Security Implications of Interoperability

Michael Boniface[a], Nic Fair[a], Stefano Modafferi[a], and Juri Papay[a]

[a] *IT Innovation Centre, Gamma House, Enterprise Road, Southampton, SO16 7NS, UK*

Abstract

The presented paper investigates the relationship between interoperability and system security. This is mainly an optimisation problem, since making a system interoperable means that some APIs need to be exposed, which can potentially open the system to malicious attacks. The paper explores the use of the System Security Modeller (SSM) tool which allows an assessment of the cost of interoperability by calculating the security risks. The security implications of interoperability are illustrated through a case study representing a smart manufacturing scenario.

Keywords 1

Interoperability, System Security, Security Risks, ISO 27005, Threat Analysis

1. Introduction

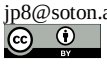
"Interoperability can be defined as the ability of two or more systems or components to exchange information and use the information that has been exchanged" [1]. Interoperability means not just that the system provides the required functionality, but that it is also secure and complies with the relevant regulations. Without due consideration of potential security flaws resulting from complex data flows stemming from interoperability actions, it is impossible to quantify the 'true cost' of interoperability. This is even more the case given that higher levels of interoperability generally means more links between components, but also means a higher number of potential security threats.

The paper is laid out as follows: Section 2 provides a literature review. Section 3 describes an industrial scenario which illustrates the security implications of interoperability and how it can be modelled by the SSM tool. Section 4 details the outcome of threat analysis and Section 5 provides a summary.

2. Literature review

Interoperability between systems is especially important in the case of smart manufacturing systems integrating large volumes of data generated by Internet of Things (IoT) devices. An example of smart manufacturing is the EFPF [2] project which aims to develop a federated system of several digital manufacturing platforms such as DIGICOR [3], COMPOSITION [4], vf-OS [5], and NIMBLE [6]. Another example with a strong emphasis on interoperability between factories is the ZDMP [7] project which intends to develop a digital platform that allows reductions in the level of manufacturing defects by using AI technologies.

Threat modeling can be described as a systematic approach to the identification, prioritisation and mitigation of potential threats during design, development, deployment and operation of a system. This activity focuses on three questions: a) what is being designed, b) what can go wrong, and c) what to do about it [8]. Threat modelling tools can focus on various aspects, for example system assets, software and/or attacks/attackers. Examples of software centric tools are ThreatModeler [9], VsRisk [10], and the Threat Modelling Tool [11]. The main components of ThreatModeler are the threat library, threat

Proceedings of the Workshops of I-ESA 2020, 17-11-2020, Tarbes, France
EMAIL: m.j.boniface@soton.ac.uk (M. Boniface); n.s.fair@soton.ac.uk (N. Fair); S.D.Modafferi@soton.ac.uk (S. Modafferi); jp8@soton.ac.uk (J. Papay)


engine and advanced reporting. The threat library is regularly updated with information drawn from threat catalogues such as WASC-TC [12], CAPEC [13] and OWASP [14]. ThreatModeler distinguishes between Application Threat Models (ATM) and Operational Threat Models (OTM). The ATM is described by a Process Flow Diagram (PFD) and is concerned with the risks to the application. The OTM uses a Data Flow Diagram (DFD) and reflects the risks to the infrastructure. VsRisk is a checklist-based security assessment tool that can perform asset and scenario based evaluations, and generates ISO 27001 [15] compliant reports. The Threat Modelling Tool (TMT) developed by Microsoft identifies threats according to the STRIDE model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) [16]. SeaMonster [17] and Securicad [18] belong to the category of attacker centric tools. These approaches are much more difficult to automate, as they depend on expert knowledge about the attackers and the methods they are likely to use. Unlike the previous tools, the Systems Security Modeller (SSM) [19] takes an asset-based approach to system security and enables automated and systematic identification of potential security risks to all assets (both human and technological). SSM also allows the identification of knock-on consequences of a threat and recommends countermeasures to mitigate these risks.

3. The security cost of interoperability

Modelling of data flow allows an understanding of where the data is created, stored and processed (Figure 1). The "Machining Data" is generated by the "Machining of Moulds" process, then it travels through the "FoFLimited Portal" and is stored in the "FoFLimited Database". This data is then accessed by "Machine Monitor" and "Quality Control" services which create "Monitoring" and "Quality Control" data which is also stored in the "FoFLimited Database". This newly created data can be accessed by the "Operator" and "Quality Controller" persons via the "Quality Control Web Client" and "Monitoring Web Client" processes running on their tablets.

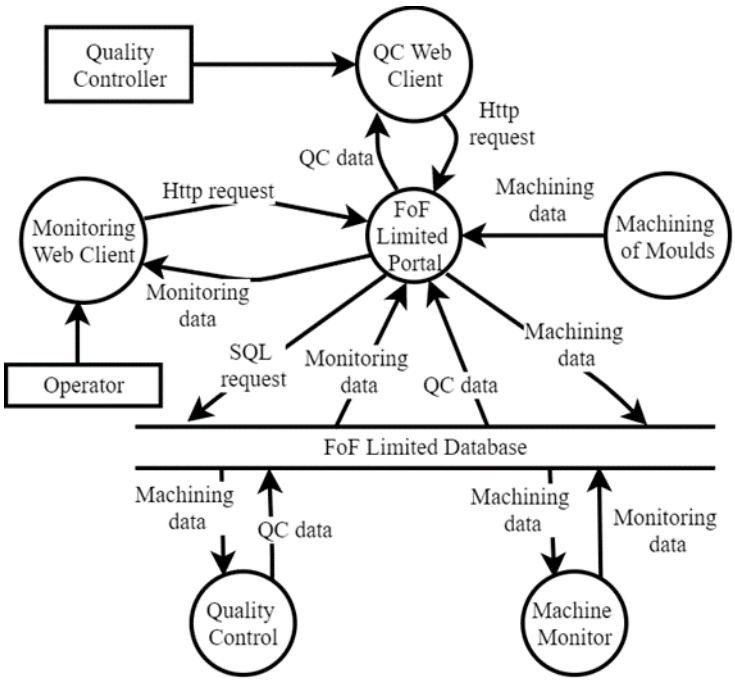


Figure 1: Dataflow diagram of use case

The security diagram models two factories these are the "ACME" factory and "FoFLimited" (Figure 2). The connection between these factories is represented by the internet, two routers, one LAN and one WiFi. The physical locations for the hardware are the "ACME factory" and "FoFLimited DataCentre". In the ACME part of the diagram there are three human operators: the "Quality Controller", "ACME Factory Sysadmin" and "Operator". The "FoFLimited Portal" is the proxy between the ACME and the

FoFLimited systems. The ACME part of the diagram contains the “ACME Milling Platform” which generates a stream of data.

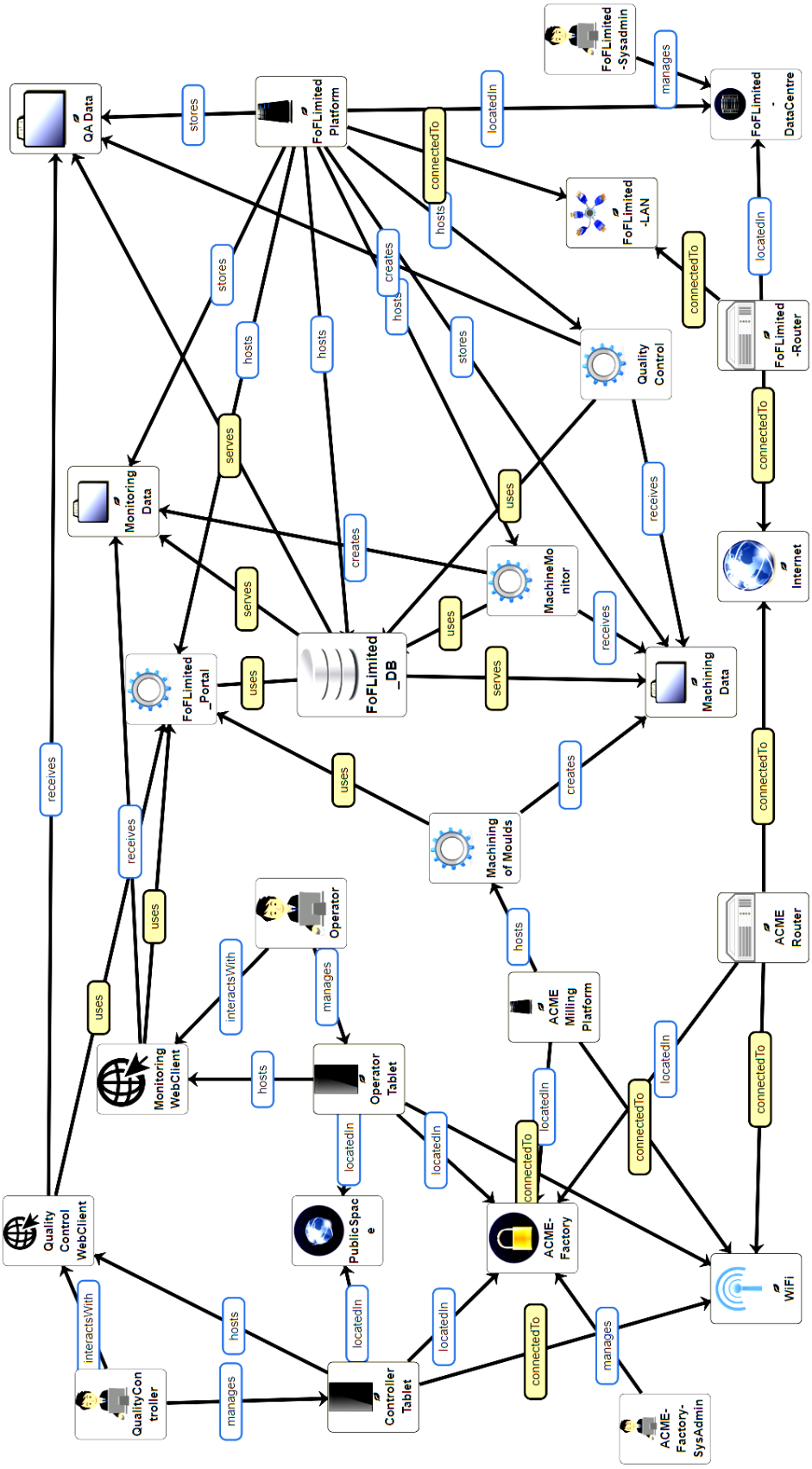


Figure 2: Modelling industrial use case

4. Threat Analysis

The security model presented in Figure 2 consists of 158 assets (including the inferred assets generated by SSM), there are 684 relations and 56 controls. SSM has identified 711 primary and secondary threats in total. Primary threats are caused by system faults or malicious activity. Secondary threats represent the propagation of threats through the system. Threat resolution is an iterative process the aim of which is to select the appropriate controls that allow a reduction in the number of threats. For illustration purposes we may consider the effect of software patching. By applying this control alone, the number of threads can be reduced by 120.

SSM also enables the calculation of risk levels according to ISO 27005 [20]. The risk calculations produce several parameters: a) likelihood of a negative event happening, b) impact levels which describe the consequences of threats, c) trustworthiness levels which measure the effectiveness of controls for mitigating a threat and d) risk levels representing the urgency with which threats have to be treated. According to these calculations the loss of availability of tablets and web clients have the highest likelihood of happening. In terms of impact the loss of confidentiality of "QA data" and the "FoFLimited Database" are the most critical.

Even if we applied all possible security controls some unresolved threats will remain, which need to be handled individually. In this case the security expert should make a decision whether the threat is acceptable or not. If the threat is not acceptable then the system needs to be re-designed and the security risks re-calculated.

5. Summary

This paper argues that the 'true cost' of interoperability can only be accurately described by including assessment of the potential risks of possible malfunctions or misbehaviours of interoperative systems. The SSM tool provides automated identification of security threats and their concomitant mitigation strategies, is one, effective method for understanding the 'true cost' of undertaking interoperability activities. SSM is underpinned by semantic reasoning technologies in order to ensure that this automated approach does not overlook possible threats, providing manufacturers with an accurate cost assessment of interoperability. On the system model diagram interoperability is represented by links between components (Figure 2). In general, it is desirable to have as many links as possible in order to accurately model the necessary system functionality, however this also increases the number of security risks that will be identified.

Regarding future work, the long-term goal is to promote security as a first order architecture design concern, encompassing assumptions that are often considered only implicitly. The aim is to apply the SSM approach to other complex socio-technical systems by developing security knowledge bases for interoperability architectures.

6. Acknowledgements

The research leading to these results received funding from the European Union H2020 Program under grant agreement No. 825631 "Zero Defect Manufacturing Platform (ZDMP)".

7. References

[1] 610.12-1990-IEEE Standard Glossary of Software Engineering Terminology, 2020. URL: https://ieeexplore.ieee.org/document/159342
[2] EFPF, 2020. URL: www.efpf.org.
[3] DIGICOR, 2020. URL: www.digicor-project.eu.
[4] COMPOSITION, 2020: URL: www.composition-project.eu.
[5] vf-os, 2020. URL: www.vf-os.eu.
[6] NIMBLE, 2020. URL: www.nimble-project.org.
[7] ZDMP, 2020. URL: www.zdmp.eu.

[8] SHOSTAK A., Threat Modeling: Designing for Security, John Wiley & Sons, 2014.
[9] Threat Modeler, 2020. URL: threatmodeler.com.
[10] VsRISK, 2020. URL: www.vigilantsoftware.co.uk.
[11] Threat Modelling Tool, 2020. URL: aka.ms/tmt.
[12] Threat Classification, 2020. URL: projects.webappsec.org.
[13] Common Attack Pattern Enumeration and Classification, 2020. URL: capec.mitre.org/about/index.html.
[14] OWASP, 2020. URL: www.owasp.org.
[15] ISO/IEC 27001, 2020. URL: www.iso.org.
[16] STRIDE Model, 2020. URL: en.wikipedia.org/wiki/STRIDE_(security).
[17] MELAND, P.H., et al., SeaMonster: Providing tool support for security modeling, NISK 2008, Kristiansand, 2008.
[18] SecuriCad, 2020. URL: www.foreseeti.com.
[19] SURRIDGE M., et al., Modelling Compliance Threats and Security Analysis of Cross Border Health Data Exchange, MEDI 2019: New Trends in Model and Data Engineering: Communications in Computer and Information Science, vol. 1085, 2019, 180-189.
[20] ISO/IEC 27005, 2020: URL: www.iso.org.