Access Control and Availability Vulnerabilities in the ISO/IEC 61850 Substation Automation Protocol

James G. Wright[1] and Stephen D. Wolthusen[1,2] ⋆

[1] School of Mathematics and Information Security, Royal Holloway, University of London, Egham TW20 0EX, United Kingdom
[2] Norwegian Information Security Laboratory
Norwegian University of Science and Technology
Norway james.wright.2015@live.rhul.ac.uk,
stephen.wolthusen@rhul.ac.uk

Abstract. The ISO/IEC 61850 protocol for substation automation is a key component for the safe and efficient operation of smart grids, whilst offering a substantial range of functions. While extension standards, particularly ISO/IEC 62351 provide further security controls, the baseline protocol offers the assurances of access control and availability. In this paper a systematic study of selected aspects of the basic ISO/IEC 61850 protocol demonstrates that protocol-level vulnerabilities exist. The main finding is the development of a credential interception attack allowing an adversary, without credentials, to hijack a session during an initial association; the feasibility of this attack is proven using a formal language representation. A second attack based on a workflow amplification attack which relies on the assumptions in the protocol's substation event model, which is independent of layered security controls and only relies on the protocol's communication patterns is shown.

Keywords: Smart Grid, ISO/IEC 61850, Access Control, Amplification Attack, Substation Automation Protocol

1 Introduction

Smart grid technologies allow for more flexible generation and demand coordination whilst reducing costs with their greater bidirectional communication and control requirements [24]. However, this technological advancement degrades the "air gap" security principle that has been used in the power systems engineering community for the past few decades. The addition of networked intelligent electronic devices to the existing distribution infrastructure makes security through the obscurity of supervisory control and data acquisition (SCADA) protocols untenable, particularly since networks are increasingly interacting with internet protocols which is substantially increasing the attack surface.

Attacks against cyber-physical systems, such as electrical distribution networks, in recent history have shown that the threat is no longer a theoretical one. Whether it is a direct attack against the industrial control systems itself [7], or an attempt to remove the ability to control as in the case of Shamoon [19], or to manipulate control as seen with BlackEnergy3 [21], comprehensive strategies are needed to protect critical infrastructure systems. Whilst both the academic and industrial research communities are now focusing on solving the unique security challenges faced in the deployment of smart grid technologies, there is very little focus dedicated to checking if the security

⋆ Contact author

promises made by the various smart grid protocols hold true. Having a secured protocol could prevent some of the theorised attacks against smart grids.

The following analysis focuses on the limited security objectives that are explicitly stated in IEC61850. These are access control and accessibility. It does not look at the objectives defined in IEC 62351, the protocol which is designed to extended the security specified of the information network controlling a smart grid's substation automation. The key contribution of this paper is to show that these explicit objectives are not upheld. A credential intercept attack against the protocol's two party association model is proved, through the use of context-free grammar, which undermines access control. It is also shown that the generic substation event model can be used against the smart grid's information network. A workflow amplification attack is shown, by example, to create the conditions to deny the flow of packets across communications infrastructure.

The remainder of this paper proceeds as follows: Section 2 describes the related work in the field. Section 3 then describes the aforementioned attacks against IEC61850, before giving conclusions and a sketch of future work in section 4.

2 Related Work

Research into the cyber-physical security of power grids has been under way for over a decade, starting with North American Electric Reliability Corporation published its Critical Infrastructure Protection Cyber Security Standards [1]. However, there has been limited research into the specific threats facing individual protocols. There are plenty of taxonomies of attacks against general smart grid technologies [8, 15, 25, 27], but only since 2010 have there been taxonomies focusing on specific attacks against IEC61850 [5, 17, 18]. Most of the theorised attacks against smart grids are either derivatives of computer network exploits, or an infiltration into the smart grid's information network via compromising the affiliated corporate network. Most taxonomies put forward solutions for there proposed attacks based upon their computer network counter parts, without considering if it will conflict with the quality of service requirements of the protocols. For example to validate the authenticity of the packets passing through the computer network, IEC62351 recommends using asymmetrical encryption schemes. However, as this comes into conflict with the latency requirements for packets declared in IEC61850, IEC62351 states "*for applications using GOOSE and IEC 61850-9-2 and requiring 4ms response times, multicast configurations and low CPU overhead, encryption is not recommended*" [11].

There has been some research directly focusing on attacks using IEC61850's generic object oriented substation events (GOOSE) multicast messaging service. Hoyos *et al.* proposed a GOOSE spoofing attack where the adversary injects malicious copies of legitimate packets, but with the values in the data sets switched [6]. The aim of their attack is to get an intelligent electronic device to perform an undesirable action, like tripping a circuit breaker, by providing it with incorrect information. Another GOOSE attack authored by Kush *et al.*. They developed a denial of service attack using the GOOSE status number variable [9]. In this attack the adversary injects a GOOSE message with a higher status number than all the legitimate GOOSE messages on the network. This forces the intelligent electronic device to process this malicious message before any legitimate ones.

Substantial efforts have been made to analyse and secure the older DNP3 protocol. Although it was designed to be a SCADA protocol that could be applied across the general spectrum of critical infrastructure, proposals have been made to use it in the substation automation space. East *et al.* published a taxonomy of attacks against DNP3, which specifically distinguishing how traditional network attacks can be applied against different abstraction layers of the communications network [4]. They also proposed the use of the security promises of awareness and control for SCADA systems. Mander *et al.* developed a system to extend the traditional IP security applied to DNP3, by creating a set of rules that are based upon DNP3's data objects to make sure that only legitimate packets flow across the network [14].

Finite state machines have been used to validate the general promises of communications protocols for decades [2]; however, they have only recently been applied to security promises. Poll and Rutiter used automata, along with black box fuzzing techniques, to show that session languages are usually poorly defined leading to vulnerabilities [16]. Wood and Harang proposed a framework for using formal language theory to secure protocols, as it is better at defining the data transiting between points of a network[26].

The use of context-free grammars has been applied to various aspect of the security theatre. Sassaman *et al.* used context-free grammars and pushdown automata to create a framework for a language based intrusion detection systems [20]. Liu *et al.* used probabilistic context-free grammar to prove that an adversary could impersonate authentication server in a Point-to-Point Protocol over Ethernet protocol [10].

3 Attack Taxonomy

Below the attacks against IEC61850 that serve to invalidate its stated security objectives are described. It is assumed throughout that the attacks are instigated on a reliable communications channel that are implemented on a network substrate, such as IP.

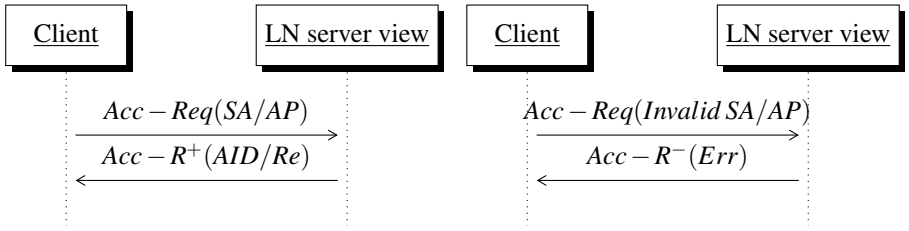
3.1 An Attack on Access Control: Credential Intercept Attack

The first security promise that was analysed was access control. This is proposed in IEC61850-5[13], as a solution to denial of service attacks against the communication infrastructure of the grid. During the investigation it was found that an attack against two party association model, described in IEC61850-7-2 section 8.3, undermines this promise [12].

An adversary, who has no login credentials on the network, is able to hijack the login credentials of legitimate user whilst they are logging into their logical node server view. This attack can be perpetrated against a client that is logging into the logical node for the first time, or who hasn't already been given a predetermined authentication parameter. This scenario is predicated on the adversary doing some passive surveillance of the communications network, as the two party association model is only instigated when a new entity is connected to the it. Once this precondition is fulfilled the attacker is able to proceed with the attack.

The Two Party Association Model The two party association model describes how a client program can connect and transfer packets with a logical node server view. The standard procedure for the model is that the client sends an access request, shortened to $Acc-Req(SA/AP)$, message to a virtual view on the logical node server, *LN*. Included within the request are the client's login credentials, which includes an authentication parameter, *AP*, and the server access point reference, *SA*.

Once the server has received this request, it then decides how to proceed. If the client's login credentials are correct then the server will reply to the client with an affirmative message, $Acc-R^{+}(AID/Re)$, that will include an authentication ID, *AID*, and the result of the attempt, *Re*. However, if the client's login credentials are invalid then the server will reply in the negative, $Acc-R^{-}(Err)$, with an error message, Err.



(a) The logical nodes affirmative response (b) The logical nodes negative response

Fig. 1: Session diagram depicting the two party association model.

The Adversary Model The adversary in the this scenario is based on upon the one described by the Dolev-Yao model[3]. This adversary is constrained by the following requirements:-

- The adversary can see all packets passing between the client and the LN server
- The adversary cannot send any message that they have not already seen.
- The adversary has no buffer on messages they have seen. They have to send the message directly after seeing it.
- The adversary can forward and intercept packets.

Whilst there are some similarities, the reason that this model doesn't duplicate the Dolev-Yao model is the protocol being attacked is a SCADA protocol rather than a cryptographic one.

The Attack premise The attack happens by combining the two potential responses of the server into one session. It begins when the client sends a legitimate login request to their own virtual view of the LN server. The adversary sees the client's packet go through their intercept and then sends a invalid login attempt to their own server view. When the client's view responds in the affirmative with the authentication ID, the adversary intercepts this packet. When the adversary's view replies in the negative, the

adversary forwards the packet with the error message to the client. After this the client cannot use their login credentials.

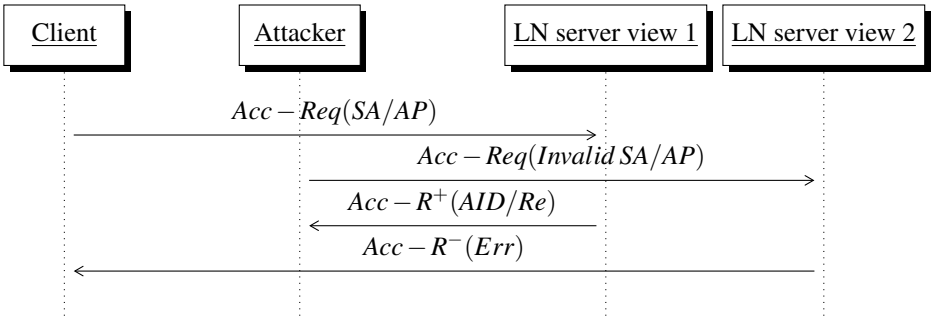


Fig. 2: Session diagram of the proposed attack.

The Automata [22] Figures 3 and 4 depict the automaton modelling the process of one client logging in, and the union of two one client automata to form one that can model two users logging in simultaneously. The two user automaton allows the depiction of the attack described in the previous section. In the two person automaton S represents the standby state, C represents the check state, and A represents the awaiting state.

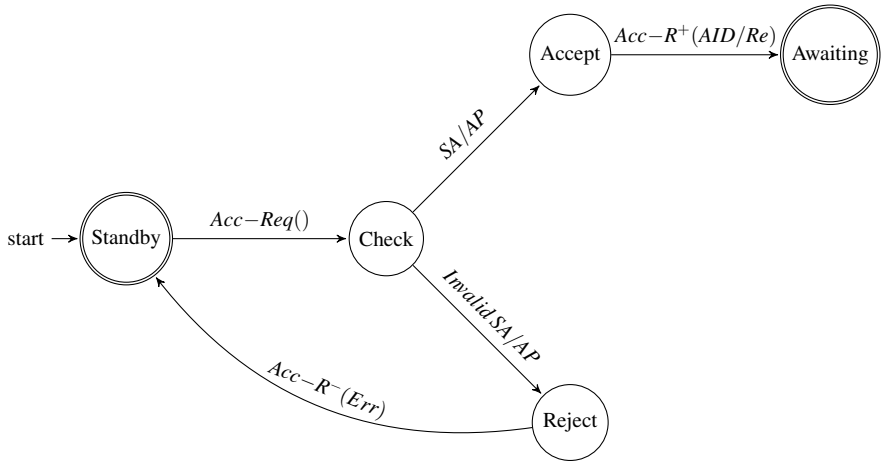


Fig. 3: The automaton depicting one client logging into a logical node server.

The Context Free Grammar The rules that describe a legitimate message that passes through the two person automaton are as follows:-

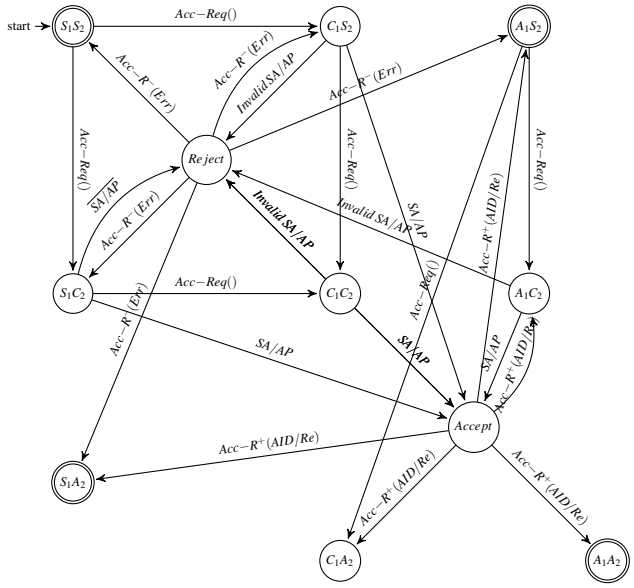


Fig. 4: The automaton depicting two clients logging into a logical node server simultaneously.

- A login attempt for one access view must be completed before a second login can be attempted.
- There can only be two successful attempts per run of the automaton.
- An infinite number of failed attempts can be made before the first successful message and between the first and final successful message.

The following rules describe the form of the message that can pass through the two person automaton that leads to an undesired result:-

- The adversary can only duplicate a message that has passed their intercept.
- The adversary's duplicate message can only be sent immediately after seeing it. They have no buffer.
- The adversary's '$Acc-Req()$' must come before the client's 'AP/SA' is processed by their login view.
- The adversary can only send invalid SA/AP credentials. This is to make sure it ends up in the state they desire (S_1A_2 or A_1S_2)
- The legitimate user cannot login after the attacker has intercepted their credentials.

The objective of the adversary is to make sure that the automaton is driven through the C_1C_2 state. This collision state represents the adversary's intercept where they hijack the authentication ID and forward their error message.
The context free grammar that represent the above rules are as follows:-

$$
\begin{array}{c}
S \rightarrow TATV|TWTW|TV|TW \\
R \rightarrow Acc-Req() \\
V \rightarrow Invalid\,SA/AP\,Acc-R^{-}(Err) \\
W \rightarrow SA/AP\,Acc-R^{+}(AID/Re) \\
T \rightarrow RU \\
U \rightarrow VT|\varepsilon \\
A \rightarrow W|RVW|RWV
\end{array}
$$

Mapping to IEC61850-7-2 The above grammar maps to the two party association model in the following way:

- Rule S: Presents the four different message types. From left to right.
  1. Is the comprised attack form. If the attack is not attempted this leads to $n = 0...$ failed attempts, followed by a successful login and then another $n = 0...$ failed logins. However if rule inserts either 'rVW' or 'RWV' instead of 'W', then the undesired form of the message begins. This leads to two '$Acc-Req()$' messages in a row. They can both be seen as undesired as the attacker controls all messages passing through its intercept.
  2. A word with two successful logins with $n = 0...$ failed messages before the first and between the subsequent successful logins.
  3. $n = 0...$ failed logins.
  4. $n = 0...$ failed logins followed by one successful message.
- Rule R: Maps to the request message parameter.
- Rule V: Maps to the incorrect form of 8.3.2.2.2.1, the server access point reference, and 8.3.2.2.2.2, the authentication parameter. Followed by 8.3.2.2.5, response showing the failed attempt error, which "*shall indicate that the service request failed*".
- Rule W: Maps to the correct form of 8.3.2.2.2.1, the server access point reference, "*which shall identify the server, with which the application association shall be established*", and 8.3.2.2.2.2, the authentication parameter, "*for this application association to be opened*". Followed by 8.3.2.2.3, response showing the successful login returning the authentication ID, which "*may be used to differentiate the application associations*", and request message, which indicates "*if the establishment of the application association was successful or not*".
- Rule T: Is the rule that facilitates the $n = 0...$ repeats of the failed login, or it provides an '$Acc-Req()$' packet before terminating the loop.
- Rule U: Provides the terminals to facilitate rule 'T'.
- Rule A: Is the production rule for the attack. From left to right.
  1. Facilitates the normal success message stuck between to infinite failed attempts.
  2. Two '$Acc-Req()$' packets followed by a failed login attempt and then a successful login.
  3. Like 2, but the error and success messages are reversed.

  2 and 3 are the undesired message forms

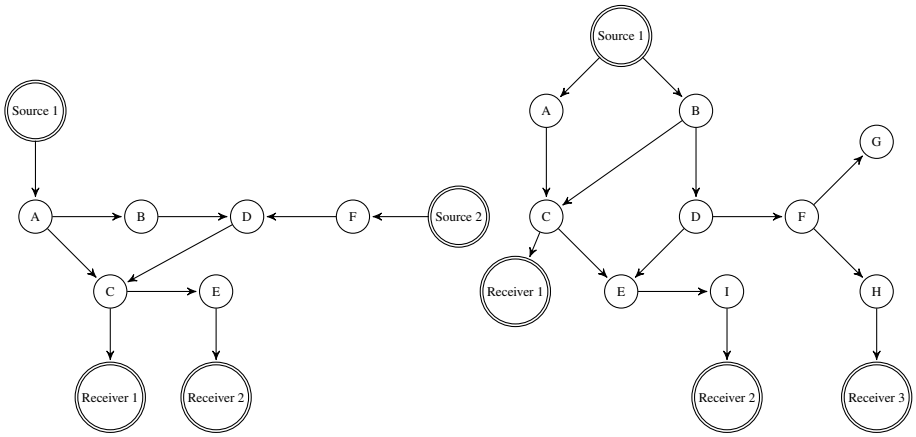
The above shows that the security promise of access control does not hold for the two party association model.

3.2 An Attack on Availability: Generic Workflow Event Amplification Attack

The second security promise that was analysed was that of availability of service. This promise is proposed in IEC61850-5 section 13 as the general message performance requirements. During the investigation it was found that an attack using the generic substation event class model, as described in IEC61850-7-2 section 15, could be used to create a denial of service of attack to undermine this promise.
The aim of the adversary in this scenario is to degrade the performance of packet transfer between points on the smart grid topology to below the acceptable standard. The adversary achieves this by sending messages that connects additional subscribers or topological branches to a LN's generic substation event subscriber list. This leads to the routers and LNs on the network having to process, and potentially discard, extra messages. Whilst the analysis allows for the calculation of the number of extra bits processed by the grid, it doesn't cover the additional latency. This is due to the amount of time for a computation to take place on a LN being beyond the scope of IEC61850.
This analysis assumes that generic substation event model has been implemented on PIM multicast framework that has been applied to a network substrate that supports it.

The Generic Substation Event Class Model The generic substation event class model describes the way a LN can broadcast data regarding its current, or changing, status to the devices that subscribe to its announcements. It is based on a producer/subscriber multicast model, and is implemented as an unidirectional process. There are two types of message in this model. Firstly, the GOOSE message, that is used to broadcast the LN's data, and the second is the generic substation state events (GSSE) message, which broadcasts any changes in state. When a LN is connected to the network it sends a GOOSE message that announces to devices its current status.
A LN on a generic substation event network will only check to see if the message it has received is a duplicate of a previous message, or if parts of it are missing. The method used to check for this is, again, beyond the scope IEC61850. In this analysis it is assumed that the logical node does not have access to the complete address space of the network and the packets received aren't cryptographically signed.

PIM multicast[23] In PIM sparse mode when a receiver issues a join request to be added to the network, a reverse path forwarding (RPF)check is triggered. A PIM-join message is sent toward rendezvous point (RP), in Figure 5a that is *D*. The join message is multicast hop by hop upstream to the all the PIM routers until it reaches the RP. The RP router receives the PIM-join message and adds it to the outgoing interface list. The same process is done for when a router wishes to leave the network, but instead sends a PIM-prune message. When a source is added, it multicasts a PIM-register message and sends them by means of unicast to the RP router.
In PIM dense mode the outgoing interface list is created by the source sending out a PIM-flood message periodically. This registers all devices on the network to the list. If a receiver no longer wishes to be on the list, it sends a PIM-prune message upstream to the source, which then removes it from the list. If a new receiver wishes to join before the next PIM-flood, they can send a PIM-graft message to the source to be added.



(a) A sparse topology. (b) A dense topology.

Fig. 5: Examples of PIM multicast system topology.[23]

The Adversary Model The adversary model is the same as the one described in section 3.1, however this adversary has a buffer so they are not required to send messages they have discerned straight away.

The Attack premise The attack is predicated on the adversary performing some passive surveillance on the communications network. Through the adversary's observation they decide which branch or LN they which to attach to the LN's subscriber list, and which type of PIM network it is. They also discern the logical node's specific application ID, which is required for subscribers to receive the GOOSE messages. The adversary sends either a PIM-flood or PIM-graft, for dense PIM networks), or PIM-join or PIM-register for sparse PIM-networks. The next time the publisher LN sends out a generic substation event message to the network the LNs that have been maliciously subscribed to the network will receive messages they weren't expecting. As they have no access to the address space they cannot tell whether they were meant to receive the message.

The Workflow Amplification factor The workflow amplification factor describes the ratio of messages produced to messages the adversary sent to initiate the attack in the number of bits.

$$\text{Amplification factor} = \frac{\text{Message produced as a consequence of the attack}}{\text{Messages sent by the adversary}} \tag{1}$$

The amplification factor for a GOOSE message is,

$$\text{Amplification factor}_{\text{GOOSE}} = \frac{A + \text{length of data set} + \text{data set}}{B + C}, \tag{2}$$

where is $A = 187$, $B = 65$, and $C = 4 or 32$ depending on whether the adversary chooses to edit the PIM message type, or create a new PIM message.

For a GSSE,

$$\text{Amplification factor}_{\text{GSSE}} = \frac{D + (2 * \text{length of data set})}{B + C}, \tag{3}$$

where $D = 170$

Examples Below are example calculations given for the workflow amplification factor for an adversary instigating the attack from various points in the networks depicted in figures 5*a* and 5*b*. All of the below examples takes the average number of status logical node variables, which is three, as the length of the data set. As the status variables are usually a boolean variable type, it is assumed for these calculations that they are boolean. For the purpose of these examples the adversary will create a whole new PIM message for their attack.

	AF_{GOOSE}	AF_{GSSE}
Case 1	3.96	3.63
Case 2	23.75	22.14
Case 3	11.87	11.07

Case 1 is set in the depicted dense PIM network. In this case the adversary has chosen to connect router *I* to the network, so to send malicious messages to *Receiver* 3. Case 2 is when the adversary connects a new source to the network.
Case 3 is the attack scenario applied to the sparse PIM network example. In this instance the adversary connects source 2 to the network to send malicious messages to both *Reciever* 1 and *Receiver* 2. In the case of adding another receiver to the network, the amplification factor would be the same as case 1.

4 Conclusion

The above analysis has shown that the explicit security promises of IEC61850 are not upheld throughout the protocol's technical specification. A credential intercept attack has been developed and proved using context-free grammar against the two party association model. This attack undermines the promise of access control, and would allow the adversary to potentially completely control a logical node if the they intercepted someone with administrative privileges. This scenario would allow them to cause physical damage to the smart grid, for example they could trip circuit breakers and cause undue stress on the distribution network. The second attack developed undermined the security promise of accessibility. It was shown by example that a workflow amplification type denial of service attack could be instigated against an intelligent electronic device by an adversary generating a malicious message that would connect the target node to a GOOSE subscriber list that it did not want to receive messages from. The denial of service comes from the intelligent electronic device having to process more messages than it was expecting. The scale of the amplification factor of the attack is proportional to the number of nodes and routers that have to process the extra malicious messages.
Although the attacks mentioned above are limited to IEC61850, there is a reasonable

likelihood that other smart grid protocols, such as DNP3, will also be found deficient when upholding their security promises. The above methodologies can be used to perform the same analysis on these protocols to develop, and attempt to mitigate, such attacks.

Progressing onwards from the above analysis the intention is to see if there are any other protocol models that contain flaws that would undermine the security promises we have access to. The next vector of attack that has been considered is to see if we can get a client and/or the logical node server to be uncertain what state it is in due to an interruption in the communication channel. It is hoped that it will be possible to formally verify theses future attacks with a context-free grammar approach
Once this line of inquiry has been exhausted, the focus of the investigation will proceed to see if the attacks that have been discovered can still be executed when IEC62351 has been used to secure IEC61850.

5 Acknowledgement

This work is supported by an EPSRC Academic Centres of Excellence in Cyber Security Research PhD grant.

References

1. NERC implementation plan for cyber security standards CIP-002-1 through CIP-009-1. Technical report, NERC, 2006.
2. D. Brand and P. Zafiropulo. On Communicating Finite-State Machines. *Journal of the ACM*, 30(2):323–342, April 1983.
3. D. Dolev and A. Yao. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, Mar 1983.
4. S. East, J. Butts, M. Papa, and S. Shenoi. *A Taxonomy of Attacks on the DNP3 Protocol*, pages 67–81. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
5. A. Elgargouri, R. Virrankoski, and M. Elmusrati. IEC 61850 Based Smart Grid Security. In *2015 IEEE International Conference on Industrial Technology (ICIT)*, pages 2461–2465, March 2015.
6. J. Hoyos, M. Dehus, and T. X. Brown. Exploiting the GOOSE Protocol: A Practical Attack on Cyber-Infrastructure. In *2012 IEEE Globecom Workshops*, pages 1508–1513, Dec 2012.
7. S. Karnouskos. Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, pages 4490–4494, Nov 2011.
8. C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, and Y. Jin. Cyber-Physical Systems: A Security Perspective. In *2015 20th IEEE European Test Symposium (ETS)*, pages 1–8, May 2015.
9. N. Kush, E. Ahmed, M. Branagan, and E. Foo. Poisoned GOOSE: Exploiting the GOOSE Protocol. In *Proceedings of the Twelfth Australasian Information Security Conference - Volume 149*, AISC '14, pages 17–22, Darlinghurst, Australia, Australia, 2014. Australian Computer Society, Inc.
10. F. Liu, T. Xie, Y. Feng, and D. Feng. On the Security of PPPoE Network. *Security and Communication Networks*, 5(10):1159–1168, October 2012.
11. TC 57 Power Systems Management and Associated Information Exchange. Power Systems Management and Associated Information Exchange, Data and Communication Security. IEC standard 62351. Technical report, International Electrotechnical Commission, 2007.

12. TC 57 Power Systems Management and Associated Information Exchange. Communication Networks and Systems for Power Utility Automation - Part 7-2: Basic Information and Communication Structure - Abstract Communication Service Interface. IEC standard 61850-7-2. Technical report, International Electrotechnical Commission, 2010.
13. TC 57 Power Systems Management and Associated Information Exchange. Communication Networks and Systems for Power Utility Automation - Part 5: Communication Requirements for Functions and Device Models. IEC standard 61850-5. Technical report, International Electrotechnical Commission, 2013.
14. T. Mander, F. Nabhani, L. Wang, and R. Cheung. Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security. In *2007 IEEE Power Engineering Society General Meeting*, pages 1–8, June 2007.
15. Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Physical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE*, 100(1):195–209, Jan 2012.
16. E. Poll, J. D. Ruiter, and A. Schubert. Protocol State Machines and Session Languages: Specification, implementation, and Security Flaws. In *2015 IEEE Security and Privacy Workshops (SPW)*, pages 125–133, May 2015.
17. U. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, and J. C. Tan. Security analysis and auditing of iec61850-based automated substations. *IEEE Transactions on Power Delivery*, 25(4):2346–2355, Oct 2010.
18. M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail. A review of Security Attacks on IEC61850 Substation Automation System Network. In *2014 International Conference on Information Technology and Multimedia (ICIMU)*, pages 5–10, Nov 2014.
19. Kaspersky Lab's Global Research and Analysis Team. Shamoon the wiper copycats at work. `https://securelist.com/blog/incidents/57854/shamoon-the-wiper-copycats-at-work/`.
20. L. Sassaman, M. L. Patterson, S. Bratus, and M. E. Locasto. Security Applications of Formal Language Theory. *IEEE Systems Journal*, 7(3):489–500, Sept 2013.
21. U. Shamir. Analyzing a new variant of blackenergy 3 likely insider-based execution. Technical report, SentinelOne, 2016.
22. M. Sipser. *Introduction to the Theory of Computation*. International Thomson Publishing, 1st edition, 1996.
23. Cisco systems. Ip multicast technology overview. `https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html`.
24. W. Wang and Z. Lu. Survey Cyber Security in the Smart Grid: Survey and Challenges. *Computer Networks*, 57(5):1344–1371, April 2013.
25. D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde. Protecting Smart Grid Automation Systems Against Cyberattacks. *IEEE Transactions on Smart Grid*, 2(4):782–795, Dec 2011.
26. D. K. N. Wood and D. R. E. Harang. Grammatical Inference and Language Frameworks for LANGSEC. In *2015 IEEE Security and Privacy Workshops (SPW)*, pages 88–98, May 2015.
27. Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang. Impact of Cyber-Security Issues on Smart Grid. In *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, pages 1–7, Dec 2011.