status of the certificate (e.g. valid or revoked) by querying a validation authority (VA).

The public key stored in the digital certificate in combination with a peer-to-peer authentication protocol provides message confidentiality, integrity, EP entity authentication and EP authorisation.

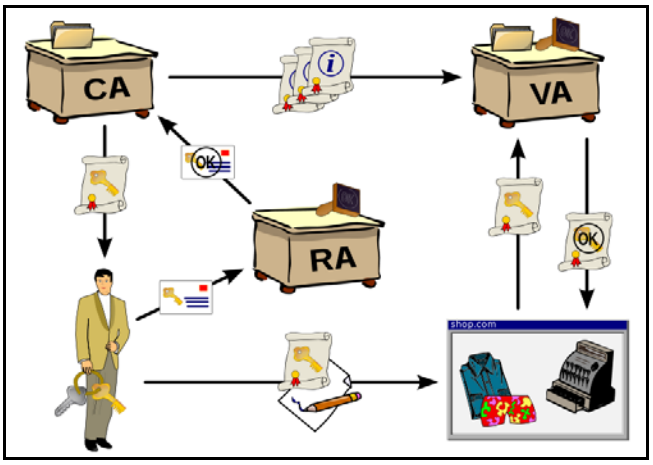

Figure 5: A PKI and its Interactions

IV. PKI AND DEVICE AUTHENTICATION IN SMART GRID

A. *The EP Authentication Protocol*

In order to provide adequate security, a network of N individual EPs must be separated into (N-1) individually negotiated secure peer-to-peer connections. It is imperative to provide secure end-to-end communication and not to rely on some intermediate (e.g. link-layer) security, as for example implemented in many wireless protocols. The onus lies with each EP to provide and guarantee a secure communication channel to some other peer.

Because of the network security requirements in Figure 4 end-to-end security must be provided on transport or application layer, as network layer security (e.g. IPSec) provides only message confidentiality, message integrity and end point authentication, but no end point authorisation (see also section C).

In an IP-based environment the most applicable protocol is Transport Layer Security (TLS) in its most recent version 1.2 as specified in RFC 5246 [11]. It must accommodate the recommendations of RFC 6176 [12], e.g. TLS sessions will not negotiate the use of Secure Sockets Layer (SSL) version 2.0, which has known security flaws including a cryptographic weak hash function (MD5), unprotected handshake messages (which allows man-in-the-middle to trick the client into picking a weaker cipher suite than it would normally choose) and the termination of EP sessions via man-in-the-middle TCP FIN insertions.

TLS must also be configured to provide a client-authenticated handshake, e.g. a mutual authentication of both EPs where both peers exchange and validate the other peer's certificate during the handshake. This is in contrast to the typical use of TLS in secure browsing, where only the server certificate is validated by the client.

A smart grid infrastructure deployment is a static system. Its EPs have a defined functionality as well as defined static interfaces / communication links to other EPs (to execute management and control tasks). Therefore secure communication links between EPs are active over extended periods of time. Further on, a TLS handshake on an embedded system is a resource expensive tasks that can take a considerable amount of time (between a few milliseconds to tens of seconds, depending on the underlying hardware architecture and the cryptographic algorithms / cipher suits). Therefore there is no need to implement the TLS Heartbeat extension as defined in RFC 6520 [13].

However, the recent discovery of the Heartbleed bug in the OpenSSL implementation of RFC 6520 as well as recent revelations about the widespread capture and storage of encrypted network communication (for later cryptanalysis) by some government agencies emphasises the need for perfect forward secrecy (PFS). PFS is a property of cryptographic systems which ensures that a session key derived from a set of public and private keys will not be compromised if one of the private keys is compromised in the future. An implementation of TLS can provide forward secrecy by requiring the use of ephemeral Diffie-Hellman key exchange to establish session keys.

The negotiated session key will be used for 128-bit AES, which can be used in Cipher-Block Chaining (CBC) mode, Galois/Counter Mode (GCM) or CCM mode (Counter with CBC-MAC), depending on what combination of message confidentiality, integrity, and authenticity assurances is required.

It should be noted though that some protocols (most prominently the GOOSE protocol mentioned before) requires messages to be transmitted in real-time (with latencies in the order of a few milliseconds). This might require hardware-accelerated encryption and packet handling by EPs.

TLS is an application layer protocol and requires an underlying TCP/IP stack. While there is a general convergence towards IP-enabled networks there are M2M deployments, for example based on link-layer radio communication or serial DNP3 packet transmission, where TLS cannot be adopted.

Also the majority of legacy EP hardware cannot be retrofitted with a TLS software stack. Such devices could instead be complemented by security appliance that operates as a TLS-enabled gateway between the EP and the network.

B. *EP Certificate Management*

Each EP has to be provided with one or more digital certificates that contain the device's identity as well as additional attributes. These certificates are based on X.509 version 3, which is the de-facto internet standard for digital certificates. Considering that typical EPs are deeply embedded devices, some important certificate management decisions are required:

- The first decision relates to the lifetime of a certificate. For example, server-certificates have a typical lifetime of 24 months [14], after which they need to be renewed and redeployed. However, in a deeply embedded and potentially only remotely accessible EP (like a smart meter) this feature requires additional code and hardware (to re-flash and replace certificates) as well as a network API to access new certificates; particularly the latter opens a potential backdoor

for cyber attacks. Likewise the logistics of managing a large number or devices as well as the problem that the new certificate must be signed by a trusted certification authority adds to the problem.

- The second decision relates to the question of how many certificates should be deployed on an EP. The underlying idea is that each device should have not one, but multiple certificates installed prior to deployment. These certificates can
    - be valid over different time periods (therefore reducing the risk of compromising a certificate during its lifetime),
    - be remotely activated / disabled on demand, if a certificate has been identified as being compromised,
    - be used for different purposes (e.g. communication links to different EP types).

  However, multiple certificates require additional storage resources (a typical X.509 certificate requires approximately 2 Kbyte of memory space). The above examples also imply access to secure time or a management interface to enable / disable certificates, therefore opening other potential backdoors for cyber attacks.

It is therefore suggested that each EP contains only one certificate; its lifetime is the anticipated operational lifespan of the device. Compromised devices (e.g. devices with compromised certificates) must be either discarded or re-flashed in the factory.

C. EP Certificate Format

End point authorisation (see Figure 4) is an important requirement in M2M communication, as it declares the rights of a device to connect to or to interact in a certain way with another device. For example, a base station in a smart meter deployment has the authority to retrieve meter readings from a domestic smart meter, but it is not allowed to reset the meter readings. Similar to role-based access control there must be a mechanism to declare such rights to an individual device.

Further on, a device must be able to declare its features and characteristics to another peer in a verifiable fashion.

For this purpose X.509 complements identity certificates with attribute certificates, see also RFC 3281 [15]. The former binds an identity to a public key, while the latter binds an identity to a set of attributes (Figure 6). These attributes might relate to access control (as done in Digital Rights Management) or describe some characteristics of the owner. Both certificate types are issued by specific authorities (certificate authority versus attribute certificate issuer) and have their own lifecycle.

In a smart grid / M2M context the differentiation between identity and attribute certificates needs to be revised. First of all the attributes or rights of a device will not change over its lifetime (a smart meter will always be a smart meter). Secondly, multiple certificate types would need be generated and integrated on a device prior to deployment, which results in logistical / management issues as well as resource / memory issues on the device itself.

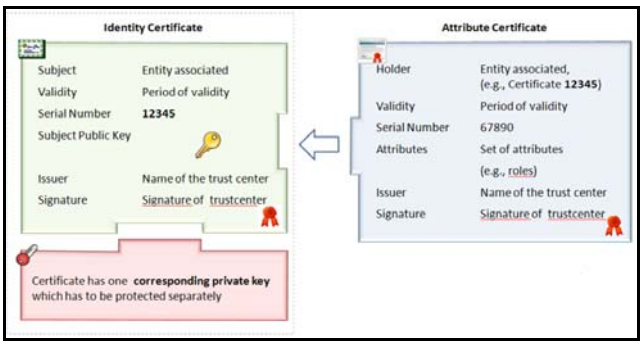

Figure 6: Identity Certificates versus Attribute Certificates

It is therefore suggested to use extension fields of the X.509 version 3 certificates (in combination with the criticality indicator that forces a device to read these fields) to encode device attributes and authorisation levels.

Current TLS implementations cannot provide EP authorisation, as this is a customised extension. However, applications can access certificate information via TLS callback functions and other APIs, so EP authorisation can be implemented on application layer.

Another problem, particular in the context of smart meters with limited processor resources, relates to the size and the complexity of digital certificates, as their DER encoding [16] is relatively inefficient and requires a complex parser. A potential alternative is the use of card–verifiable certificates (CVC), which can be found in ePassports and smart cards. CVC use a simple TLV (Tag Length Value) encoding scheme.

Likewise the underlying public-key cryptosystem has to be determined. There are 2 potential candidates, RSA and ECC. RSA is based on the factoring problem, e.g. the difficulty of factoring large integers into their prime factors. It is being widely used in PKIs for many years. Elliptic curve public key cryptosystems (aka Elliptic Curve Cryptography - ECC) in contrast are based on the assumption that finding the discrete logarithm of a random elliptic curve element over a finite field with respect to a publicly known base point is infeasible. ECC only became mainstream in recent years, but has been adopted by Suite B Cryptography, a set of cryptographic algorithms promulgated by the NSA. ECC requires significantly shorter keys than RSA to provide the same level of security, resulting in smaller digital certificates. For example, it is claimed that a 3072-bit RSA key has the same strength as a 256 ECC key or a 128-bit symmetric (e.g. AES) key.

While ECC seems to be the better choice, there are some unresolved patent and licensing issues around some EC algorithms.

D. The CA Hierarchy

Trust in today's internet is provided by more than 600 publically operating certification authorities, which are in turn

interconnected via CA hierarchies. Such a tree-like hierarchy consists of root CAs with self-signed certificates on the top and a set of intermediate CAs, whose certificates are signed either by another intermediate CA or a root CA. To facilitate the process of verifying a "chain" of trust, every certificate includes the fields "Issued To" and "Issued By". This network of trust allows in principal every device certificate issued by any CA to be validated as part of the TLS handshake. However, recent high-level breaches in CA organisations (like Comodo in 2011) [17] and the theft or generation of counterfeit certificates has shown that this network of trust has some significant flaws.

A smart grid deployment is only operational within its own perimeter, e.g. there is no need to issue certificates that can be globally validated. Also a utility company or its PKI proxy must tightly control the generation of EP certificates (to avoid the generation of counterfeit certificates that would become instrumental in a cyber-attack) while giving suppliers and system integrators the ability to issue certificates on-the-fly.

Therefore it is suggested to use a 2-tier CA hierarchy consisting of a root CA and a set of intermediate CAs. Each iCA is used by a defined set of integrators / suppliers, while being in full control of the utility or its CA proxy.

Another problem relates to the process, in which certificate are issued and generated for EPs. EPs based on embedded devices are not able to generate their own public / private key pairs, as they don't have sufficient entropy (e.g. their random number generators are too deterministic). Therefore the registration authority as the interface between the device and the CA has to step in and provide such information. It is important to note that the RA has to dispose any generated key material after the certificate has been issued to the EP, as otherwise the integrity of the entire deployment could be compromised.

Likewise the RA requires a suitable interface to transmit key materials securely back to the device (for an embedded EP a JTAG interface could be used) as well as a sound mechanism to acquire device-specific attributes (like its MAC address, device capabilities etc.) which are inserted into the EP's certificate [18].

E. Certificate Validation

Smart grid network deployments must be resilient from external cyber-attacks and are therefore isolated from the internet as well as being self-contained. This is accommodated by the above CA hierarchy, which allows for a straight forward certificate validation during the TLS handshake:

- Each EP has a copy of the (self-signed) root CA certificate, as well as a device certificate and a copy of its iCA certificate.
- During the initial handshake both EP exchange their device certificates. If both have been signed by the same iCA, their validation is straight forward.
- In situations where devices received their certificates from different iCAs, their certificates will be swapped and validated using the root CAs public key.

A certificate can be invalidated (e.g. revoked) by a PKI before its expiration time, for example if the private key that correspondents to the certificate's public key has been compromised (Figure 7).

It is best practice to perform a certificate status check before completing the handshake, as highlighted in a recently discovered configuration flaw in the Java runtime environment: the JRE was by default configured to validate signed jar files, but the underlying certificate was not checked for revocation. This resulted in malicious Java code (signed by a compromised and revoked certificate) to be executed on client computers.

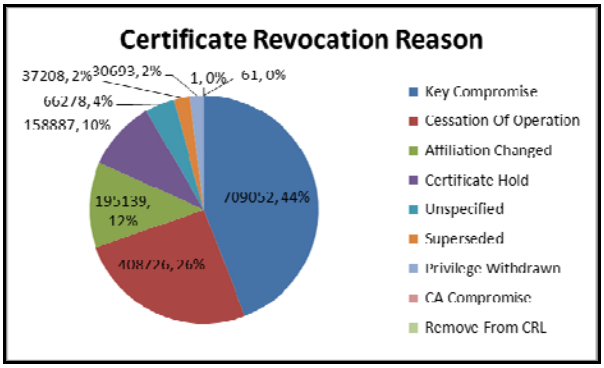

Figure 7: Typical Distribution of Certificate Revocation Reasons

X.509 provides two principal mechanisms to validate the status of a certificate (by means of a VA in Figure 4):

- A certificate revocation list (CRL) is a list of revoked certificates signed by a CA. CRLs are regularly updated with newly revoked certificates being inserted into the CRL or compiled into a delta CRL. EPs that wish to obtain revocation information need to download the CRL from some repository and process it locally.

  However, CRL can be rather large and are only updated infrequently; therefore they are not a suitable vehicle for EPs.

- The Online Certificate Status Protocol (OCSP) as defined in RFC 2560 [19] allows clients to query the status of an individual certificate in real time via an OCSP server. Revoked certificates can be added on-the-fly, making OCSP far more responsive than CRL and more suitable for real-time certificate status validation in a smart grid environment.

  However, EPs should only retain a connection to another client if the OCSP server returns an ok message for its certificate. This makes an OCSP server a single point of failure, as a DoS attack on the server will prevent it from responding to requests.

RFC 6066 [20], also called OCSP stapling, provides a solution to the DoS issue of OCSP. Here, a client requests a validation of its own cert by an OCSP server on a regular base

and keeps the response (that is time-stamped and digitally signed by the server) locally in storage. Whenever a new TLS handshake is initiated, the EP sends his own cert as well as the OSCP response to the other peer. By doing so, a temporary unavailability of an OCSP server can be compensated.

However, OCSP stapling only operates during the handshake of a TLS connection, e.g. it does support the validation of a certificate once a connection is established. Since it is not economic for an EP to terminate a connection and to re-do the handshake with a given peer, an extension of OCSP stapling should be considered that allows certificate validation for established connections. This feature could be implemented similar to the TLS Heartbeat Extension in RFC 6520, so that OSCP update queries and responses between two peers are implemented on record layer.

V. Conclusion

This paper discusses cyber security solutions for the protection of critical infrastructure with particular emphasis on smart grids. It focuses on M2M communication-specific aspects and presents a suite of adopted Internet standards and methodologies that increases the robustness and cyber resilience of smart grid deployments. The paper promotes the use of TLS in combination with various configuration settings for inter-EP communication, therefore providing message authentication, message integrity and EP authentication. It also highlights TLS constraints and possible solutions in regard to EP authorisation and OCSP stapling.

An EP authentication protocol like TLS is only as good as the digital certificates it relies on. Therefore this paper makes a number of recommendations on how X.509 certificates should be structured, used, generated and deployed. It also recommends the use of integrated identity and attribute certificates.

The recommendations outlined in this paper are the basis for two separate development projects conducted by the author's OSNA cyber security research group at NUI Galway. The first one relates to a protocol-stack independent implementation of an authentication protocol based on TLS suitable for resource-constrained embedded systems. The second project deals with a PKI architecture that issues and manages CVC-like combined identity and attribute certificates for embedded devices. Further details can be found at www.osna-solutions.com.

References

[1] J,J. Walker, T. Jones, R. Blount, "Visualization, modeling and predictive analysis of cyber security attacks against cyber infrastructure-oriented systems", IEEE International Conference on Technologies for Homeland Security (HST), 2011, p. 81 - 85

[2] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon", IEEE Security & Privacy, Volume: 9 , Issue: 3, 2011, p. 49 - 51

[3] A. Chopra, V. Kundra, P. Weiser, "A Policy Framework For The 21st Century Grid: Enabling Our Secure Energy Future", Washington, DC Government Printing Office, 2011

[4] S. Fries, H.J. Hof, M. Seewald, "Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments", Fifth International Conference on Internet and Web Applications and Services (ICIW), 2010, p. 135 - 142

[5] L. Xiang et al, "On Network Performance Evaluation toward the Smart Grid: A Case Study of DNP3 over TCP/IP", IEEE Global Telecommunications Conference (GLOBECOM 2011), 2011, p. 1 - 6

[6] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, [Online], Available: http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf

[7] NIST CIP, [Online], Available: http://www.nerc.com/pa/comp/ce/pages/actions_2013/2013_table.htm

[8] R.S.H. Piggin, "Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security", IET conference on Control and Automation 2013, p. 1 – 6

[9] E. Byre, "DNP3 Vulnerabilities Part 1 of 2 - NERC's Electronic Security Perimeter is Swiss Cheese", [Online], Available: http://www.tofinosecurity.com/blog/dnp3-vulnerabilities-part-1-2-nerc's-electronic-security-perimeter-swiss-cheese

[10] F. Hohlbaum et al, "Practical considerations for implementing IEC 62351", [Online], Available: http://www05.abb.com/global/scot/scot387.nsf/veritydisplay/b3427a5374a35468c1257a93002d8df5/$file/1MRG006973_en_Cyber_Security_-_Practical_considerations_for_implementing_IEC_62351.pdf

[11] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008

[12] S. Turner, T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, March 2011

[13] R. Seggelmann et al, "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension", RFC 6520, February 2012

[14] J. Buchmann et al, "Introudction to Public Key Infrastructures", Springer Verlag 2013, ISBN 978-3-642-40656-0

[15] S. Farrell, R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002

[16] N. Mitra, "Efficient encoding rules for ASN.1-based protocols", AT&T Technical Journal, Volume 73 , Issue 3,1994 , p. 80 – 93

[17] Comodo, "Comodo SSL Affiliate The Recent RA Compromise", [Online], Available: https://blogs.comodo.com/uncategorized/the-recent-ra-compromise/

[18] A. R. Metke, R. L. Ekl, "Security Technology for Smart Grid Networks", IEEE Transactions on Smart Grid, Volume 1, Issue 1, 2010, p. 99 – 107

[19] M. Myers et al, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999

[20] D. Eastlake, "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011

[21] NIST, "Smart Grid" [Online], Available: http://www.nist.gov/itl/antd/emntg/smartgrid.cfm