ofgem
Making a positive difference for energy consumers

Report

Analysing the cyber-security of industrial control systems

Publication date:	27 July 2021	**Contact:**	Alan Jamieson
		Team:	Cyber regulatory team
		Tel:	020 3263 9727
		Email:	Alan.jamieson@ofgem.gov.uk

This report describes a trial of the use of attack graphs for analysing the cyber-security of an Industrial Control System (ICS) used by an operator within the Downstream Gas & Electricity (DGE) subsector.

Attack graphs provide a structure for capturing system security data which enables automated analysis of potential attack paths. Attack paths are the possible sequences of steps that cyber-attackers could take to cause harm. Understanding the exploitability of attack paths enables organisations to identify security enhancements that make it harder for attackers to do so.

Today, some organisations may use manual threat modelling and this trial was to examine whether computer aided techniques for developing and analysing attack graphs were useful for managing the cyber-security of ICS in the DGE subsector.

Status of this report

This report has been prepared by Ofgem for illustrative purposes only with the intention of providing practical assistance for security professionals within organisations operating in the Downstream Gas & Electricity (DGE) subsector.

This report is not intended to be comprehensive and is not intended as relevant guidance within the meaning of Regulation 10(4) of the Network & Information Systems Regulations 2018 [1]. Please ensure that your business obtains any appropriate legal or other advice, where relevant.

Any views or commentary provided by Ofgem do not amount to Ofgem's approval or endorsement of any particular approach and you should consider further what approaches may be suitable for your business needs and meets any relevant regulatory or other obligations.

Any reference to any organisation or services related to such person or organisation, do not constitute or imply the endorsement, recommendation, or favouring by Ofgem, or any of its employees or contractors acting on its behalf.

Acknowledgements

This report was authored by Chris Few, Head of cyber research and development at Ofgem. Ofgem wishes to thank all other parties who contributed to this report.

© Crown copyright 2021
The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the **Open Government Licence**.

Without prejudice to the generality of the terms of the Open Government Licence the material that is reproduced must be acknowledged as Crown copyright and the document title of this document must be specified in that acknowledgement.
Any enquiries related to the text of this publication should be sent to Ofgem at:
10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at **www.ofgem.gov.uk**. Any enquiries regarding the use and re-use of this information resource should be sent to: psi@nationalarchives.gsi.gov.uk

Contents

List of figures

1. Introduction

1.1. As the DGE subsector adapts to the needs of decarbonisation and digitalisation, the complexity of its control systems is expected to increase. Effective cyber risk management of the energy networks will therefore require more detailed analysis of potential cyber vulnerabilities. This analysis includes what is known as threat modelling or attack path analysis (APA). Attack graphs provide a data structure for capturing the information needed to perform APA. Attack graphs can be produced in a machine readable form enabling Computer Aided Attack Path Analysis (CA-APA).

Trial goals

1.2. In order to improve its understanding of the effectiveness of attack graphs, Ofgem ran a trial on an industrial control system used by a DGE operator. The purpose of the trial was to assess whether computer aided techniques for developing and analysing attack graphs:

1.2.1. Provided insights into system level cyber security which were not readily apparent through other techniques.

1.2.2. Were cost-effective for managing ICS cyber security.

1.2.3. Provided a means of evidencing system level cyber security to risk owners.

2. What are attack graphs?

Section summary

- Attack graphs provide a format for capturing data, needed to understand the cyber-security of a computer network.
- Analysis of attack graphs, can reveal the easiest route for cyber-attackers to compromise the system.
- The market for tools to build and analyse attack graphs is growing, but their use is not widespread.

Purpose of attack graphs

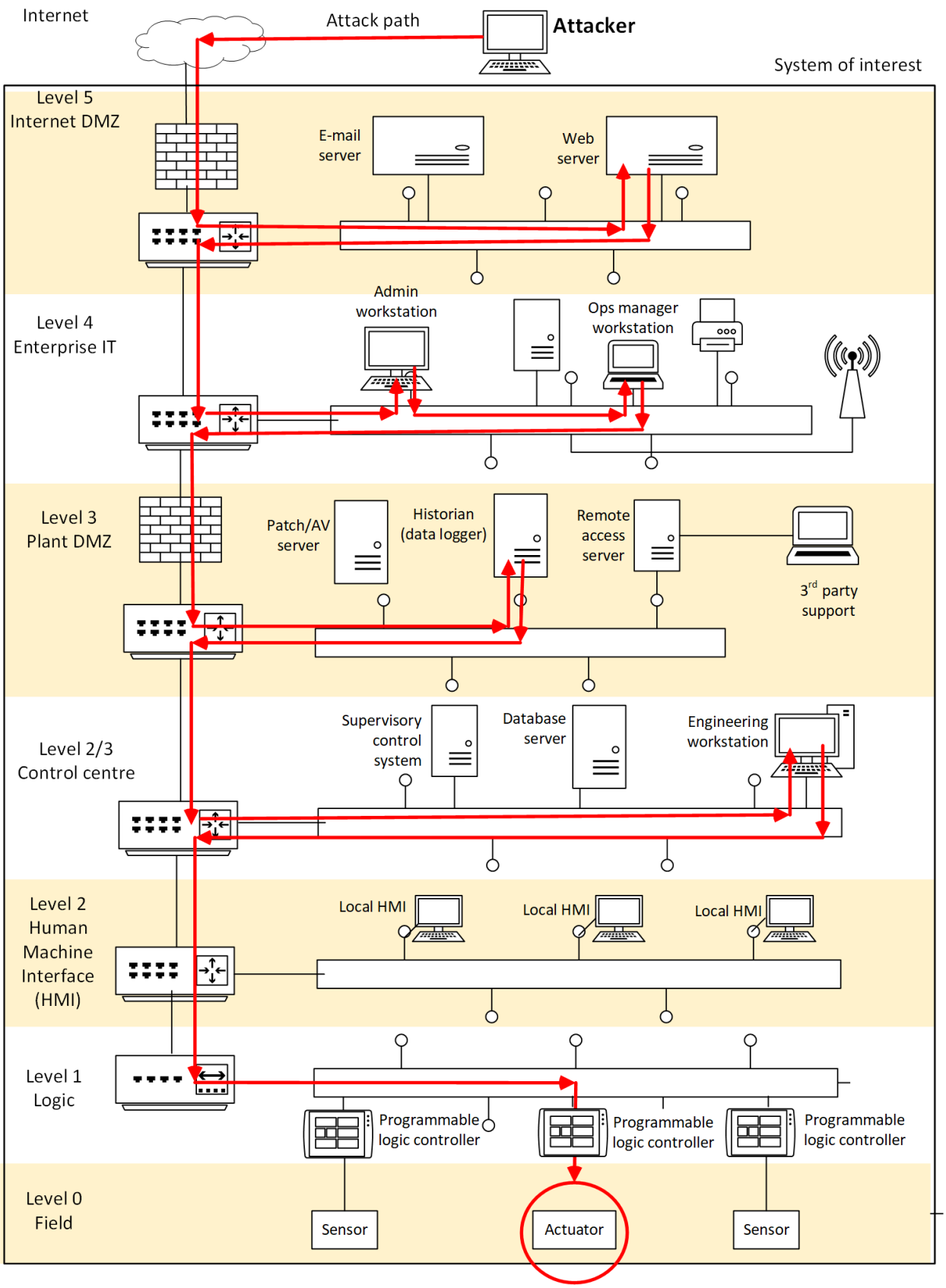
2.1. Attack graphs provide a means of capturing system security related data that enables detailed analysis of attack paths. Understanding the exploitability of attack paths is key to targeting security improvements to best effect; i.e. making the attacker's task harder. Attack graphs are not primarily used for assessing compliance with security requirements, but for answering the question, 'given my level of compliance and my implementation of other security controls, what is the easiest way for cyber-attackers to compromise my system of interest?' Other potential benefits of the use of attack graphs are described in Appendix 2.

What is an attack graph?

2.2. In order to understand how attack graphs can help identify the most exploitable attack paths, consider the ICS illustrated in Figure 1. The ICS is structured in line with the the Purdue reference architecture as detailed at [2]. The attack path marked in red assumes there is a chain of connections and vulnerabilities[1], which would enable an Internet based attacker to reach the Programmable Logic Controller (PLC) in level 1. The attacker could then manipulate commands to the generator causing disruption or damage. If we want to know how difficult it is likely to be to mount this attack, we need to capture a detailed understanding of the system configuration at each stage of possible attack paths. In particular, at each stage we want to know what types of attack steps are possible and what defences are in place, as these factors determine whether an attacker can penetrate the network.

[1] According to NIST, over 18,000 new vulnerabilities were recorded in 2020 [25].

Figure 1 - Illustration of an attack path in an industrial control system

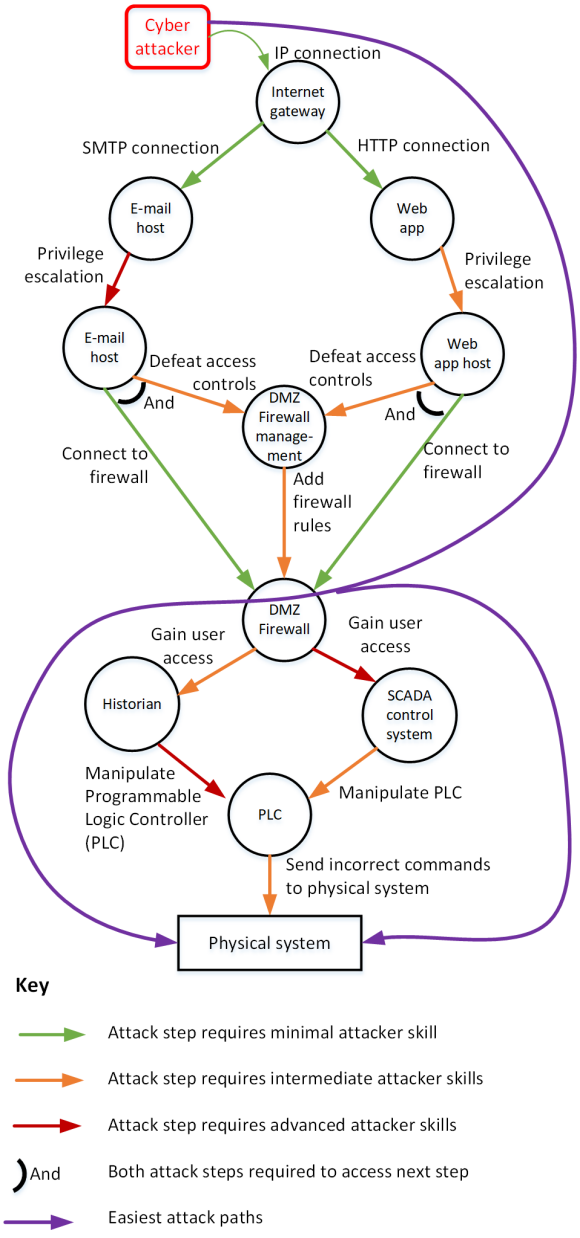


Note: DMZ = De-Militarised Zone.

2.3. Attack graphs provide a way of decomposing an ICS into the level of detail needed to find the easiest attack paths. They come in many forms and so far there is no de facto standard format. A survey in 2014 [3] gave an overview of 300 papers on the topic and many more have been written since. Typically, an attack graph consists of a set of nodes connected via links. The nodes represent a level of privilege, or access achieved by an attacker on the target network; e.g. user privileges on a particular device and application. The links represent attack steps to gain further access or privilege. Figure 2 illustrates the concept with a simple attack graph.

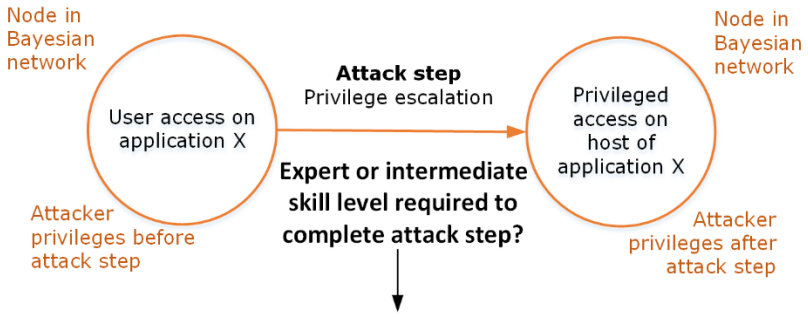
2.4. Each attack step in Figure 2 is coloured according to its level of difficulty. In this example, difficulty is defined in terms of the level of sophistication required by an attacker to complete it. This concept is elaborated by NCSC in an article on 'Rating hackers, rating defences' [4]. A widely used set of 'threat actor' sophistication levels is defined in the Structured Threat Information eXchange standard [5]. Given the level of difficulty of each attack step, the easiest attack path through the attack graph can be identified. As shown, there is an attack path from the Internet gateway to a DMZ firewall via the Web server that is accessible to an attacker with an intermediate level of skill but both onward paths to the PLC require completion of one attack step needing advanced skills. Thus, as modelled, only an advanced attacker can compromise the PLC. In practice, there will be many other potential attack paths. The attacker skill level required to complete the hardest step on the easiest attack path to critical assets is a useful indicator of the overall system security.

Figure 2 – A simple attack graph



2.5. The level of difficulty of an attack step can be derived by considering the availability of exploits and the type of defences in place. This is illustrated in Figure 3 showing privilege escalation by using either publicly known exploits or non-publicly known exploits, commonly referred to as zero-day exploits. If patches exist to defeat all known exploits, and these have been applied, then the attacker must find a zero-day exploit. This is beyond the skills of an advanced attacker as defined in STIX v2.0.

Figure 3 – Assigning attack step difficulty



	Availability of application exploits	
Application patching status	**Public exploits exist**	**No public exploits exist**
Patched	Expert	Expert
Not patched	Intermediate	Expert

2.6. Whilst the above examples are simplistic, the state of the art is much more sophisticated and continues to advance year by year. For example, a paper published in 2013 on the Cyber Security Modeling Language [6] describes a tool for building and analysing attack graphs. It was used to modela SCADA system. The model included 22 different types of assets (e.g. firewall, network, dataflow, software product); 102 types of attack steps and defensive attributes, and 32 types of relations between assets. This approach has since been extended to become the Predictive, Probabilistic Cyber Security Modeling Language (P^2CySeMoL) and has been applied to IT systems [7]. A further level of abstraction defined in the Meta Attack Language (MAL) [8] enables models to be customised to specific technology domains. An example of its application in the energy sector is described in 'powerLang: a probabilistic attack simulation language for the power domain' [9]. MAL enables increasing model fidelity and hence more accurate predictions of system security but does not address the likelihood of being attacked. 'A Bayesian Network Approach for the Interpretation of Cyber Attacks to Power Systems' [10] attempts to address this issue by incorporating data on the prevalence of specific types of attack into attack graphs.

Building attack graphs

2.7. The more sophisticated attack graphs become, the more work is required to build and maintain them. If the system of interest is in design stage, attack graphs can be built by human analysis of system design documents. This is time consuming but potentially yields a system that is secure by design with an evidence trail to support the security analysis.

2.8. If the ICS has been built, a vulnerability scanner or network monitoring tool can reveal whether there are publicly known vulnerabilities and if so, a level of difficulty can be assigned to applicable attack steps. The Common Vulnerability Scoring System [11] provides a means of translating vulnerability data into attacker skill levels required to exploit them. If an attack graph is produced in a machine readable format it is feasible to automate the import of system security data. This can be done through parsers which receive data from sources such as network monitoring tools and write data into the attack graph format. An example of this in development is an EU Horizon 2020 project, Energy Shield [12].

Analysing attack graphs

2.9. Attack graphs are designed to enable analysis of the most exploitable attack paths through a computer network to critical assets. A network of nodes and links where the links have some numerical value is widely known as a Bayesian network [13] and there are many algorithms for finding the shortest paths through them. A description and animation of Djikstra's shortest path algorithm is given in Wikipedia [14].

2.10. It should be noted that calculating the shortest path generally requires consideration of the combined effect on the attacker of all system security data. It can therefore be a more reliable guide to system security than metrics which consider component vulnerabilities independently of each other. This proposition was empirically tested and evidenced in an 'Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks [15].

2.11. An example of a common use of shortest path algorithms is in mapping software applications which calculate the shortest route and quickest time between two locations on a road network.

2.12. Understanding which attack paths are most readily exploitable is key to targeting security investment to best effect. In the simplistic example of Figure 2, the PLC can be compromised by completing a single sophisticated attack step. If we want the PLC to be protected by two independent sophisticated attack steps, care has to be taken on where to strengthen defences. One option is to improve security on the web application and its host to make privilege escalation harder. Another, is to improve security of the access controls to the DMZ management interface. Conversely, improving security on either the engineering workstation or the SCADA control system still leaves an attack path with only one sophisticated attack step.

2.13. Even without studying the details of an attack graph, its topology can be revealing. In Figure 2, the DMZ firewall forms a choke point in the sense that all attack paths pass through it. The security of the ICS is therefore strongly influenced by the security of the firewall and access to its management interface. If its security is low, it is a natural focus for security improvement. Conversely, if an ICS attack graph has no major choke points it implies that there are multiple independent attack paths of similar difficulty exploitable by a sufficiently skilled attacker. This means that no single change to the ICS will significantly increase the work required by the attacker to compromise it.

Alternative approaches for vulnerability analysis

2.14. Organisations today typically use alternative approaches to analysing and managing cyber vulnerabilities. These approaches include network monitoring, vulnerability scanning and attack trees. The benefits and limitations of these approaches are described in Appendix 3. The potential benefits of combining these approaches with the use of attack graphs is also presented.

3. Attack graph trial

Section summary

- The scope of the trial was influenced by the use of attack graphs in the energy sector in an EU Horizon 2020 research programme.
- A contract was let to develop and analyse an attack graph for a representative part of an ICS used by a DGE operator.
- The attack graph requirements were stated in terms of the information to be captured and the ability to automate analysis of attack paths.
- The attack graph was developed over 3 months using operator provided data.

Trial reference case

3.1. Despite the considerable advances by academia in modelling the cyber security of IT and SCADA systems, there has been little use of the techniques by industry. Prior to the trial described below, the most detailed example use of attack graphs within the energy sector known to the author of this report was performed under an EU Horizon 2020 research programme, SEGRID, Security for Smart Electricity Grids [16]. The SEGRID research programme describes itself as follows:

> "*The main objective is to enhance the protection of smart grids against cyber-attacks. We do this by applying a risk management analysis approach to a number of smart grid use cases (the SEGRID use cases), which will define security requirements and determine gaps in current security technologies, standards and regulations. The identified gaps and the analysis itself will give input to the enhancement of risk assessment methodologies and the development and testing of novel security measures for smart grids*."

3.2. The programme included the use of attack graphs for specifying and analysing the detailed reference architecture of the load balancing mechanism for a smart grid. This was described in the SEGRID detailed component reference model [17] and 'Load balancing of renewable energy: a cyber security analysis' [18]. The generated attack graphs each included over 500 nodes and 1000 connections between nodes. The tool used was a commercial derivative of the P^{2}CySeMoL tool developed by academics at KTH, a Swedish University.

3.3. The SEGRID use case influenced the scope and style of the trial because:

3.3.1. Smart grids are very relevant to Ofgem's interests.

3.3.2. The development and analysis of the attack graphs were particularly detailed.

3.3.3. P^{2}CySeMoL had previously been shown to produce predicted times to compromise that correlated with actual times to compromise IT systems by experienced penetration testers [7] [15].

Trial stages

3.4. The trial structured the work in 4 stages:

3.4.1. Stage 1 – Letting the modelling contract

3.4.2. Stage 2 - Information gathering

3.4.3. Stage 3 – Build system model

3.4.4. Stage 4 – Identify and analyse attack paths

Stage 1 - Letting the modelling contract

3.5. An operator in the DGE subsector offered to host a trial on whether attack graphs were useful at predicting the security of cyber-physical systems. In order to reduce the workload upon Ofgem and the operator a contract was let to build and analyse an attack graph of one of its ICS. The process for letting the contract is described in Appendix B.

Stage 2 – Information gathering

3.6. After an initial meeting with the operator, the supplier was provided with comprehensive documentation of the ICS. This included the asset register, network diagrams, firewall rule sets, mapping of applications to assets and a list of which assets would have most operational impact if compromised. This information was elaborated during subsequent stages in response to clarification questions from the supplier.

Stage 3 - Build system model

3.7. The modelling tool selected under open competition was securiCAD as described in 'Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management' [19]. It enables a user to model a computer network from a cybersecurity perspective. Initial model views can look similar to Figure 1 without the highlighted attack paths. The initial intention was to build the model on the operator site. Covid-19 prevented this and other than an onsite pre-meet just before lockdown, all modelling work was done remotely. The model was built by two consultants with combined experience in both the modelling tool and ICS security. On-line meetings were held on a weekly basis at which the supplier reported progress on the model build and typically asked for additional information to make the model more accurate. The supplier estimated 200 hours were spent developing the model. Once built, the model included 250 objects, typically each with 2 – 6 defensive attributes, and 580 relationships between objects.

Stage 4 – Identify and analyse attack paths

3.8. SecuriCAD includes an automated process for converting a model into an attack graph of similar format to that in Figure 2 and exhaustively searching through the attack graph to find all possible paths from a given attacker entry point. The possible attack paths are ranked using the style of logic illustrated in Figure 3, but assigning each attack step with an expected time to complete for an experienced penetration tester. Once the model was representative of the ICS, the automated attack path analysis provided by securiCAD was applied. The model was sufficiently complex that none of those involved were confident of predicting which attack path securiCAD would find as being most exploitable. The automated analysis found no easily exploitable attack paths. Although this was expected, it was welcome additional assurance of the system security.

3.9. The automated analysis also enabled identification of 2 specific attack steps of interest. Making these two steps harder, secured the two most exploitable attack paths and hence improved the overall system security. According to securiCAD's analysis, the predicted time to compromise by an experienced penetration tester would then be increased by a factor of 4.5. A key benefit of the tool was in creating an informed discussion between subject matter experts on whether this prediction was realistic. The prediction stimulated much analysis between the modeller, the operator cyber security lead and the control systems engineer on whether the automated analysis was correct. The absolute values of the predicted times to compromise were largely ignored, but the change in value as the hardest steps in the easiest attack paths were made harder, was of interest.

They concluded that the securiCAD analysis of the most exploitable attack paths was reasonable. This refined the operator's view on the ICS security. Although the identified attack paths were already known to the operator, recognising them as the least difficult ones to exploit gave new insights into the best options for improving system security.

3.10. An interesting result of the trial was that reducing component vulnerabilities unrelated to these attack paths made very little difference to the predicted time to compromise and hence to system security. This analysis was also considered reasonable by the operator cyber staff. This style of analysis may therefore assist in prioritising system security improvements.

4. Trial findings

Section summary

- The use of attack graphs enabled a more detailed understanding, and discussion of the cyber risks to the associated essential service, than would typically be achieved through analysis of system documentation and component level vulnerability analysis.
- Attack graphs are not a panacea for cyber risk analysis. The automated predictions should be treated with caution. Cyber expertise is required to understand their limitations and interpret attack paths.
- The use of a suitable supplier removed the need for any prior attack graph expertise by the operator.
- The general approach could be applied at the system design stage, when it is easiest to implement security improvements.

4.1. After the supplier's initial development and analysis of the model, they produced a report of the model building process, the model analysis and their findings on its usefulness. The operator then conducted some further analysis on the options for improving the ICS security. Ofgem's findings based upon reports from the supplier and operator are described below. To preserve confidentiality, the details of the attack paths themselves are not presented.

Positive findings

4.2. It was found that the process of building and analysing the model:

4.2.1. Helped to translate asset information into a model in a systematic fashion.

4.2.2. Helped facilitate detailed discussion about attack paths and consequent cyber risks.

4.2.3. Enabled risk driven prioritisation of existing vulnerabilities.

4.3. It is believed that the method trialled has potential for analysis and quantitative assessment of;

4.3.1.1. Existing systems.

4.3.1.2. New systems at design stage.

4.3.1.3. Modifications before implementation.

Limitations

4.4. The following limitations were found in the trial methodology:

4.4.1. Understanding the model is necessary for understanding the predictions.

4.4.2. It is not a silver bullet for all risk management. An ICS/OT specialist is still required to understand the model and interpret the results such that appropriate changes to designs, security controls, policies and procedures can be made.

4.4.3. The attack path analysis is highly dependent on accurately modelling the ICS.

4.4.4. Any risk analysis requires an understanding of the business consequences of cyber-attacks. This information is therefore a key input to the methodology.

4.4.5. The methodology only modelled a single type of attacker; sophisticated with high capability and dedicated to attacking from whatever the selected entry point. In practice, a wider range of attacker capabilities should be considered.

5. Conclusions

Section summary

Building accurate attack graphs requires skill, information and time. Given these, the trial indicated that computer aided analysis of attack graphs could:

- Provide security insights that were easily overlooked by other methods.
- Be cost-effective if applied early in the system lifecycle.
- Improve assurance of system level cyber security.
- Be usefully combined with other forms of vulnerability analysis.

5.1. Attack graphs are potentially powerful tools for improving cyber risk management, particularly when combined with other forms of vulnerability analysis. They enable much data to be captured into a data structure for automated analysis and a summary of its implications for cyber risks. In principle, the cyber resilience of ICS can be analysed in greater detail than humans can unaided, leading to better understanding of cyber risks and more targeted measures to protect them. The observation that securiCAD's predicted times to compromise were heavily dependent upon many details in the model, implies that reliable predictions of ICS security requires detailed analysis.

5.2. However, analysing attack graphs is far from a silver bullet. Building accurate models requires skill, information and time. The content of models can be manipulated to give a desired risk assessment. Computer aided techniques could give a false sense of precision in the system vulnerability assessment. These considerations do not mean that they are not useful; merely that their predictions have to be treated with caution.

5.3. The value for money of attack graph analysis is heavily dependent upon when in the system lifecycle it takes place. It would be most beneficial when undertaken at the system design stage for complex systems with a long expected life and a high impact if disrupted by cyber-attack. These conditions are often the case with critical national infrastructure. They increase the likelihood that the costs of attack graph analysis are recovered through reductions in losses from cyber-attack due to better targeted security measures. The approach taken in this trial in which the model was initially built from documented information could have been undertaken at the system design stage.

5.4. Attack graph analysis also captures the system configuration and the security analysis of it such that it can be scrutinised and validated by independent people and

organisations. The models and their analysis can therefore help provide assurance of system security.

5.5. As the DGE subsector embarks upon considerable investment in ICS to enable decarbonisation and digitalisation it is recommended that consideration be given to the use of attack graphs and computer aided modelling from the system design stage onwards.

References

[1] HMG, "Network & Information Systems Regulations," 10 May 2018. [Online]. Available: https://www.legislation.gov.uk/uksi/2018/506/made.

[2] T. J. Williams, "The Purdue enterprise reference architecture," *Computers in Industry,* pp. 141-158, 1994.

[3] B. Kordy, L. Piètre-Cambacédès and P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," *Computer Science Review, ,* Vols. Volumes 13–14,, pp. 1 - 38, 2014.

[4] "Rating hackers, rating defences," [Online]. Available: https://www.ncsc.gov.uk/blog-post/rating-hackers-rating-defences.

[5] Oasis, "STIX™ Version 2.0. Part 1: STIX Core Concepts," 2017. [Online]. Available: http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html#_Toc496709306.

[6] H. Holm, T. Sommestad, M. Ekstedt and L. Nordstrom, "CySeMoL: A tool for cyber security analysis of enterprises," in *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)*, Stockholm, 2013.

[7] H. Holm, K. Shahzad, M. Buschle and M. Ekstedt, "P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language; https://ieeexplore.ieee.org/abstract/document/6990572/," *IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6,* pp. 626-639, 2015.

[8] Royal Institute of Technology, Sweden (KTH), "Meta Attack Language," [Online]. Available: https://mal-lang.org. [Accessed October 2019].

[9] S. Hacks, S. Katsikeas, E. Ling, R. Lagerstrom and M. Ekstedt, "powerLang: a probabilistic attack simulation language for the power domain," *Energy Informatics,* vol. 3, 2020.

[10] D. Cerotti, D. Codetta-RaiterI, G. Dondossola, L. Egidi, G. Franceschinis, L. Portinale and R. Terruggia, "A Bayesian Network Approach for the Interpretation of Cyber Attacks to Power Systems," *Proceedings of the Third Italian Conference on Cyber Security,* vol. CEUR Workshop Proceedings 2315, 2019.

[11] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System Special Interest Group," [Online]. Available: https://www.first.org/cvss/. [Accessed 24 May 2021].

[12] Energy Shield project, "Developing the cyber toolkit that protects your energy grid," EU Horizon 2020 Research & Innovation programme under grant agreement 832907, September 2020. [Online]. Available: https://energy-shield.eu.

[13] Wikipedia, "Bayesian network," [Online]. Available: https://en.wikipedia.org/wiki/Bayesian_network. [Accessed February 2021].

[14] "Dijkstra's shortest path algorithm," [Online]. Available: https://en.wikipedia.org/wiki/Dijkstra's_algorithm..

[15] H. Holm, M. Ekstedt and D. Andersson, "Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks," *IEEE Transactions on Dependable and Secure Computing,* vol. 9, no. 6, pp. 825-837, 2012.

[16] SEGRID , "Security for Smart Electricity Grids," [Online]. Available: https://segrid.eu/. [Accessed March 2021].

[17] SEGRID, "Detailed component reference model," 26 January 2018. [Online]. Available: https://segrid.eu/detailed-component-reference-model-description/. [Accessed 30 January 2021].

[18] A. Vernotte, A. Valja and M. Korman, "Load balancing of renewable energy: a cyber security analysis," *Energy Informatics 1,* no. Article 5, 2018.

[19] M. Ekstedt, P. Johnson, R. Lagerstrom, D. Gorton, J. Nydren and K. Shahzad, "Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management," in *IEEE 19th International Enterprise Distributed Object Computing Workshop*, Adelaide, 2015.

[20] Forum for Incident Response and Security Teams, "Common Vulnerability Scoring System SIG," [Online]. Available: https://www.first.org/cvss/. [Accessed 6 July 2021].

[21] B. Schneier, "Attack trees," 1999. [Online]. Available: http://macs.citadel.edu/baniks/427/Homework/attacktrees.pdf. [Accessed 12 January 2021].

[22] NCSC, "Cyber Essentials - Requirements for IT infrastructure v2.1," August 2020. [Online]. Available: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-1.pdf. [Accessed 30 January 2021].

[23] "Cyber Essentials overview," September 2020. [Online]. Available: https://www.ncsc.gov.uk/cyberessentials/overview.

[24] "Mitre ATT&CK for ICS, Initial access," 4 December 2019. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Initial_Access.

[25] US National Institute of Standards & Technology, "National Vulnerability Database, CVSS Severity Distribution Over Time," [Online]. Available: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time. [Accessed 25 June 2021].

Appendix 1 – Abbreviations

APA	Attack Path Analysis
CA	Competent Authority
CA-APA	Computer Aided Attack Path Analysis
CAF	Cyber Assessment Framework
DGE	Downstream Gas & Electricity
DMZ	De-Militarised Zone
GPS	Global Positioning System
ICS	Industrial Control System
ITT	Invitation to Tender
KTH	Royal Institute of Technology (Sweden)
LAN	Local Area Network
NCSC	National Cyber Security Centre
NIS	Network & Information Systems
OT	Operational Technology
PLC	Programmable Logic Controller
RIIO	Revenue=Incentives+Innovation+Outputs
SCADA	Supervisory Control And Data Acquisition
STIX	Structured Threat Information eXchange

Appendix 2 – Potential benefits of CA-APA

1. This appendix describes the main benefits anticipated from CA-APA.

Assessing the attacker skill level needed to cause harm

2. For many risk owners or managers, a useful guide to system security is the level of attacker skill needed to compromise the system. This can be derived through APA, whether computer aided or not. APA is designed to reveal the most exploitable attack path which will comprise a series of attack steps each with its own level of difficulty. The difficulty of the hardest step on the easiest attack path is a good guide to the minimum attacker skill level needed to compromise the system.

Recording the security analysis

3. A limitation of human security analysis is that creating a detailed record of what was analysed is time consuming. Over the system's operational lifetime there may be many changes in security staff such that early knowledge of the system's security and vulnerability is largely lost. A detailed system model and the associated attack path analysis provides a way of preserving this knowledge.

Scalability

4. ICS quickly become too complex for a human to consider all possible attack paths. Computer aided techniques enable larger systems to be analysed in greater detail.

Applicability at the system design stage

5. CA-APA can be performed during the system design stage whilst the best options for balancing security with other business objectives are still available. It complements vulnerability scanning and penetration testing which cannot be performed until later in the system lifecycle. In combination, these techniques enable a model of the system developed at the design stage to be refined so that it more accurately represents what was actually built. The model can then be used by security staff to understand and manage the system security through its operational life.

Appendix 3 – Combining the use of attack graphs with other forms of vulnerability analysis

1. This appendix briefly explains alternative approaches to assessing the security of ICS and their limitations when used in isolation. When used in conjunction with attack graphs, they can be more powerful than any single approach on its own.

Network monitoring

2. Many open source and commercial tools are available to monitor traffic on IT and OT networks. Analysis of network traffic reveals details of devices which are sending or receiving data. From this, a picture can be produced of the network connectivity between many devices. On its own, this is not sufficient to predict the exploitability of attack paths. For example, from network monitoring alone we cannot tell whether the absence of traffic between 2 devices is enforced by network controls or arises simply because there is no need for them to communicate.

Vulnerability scanning

3. Vulnerability scanners are commonly used to enumerate known vulnerabilities in detected details. This can be achieved by searching databases for details of vulnerabilities in the detected software versions. The ease or difficulty of exploiting vulnerabilities is often captured in a score between 0 – 10 defined by the Cyber Vulnerability Scoring System (CVSS) [20]. This can provide very useful information for security managers but it has the following limitations:

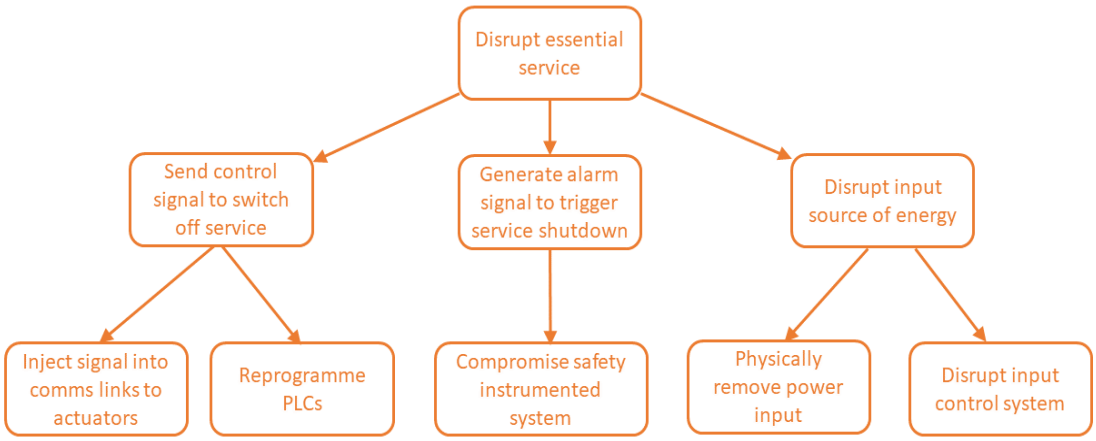
    a. For the reasons outlined above, a list of detected vulnerabilities is not sufficient to determine which are the most exploitable attack paths, and hence which vulnerabilities have most impact upon system security.

    b. The ICS has to be built before a vulnerability scanner can be used. The technique is not designed for use at the system design stage when system level vulnerabilities are best addressed.

Attack trees

4. Attack trees provide a graphical way of showing possible ways in which an attacker could compromise a target system. The concept was popularised by B Schneier in the 2000s [21]. An example simplistic attack tree is shown in Figure 4.

Figure 4 - Example attack tree

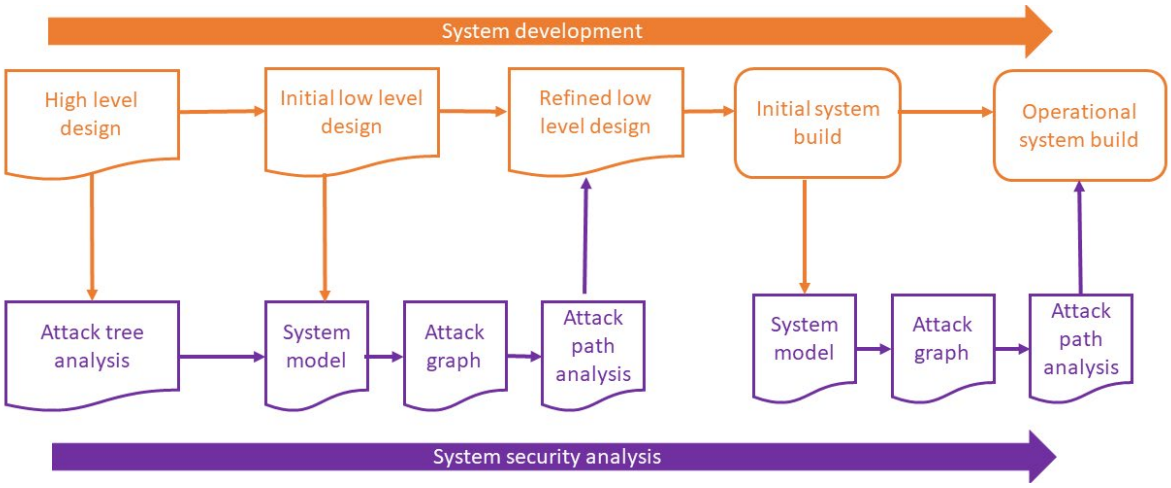


5. Workshops to develop attack trees can be very effective at improving a collective understanding of system vulnerability. They naturally stimulate ideas on how best to compromise the system of interest. However, on their own, they provide limited assurance on whether the most likely attack vectors have been identified or easy they would be to exploit. If they are solely derived from human knowledge of the system there is no independent validation of whether that knowledge was correct or complete.

Combining attack graphs, attack trees, vulnerability scanning and network monitoring

6. Although each of the approaches described above has its limitations, in combination they can complement each other. Attack trees can be developed early in the system design stage and be used to refine the low level system design. With this information, an initial system model can be produced as done from the documents used in this trial. From the model, an attack graph can be generated and analysed from which the design can be further refined. Once the system has been implemented, vulnerability scans and network monitoring can be used to validate or refine the model. The model, and the analysis of it, then provides a source of assurance of system security. It can also be used to analyse the security implications of potential system changes before they are implemented. The combination of approaches is shown in Figure 5.

Figure 5 - Combining security analysis techniques



7. Figure 5 illustrates that attack tree analysis can be undertaken when the system is at the high level design stage. Once a more detailed design is available, it can be modelled using a suitable software tool and incorporate the information in the attack tree. The resulting attack path analysis can be used to refine the system design. Once the system has been built the system model can be refined using data from network monitoring and/or vulnerability scans. Further attack path analysis can be used to the refine the system build before it enters operational use.

Appendix 4 – Letting the modelling contract

Introduction

1. This appendix is included for readers with an interest in the practicalities of letting a contract for modelling an ICS.

2. The scope of the trial was agreed with a commercial operator in the DGE subsector.

Requirements

3. The key contract requirements were to build and analyse a model of similar detail to that produced by the SEGRID project in its reference model of the load balancing control system of a smart grid. This level of detail was described in the Invitation to Tender (ITT) as including the following information.

    a. The network connected cyber-attack surface including wired and wireless network access points.

    b. The physical system boundaries; e.g. by referencing a site or zone.

    c. All the information needed to demonstrate whether or not the Requirements for IT Infrastructure [22] defined in the HMG Cyber Essentials [23] scheme have been met by the trial Operational Technology (OT) network.

    d. All application hosts.

    e. A representative sample of end user devices.

    f. Representative components from Level 0 to the Level 4 firewall in the Purdue Enterprise Reference Architecture [2] and the barriers between them.

    g. Fifty data flows as a representative sample of all system data flows.

    h. Device security configuration data such as whether patched, locked down, user authentication requirements, anti-virus software installed.

    i. Cyber assets which if modified can directly impact upon the essential service.

4. Once the model was built, the supplier was tasked with identifying attack paths, from untrusted networks or physical zones, which disrupt the essential service and rank them according to the expected ease of exploitation. Where there were gaps in the system information available, they were to show the best and worst case scenarios. They were also asked to take into account the applicable initial access vectors described by the Mitre ATT&CK for Industrial Control Systems framework [24].

Supplier selection process

5. Ofgem selected a suitable supplier for the modelling activity through open competition. Seven bids were received and assessed against weighted criteria as defined in the ITT. Although the ITT stated that use of securiCAD was not mandated, the 3 highest scoring bids all proposed using it.

Constraints

6. At the time that the model was initially built, the operator had yet to install asset discovery or network monitoring tools on the OT network. This meant that the supplier was dependent upon documentation provided by the operator. Asset discovery tools were subsequently installed on the OT network and where needed the attack graph was updated before its final analysis.

7. Had asset discovery or network monitoring tools been installed earlier, it could have changed the way the model was built. It would have been feasible to automate the import data from these tools into the securiCAD model. However, the more manual approach taken to building the model enabled human understanding of its content, accuracy and limitations.