Initial Plan: Framework for Forensic Analysis of Cyber-Physical Attacks: Correlating Digital Traces with Physical Outcomes

School of Computer Science and Informatics

Author: Jake Palmer

Supervisor: Erini S Anthi

Project Description

In response to the growing integration of cyber-physical systems (CPS) and the subsequent emergence of security vulnerabilities within essential infrastructures [1, 8], this project intends to develop a comprehensive framework for the forensic analysis of these systems. This framework aims to provide an approach for analysing breaches across a variety of cyber-physical systems, including autonomous vehicles, industrial control systems, and smart grids by linking the digital consequences of the attack to its physical effects. Given the vital role of cyber-physical systems in modern society, the development of this framework is crucial for forensic investigators in critical sectors such as healthcare, energy, and transportation. It will allow investigators to quickly and accurately identify the source and scope of a breach and provide a methodology for mitigating the damage caused.

Crucially, the framework will focus on correlating the relationships between the digital evidence as well as the physical impact of breaches in cyber-physical systems. This will be a critical component of the framework, as the improper operation of any cyber-physical system will always have ramifications for both the digital and physical domains. By having a full understanding of the interdependencies of these systems [7], and a clear methodology on how to mitigate the damage posed by breaches in these systems, this framework will ensure that forensic investigators are better equipped to respond to breaches within cyber-physical systems effectively and can reconstruct the full sequence of events that occurs.

This project will be carried out by researching cyber-physical systems, pinpointing potential security vulnerabilities that apply to all cyber-physical systems [1, 5], as well as determining optimum data analysis procedures, which will be able to stipulate exactly what data will need to be collected and at what point during the investigation, and how to analyse this. To do this, I will use existing data sets taken from various systems such as:

- Physical Devices Connected to the System: Cataloguing every device that is connected to the system as soon as a breach is detected helps to immediately identify anomalous intrusions and can help to begin a timeline of events.
- Preservation and Examination of Digital Artefacts: Digital artefacts found in volatile memory such as RAM and critical system configurations can prove invaluable when determining the severity of a breach.
- Sensor Data: This allows quick identification of a location where the breach may have affected the system and helps to mitigate the impact as it can be resolved more efficiently through a better-targeted response.
- Assessment of Physical Damage: If any physical damage has occurred to sensors, systems, or actuators within the cyber-physical system, then this will be crucial in determining the nature and severity of the attack.

This is a suitable final-year project as it has a relatively high difficulty but is suitable to complete within the given time frame. I do have experience in forensic analysis, and I am familiar with exploring PCAP files and system images for forensic information, however this is an excellent opportunity to further my expertise in forensic analysis and allows me to explore vulnerabilities within cyber-physical systems [1, 5] and the challenges of having them interlink with the physical and digital domains. Furthermore, this project has a high potential for a real-world impact, contributing to security procedures needed for vital cyber-physical systems.

Aims and Objectives

The primary aim of this project is to create a forensic framework for the analysis of cyber-physical systems [2, 3], specifically focusing on correlating the digital aspect with the physical consequences of the attack. This framework will need to be diverse enough to apply to a variety of cyber-physical systems and will require research into common shared vulnerabilities across all cyber-physical systems [1, 5] as well as research into some existing approaches to this problem. I plan on completing the following objectives:

1. Literature Review: A thorough literature review of some of the current approaches for the forensic analysis of various cyber-physical systems [4], and further analysis of these methods to pinpoint potential improvements and challenges so that my project can be more widely applicable and better suited to all systems.

Risk: Given the rapid progression of security features of cyber-physical systems, there is a risk that the information taken from older papers may be obsolete.

Mitigation: Prioritise more recent research efforts to begin with while still considering older projects, combining these for a better overall approach that applies to both current and legacy systems.

2. Catalogue Common Vulnerabilities: By researching various cyber-physical systems, it is vital to record the most common points of entry for an attacker [6] so that the framework can be more targeted towards finding the breach more efficiently, thus strengthening the security of the system.

Risk: Since the framework must apply to all cyber-physical systems, this may not be able to cover all potential points of entry in more complex systems with many interfaces.

Mitigation: I would mitigate this by incorporating a more modular approach to cataloguing known failure points, therefore making the framework more scalable to larger cyber-physical systems.

3. Identify Optimum Procedures for Analysing Data: Using pre-existing data sets from various systems, as well as potentially collecting some new data if time allows. This aims to identify optimum ways of analysing data from cyber-physical systems to identify a breach quickly.

Risk: Inadequate methods for processing and analysing data may lead to missing critical evidence for the investigation.

Mitigation: Evaluate the effectiveness of the procedures created by simulating a breach on a cyber-physical system.

4. Simulation and Framework Validation: This aims to simulate a breach on a cyber-physical system to evaluate the effectiveness of the framework on an actual breach, refining it if necessary. Utilising this in conjunction with pre-existing data from various systems ensures that the framework is sufficiently strong and varied to be applied to various cyber-physical systems.

Risk: A simulated breach may not accurately represent real-world scenarios, misrepresenting the framework's effectiveness.

Mitigation: Test a breach that is common to many cyber-physical systems, making the framework applicable to all systems, and ensuring that the breach represents a real-world scenario.

Feasibility

There are some factors which could affect the feasibility of this project:

- Ethical Approval: Due to the nature of this project prior ethical approval will not be a prerequisite as this project does not involve the utilisation of any human data and will not require human participation in the testing or review phase of developing the framework.
- Legal Issues: The simulation of a breach on a cyber-physical system must be conducted properly, ensuring that there is no unauthorised access to other systems or devices to comply with the Computer Misuse Act [9].
- Special Resources: The use of resources given by the university such as their cyber-physical system is crucial for this project to simulate a breach and evaluate the effectiveness of the framework.

These can be addressed by obtaining explicit permissions for testing the breach on the universities' cyber-physical system, ensuring that these are isolated from any wider networks. All actions taken during the simulation will be documented with timestamps, detailing exactly what occurred and when. Regarding the use of resources given by the university, the request for this will be made in advance, and a detailed plan will be made outlining the specific uses that I intend will be made which will be helpful for the development of the project.

Work Plan

The following is a structured timeline of the milestones that I am setting out to achieve in this project and the work required to complete each one.

Weeks 1-2: Project Planning and Background Research

- Complete the initial plan for the project.
- Organise a meeting schedule with the supervisor.
- Complete initial research surrounding the background of the project.
- Begin a literature review of current approaches that address the problem.

Weeks 3-4: Research Vulnerabilities in Cyber-Physical Systems and Identification of Optimum Procedures for Analysing Data

- Document any shortcomings in current approaches to this problem during and after the literature review.
- Analyse and research current cyber-physical systems to catalogue common vulnerabilities to ensure that the framework is better targeted to these.
- Identify the types of data that need to be collected for forensic examination and how the data can be used and analysed throughout the investigation.

Weeks 5-6: Further Develop the Framework by Defining Optimum Data Analysis Procedures

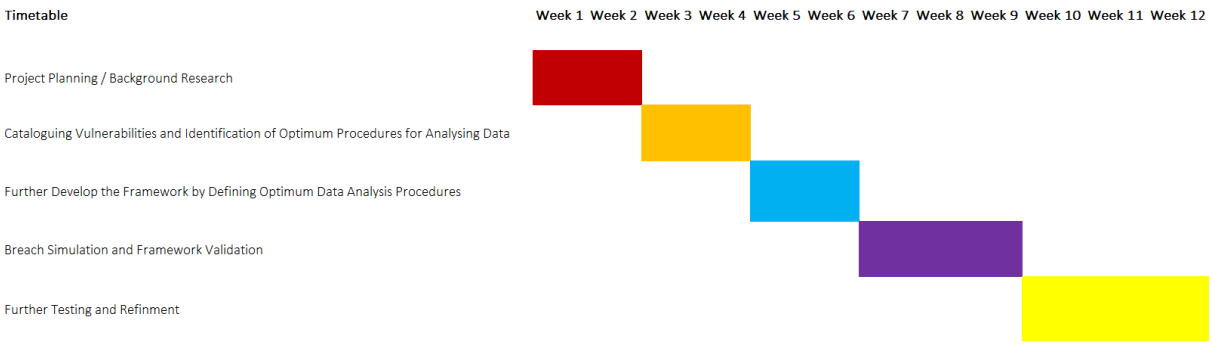
- Establish methods for data analysis ensuring that a clear chain of custody is maintained using pre-existing data sets.
- Investigate methods of correlating this data with the physical impacts that the data shows.

Weeks 7-9: Breach Simulation and Framework Validation

- Simulate a breach on the cyber-physical system provided by the university to determine the effectiveness of the framework which closely mimics real-world scenarios.
- Collect and analyse data from the breach to validate the framework.
- Develop methods for correlating this data with physical sensor data and system logs to understand the effects of the breach on the physical domain.
- Ensure the framework is adaptable enough to apply to any cyber-physical system.

Weeks 10-12: Further Testing and Refinement

- Using the data collected in the simulation phase, evaluate and review any changes that may need to be made to the framework.
- Evaluate how further changes can be made in future framework iterations.
- Complete the final report and ensure that it is ready for submission.



As shown above, I aim to complete the simulation phase over three weeks. This allows enough time for any issues that may occur, and it ensures that I have enough time beforehand to fully research exactly what the breach will be so that it fully tests the framework that I have developed. This may overlap with week 10, however, three weeks should be enough time to complete this.

References

1. Aldabbas, O., Aydin, M., Dehghantanha, A., Hammoudeh, M., and Walker-Roberts, S. (2019). Threats on the horizon: understanding security threats in the era of cyber-physical systems. The Journal of Supercomputing. Available at: https://doi.org/10.1007/s11227-019-03028-9
2. Al-Jaroodi, J., Jawhar, I., and Mohamed, N. (2020). Cyber–Physical Systems Forensics: Today and Tomorrow. Journal of Sensor and Actuator Networks. Available at: https://doi.org/10.3390/jsan9030037
3. Al-Saleh, M.I., Alawneh, L.M., Gupta, B., Jararweh, Y.I., and Al-Sharif, Z.A. (2020). Live forensics of software attacks on cyber–physical systems. Future Generation Computer Systems, 108, pp.1217–1229. Available at: https://doi.org/10.1016/j.future.2018.07.028
4. Bhirud, S.G., Kazi, F., and Pranita Binnar (2024). Security Analysis of Cyber-Physical System using Digital Forensic Incident Response. Cyber Security and Applications, pp.100034–100034. Available at: https://doi.org/10.1016/j.csa.2023.100034
5. Gao, Y., et al. (2013). Analysis of security threats and vulnerability for cyber-physical systems. Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, Dalian, China, pp. 50-55. Available at: https://doi.org/10.1109/ICCSNT.2013.6967062
6. Jain, A., and Singh, A. (2019). Study of Cyber Attacks on Cyber-Physical System. SSRN Electronic Journal. Available at: https://doi.org/10.2139/ssrn.3170288
7. Marashi, K., Sarvestani, S.S., and Hurson, A.R. (2016). Quantification and Analysis of Interdependency in Cyber-Physical Systems. 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), Toulouse, France. Available at: https://doi.org/10.1109/DSN-W.2016.47
8. Salman, O., Yaacoub, J.-P.A., Noura, H.N., Kaaniche, N., Chehab, A., and Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, p.103201. Available at: https://doi.org/10.1016/j.micpro.2020.103201
9. Walton, R. (2006). The Computer Misuse Act. Information Security Technical Report, 11(1), pp.39–45. Available at: https://doi.org/10.1016/j.istr.2005.11.002