Towards a security architecture for substations

Shailendra Fuloria, Ross Anderson
Computer Laboratory,
University of Cambridge, UK

Abstract—**The security of the electricity delivery system has received much attention recently with increasing focus on Smart Grids. While substations used to be protected by concrete walls and barbed wire, today the industry is getting worried about attacks over the communication infrastructure.**

In this paper, we analyse the primary threats and present a first cut of a security architecture. We suggest security policy options for utilities, as well as protocols to do key management for substations. We conclude that the priority should be to secure the electronic perimeter of substation—as this has the maximum impact. Authentication should be done at the level of the substation station room rather the substation bays. Using cryptography for authentication inside substation bays does not have significant benefits, but is likely to bring fragility instead.

Index Terms—**Substation protection, Cryptographic protocols, Communication System Security**

I. Introduction

There has been much talk about modernising electricity transmission and distribution to support better demand response mechanisms and lower the carbon intensity of energy production [12, 23]. Electricity is perhaps the most critical infrastructure – oil, gas, banking, transport and telecommunications rely on it. When it stops, so do the others. And the last decade has seen rapid computerisation; this step has helped utilities to monitor their systems better, but the spread of IP-based networking has led to concerns about online attacks [7, 24]. Vulnerabilities could be exploited at several points in the network – at generation plants, in the transmission and distribution net- work, and even in customer meters.

Substations are particularly critical nodes; random accidents have often resulted in thousands of people being disconnected [6]. Their criticality is understood not only by governments and utilities but also by terrorist groups like the IRA who, in 1996, attempted to take down three supergrid substations that provided much of London's electricity [16]. Luckily, the attempt failed because one of the IRA members was an undercover British agent. But had the attack been successful, the results could have been similar to the six week power outage in Auckland, New Zealand, the same year where almost eighty percent of employees had to work from home or from relocated offices while most of the area's sixty thousand apartment dwellers were forced to move out for the duration [15].

Protection against immediate physical damage to the substations was the utilities' priority ten years ago. It was extended by the mandates for NERC-CIP compliance to electronic security, particularly against remotely executable attacks.

At present, the security of substations against cyber attack relies largely on boundary control devices – firewalls and VPNs, which connect the substation to the net- work control center and sometimes to other networks too. However, there has been work on mechanisms to support authentication at the individual IED level within substations. The IEC 62351 series of technical specifications was the first step to design authentication mechanisms for substation communication [18]. IEC 62351-6 aimed to build security into IEC 61850, mandating that all GOOSE and SMV messages within substation would have to be digitally signed. This was completely misconceived; the latency limit on GOOSE messages is 4ms, and even the CPUs found in modern servers are not powerful enough to perform 1024 bit RSA signatures that quickly. (Other industries have also found it hard to get information security designs right at the first attempt.) It looks like the next version of the standard will suggest the use of message authentication codes instead for integrity assurance. Further standardisation efforts in play include IEEE 1686 on substation IED cyber security capabilities [17]; IEEE P1711, a trial-use standard for SCADA serial-link cryptographic modules [21]; IEEE P1689, a trial-use standard for cyber security of serial SCADA links and IED remote access; IEEE H13 on understanding requirements and applications of the substation cyber security standards; and the AMI-SEC or Advanced Metering Infrastructure system security requirements [1]. In this paper, we challenge the assumption that authentication within a substation is generally a good thing.

Shailendra Fuloria is a PhD candidate at the Computer Laboratory, University of Cambridge. (email: Shailendra.Fuloria@cl.cam.ac.uk)

Ross Anderson is a professor of Security Engineering at the Computer Laboratory, University of Cambridge. (email: Ross.Anderson@cl.cam.ac.uk)

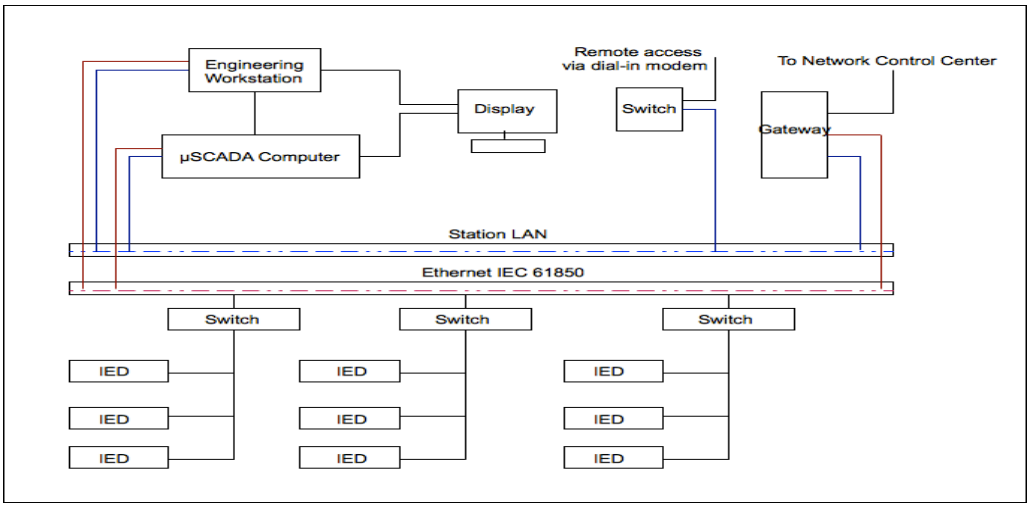

Figure 1: Substation architecture

II. Threat Model

It is against good security engineering practice to rush into the design of protection mechanisms before establishing precisely what adverse events we are trying to prevent or mitigate. In short, security architecture should be based on a threat model. For a detailed discussion on threat models for substations, see [13, 14, 19, 28].

Utilities are concerned about the following threats to substations:

1. Intruders, who could be thieves trying to steal copper [9], vandals [5], members of a protest group, organised criminals or even skilled saboteurs from a national intelligence service. While teenage vandals might be interested in doing immediate harm to the system, secret service agents might be more inclined to leave behind vulnerabilities that could be exploited at times of international tension—perhaps with simultaneous strikes at multiple substations [3, 4].

2. There might also be malicious insiders, who could be maintenance personnel from the utility, the vendor or even a third party. Not only does the insider have the knowledge of the system, but he might also have access to a number of substations before he's discovered (if he's discovered at all).

3. There can be supply chain attacks where malicious hardware or software is inserted into IEDs, perhaps during an upgrade cycle.

4. There may be attacks over the communication network, ranging from damage done as a side effect by malware aimed at other targets (as with the Blaster and Slammer worms which jammed some SCADA systems leading to precautionary plant shutdown) to targeted attacks mounted by capable motivated opponents, such as Stuxnet [8].

III. Security Architecture

The starting point for a security architecture is a secure perimeter at the substation. The attacker can cause major disruption to the substation if he gains physical access to the substation or manages to gain capability to interfere with the substation bay level LAN which connects the Intelligent electronic Device (IEDs) to the substation computer/controller (Micro-SCADA server) in the station room.

While the attacker could follow a bottom-up approach—try to enter the substation network by hacking into an IED and subsequently hack upwards to take over the substation computer, the still easier path to achieve the same result would be to first try and compromise the station level LAN and associated devices. This could be achieved by exploiting vulnerabilities in the underlying OS running the station level firewall or taking advantage of a misconfigured firewall; after all, the firewall is exposed to the outside world. Once on the LAN, the station computer and the engineering workstation (which also serves as the HMI) are the prime targets. Since most of the applications still run with system or root privilege, a compromise of the devices in the station room means compromise of the entire substation. Once an attacker has the privilege to send messages to individual IEDs, making them do unwanted things is trivial.

A. Mapping connections to and from a substation

To ensure that the perimeter is secure, it is necessary to know and document all the network connections to and from the substation—not just to the station room but also to individual field devices. These connections could include (but not be limited to) the following.

1. The substation normally has a dedicated connection via a gateway to the network control center (NCC). The substation automation host processor communicates with the NCC to receive control information from the utility's dispatcher and to upload substation data.

2. Another remote connection (possibly through a dial-up modem) enables the vendor or a third party contractor to access substation devices for diagnosis or repair work.

3. There may be connections to third-party systems for a range of services; for example, companies providing better monitoring services by rendering the raw data in a format that is easy to understand or companies providing CCTV monitoring for physical protection.

4. There may be connections to asset management systems on the utility corporate network.

5. Remote connection to bay level devices, bypassing the substation gateway and the firewall, for repair and diagnostic purposes. These could be a dedicated connection or enabled through a web server in the device.

6. There may be local radio access (wifi or bluetooth) to let repair crews access substation data from the comfort of their truck.

B. Security architecture based on 're-perimeterisation'

Given that most IEDs do not support authenticated communication, an attacker who can get access to them can generally read sensors and operate actuators. This state of affairs is likely to continue for many years because of the sheer number and diversity of IEDs in use. Protecting a substation against online attack therefore requires 're perimeterisation':

1. Communication must be funnelled through an authenticated channel to one or more boundary control devices. The obvious implementation is that the connection between the substation and the network control center should be secured using Transport Layer Security (TLS) and terminated at the station firewall. The substation gateway is best suited to run this firewall. This channel should carry not just the main operational communications but also the supporting communications with vendors, maintainers and corporate. The firewalls must be properly configured and the underlying operating systems regularly patched. If the host device is running other applications (like Adobe products) they must be regularly patched as well. A properly configured firewall between the substation and the utility's corporate network will also ensure that the devices in the substation can still talk to each other in the event of a network failure, or a denial-of-service attack on the corporate network. The substation gateway, which connects the substation network to the outside world, appears best suited to run the firewall, and must be the only path used to connect to any device in the substation.

2. Authentication and authorisation should be done at the station level rather than at individual device level in substation bays. The substation controller (substation computer/micro-SCADA server) appears best suited for this task. This must be done to ensure the integrity of the security perimeter. Some may argue that using authenticated communications for direct access to an IED bypassing the station room could make access more secure, we take the view that it will almost always be preferable to maintain the integrity of the security perimeter.

3. The enemy of security is complexity; and while direct access to an individual IED from outside the substation network might make things convenient for engineers doing diagnostics, the accumulation of such access paths over time destroys the possibility of a protectable architecture. So it should be policy that engineers wishing to access an IED must first access the station computer (either remotely through a VPN or in person inside the station room) and only get to the IED via that controllable channel.

4. If there is a need to connect an IED to another device that lies in the logical trust network of the substation but is not in the physical network, such as an off-site sensor, then that device should be brought within the logical network using a secure communications channel.

C. Using cryptographic mechanisms

Once past the security perimeter, the local area network within the substation bays should, by default, be left as it is today. There have been discussions on standards for cryptography to protect communications between the IEDs in the substation bay. There must also be clarity on what we add to the system level security by using cryptography for secure communication between the IEDs and the station computer as well as among the IEDs themselves. If someone can gain access to the LAN, then they are inside the substation and can tamper with the IEDs directly. Thus a properly monitored physical perimeter is both necessary and, in normal cases,

sufficient to protect the LAN.

Utilities in some countries may however wish to encrypt or authenticate LAN traffic for reasons of compliance with ill-advised regulations. As for utilities in well-governed countries, the one area where cryptographic protection may be relevant is where utilities decide to field wireless enabled devices in substation bays. WirelessHART and ISA100.11a enabled devices have been deployed by utilities in oil & gas, primarily for non-critical monitoring. If there were a similar move towards the adoption of wireless in substations, it would be useful to have cryptographic support. We discuss this in detail in the next section.

IV. Cryptography in Substations

Designing authentication into the protocols is just one part of communication security. Much of the hard work lies in key management over the complete life cycle of the substation. This can be achieved using either symmetric (secret-key) or asymmetric (public-key) mechanisms.

Symmetric keys are still preferred in many applications, including ATMs, prepayment meters and pay-TV [27]. Kerberos is an example of a secret-key authentication system in wide use on corporate networks; it's been supported in Windows since Windows 2000 [22, 25]. Public-key based systems are widely used in browsers to verify the server using SSL/TLS. SSH also uses public- key crypto to protect remote access to computers.

WirelessHART does specify authentication mechanisms for wireless devices in industrial networks, but does not provide much detail on key management [29]. Key management has also become a concern for vendors of smart meters – while the DLMS/COSEM set of globally acceptable standards do provide some details on authentication, they stop short of a clear specification on how to manage key material between the customer and the energy supplier of its choice [11]. With respect to substations, the IEC 62351 has now initiated efforts for technical specification to draft protocols for key management [20].

A. Symmetric key based architecture for substations

Since substations normally have a star network topology with a limited number of devices, symmetric key management system is likely to be less expensive. Each IED would share a key with the station computer or micro- SCADA server (which we shall refer to as the 'substation controller'). Each IED could come with a factory installed 128-bit AES key (which we shall refer to as the 'ignition key') that would also be printed on its packaging. To add this new IED to the substation network, the engineer would physically connect it and then type the ignition key into the controller. A join protocol would then run between the substation controller and the IED.

In the first step, the IED *Y* would send a join request to the controller, encrypted under the ignition key *m*. The random challenge *N* in this message is to let the IED verify that the controller's response is not a replay. The substation controller will decrypt this request and send back the message containing the random challenge, the device serial number, a unique device key *KY*, and the network key *KN* currently in use – all encrypted under the ignition key. The IED will confirm the receipt by sending back the random challenge *N* encrypted under the unique device key *KY*. In formal notation, the join protocol can be written as,

$$Y \rightarrow C: \quad \{Y, N\}_m$$
$$C \rightarrow Y: \quad \{N, Y, KY, KN\}_m$$
$$Y \rightarrow C: \quad \{N\}_{KN}$$

Once the join protocol is successfully completed, a green light will appear on the substation controller, which will tell the engineer that the new IED has been enrolled into the LAN. The controller will record an entry for Y in its key database containing *m* and *KY*. The IED will now use the network key *KN* to authenticate communications with the controller as well as multicast messages (GOOSE and SMV) to and from other substation IEDs in the VLAN. The unique device key *KY* would be used for device-specific operations. For example, it would be used from time to time for a key update, where the old device key is replaced with a new one:

$$C \rightarrow Y: \quad \{Y, N, KN'\}_{KY}$$
$$Y \rightarrow C: \quad \{N\}_{KN'}$$

For detailed discussion on key management using symmetric keys, see [14]

B. Asymmetric key based architecture for substations

In this approach, the ignition key *m* printed on the de- vice packaging would be the hash of an X.509 certificate, issued by either the utility or the equipment vendor. Standard public-key protocols like TLS are used to establish a secure channel for communication between the newly installed IED and the substation controller. Once a secure session has been established, the substation controller would pass the network key *KN* to the IED. The complexity of this approach would depend on the mechanism in which the IEDs acquire the certificates. There are several ways to do this. The IEDs could get their certificates and the utility's root certificate at purchase time; they could get a vendor certificate at manufacture time and use that for communication; they could get a vendor certificate at manufacture time, which must then be replaced by a utility certificate; or the certificate management could be outsourced to a commercial certification authority like Verisign. Another option is to use TLS in the

way it's used in commercial websites: here the utility's X.509 certificate hash would be embedded in devices on purchase, and *m* used simply as a logon password, with client (IED) certificates not used at all.

In the cases where client certificates installed in each IED at purchase time, each device must be brought in to a key management facility where device *Y* is provisioned with its public key *KY*, the corresponding private key KY^{-1}, a certificate $cert_u(KY)$ signed with the utility's key, and an ignition key *m* which is the hash of the certificate [$m = hash(cert_u(KY))$] printed on the device package. The root certificate of the utility is also installed in the IED so that it can verify other certificates signed by the utility's public key.

Whether we rely on client certificates issued by the utility, or a factory-installed vendor certificate, or even device passwords, device installation is physically much the same as for the secret-key case. To add the IED to the substation LAN, the engineer physically install it on the LAN and then type in the ignition key into the substation controller, initiating the join protocol. In the vendor-certificate case, the IED sends its cert to the controller:

$$Y \rightarrow C: \ cert_v(KY)$$

The controller checks the asset management database to verify that such a certificate is indeed assigned to the said IED and upon verification, establishes a secure TLS session that is used to pass on the network key *KN* to the IED. There are many possible variants; for example, the vendor certificate might be replaced by a utility certificate on installation rather than at a key management facility. For this, the join protocol would have the IED send its vendor certificate to the controller, which then forwards it to the NCC via a secure TLS session; the NCC verifies the IED's certificate and issues it a new utility certificate. Once the IED has obtained these, things proceed as before.

If the utility or the vendor finds the certificate provisioning process very complex, they could decide to out- source it to a commercial CA; but this might involve a higher lifecycle cost since the CA industry is somewhat concentrated with just a few major commercial players.

C. *Migrating from test to live*

Migrating cryptographic systems from the vendor's test environment to a live customer environment adds extra considerations. The keys used in the test environment should be changed before the system goes live. There have been numerous cases of security failure resulting from systems going live with default, or test, key material or passwords – even industries like banking that should know better [2, 10].

With the symmetric key approach, the problem may not be too acute. Even if the ignition key *m* becomes known to the engineers at the test site, there is no real attack they can perform on the live system – as once the system goes live, a new unique device key *KY* and a new network key *KN* are provisioned for each IED by the substation controller and the ignition key will not normally be used after that. Since the test engineers would not know the new de- vice and network keys, they would not be in a position to carry out an attack. Nonetheless, in an ideal world, one might use a variant of the protocol for the test environment perhaps using a one-way hash of the actual live keys.

If it is preferred to use a public key based system, the security of the ignition key is of even less concern since *m* would just be the hash of a certificate containing a public key; its value should not help a potential attacker.

D. *Identification of the 'zero-exploit boundary'*

The zero-exploit boundary is one within which there is no more security checking and an opponent can cause damage without exploiting systems or breaking cryptographic protection. In case of substations, this could exist either at the device level within substation bay or at the boundary control device. We believe that moving the zero-exploit boundary nearer to the device brings added cost with little benefits and hence, the ideal location of this boundary is at the interface of the substation station room and the substation bay. This is beneficial not only from a cost perspective but also from a safety point of view. In an emergency, any delay due to authentication and authorization at the bay level could prove hazardous.

Experience with industries like banking has shown that cryptography often adds fragility to systems if not implemented correctly. With critical substations, this would be too big a risk to take. The correct approach would be to perform all checks at the level of substation control room and leave the substation bays as they are today.

V. CONCLUSIONS

While utilities should use cryptography to secure wide area communication – the link from substations to the net- work control center, the utility's corporate network and any other third party network – it has little to offer within the substation itself. Unless the substation LAN contains wireless devices or devices outside the physical perimeter, encryption adds no material protection as an attacker with access to the LAN can just access the IEDs directly. Furthermore, encrypting the LAN traffic will add to cost and complexity; it is likely to make the system more fragile. We particularly reject the argument that it's convenient for maintenance engineers to have direct access to some IEDs without proxying their communications through the station firewall or controller. While it may be convenient in the short term to add such

hacks, it's fatal in the long term; once there are numerous separate communications channels to the substation it becomes impossible to maintain a clean perimeter.

Utilities should focus on getting the basics right. They should have a clear threat model, a well-documented security policy, and proper mechanisms to enforce that policy. Our analysis here shows that tightening up the electronic perimeter of the substation network still has the maximum impact on ensuring its security. Regular patching and properly maintained firewalls with authenticated connections into the substation should be the priority. It is only in the case of remote or radio-enabled devices that utilities should think about using cryptography on some part of the substation LAN; even then, utilities should keep it simple and pay attention to the station lifecycle.

VI. References

[1] OpenSG Users Group, *'Advanced Metering Infras- tructure Security'* at http://osgug.ucaiug. org/utilisec/amisec/default.aspx

[2] RJ Anderson, 'Why Cryptosystems fail?', in proceedings of the 1st ACM conference on Computer and communications security (1993), pp. 215-227.

[3] R Anderson, S Fuloria, 'Security Economics and Critical National Infrastructure', at Workshop on Economics of Information Security (WEIS), UCL London, June 2009

[4] R Anderson, S Fuloria, 'On the security economics of electricity metering', at Workshop on Economics of Information Security (WEIS), Harvard University, June 2010

[5] BBC, 'Warning to substation vandals', at http: //news.bbc.co.uk/1/hi/england/ southern_counties/3337185.stm

[6] BBC, 'Power supply restored after fire', at http://news.bbc.co.uk/1/hi/ england/london/7442424.stm

[7] EJ Byres. *'Network Secures Process Control'*, Tech Magazine, Instrumentation Systems and Automation Society (Oct 1998).

[8] Eric Chien, 'Stuxnet: A Breakthrough', at http://www.symantec.com/connect/blogs/stuxnet-breakthrough

[9] BBC, 'Copper theft at Sheffield substation sparks power surge', at http://www.bbc.co.uk/news/ uk-england-south-yorkshire-11558324

[10] A Collins, 'The Machines That Never Go Wrong', in Computer Weekly, 27 June 1992, pp 24 – 2

[11] DLMS User Association, 'Device language message specification', at http://www.dlms.com/

[12] European Parliament and Council, *'Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC'* , at http://eur-lex.europa. eu/LexUriServ/LexUriServ.do?uri= OJ:L:2009:211:0055:0093:EN:PDF

[13] S Fuloria, R Anderson, K McGrath, K Hansen, F Alvarez, The Protection of Sub- station Communications in proc. of SCADA Security Scientific Symposium, Jan 2010, at http://www.cl.cam.ac.uk/ sf392/publications/S4- 2010.pdf

[14] S Fuloria, R Anderson, F Alvarez, K McGrath, 'Key Management for Substations: Symmetric keys, Pub- lic keys or no keys', at IEEE conference on power systems, March 2011

[15] P Gutmann, "Auckland's Power Outage, or Auckland – Your Y2K Test Site", at www.cs.auckland.ac.nz/ ~pgut001/ misc/mercury.txt

[16] W Hope, "Britain Convicts 6 of Plot to Black Out London", New York Times, July 3 1997

[17] IEEE, *'IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities'* at http://standards.ieee.org/ standardswire/archives/sw_apr08_ email.html

[18] IEC, *'Power systems management and associated information exchange - Data and communications security'*

[19] IEC, 'Communication network and system security – Introduction to security issues'

[20] IEC, 'Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment'

[21] IEEE, *'IEEE approves substation data file standard, begins standard for substation cyber-security'* at http://standards. ieee.org/announcements/PR_ IEEEDataFileStandard.html

[22] MIT, 'Kerberos: The Network Authentication Protocol', at http://web.mit.edu/kerberos/

[23] M LaMonica, "Obama signs stimulus plan, touts clean energy", CNN, Feb 7 2009, at http://news.cnet.com/8301-11128_ 3-10165605-54.html

[24] J Meserve. *'Sources Staged cyber attack reveals vulnerability in power grid'*, CNN Sep 26 2007, at http://edition.cnn.com/2007/ US/09/26/power.at.risk/index.html

[25] R Needham, M Schroder, 'Using Encryption for Authentication in Large Networks of Computers', Communications of the ACM 21 (12): 993999

[26] NERC, 'Critical Infrastructure Protection (CIP)' at http://www.nerc.com/page.php?cid= 2|20

[27] R Anderson, 'Security Engineering A Guide to building Dependable Distributed Systems', Second edition, Wiley 2008

[28] J Weiss, M Delson, 'Cyber Security of Substation Control and Diagnostic Systems', CRC Press LLC, 2003

[29] HART communication foundation, 'WirelessHART Technology', at http://www.hartcomm. org/protocol/wihart/wireless_technology.html

VII. Biographies

Shailendra Fuloria is a PhD candidate at the Security Group, Computer laboratory, University of Cambridge. His research interests include security of industrial control systems, security of the electricity network and critical national infrastructure. Contact him at *Shailendra.Fuloria@cl.cam.ac.uk*

Ross Anderson is the professor of security engineering at the Computer Laboratory, University of Cambridge. His research interests range from security protocols and APIs through hardware tamper-resistance and critical national infrastructure to security economics and security psychology. Anderson is a fellow of the Royal Society, the Royal Academy of Engineering, the Institute of Engineering and Technology, and the Institute of Mathematics and its Applications. He's also the author of the standard textbook *Security Engineering—A Guide to Building Dependable Distributed Systems (Wiley, 2001).* Contact him at *Ross.Anderson@cl.cam.ac.uk*