A SYSTEMATIC APPROACH TOWARDS ENHANCING DIGITAL PRIVACY IN INDUSTRIAL APPLICATIONS

Sara Abbaspour Asadollah

School of Innovation, Design and Engineering, Mälardalen University
Västerås, Sweden

ABSTRACT

Ensuring digital privacy is critical to protecting sensitive information and guarding against malicious actors in today's interconnected world. This paper explores the concept of digital privacy and its importance in maintaining online security. We highlight the importance of robust strategies to protect information by examining the consequences of failing to prioritize digital privacy, including identity attack scenarios in industrial applications by proposing a systematic approach to improving digital privacy. Our methodology includes creating a Data Flow Diagram (DFD) to visualize the data flow within the system and applying the STRIDE threat modelling framework to identify potential threats, with a focus on privacy-related aspects. We then extract privacy-related threats and create attack vectors and scenarios to guide testers to validate system security. To validate our methodology, we plan to conduct a case study in an industrial application, an automated train control system. By analyzing the data flow and identifying potential attack scenarios, we want to demonstrate the effectiveness of our approach in real-world applications. We also want to automate the process and collaborate with more industries to ensure scalability and practical applicability.

KEYWORDS

Privacy-related threats, Cyberattack, attack vector, attack scenario, Information security, Data protection.

1. INTRODUCTION

Digital privacy refers to the protection of online information, including personal, industrial, and sensitive data. This involves maintaining control over one's identity and personal data to prevent unauthorized access and misuse [1]. This is important because it is the primary method to protect online identities, defend against fraud and cyberattacks, and retain control over personal data. Failure to prioritize digital privacy can have serious consequences such as identity theft, financial fraud and the violation of privacy rights.

In today's digital age, understanding the importance of digital privacy is important for ensuring online safety and security. Digital privacy is a significant concern in today's interconnected world, where an increasing amount of information is being shared and stored online. Users can take practical steps to protect their digital presence, such as using strong passwords, regularly updating software, managing privacy settings, limiting information sharing and using encryption tools. Laws and regulations also play an important role in protecting digital privacy by establishing clear guidelines for the responsible and transparent handling of personal data by

David C. Wyld et al. (Eds): SPTM, AIS, SOENG, AMLA, NLPA, IPPR, CSIT – 2024
pp. 55-62, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141105

companies. By advocating for robust laws and regulations that protect users' rights to digital privacy, an approach can be proposed that promotes and protects digital privacy.

Moreover, securing information in industrial settings is important for a few key reasons. First, it keeps sensitive data safe from unauthorized access and potential breaches. Second, it helps companies follow rules like the General Data Protection Regulation (GDPR), avoiding legal trouble and big fines. Third, making information protection a priority builds trust with customers and users, which is good for business success in the long run. On the other hand, the increasing frequency and severity of data breaches underscore the critical importance of addressing digital privacy concerns in today's interconnected world. The results of the IBM X-Force report for 2023 [2] reveal that the average cost of a data breach has reached the staggering sum of $4.45 million, representing an increase of 2.3% from the previous year and a significant rise of 15.3% since 2020. Alarmingly, despite the escalating financial repercussions of breaches, only 51% of organizations are planning to enhance their investment in security measures following such incidents. These organizations are directing their efforts towards bolstering incident response planning, enhancing employee training initiatives, and deploying advanced threat detection tools. These statistics underscore the urgent need for robust strategies and proactive measures to protect digital privacy in an increasingly vulnerable landscape. Overall, protecting information is super important in the industry because it keeps data safe, follows rules, builds trust and helps companies stay competitive in the digital world. In this context, we propose a method to help industries effectively protect the information in their application and explain it in this work-in-progress paper.

The first step in our process involves creating a comprehensive data flow diagram that accounts for all system requirements and application architecture. Once this is completed, we utilize the STRIDE threat modeling framework [3] to generate a list of potential threats to the application. Specifically, we focus on threats related to data privacy and extract relevant data to identify potential attacks. Next, we create corresponding vectors for each element and then integrate them with vectors created for other interconnected elements to make attack scenarios. These scenarios can be passed on to testers during the application testing phase.

2. RELATED WORK

In [4], Lustgarten et al. examine the growing use of technology in mental healthcare services. This includes the ability for professionals to communicate, store information and use digital tools such as email, text messaging, telepsychology, electronic medical records, cloud-based storage, apps and assessments. While these advances can improve efficiency and service delivery, they also pose potential risks to digital privacy and confidentiality. The study concludes by highlighting the significant impact of technology on mental health care, pointing to the shift from traditional methods to modern digital solutions. Providers face the challenge of maintaining privacy amidst technological advancements, and the study emphasizes the importance of education, engagement with relevant literature, and ethical considerations to ensure client privacy in the future of mental health care. The study reviews common technologies, identifies potential vulnerabilities, and makes suggestions for strengthening privacy in mental health care.

The paper [1] analyzes the relations between contemporary technologies of the digital age and the principles of information security, privacy and protection of personal data. The authors identify special features of information and personal data protection and summarize the main challenges of the digital age for the security and privacy of users. They briefly present the basic legislation in the fields of privacy and personal data protection. They propose components of information security to counter threats and attacks and discuss basic principles in organizing the protection of personal data. In addition, they systematize the main risk issues of the digital age for user

privacy, focusing particularly on modern technologies. They propose requirements to limit their negative impact on users of e-services in the global network by classifying appropriate methods and means to ensure reliable data protection and explaining the relations between the participating components.

In [5], Pattakou et al. attempted to fill a gap in the current literature by investigating how the methods of usability and privacy requirements engineering overlap. Their main goal was to find out how usability criteria can be integrated into privacy requirements methods to improve their effectiveness. To achieve this, they started by defining and refining usability criteria and then evaluated existing privacy requirements approaches. During their analysis, they identified relevant usability criteria for each phase of these methods. The authors emphasize that security and privacy aspects must be considered together in the development of information systems to prevent potential incidents. Their study contributes to the evaluation of the usability of methods for developing privacy requirements and lays the foundation for extending these considerations to methods for developing security requirements. Finally, the authors emphasize the importance of incorporating usability considerations into privacy requirements methodologies to ensure effective use by developers and stakeholders and highlight the importance of usability to the success of these methodologies.

Although several studies have investigated threat modeling in a general context, our research addresses the intricacies of privacy-related threats, a relatively under-explored area in the field of threat modeling, especially for industrial applications. Our goal is to provide a comprehensive understanding of the privacy-related threats that can occur in different systems and applications.

3. METHODOLOGY OVERVIEW: PLANNED APPROACH WORKFLOW

A systematic approach is required to ensure the security of sensitive data and to protect against malicious actors. In this section, we present a solution that aims to confront digital privacy against the flow of data. Our planned approach, as shown in Figure 1, outlines the proposed sequence of steps for conducting the study. Below is a detailed description of the five-step process:

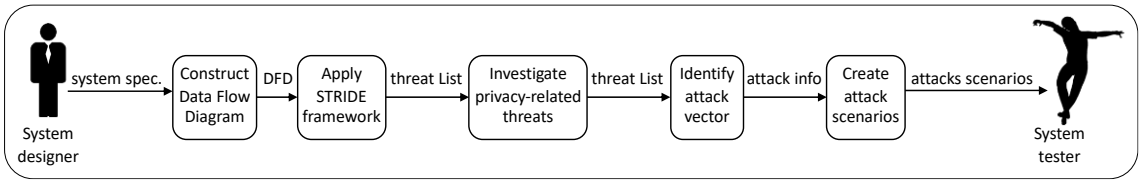

Figure 1. Planned approach workflow diagram.

Step 1: Construct a Data Flow Diagram. The first step is to create a DFD based on the system specifications provided by the system designer(s). This diagram represents the flow of data within the system. Our DFD consists of five elements: (a) Process. Shows a task that receives input, modifies it, or redirects it to produce output. (b) Data store. Shows the storage for both permanent and temporary data. (c) External entity. Shows task, entity, or data store outside of our direct control, for example, third-party APIs or an application user can be external entities. (d) Data flow. Shows the movement of data among processes, data stores, and external entities. (e) Trust boundary. Represents the point at which data transitions from one level of trust to another. It delineates areas with different security levels within a system and marks the boundary between trusted and untrusted areas. The DFD serves as a foundation for further analysis and security assessment.

Step 2: Apply STRIDE framework. Using the DFD as our guide, we can apply the STRIDE framework to identify potential threats to the system. The STRIDE framework comprises the six dimensions of Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. By analyzing the DFD, we generate a comprehensive list of identified threats, which forms the basis for the subsequent security measures.

Step 3: Investigate privacy-related threats. In this step, we can refine the generated threat list to focus specifically on threats related to data privacy. We will consider privacy-related threats as potential privacy attacks for the applications. Table 1 represents the threats and their corresponding effects (potential attacks) that can be derived for each threat. To determine the appropriate effect for each type of threat, we explored all descriptions of each type of threat in the threat report and investigated the key elements for each type. Table I shows the results of our exploration of many threat lists generated by the Microsoft threat modeling tool [6].

Table 1. Threats and their corresponding effects.

Threat	**Effect**
Spoofing	Data flow sniffing Data breach Unauthorized access
Tampering	Data flow sniffing
Repudiation	-
Information Disclosure	Data flow sniffing
Denial of Service	Prevent access to the data store
Elevation of Privilege	Impersonate

The following list shows the potential attacks and their definition:

1) **Impersonate:** This attack involves an unauthorized individual pretending to be a legitimate user or device to gain access to a system or network. By impersonating a trusted entity, attackers can gain access to sensitive information or perform actions that violate privacy, such as accessing confidential data or manipulating system settings. For instance, an attacker could use a phishingemail to imitate a company's HR department and request sensitive information from an employee.
2) **Data flow sniffing:** In this attack, an adversary intercepts and monitors data flowing between different components or subsystems of the system to capture and analyze sensitive information. By intercepting data transmissions, attackers can capture confidential information, such as passwords or personal data, compromising digital privacy and confidentiality. For instance, an attacker could capture a user's login credentials and use them to login to their account, allowing them to access sensitive information.
3) **Data breach:** This attack involves unauthorized access to sensitive information, such as personal data or financial records. It exposes confidential information to unauthorized access or disclosure, violating privacy and potentially leading to identity theft, financial fraud, or other privacy-related risks. For instance, a leak of customer data from a retail website could result in the theft of credit card information, which could be used fraudulently or shared with malicious actors.
4) **Unauthorized access/Unauthorized intrusion:** This attack involves gaining entry or acquiring privileged access to a system, network, or device without proper authorization. Unauthorized access allows attackers to view, steal, or manipulate sensitive information, compromising digital privacy and confidentiality. For instance, if an attacker gains access to a company's database, they could access customer records, financial information, and other confidential information that should not be shared.

5) **Prevent access to the data store:** This attack disrupts or denies access to data stores within a system or network. While it may impact operational efficiency or decision-making processes, denying access to data stores does not directly compromise the privacy of individuals by revealing their sensitive information. For example, if a company denies access to customer records, it may hinder customer service operations or data analysis efforts, but it does not expose personal data such as addresses, phone numbers, or credit card numbers.

By filtering out privacy-related threats, we can ensure that our analysis prioritizes the protection of sensitive data. This step is essential to effectively address privacy concerns and ensure compliance with data protection regulations.

Step 4: Identify attack vector. With the filtered threat list in hand, we can proceed to analyze each identified threat in detail to understand the potential attack vector. An attack vector refers to a method or path through which cybercriminals can gain unauthorized [7]. The difficulty of identifying a specific attack vector depends on several factors, including the complexity of the system or network, the level of security measures in place, and the attacker's skills and resources. Sometimes, the attack vector can be easily identified when known vulnerabilities are present and not addressed. Other times, it can be more challenging to detect when advanced techniques or a combination of vectors are used. This critical step strengthens the system's resistance to potential attacks, thereby ensuring its security.

Step 5: Create attack scenarios. Finally, based on the information gathered about potential attacks and their attack vectors, we can create attack scenarios. These scenarios outline hypothetical but realistic situations in which attackers could exploit vulnerabilities to compromise the security of the system. The resulting attack scenarios are then made available to system testers for testing and validation during the system test phase. This step allows us to proactively identify and address security risks to ensure the robustness of the system against potential threats. By testing the system against attack scenarios, we can identify any weaknesses that could leave us vulnerable to attacks related to data privacy. This helps to ensure that the security of the system is robust, and that the system's data is secure and protected from malicious actors.

To the best of our knowledge, there are limited industry-based descriptions of threat modeling approaches [8], [9], concerning the STRIDE framework. Furthermore, some case studies can be found in the domains of cloud infrastructure [11] and hardware [12]. While these examples demonstrate the widespread applicability of threat modeling, they do not sufficiently address best practices and barriers to industry adoption. Typically, these studies concentrate on general threat modeling principles rather than specifically addressing privacy-related threats. However, our study focuses on the examination of privacy-related threats in the context of threat modeling.

To validate the effectiveness of our methodology, in future work, we will conduct a comprehensive evaluation during the system test phase of the automated train control system. This evaluation will be carried out by testers who will receive the attack scenarios created in Step 5, create test scenarios based on them, run the test scenarios, and observe the system's response to each scenario. Here, testers can collect the required data during and after the execution of the test scenarios. This data could include response time, system stability, and the effectiveness of security measures. The collected data will be analyzed to assess the system's resilience to privacy-related potential attacks. The simplified data flow diagram presented in Figure 2 depicts the five interconnected components that illustrate the data flow within our prospective case study. The DFD is described as follows:

- *Controller* is a process in our DFD diagram and acts as the central component responsible for coordinating system operation. It receives the input from sensors, the train driver and external

sources, processes the data and sends corresponding control commands to the actuator. This process also sends the updated break status to the Train Driver.

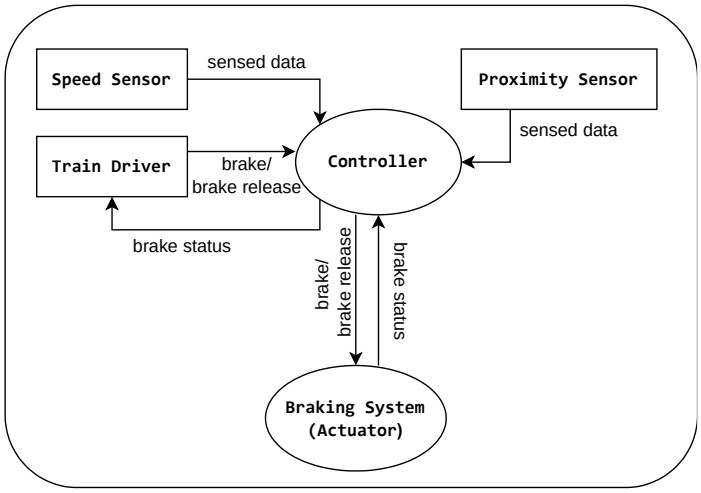

Figure 1. DFD of an automated brake train control system.

- *Speed Sensor* is an external entity in our DFD diagram and collects data on the train's speed.
- *Proximity Sensor* is an external entity in our DFD diagram that determines the presence of obstacles or other trains nearby.
- *Braking System* is a process in our DFD diagram that acts as an actuator responsible for applying or releasing the train's brakes based on the control commands received from the Controller. It also sends updates on the brake status to the Controller after each command.
- *Train Driver* is the human operator and an external entity in our DFD diagram, responsible for manual control anddecision-making in the train's operation. The train driver provides manual control inputs to the Controller, enabling human intervention alongside automated processes. To act as a decision-maker, the train driver receives updates on brake status from the Controller and then sends a command (brake/brake release) if necessary.

  We believe that this case study will provide valuable insights into the usability and scalability of our approach, while also offering feedback to refine our methodology and tackle real-world challenges. By integrating our research with industrial applications, we ensure that our methodology remains up-to-date and applicable to modern privacy needs in various industries. This case study serves as a crucial step toward opening the way for its wider adoption in industrial applications. Through practical experimentation and analysis, our goal is to demonstrate the tangible benefits of our approach in enhancing data privacy and security within industrial systems.

4. CONCLUSIONS AND FUTURE WORK

To conduct a comprehensive security assessment in software development, it is crucial to provide testers with a set of attack scenarios. When the privacy of data is a concern, testers should be given attack scenarios that specifically target digital privacy. These scenarios offer clear guidelines and help focus testers' efforts on specific threats and vulnerabilities that can compromise users' privacy. Through meticulous testing, vulnerabilities can be identified and resolved, minimizing the risk of data breaches or privacy violations. This study focuses on enhancing digital privacy within industrial applications. We plan to do this by proposing a methodology in which we first create a data flow diagram and then apply the STRIDE threat modeling framework to investigate all possible threats for our target application. We then extract

the privacy-related threats and consider them as potential privacy attacks. After identifying the attack vectors and scenarios for all extracted threats, we prepare them to give to the system testers for use in their test cases and test scenarios. The cooperative approach among testers, designers, and developers enhances the security of the application and instills user confidence in their digital privacy. By doing so, we hope to equip developers, security professionals and industries with the knowledge they need to proactively identify and mitigate these threats, improving the overall privacy and security of the systems and applications they develop and maintain.

For future directions, our proposed approach offers promising opportunities for further exploration and refinement. First, we apply our approach to the given case study and analyze the result. Then we aim to automate the process and discuss it further with system testers to automatically create test scenarios with some input from testers. Finally, we aim to work with more industries to conduct large-scale testing and deploy our approach in operational environments to enable practical evaluation and validation in the field.

ACKNOWLEDGMENTS

This work was supported by the Swedish Foundation for Strategic Research through the Serendipity project and the Knowledge Foundation through the SACSys project.

REFERENCES

[1] R. P. Romansky and I. S. Noninska, “Challenges of the digital age for privacy and personal data protection,” Mathematical Biosciences and Engineering, vol. 17, no. 5, pp. 5288–5303, 2020.
[2] “Ibm x-force threat intelligence index 2024,” library Catalog: www.ibm.com. [Online]. Available: https://www.ibm.com/reports/threat- Intelligence
[3] A. Shostack, “Experiences threat modeling at Microsoft.” MODSEC@ MoDELS, vol. 2008, p. 35, 2008.
[4] S. D. Lustgarten, Y. L. Garrison, M. T. Sinnard, and A. W. Flynn, “Digital privacy in mental healthcare: current issues and recommendations for technology use,” Current opinion in psychology, vol. 36, pp. 25–31, 2020.
[5] A. Pattakou, A.-G. Mavroeidi, V. Diamantopoulou, C. Kalloniatis, and S. Gritzalis, “Towards the design of usable privacy by design methodologies,” in 2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE). IEEE, 2018, pp. 1–8.
[6] Microsoft. (2024) Microsoft threat modeling tool. [Online]. Avail- able: https://learn.microsoft.com/en-us/azure/security/develop/threat- modeling-tool.
[7] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, “Avoidit: A cyber-attack taxonomy,” University of Memphis, Technical Report CS- 09-003, 2009.
[8] J. Steven, “Threat modeling-perhaps it’s time,” IEEE Security & Privacy, vol. 8, no. 3, pp. 83–86, 2010.
[9] P. Torr, “Demystifying the threat modeling process,” IEEE Security & Privacy, vol. 3, no. 5, pp. 66–70, 2005.
[10] Asadollah, Sara Abbaspour. "Cyberattacks: Modeling, Analysis, and Mitigation." In 2022 6th International Conference on Computer, Software and Modeling (ICCSM), pp. 80-84. IEEE, 2022.
[11] Dominicbetts. (2023) Security architecture for IoT solutions. [Online]. Available: https://learn.microsoft.com/en-us/azure/iot/iot-security- architectureperforming-threat-modeling-for-the-azure-iot-reference- architecture
[12] Arm. (2024) Confidential compute architecture. [Online]. Available: https://www.arm.com/architecture/security-features/arm- confidential-compute-architecture

AUTHOR

Sara Abbaspour is a lecturer specializing in safety and security-relevant cyber-physical systems. She works in the Cyber-Physical Systems Analysis group at Mälardalen University in Sweden. Sara served as a Postdoctoral researcher from 2018 to 2020 at Mälardalen University. She has successfully completed her PhD and defended her thesis titled 'Concurrency Bugs: Characterization, Debugging, and Runtime Verification'. Her primary research interests encompass safety and security-relevant cyber-physical systems, debugging, testing, and runtime verification of concurrent, parallel, and multicore software, security for wireless networks, service-level agreements in Industrial IoT, autonomous driving, and advanced driver assistance systems (ADAS). Sara also has work experience in various aspects of industrial environments such as Mobile Development Systems, Multimedia Technologies and eLearning applications, RFID, Smart card technologies, and Software System Testing.