

Cybersecurity Landscape in the Manufacturing Sector

Research Proposal - Sony UK Technology Centre
Scott Roberts - 2306895



Preamble (short story)



June 17th 2010, Belarus



- New malware discovered on a PC in Iran running Siemens industrial control software
- Malware code 20x larger than most other malware (complexity)
- Malware used four previously unseen zero-day exploits in Windows



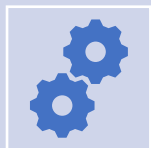
Stuxnet



Highly targeted attack – Malware only deploys when inside the Natanz uranium enrichment facility in Iran



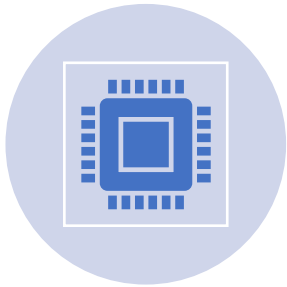
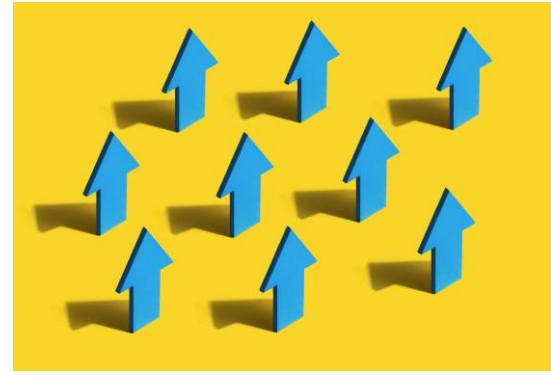
First ever discovered PLC rootkit – direct attack on industrial control systems



Specifically designed to attack the production process – damaging centrifuge hardware



Outcome



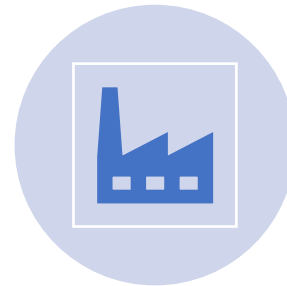
First recorded cyber attack to result in the destruction of physical infrastructure (outside of a lab)



Pushed security vendors, researchers and ICS experts to look closer at the defence of these systems



Raised awareness of attacks on physical infrastructure for the first time



More focus is needed on defending production processes in the industrial sector...



Background Rationale – Why do we need to research this?

- The manufacturing sector is at risk
- If we don't understand it, how can we defend against it?
- Better understanding = better outcomes...



Aim

To identify the **specific** cybersecurity risks that **uniquely impact** the manufacturing sector, so that our industry can **better defend itself against those risks.**

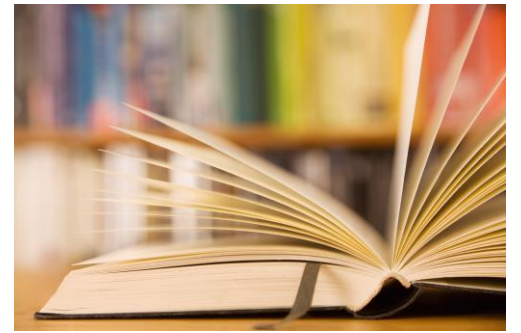


Objectives

Identify	Identify industry-specific threats – Understand our unique vulnerabilities
Evaluate	Evaluate the vulnerabilities present in Industrial Control Systems (ICS, IIoT, SCADA)
Develop	Develop specific and targeted cyber-defence strategies and guidance for manufacturers



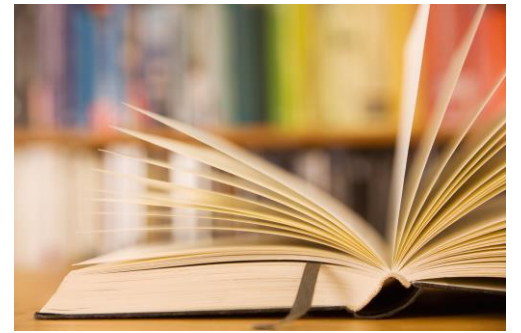
Summary of Existing Literature



- Symantec – Comprehensive technical report on the Stuxnet malware
- Gritsai et al. – A review of vulnerable SCADA Systems exposed to the internet
 - Summary: Two in five SCADA systems on the internet are vulnerable to attack by low-skilled attackers
- Leverett – Builds on this knowledge, challenging the widely held (at the time) assumption that ICS are not exposed to the internet



Summary of Existing [cont.]



- Enck et al. identified that more research into software supply chain is needed
- Vint Cerf (recognise the name?) et al. – Recommends that a specific focus is put on the safety of digital systems, especially where large machinery and human beings work side-by-side
- Further literature exploration available within the proposal document



Research/Development Methodologies



Collection – Comprehensive literature review (journals, case studies, incident reports)



Analysis – Qualitative analysis of the data



Evaluation - Thematic. Identifying patterns across manufacturing sector



Resources/Materials

Computer generated information (logs, reports, summaries)

- Firewalls
- ID(P)S
- Email Gateway

Case studies/incident reports

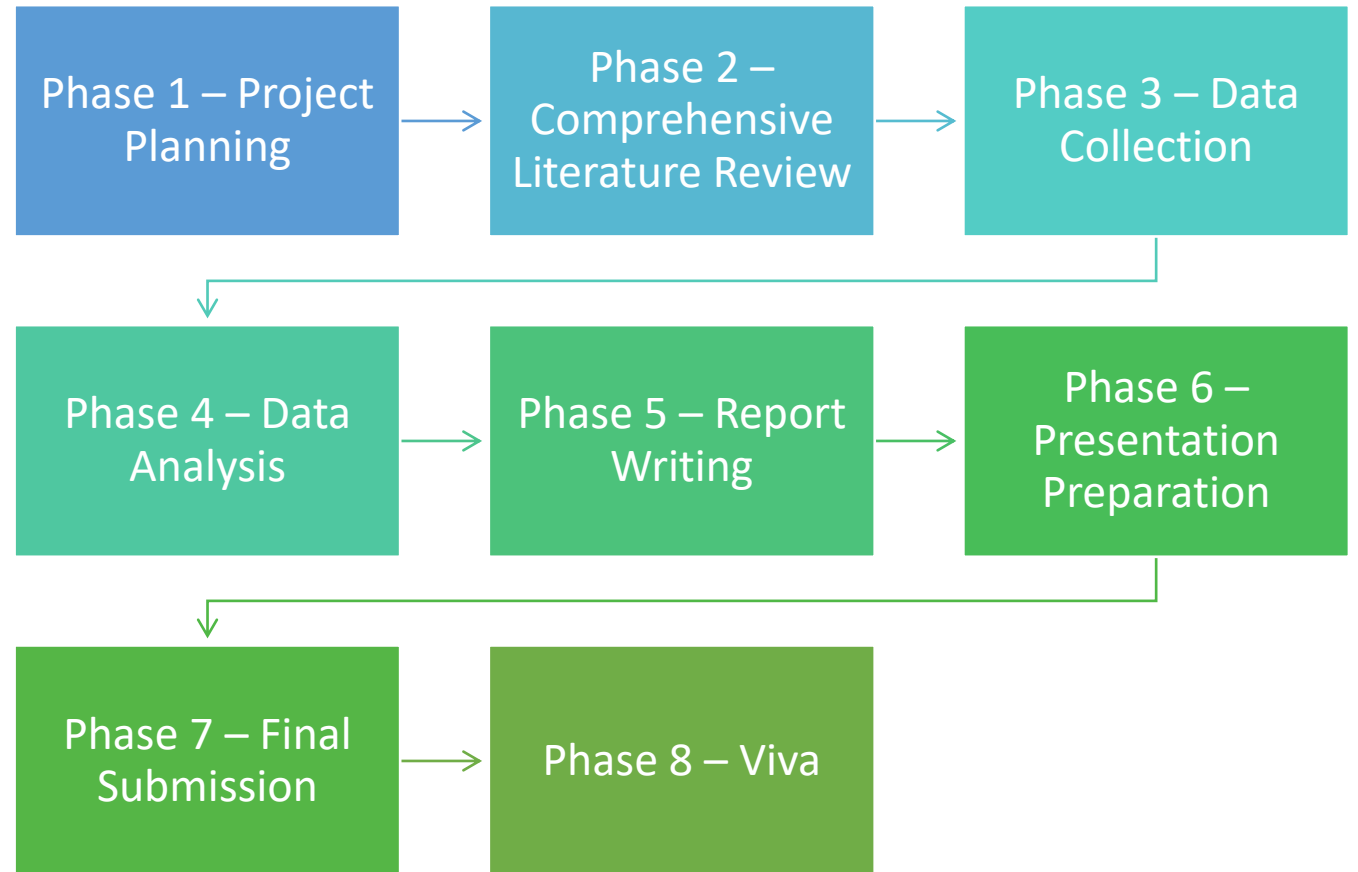
- Real-life examples

Internal reports

- Threat actors
- Originating countries



Project Plan



Thank you & References

- G. Gritsai, A. Timorin, Y. Goltsev, R. Ilin, S. Gordeychik, and A. Karpin, “SCADA SAFETY IN NUMBERS,” Dec. 2012.
- E. P. Leverett, “Quantitatively assessing and visualising industrial system attack surfaces,” Master’s thesis, University of Cambridge, Cambridge, UK, 2011.
- V. G. Cerf, P. Ryan, M. Senges, and R. S. Whitt, “IoT safety and security as shared responsibility,” *Journal of Business Informatics*, no. 1, 35, pp. 7–19, 2016, Available: <https://ssrn.com/abstract=2735642>
- W. Enck and L. Williams, “Top five challenges in software supply chain security: Observations from 30 industry and government organizations,” *IEEE Security & Privacy*, vol. 20, no. 2, pp. 96–100, 2022, doi: 10.1109/MSEC.2022.3142338.
- N. Falliere, L. O. Murchu, and E. Chien, “W32.stuxnet dossier,” Symantec Security Response, 2011. Available: https://cockpitci.itrust.lu/wp-content/uploads/2012/01/w32_stuxnet_dossier.pdf



Video Link

https://uowtsd-my.sharepoint.com/:v:/g/personal/2306895_student_uwtsd_ac_uk/EW0eFjbNSe1Mm8vV5_Crym8Budo4UUMB7Ib7njLstNcqUg?e=BOkpYv&nav=eyJyZWZlcnJhbEluZm8iOmsicmVmZXJyYWxBcHAIoiJTdHJlYW1XZWJBcHAIJCJyZWZlcnJhbFZpZXciOiJTdGFyZURpYWxvZy1MaW5rliwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D