Development Team Project: Design Document

I. Introduction

This report evaluates a Cyber-Physical System (CPS) case study presented by Bhattacharjya (2022). Vulnerabilities are enumerated along with their Common Weakness Enumeration (CWE) class and quantified using the Common Weakness Scoring System (CWSS v 1.0.1). This allows for prioritised mitigations, which are then visualised in an Attack-Defence Tree (AD Tree).

## II. Domain Selection

Alternative scoring schemes were reviewed before selecting the Common Weakness Scoring System (CWSS v1.0.1). CVSS v4 was rejected because it is calibrated for known, existing vulnerabilities rather than to evaluate systemic weaknesses. CWSS, by contrast, was built to prioritise weakness *types*. The composite CWSS score expresses the relative technical risk of leaving a weakness unmitigated, combining exploitability, impact and environmental factors into a single comparable metric. Scores reflect the relative severity of each weakness.

Promoted as “a consistent, flexible, open” mechanism for ranking software errors, CWSS can be tuned to domain-specific risk profiles (MITRE Corporation, n.d.). Its native alignment with CWE and strength in identifying attack chains make it well suited for our modelling.

III. Vulnerability Identification

Bhattacharjya (2022) lists attacks that endanger every pillar of the CIA triad. Buxiang et al. (2022) extend the discussion by mapping additional threats to a CPS’s control, network and physical layers. Table One consolidates representative weaknesses from their combined analysis, mapping each one to its corresponding CWE class and CWSS score.

*Table One: Enumerated threats from Bhattacharjya (2022) and Buxiang et al (2022).*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CPS layer | CWE | Weakness/attack leaf | Source\* | CWSS |
| Client | 346 | ARP-spoofing / MITM | Bha22 | 66.3 |
|  | 1391 | Use of weak credentials | Bha22 | 69.3 |
| Controller | 434 | Unrestricted file upload | Bux22 | 88.9 |
|  | 016 | Critical controller misconfiguration | Bha22 | 23.5 |
|  | 290 | Phishing → authentication bypass | Bha22 | 32.3 |
|  | 1104 | Unmaintained third-party component | Bux22 | 38.0 |
| System | 319 | Clear-text machine-to-machine traffic | Bha22 | 69.3 |
|  | 770 | MQTT-broker congestion (message flood) | Bux22 | 29.5 |
|  | 400 | Uncontrolled resource consumption | Bha22 | 49.4 |

*\* Bha22 = Bhattacharjya (2022); Bux22 = Buxiang et al. (2022)*

## IV. Mitigation Strategies

The CWSS allows strategic prioritisation of mitigations. Taken from academic resources, the following mitigations are recommended to address the identified weaknesses.

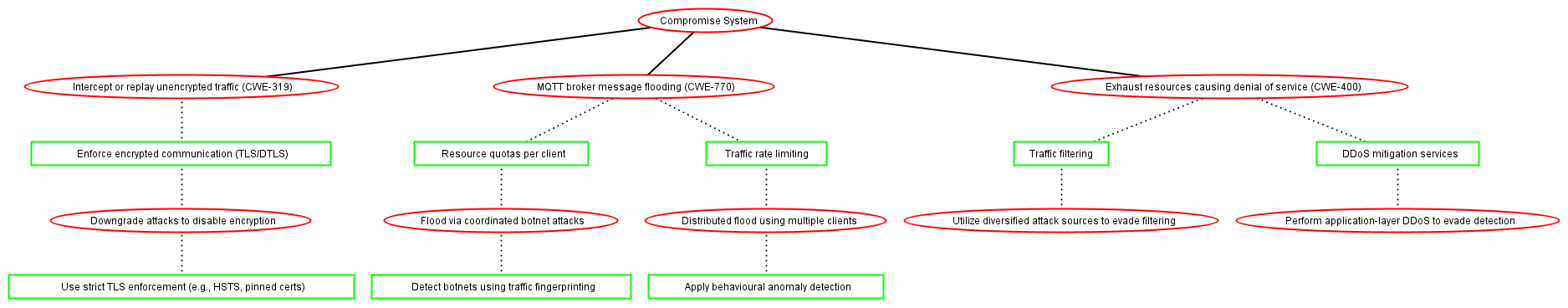
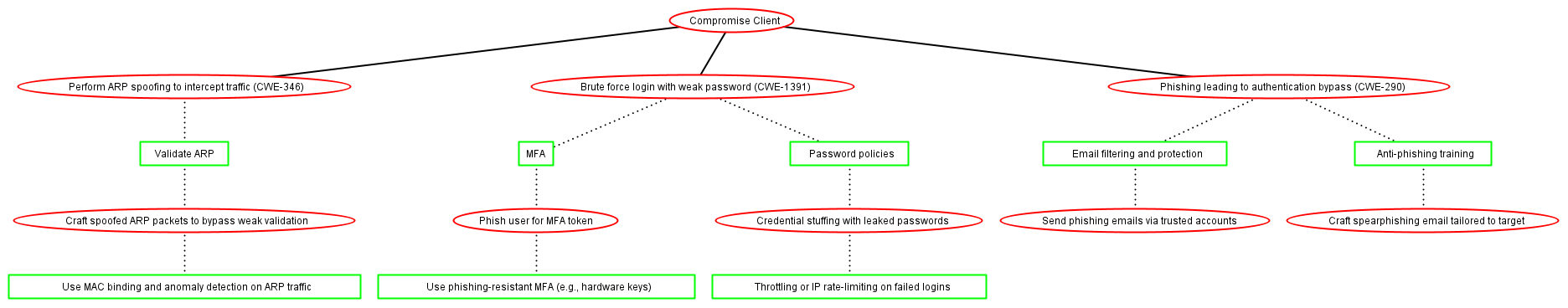
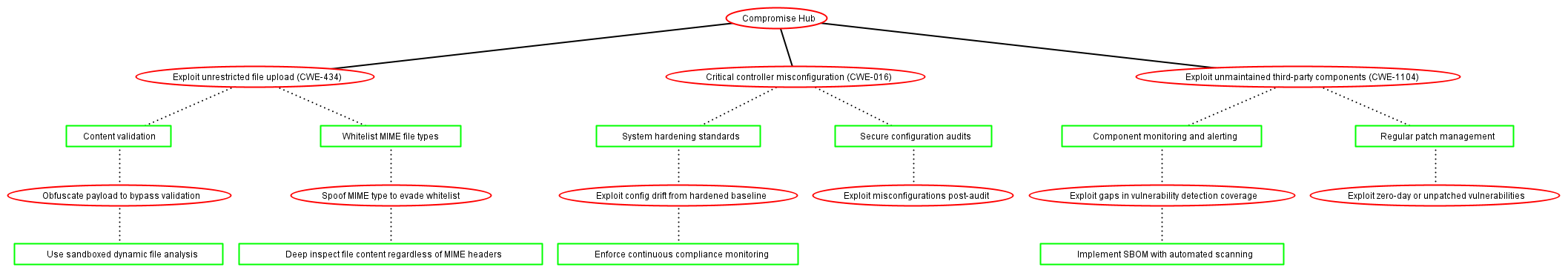
*Table Two: Mitigation recommendations to protect a CPS.*

|  |  |  |  |
| --- | --- | --- | --- |
| CPS layer | CWE | Mitigation | Severity |
| Client | 346 | Implementation of ARP packet validation & Threshold-Based Protection (Hnamte, Hussain 2024) | High |
|  | 1391 | Enforce strong password policy and implementation of multi-factor authentication (MFA) | High |
| Controller | 434 | File type and content validation, allow list for filename and extension, and malware scanning (OWASP, 2023) | Critical |
|  | 016 | Set up a configuration baseline and regularly review and audit controller settings. (NIST, 2018) | Low |
|  | 290 | Security Awareness Training & Implementation of SPF, DKIM and DMARC (AlwaysData, n.d.) | Low |
|  | 1104 | Continuous monitoring of third-party components including versioning, known vulnerabilities and dependency chains. Apply updates and install patches promptly (OWASP, 2021) | Medium |
| System | 319 | Deploy approved encryption algorithms for data transfer and ensure servers are configured to use encrypted secure protocols for communication (MITRE Corporation, 2025a) | High |
|  | 770 | Input validation and resource limitation (MITRE Corporation, 2023) | Medium |
|  | 400 | Authentication and access control, as well as implementation of rate limit and restricted database access. (MITRE Corporation, 2025b) | Medium |

## V. AD Tree

The following AD Tree provides a graphical representation of how the CPS system discussed by Bhattacharjya could be attacked. The structure is divided into three branches representing client, controller, and system-level vulnerabilities. Each attack node (red) highlights a security weakness, while corresponding defence nodes (green) represent preventative or mitigative measures. This model enables stakeholders to identify high-risk areas and prioritise defences. For clarity, the three branches have been separated from the root in Figure One.

*Figure One: The three branches of a CPS AD Tree*



## VI. Conclusion

This document presents a structured security assessment of a CPS using an AD Tree model. Threats were identified, prioritised using CWSS scoring, and matched with tailored mitigation strategies. This approach helps visualise attack surfaces, supports defence planning, and aligns with secure system engineering principles. Future iterations could include automated identification of weaknesses and integration with threat modelling frameworks like MITRE ATT&CK.

## VII. References

Always Data (n.d.) *Configuring SPF/DKIM/DMARC*. Available at: <https://help.alwaysdata.com/en/e-mails/set-up-spf-dkim-dmarc/> (Accessed: 17 May 2025).

Bhattacharjya, A. (2022) ‘Securing cyber-physical systems: A case-study analysis’, *Cybersecurity Journal*, 8(3), pp. 145–159. Available at: <https://www.researchgate.net/publication/365891730_A_Holistic_Study_on_the_Use_of_Blockchain_Technology_in_CPS_and_IoT_Architectures_Maintaining_the_CIA_Triad_in_Data_Communication> (Accessed: 17 May 2025).

Hnamte, V. and Hussain, J. (2024) ‘Enhancing security in software-defined networks: An approach to efficient ARP-spoofing-attack detection and mitigation’, *Telematics and Informatics Reports*, 14, 100129. Available at: [add DOI or URL] (Accessed: 17 May 2025).

MITRE Corporation (2023) *CWE-770: Allocation of resources without limits or throttling*. Available at: <https://cwe.mitre.org/data/definitions/770.html> (Accessed: 17 May 2025).

MITRE Corporation (2025a) *CWE-319: Cleartext transmission of sensitive information*. Available at: <https://cwe.mitre.org/data/definitions/319.html> (Accessed: 17 May 2025).

MITRE Corporation (2025b) *CWE-400: Uncontrolled resource consumption*. Available at: <https://cwe.mitre.org/data/definitions/400.html> (Accessed: 17 May 2025).

MITRE Corporation (n.d.) *Common Weakness Scoring System (CWSS) & Common Weakness Risk Analysis Framework (CWRAF): Introductory handout* [PDF]. Bedford, MA: MITRE Corporation. Available at: <https://makingsecuritymeasurable.mitre.org/docs/cwss-cwraf-intro-handout.pdf> (Accessed: 14 May 2025).

National Institute of Standards and Technology (NIST) (2015) *Guide to industrial control systems (ICS) security: NIST SP 800-82 Rev. 2*. Gaithersburg, MD: NIST. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf> (Accessed: 17 May 2025).

National Institute of Standards and Technology (NIST) (2018) *Framework for improving critical infrastructure cybersecurity*. Gaithersburg, MD: NIST. Available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (Accessed: 17 May 2025).

OWASP (2021) ‘A06: 2021 – Vulnerable and outdated components’. Available at: <https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/> (Accessed: 17 May 2025).

OWASP (2023a) *OWASP Internet of Things Project*. Available at: <https://owasp.org/www-project-internet-of-things/> (Accessed: 17 May 2025).

OWASP (2023b) ‘Unrestricted file upload’. Available at: <https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload> (Accessed: 17 May 2025).

Zhou, B., Zhang, Y., Wang, J., Liu, L. and He, H. (2022) ‘Security risk assessment approach for distribution-network cyber-physical systems considering cyber-attack vulnerabilities’, *Entropy*, 25(1), p. 47. Available at: <https://doi.org/10.3390/e25010047> (Accessed: 17 May 2025).