Initial Project Plan

‘Secure Smart Grid Infrastructure’

Cardiff University

School of Computer Science and Informatics

Module Code: CM2302

Module Title: One Semester Individual Project

Author: Fraser Orr

Student Number: 1719368

Supervised by: Neetesh Saxena

Moderator: Hantao Liu

Project Description

Brief Description

This Project aims to look at the communication between Intelligent electronic devices (IEDs) and the security risks surrounding them and the critical infrastructure they are used in. Through research and testing a prototype should be made to model proposed solutions for various communication types found in a smart grid system and the problems they face. The challenge of this project is to find an elegant solution that will provide security without hindering the operation of the smart grid.

Background

The power grid is a critical infrastructure and would provide tempting targets for sophisticated and well-equipped attackers. As smart grids slowly become more and more widely used it is important to understand the protocols being used for communication, their constraints and vulnerabilities. There is currently a lot of concern over the vulnerability of critical infrastructure and what damage an attack on such infrastructure would do.

According to a report from Lloyd's and the University of Cambridge's Centre for Risk Studies, Business Blackout Attackers able to inflict physical damage on 50 generators which supply power to the electrical grid in the North-eastern US including New York City and Washington DC would trigger a wider blackout which leaves 93 million people without power the Insurance claims arise in over 30 lines of insurance. Total insured losses are estimated in excess of $20bn, rising to $70bn+ in the most extreme version of the scenario. [1]

This is a new problem as legacy utility communication was immune to security threats as most of its communication occurred through private networks and its communication protocols were secured through security vis obscurity principle however due to standardisation of protocols means this principle is on longer an effective security measure.

Communication between IEDs is handled by IEC 61850. IEC 61850-1 One of the main objectives of the IEC 61850 communications standard is to provide a set of standard model structures for data and rules defining how to exchange these data. IEDs from different manufacturers that comply with these model definitions can then understand, communicate, and interact with each other [2]

There are 3 main types of communication I will be looking at that are in current use. Manufacturing Message Specification (MMS), Generic Object-Oriented Substation Events (GOOSE) and Sampled Measured Values (SMV) [3]. The MMS is an ISO 9506 standard that is used to transfer real-time process data and control information between the network devices, such as IED and the HMI (Human Machine Interface) [3], It follows a client-server model. GOOSE however follows a publisher-subscriber model for the asynchronous multicast communication, as it is an event driven message. SMV also follows a publisher-subscriber model and is used for asynchronous multicast communication with voltage and current values [3]. The multicast messages use MAC addresses for the communication via bridge routing and do not used IP=based routing.

The publisher subscriber architecture is vulnerable against Man-in-the-middle, replay and impersonation attacks. The system also suffers from the issues of the publisher (sender) authentication, subscribers (receivers) authorization, and data integrity [3].

Aims and Objectives

1. Research the 3 types of messages sent over a smart grid including their content, time requirements and transportation protocols.
    a. Manufacturing Message Specification (MMS)
    b. Generic Object-Oriented Substation Events (GOOSE)
    c. Sampled Measured Values (SMV)
2. Research and Implement a model of secure ways to transport the different messages types across the smart grid
    a. Requirements should be based of initial research
    b. If possible different types of secure communication should be used for direct comparison.
    c. The prototype must correctly reflect the architecture of the smart grid it represents.
3. Test the secure transportation modes and produce an analysis of the time and CPU requirements per method.
    a. The testing should include multiple sizes of smart grids to test the scalability of proposed solution.
    b. Previously known vulnerabilities such as Man-in-the-Middle attacks should be performed against the prototype.
4. Produce the final report which should include secure methods for each communication types and finding from the research.
    a. Justification should be provided for all proposed solutions as to way they are viable.
    b. Full limitations, system requirements and assumptions should be mentioned.

Work Plan

Week 1 – Deliverable: Initial Plan due 03/02/2020

- Meet with Supervisor to discuss aims and objectives of the project
- Start and complete Initial plan
    - Project Description, Aims and Objectives and Workplan

Week 2

- Meet with supervisor to discuss further research and direction of project
- Research communication types mentioned, related works and known vulnerabilities
- Begin building concrete requirements for implementable solutions

Week 3 – Deliverables: Complete requirements for all 3 communication types.

- Discuss completed task with supervisor
- Begin to Introduction to dissertation covering covered research and new deliverable requirements for proposed solution.
- Further research into solutions based of researched requirements

Week 4 – Deliverable: Introduction Write up

- From research have selected security solutions to begin implementation and testing
- Confirm solution selecting with supervisor
- Begin Implementing of the base prototype model to allow selected addition of security tools
- Moved from introduction into Background

Week 5 Deliverable: Base model prototype

- Complete base model of the communication architecture with no additional security processed applied
- Keep on track with the report write-up aim to have finished background report writing and into approach and implementation

Week 6

- Begin to implement proposed solution for 1 of the selected communication types
- Review Reports progress with supervisor, discuss any implementation problems that have been noted

Week 7

- Begin to implement proposed solution for the 2nd of the selected communication types

Week 8- Deliverable: Completed or nearly completed Implementation of report

- Begin to implement proposed solution for the 3rd of the selected communication types
- Discuss solution progress and result with supervisor

Week 9- Deliverable: working security solutions for each communication type

- Start analysis and result gathering for finished Implemented solution
- Depending on progression of implementation adjust work plan as necessary

Week 10

- Based on Results start to write up conclusion for the investigation backed with evidence acquired from the testing.
- Discuss results with the supervisor

Week 11- Deliverable: End of week completion of conclusion

- Meet supervisor to discuss the conclusion and final state of the project
- Further completion of any outstanding report work.

Week 12

- Extended implementation week in the case of unexpected delay in the implementation of any of the four stages.

Week 13

- Revise and proof-read all chapters of dissertation and make additional changes

Week 14-

- Final supervisor meeting before project hand in

Week 15 -Deliverable: Final report hand in 07/05/2020

- Make last adjustments before hand-in

References

[1] Lloyd's Business Blackout Scenario, Emergin Risk Report -2015 available at: https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/lloyds-business-blackout-scenario/

[2] IEC 61850 Standard. Available: http://www.iec.ch.

[3] Saxena, N., Grijalva, S. and Jun Choi, B. (2020). Bournemouth University Research Online [BURO] - Securing Restricted Publisher-Subscriber Communications in Smart Grid Substations.. [online] Eprints.bournemouth.ac.uk. Available at: http://eprints.bournemouth.ac.uk/31172/ [Accessed 3 Feb. 2020].

Secure Smart Grid Infrastructure

Author: Fraser Orr

Mon, 1/27/2020

TASK	PROGRESS	START	END
Research			
Write Initial Plan	100%	1/27/20	2/3/20
Create Gant Chart	100%	1/30/20	2/3/20
Research into Communicatior	10%	2/3/20	2/10/20
Solution Requirements		2/3/20	2/10/20
Begin to Introduction Write up		2/10/20	2/17/20
Further research into solutions		2/10/20	2/17/20
Implementation			
Begin Base Prototype		2/17/20	3/2/20
Background Writeup		2/19/20	2/26/20
Message type 1 Implementation		3/2/20	3/9/20
Message type 2 Implementation		3/9/20	3/16/20
Message type 3 Implementation		3/16/20	3/23/20
Implementation Write-up		2/17/20	3/23/20
Testing and Analysis			
Test and gather results from finished soluti		3/23/20	3/30/20
Superviser meeting to discuss Results		4/1/20	4/1/20
Start Conclusion Write-up		3/30/20	4/13/20
Superviser meeting to discuss conclusion		4/8/20	4/8/20
Final Write-up			
Catch up week		4/13/20	4/20/20
Revise and proof-read		4/20/20	4/27/20
Revise and proof-read		4/29/20	4/29/20
Final Adjustments		4/29/20	5/6/20
Hand In		5/7/20	5/7/20