Developer Driven Framework for Security and Privacy in the IoMT

Ceara Treacy[a], John Loane[b] and Fergal McCaffery[c]
Regulated Software Research Centre & Lero, Dundalk Institute of Technology, Dundalk, Ireland

Keywords: Security, Privacy, IoMT, Threat Modeling.

Abstract: The Internet of Medical Things (IoMT), is a fast growing domain as healthcare moves out of structured health services into care in the community. As a result, the sensitive personal and health data associated with the IoMT can potentially flow through a diversity of apps, systems, devices and technologies, public and open networks. This exposes data in the IoMT to additional attack surfaces, which requires the hardening of the security and privacy of the data. Accordingly, the data is bound by regulatory safety, security and privacy requirements. Applying the regulatory compliant requirements is a struggle for developers in small to medium enterprises due to lack of knowledge, experience and understanding. This paper proposes a framework to assist in meeting regulatory compliance for security and privacy of data in flow in the IoMT, directed at developers in small to medium enterprises. The framework considers both security and privacy properties for data in flow protection in the IoMT. This framework expands on the established threat modeling steps to consider both security and privacy. To mitigate the identified security and privacy threats, the framework includes a set of categorised technical security and privacy controls developed through medical device security standards. The originality of this framework is the inclusion of security and privacy requirements in the extension of the traditional threat modeling process, as well as the security and privacy controls embedded in the medical security standards.

1 INTRODUCTION

The Internet of Medical Things (IoMT), is a connected system, consisting of a variety of networks, medical devices and applications that collect data that are then provided to medical healthcare IT systems (Alsubaei et al., 2019). The IoMT is a growing domain and as it grows, cybersecurity risks have risen (Brien et al., 2018; Papageorgiou et al., 2018). Reports (Cisco, 2017; Ponemon Institute, 2018), determined that in terms of security maturity and privacy, the medical healthcare domain is behind other domains and vulnerable to industry-related cybersecurity. Small to medium enterprises (SMEs) particulary struggle. Difficulties in budget constraints, deficiency in knowledge and lack of trained personnel (Dhillon, 2011; Cisco, 2017; Ponemon Institute, 2018), complexity and compatibility issues in terms of the variety of IoMT technologies in use (Alsubaei et al., 2019) and understanding regulatory requirements (Parker et al., 2017), are some of the issues that contribute to inadequate cybersecurity and privacy strategies within this domain (Treacy & McCaffery, 2016). In addition, the fact that data in flow in the IoMT can be through various apps, systems, devices, technologies, public and open networks, which are inherently insecure such as wireless sensor networks and the cloud, has led to many security issues (Ponemon Institute, 2018). Moreover, security and privacy issues have arisen due to the rush into the lucrative healthcare domain and the speed the healthcare domain is embracing IoT without a profound understanding of the security and privacy risks (Hatzivasilis et al., 2019; Sun et al., 2018). Recommendations are that security and privacy are designed at the beginning of a development project, into the devices, the communication protocols and the services (McManus, 2018). To address the regulatory requirements and the above-cited difficulties, this paper proposes a framework aimed at SMEs and

[a] https://orcid.org/0000-0001-7722-5628
[b] https://orcid.org/0000-0002-9285-5019
[c] https://orcid.org/0000-0002-0839-8362

Treacy, C., Loane, J. and McCaffery, F.
Developer Driven Framework for Security and Privacy in the IoMT.
DOI: 10.5220/0009828304430451
In *Proceedings of the 15th International Conference on Software Technologies (ICSOFT 2020)*, pages 443-451
ISBN: 978-989-758-443-5

developers to assist with regulatory compliance requirements in addressing security and privacy of data flow in the IoMT.

This paper is structured as follows. Section 2 positions our work with respect to existing approaches. Section 3 offers our main contributions. Section 4 details the framework. Finally, Section 5 provides the future work and conclusion.

2 RELATED WORK

There are many TM tools and methods used to identify security threats (Hussain et al., 2014). However, in the existing security TM frameworks, including STRIDE (Deng et al., 2011), privacy protection and threats are not emphasised (Gholami et al., 2014). There are tools available for security TM such as the Microsoft Tool for TM (Microsoft, 2020), and the OWASP project, Threat Dragon tool (OWASP, 2020). For privacy TM there is ongoing research with privacy extensions for data flow diagrams (DFDs) that extend on LINDDUN (Antignac, Scandariato, & Schneider, 2016). SPARTA is a tool in development for security and privacy threat analysis (Sion et al., 2018). There is also research to include in a structured way into the TM process, the already determined security decisions and constraints that are known before the project begins (Sion et al., 2018). Hatzivasilis et al (2019), presented a study of the main defence mechanisms in core security and privacy controls, for providing end-to-end security and privacy in the IoMT. They state the study can act as a best-practices guide for general IoT or specialised IoMT applications.

3 CONTRIBUTIONS

It is now required that privacy and security are built into the core of technical products, which is applied by the EU General Data Protection Regulation (GDPR) requirement of *'data protection by design and by default'* (GDPR, 2016). A requirement of the GDPR is a Data Protection Impact Assessment (DPIA). A DPIA is an effective way to assess and demonstrate the project's compliance with the data protection principles and obligations (ICO 2020). Documenting the framework process provides evidence that a development project has implemented the appropriate technical and organizational measures to ensure and demonstrate compliance with the regulations (ICO, 2020). For an inclusive DPIA the current framework would require extension to include data storage as this research looks explicitly at the security and privacy of data in flow in the IoMT. A contribution of the framework is in bringing together the dispersed standards, best practice and guidelines.

In the existing security TM frameworks, including STRIDE (Deng et al., 2011), privacy protection and threats are not emphasised (Gholami et al., 2014). This framework considers the application of both security and privacy properties in a TM process for data in flow in the IoMT. The framework adopts and expands the Developer Driven Threat Model Process (DDTM) developed by Danny Dhillon (2011), which is based on the established TM steps as referenced in (Myagmar, Lee, & Yurick, 2005; Swiderski & Synder, 2004). The DDTM uses STRIDE for security threat identification. The framework adds a TM process that addresses privacy threat identification called LINDDUN. The LINDDUN framework is a systematic approach to assist with the elicitation and mitigation of privacy threats in software systems (Sion et al., 2018). The framework also applies security and privacy-aware data flow diagram extensions to the TM. Additionally, the framework maps the STRIDE and LINDDUN threat categories to established security and privacy properties and provides a categorized set of data flow security and privacy controls (DFSPCs) to mitigate the threats, which are also mapped to the security and privacy properties. This simplifies the threat mitigation process. The framework supports collection of the DFDs, vulnerabilities, threats, annotations and mitigation controls for the development of a knowledge base library for future projects.

4 FRAMEWORK

The framework currently focuses on the legal requirements for PII protection in the EU, which is regulated by the GDPR (General Data Protection Regulation (GDPR), 2016). The proposed framework has six steps: **Step 1:** Contextual knowledge. **Step 2:** System decomposition. **Step 3:** Threat identification. **Step 4:** Threat analysis. **Step 5:** Identify security and privacy properties against threats. **Step 6:** Selection of controls to mitigate threats.

4.1 Step 1 Contextual Knowledge

Step 1 provides the contextual knowledge to assist SMEs and new or inexperienced developers to

understand the security and privacy context in order to be able to use the framework. There are three parts to step 1 summarized in the following sections.

4.1.1 Part 1 Security and Privacy Objectives

The framework is based on PII security and privacy objectives that should reflect those of the organisation and balance the regulatory data privacy and security obligations (ISO/IEC, 2017). The framework security objectives are based in the Information Security Management System standard ISO/IEC 27001 (2017) and the privacy objectives in the standard for Privacy Information Management Systems, ISO/IEC 27701 (ISO/IEC, 2019). ISO/IEC 27701 is an extension to ISO/IEC 27001 and ISO/IEC 27002 and the privacy objectives align to the ISO/IEC 27001 security objectives. As specified in ISO/IEC 27701, the names and definitions for personal and health data categorisation and definitions can vary between different regulatory regimes. The framework requires the development of a PII classification scheme for an organisation, as detailed in ISO/IEC 27701, if not already in place. The classification incorporates definitions and explanation of: the nature of the PII e.g. personal health information; PII principals concerned e.g. PII relating to children. The regulatory requirements differ in relation to age of consent and how the information is processed and used; changing or extending the purposes for the processing of PII, which will require updating and/or revision of the legal basis and additional consent for use from the PII principal user.

4.1.2 Part 2 Security and Privacy Properties

Security and privacy properties are the common goals that the framework protects for data in flow in the IoMT. The traditional data security properties are confidentiality, integrity and availability (CIA). However, Whitman and Mattord (2011) assert that the CIA model no longer adequately addresses the constantly changing environment. The security properties for the framework considered the inadequacy of the CIA model and the requirements for the IoMT. The framework examined network security and adopted the eight security properties founded in Part 3 of the ISO/IEC 27033 standard for network security (ISO/IEC, 2010). Further research added the security property Authorization added from the STRIDE model. The security properties of the framework are: Authentication, Integrity, Non-repudiation, Confidentiality, Availability, Authorization, Access Control, Communication or Transport Security, and Privacy/Opacity. The decision to incorporate all of these security principles was taken as data in flow in the IoMT requires comparable security principles required for network security. The framework incorporates the privacy properties Deng et al. (2011) used to develop LINDDUN (Wuyts, Scandariato, & Joosen, 2014). The privacy objectives are based on the LINDDUN model, which are founded in the privacy objectives defined by Pfitzmann and Hansen (2010). The privacy objectives used are: Unlinkability, Anonymity & Pseudonymity, Plausible deniability, Undetectability & Unobservability, Confidentiality, Content Awareness and Policy and Consent Compliance.

4.1.3 Part 3 Administrate Two LINDDUN Privacy Threat Categories

This part of the framework is the implementation of two soft privacy properties, Content Awareness and Policy and Consent Compliance, and management of their LINDDUN threat categories Unawareness and Non-compliance respectively. Both of these soft privacy properties are significant for GDPR regulatory requirements and the requirements of the privacy standard ISO/IEC 27701. The non-compliance threat category means not following the data protection legislation, the advertised policies or the existing user consents of the regulatory jurisdiction (Wuyts & Joosen, 2015).The framework includes details on the requirements of privacy policy and consent to address policy and consent compliance and content awareness. It outlines how development can adhere to the specifics of the privacy policy. In consent for collecting data, development obtains the consent and then applies the correct collection in line with policy reason and use of the collected data within the specifics of demographics. Developers need to understand that if data is collected or used outside the privacy policy, there is a potential breach of privacy regulatory requirements.

4.2 Step 2 System Decomposition

Step 2 of the framework is decomposition of the system. The decomposition for the framework is founded in DDTM introduced by Dhillon (2011) as it was developed to provide a process that incorporated guidelines on creating DFDs for developers with or without security expertise. DFDs were also used because they are an established tool used by TM (Osterman, 2007; Shostack, 2014) and both STRIDE and LINDDUN use DFDs for decomposition and use (Sion, Wuyts, et al., 2018). In addition, their use was

aided by the fact that DFDs support following the data flow through a system and problems tend to follow the data flow (Shostack, 2014). Likewise, ISO/IEC 27701, advises the use of DFDs as helpful tools to inform a protection impact assessment and risk assessment transfer, which assists with regulatory requirements. Additionally, STRIDE and LINDDUN provide a set of threat types in relation to the elements of DFDs. Three key features for creating DFDs to assist inexperienced developers and SMEs are outlined in the framework, which are: DFDs Elements and Symbols, Decomposition Levels and Annotations.

4.2.1 DFDs Elements and Symbols

It is important that DFDs have a defined common set of elements, element names and symbols and these are used consistently throughout by the development team and within projects (Ibrahim & Yen, 2011). DFDs use standard symbols called elements, to graphically represent the interaction between data stores, processes, data flows, and external entities (Shostack, 2014). The framework uses these standard set of symbols with the adapted change in the process symbols presented by Ibrahim and Yen (2010, 2011). The framework also applies the diversity of boundaries, Machine Boundary and Process Boundary, presented by Osterman (2007) and Shostack (2008), and used by Dhillon (2011).

While the use of DFDs for TM security in systems is well established, their use for privacy is an emerging and developing area. The framework incorporates the principles of privacy DFD models from Antignac et al. (2016) to provide for privacy in the DFD feature of the framework. Antignac et al. (2016), applied the designation of the GDPR that personal data processing involves: collection, disclosure, usage, record, retrieval, and erasure. They used these concepts to establish a link with the privacy requirements of personal data as specified in standards and regulatory texts. The research provided a usable extension to the LINDDUN TM process called Privacy-Aware Data Flow Diagrams (PA-DFDs). The PA-DFDs privacy extensions reflect the personal data processing concepts from the GDPR and references the privacy principles of the ISO/IEC 29100:2011+A1:2018 (ISO/IEC, 2018). The framework applies the PA-DFDs three different types of external entities related to privacy, which are data subjects, data controllers, and data processors and the new element called Erasure, which pertains to the purpose of ensuring that erased data comply with the GDPR *'right to be forgotten'* principle. The framework also uses the two new process elements introduced, the *usage* and *complex usage* process elements.

4.2.2 Decomposition Levels

The more you know about the system, the easier it is to uncover threats (Meier et al., 2003). The framework applies the DFDs decomposition levels presented in research by (Ibrahim & Yen, 2010) and Dhillon (2011). The DFDs hierarchical levels are: Level 0 context diagram, system as a single entity; Level 1 more detailed DFD through refinement of the system; Level 2 more complex systems requiring decomposition of some components with annotations; Level 3 further decomposition of complex systems Dhillon (2011). Level 1 and 2 of DFD abstraction would include the annotations outlined in the next section. The framework fosters documentation for both security and privacy beginning at decomposition Level 0 that include the security and privacy properties and PII classification of the project. The security and privacy documentation will change over the level of decomposition. The framework requires uniformity in information and PII use through the levels of decomposition. Given privacy in TM and DFD decomposition is an emerging field, the framework uses the eleven security privacy principles detailed in the privacy framework standard ISO/IEC 29100 (2018) to provide a knowledge foundation for developers and SMEs not experienced with privacy.

4.2.3 Annotations

Dhillon (2011) found in his experience in Microsoft that DFD elements alone do not capture all necessary details to perform a security threat model effectively. Annotations to the DFDs consider the interactions of the system that could provide additional information to assist in the TM process (Dhillon, 2011; Scandariato, Wuyts, & Joosen, 2015). Addition of annotations were revealed to quicken the TM process, by bringing focus on the typical areas attackers are interested in and which are common sources of vulnerabilities (Dhillon, 2011; Scandariato et al., 2015). The vulnerabilities can be used to identify interactions that could introduce weaknesses making the identification process faster (Scandariato et al., 2015). The framework added annotations for both security and privacy. Security annotations include critical security functions such as; authentication, password management, and cryptographic operations, network and local dataflow; HTTP, API call and file I/O. Privacy annotations are linked to the

elements and interactions between the DFD elements, as seen in Antignac et al. (2016). The framework adds the annotations to the usage and complex usage process elements, the annotation is *purp*. The annotation of purpose is to track the purposes to which the data subject has consented. The data flow element carrying personal data is labelled *pdata* with a link provided through a dotted line to the corresponding data subject, which the personal data refers to provide records of where PII is in the system.(Antignac et al., 2016). It will also support developers identifying where in development to provide the added controls to keep the data secure and private. Understanding where PII is in the system and assessing the risks to the security and privacy at that point, could influence how, in what form, the necessity and why the data is transmitted. The framework uses annotations from Level 0 of abstraction, however, annotations can be added at any level of abstraction. The annotations should evolve in line with the previous abstractions of the system.

4.3 Step 3 Threat Identification

Step 3 of the framework is the identification of threats. Categorising threats makes it easier to understand what the threat allows an attacker to do and supports in assigning priority and mitigation (Hussain et al., 2014). Threat identification is central to the TM process but, is also one of the most difficult aspects of the process to complete, for developers with little or no experience (Dhillon 2011). The framework uses the threat categories from STRIDE and LINDDUN to address security and privacy threat identification. Threat identification is completed through both element-based and per interaction-based methods used by both LINDDUN and STRIDE and is centred upon the building blocks of DFDs (Sion et al., 2018).

Threat identification per-element is where each element in the DFD is analysed through the threat categories. Both STRIDE and LINDDUN have mapped their threat categories to DFD elements. Not all threat categories from both STRIDE and LINDDUN apply to all DFD element types. The STRIDE and LINDDUN threat categories to DFD elements mapping are presented in Table 1, where the LINDDUN threat categories are in red. Two of the categories overlapped. These are non-repudiation and disclosure of information. The LINDDUN threat category non-compliance only refers to the regulatory compliance and can only be addressed by the organisation and is out of scope for developers. However, it is vital that developers understand the regulatory compliance requirements for PII and comply with the PII classification, consent and the privacy policy outlined in step 1.

Threat identification per-interaction considers all interactions taking place in the system and details the origin, destination and interaction in the system and identifies threats against them (Shostack, 2014). Particular focus is with entry and exit points, where data enters or exits the system (Burns, 2005). The framework requires identifying the entry and exit points throughout the system through establishing the interactions. This is particularly relevant to the framework as the key categories for entry points to a system offer a way-in for attackers. The IoMT provides varied and numerous entry and exit points. Examples include: communication (especially wireless), software and physical (also known as hardware). These categories generally overlap with trust boundaries. When identifying the per-interaction threats inside the IoMT, it is important to note that trust boundaries are not fixed, they are subject to change (Seeam et al., 2019), as data moves through the system.

Table 1: STRIDE and LINDDUN threats categories mapped per DFD element.

Threat Category STRIDE & LINDDUN	Entity (External)	Data Flow	Data Storage	Process
Spoofing	X			X
Tampering		X	X	X
Repudiation Non-repudiation	X	X	X	X
Information Disclosure Disclosure of Information		X	X	X
Denial of Service		X	X	X
Elevation of Privilege				X
Linkability	X	X	X	X
Identifiability	X	X	X	X
Detectability		X	X	X
Unawareness	X			
Non-compliance		X	X	X

4.4 Step 4 Threat Analysis

Threat analysis is one of the most difficult aspects of TM (Dhillon, 2011). Both the Stride and LINDDUN categories are abstract enough, which means that

attacks could apply to one or more of the threat categories. There is a degree of required understanding and knowledge to map to tangible attacks and without security knowledge, STRIDE can't be used effectively (Dhillon, 2011). To support SMEs and developers lack of knowledge and understanding required to complete threat analysis, the framework maps the STRIDE and LINDDUN threat categories to the OWASP Top 10 (OWASP, 2019). The framework recommends using the mapping as an initial direction for threat elicitation and analysis. Both STRIDE and LINDDUN have extensive threat trees, employed in the framework as guidance and additional assistance. The framework also provides guidance for SMEs and inexperienced developers to address threat explosion. Threat explosion means that the threats can grow rapidly and the effort required to take into account all threats exceeds the TM process (Shevchenko et al., 2018; Wuyts et al., 2018).

The framework threat prioritisation is guided by the NIST SP 800-30 guide for conducting risk assessments (NIST, 2012). The framework uses the formula of Risk = Likelihood x Impact, including the definitions of the standard. Appendices G and H of the standard provide sets of exemplary tables for use in determining adverse likelihood and impacts quantitatively. Threat prioritization is guided by the quantitative outcomes of the formula and managed by the sensitivity of the PII and safety of the patient associated with the threat and vulnerabilities. NIST SP 800-30, provides standardised guidance for SMEs and developers with little or no knowledge and experience.

4.5 Step 5 Identify Security and Privacy Properties against Threats

This step of the framework provides a connection between the prioritised elicited threats and the security and privacy properties the framework protects. The threat categories of STRIDE and LINDDUN map to the security and privacy property it violates. The security and privacy properties are affiliated to the standards and regulatory requirements and step 5 maps the threats identified in step 4 to the frameworks security and privacy properties. The purpose of this mapping is to simplify identification of appropriate security and privacy controls to mitigate the identified threats. This is a straightforward step in the framework necessary to complete step 6. Similar to the threat elicitation and analysis stages, there will be commonalities and overlapping of property categories.

4.6 Step 6 Data Flow Security and Privacy Controls

Step 6 of the framework is the identification of the countermeasures needed to defend the security and privacy properties breached by the threats identified and prioritised. The security and privacy controls have been classified with respect to the security and privacy properties. A key objective of this research was the establishment of a set of technical security controls to maintain the security and privacy of data in flow. These are called the Data Flow Security and Privacy Controls (DFSPCs). The aim of the DFSPCs is to provide a set of technical controls to assist developers comply with security and privacy requirements of regulation and close the gap in knowledge in this area. The DFSPCs fill the vacuum of specific technical controls for the security and privacy of data in flow to assist developers to comply with the regulatory requirements.

The DFSPCs development originate in the international standard IEC/TR 80001-2-8 (IEC/TR, 2016). IEC/TR 80001-2-8 identified over 300 security controls in a set of tables evaluated for their relevance in establishing the 19 security capabilities of IEC/TR 80001-2-2 (Jump & Finnegan, 2017). Jump and Finnegan (2017), note that this should be considered an approach for a basic foundation in security. The controls are to manage risks to CIA and accountability of data and systems and do not consider privacy of data. IEC/TR 80001-2-8 does not encompass the security and privacy properties identified for the framework. The standards used to develop the controls for IEC/TR 80001-2-8 were examined for both the security and privacy controls of the framework. IEC/TR 80001-2-8 mapped the controls from six security standards. Two standards, ISO/IEC 27002 (ISO/IEC, 2013) and IS0 27799 (ISO, 2016), are for operational and administrative security controls and were not considered suitable for the DFSPCs as they did not employ technical controls. There were four standards used for technical controls: ISO/IEC 15408-2 (ISO, 2016), ISO/IEC 15408-3 (ISO/IEC, 2008), NIST 800-53 Rev. 4 (NIST, 2014) and IEC 62443-3-3 (IEC, 2013). ISO/IEC 15408-3 defines the assurance requirements of the evaluation criteria, which was deemed out of scope for the DFSPCs and was excluded. The remaining three standards were examined to establish the DFSPCs.

5 CONCLUSIONS

In this paper, we presented a framework to assist SMEs and inexperienced developers through a TM

process to protect the security and privacy of data in flow in the IoMT. The framework considers both security and privacy objectives and properties based in standards and addresses regulatory requirements. The framework is built on established TM processes and threat and privacy threat identification categories. In addition the framework provides a set of technical security and privacy controls, the DFSPCs, from the standards to mitigate the elicited threats.

Future work is in a comprehensive validation of the framework by experts and implementation into the development environment of a SME. Three experts in the TM domain have been identified to review the framework. The security controls have been validated by two industry experts and one expert from the medical device standards domain. Experts from the privacy standard domain and industry have been identified to validate the privacy controls. On completion of the expert validation of the framework, it will be implemented in the development teams of two companies from the medical domain.

ACKNOWLEDGEMENTS

This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094.

REFERENCES

Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things*, *8*, 100123. https://doi.org/10.1016/j.iot.2019.100123

Antignac, T., Scandariato, R., & Schneider, G. (2016). A privacy-aware conceptual model for handling personal data. In *7th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation - ISoLA'16 (1)* (pp. 942–957). Springer, Cham. https://doi.org/10.1007/978-3-319-47166-2_65

Brien, G. O., Edwards, S., Littlefield, K., McNab, N., Wang, S., & Zheng, K. (2018). NIST SP 1800-8 Securing Wireless Infusion Pumps In Healthcare Delivery Organizations. Retrieved from https://nccoe.nist.gov/projects/use-cases/medical-devices

Burns, S. (2005). *Threat Modeling: A Process To Ensure Application Security*. *SANS Institute InfoSec Reading Room*. SANS.

Cisco. (2017). *2017 Annual Cybersecurity Report* (Vol. I). San Jose. https://doi.org/10.1002/ejoc.201200111

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, *1*(16), 3–32. Retrieved from http://web.b.ebscohost.com.library.capella.edu/ehost/pdfviewer/pdfviewer?sid=e7ebe3bc-59f7-43a0-ace9-60485dc3acd3%40sessionmgr111&vid=1&hid=118

Dhillon, D. (2011). Developer-Driven Threat Modeling: Lessons Learned in the Trenches. *IEEE Security and Privacy*, (9), 41–47. https://doi.org/10.1109/MSP.2011.47.

General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 of the European Parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Dir. EU. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN

Gholami, A., Lind, A. S., Reichel, J., Litton, J. E., Edlund, A., & Laure, E. (2014). Privacy threat modeling for emerging biobankclouds. *Procedia Computer Science*, *37*, 489–496. https://doi.org/10.1016/j.procs.2014.08.073

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019). Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics. In *Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019* (pp. 457–464). IEEE. https://doi.org/10.1109/DCOSS.2019.00091

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. *Sci.Int.(Lahore)*, *26*(4), 1607–1609.

Ibrahim, R., & Yen, S. Y. (2010). Formalization of the Data Flow Diagram Rules for Consistency Check. *International Journal of Software Engineering & Applications*, *1*(4), 95–111. https://doi.org/10.5121/ijsea.2010.1406

Ibrahim, R., & Yen, S. Y. (2011). A Formal Model for Data Flow Diagram Rules. *ARPN Journal of Systems and Software*, *1*(2), 60–69.

ICO. (2020). What is a DPIA? Retrieved January 13, 2020, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

IEC/TR. 80001-2-8:2016 Application of risk management for IT-networks incorporating medical devices — Application guidance Part 2-8 : Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2 (2016).

IEC. (2013). 64223-3-3 Industrial Communication Networks - Network and System Security – Part 3-3: System security requirements and security levels. European Commission. Retrieved from http://www.iec.ch/dyn/www/f?p=103:22:0::::FSP_ORG_ID:1250

ISO/IEC. (2008). 15408-3:2008 Information technology - Security techniques - Evaluation Criteria for IT Security - Part 3: Security assurance components.

ISO/IEC. (2010). 27033-3 -Information technology — Security techniques — Network security Part 3:

Reference networking scenarios — Threats, design techniques and control issues. BSI Standards Publication.

ISO/IEC. (2013). 27002:2013 - Information technology — Security techniques — Code of practice for informati on security controls. Switzerland.

ISO/IEC. (2017). 27001:2017 Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013).

ISO/IEC. (2018). 29100:2011+A1:2018 Information technology — Security techniques — Privacy framework. British Standards Publication.

ISO/IEC. (2019). 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

ISO. (2016). 27799-27002:2016 Health informatics — Information security management in health using, *27002*.

Jump, M., & Finnegan, A. (2017). Using Standards to Establish Foundational Security Requirements for Medical Devices. *Biomedical Instrumentation and Technology*, *51*(s6), 33–38. https://doi.org/10.2345/0899-8205-51.s6.33

Marr, B. (2018). Why The Internet Of Medical Things (IoMT) Will Start To Transform Healthcare In 2018. Retrieved September 9, 2019, from https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#7cbe068b4a3c

McManus, J. (2018). Security by Design: Teaching Secure Software Design and Development Techniques. *J. Comput. Sci. Coll.*, *33*(3), 75–82. Retrieved from http://dl.acm.org/citation.cfm?id=3144687.3144710

Meier, J. D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R., & Murukan, A. (2003). *Improving Web Application Security : Threats and Countermeasures*. Retrieved from https://www.microsoft.com/en-us/download/confirmation.aspx?id=1330

Microsoft. (2020). Microsoft Threat Modeling Tool - Azure | Microsoft Docs. Retrieved February 6, 2020, from https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

Myagmar, S., Lee, A. J., & Yurick, W. (2005). Threat Modeling as a Basis for Security Requirements Suvda. In *In Symposium on requirements engineering for information security (SREIS)* (pp. 1–8).

NIST. (2012). *Special Publication 800-30 Guide for Conducting Risk Assessments*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:NIST+Special+Publication+800-30#0

NIST. (2014). 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations. *Joint Task Force Transformation Initiative*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53Ar4

Osterman, L. (2007). Threat Modeling, once again – Larry Osterman's WebLog. Retrieved November 18, 2019, from https://blogs.msdn.microsoft.com/larryosterman/2007/08/30/threat-modeling-once-again/

OWASP. (2019). OWASP Top Ten. https://doi.org/10.1007/s11623-006-0164-8

OWASP. (2020). OWASP Threat Dragon. Retrieved March 3, 2020, from https://owasp.org/www-project-threat-dragon/#

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access*, *3536*(c), 1–13. https://doi.org/10.1109/ACCESS.2018.2799522

Parker, L., Karliychuk, T., Gillies, D., Mintzes, B., Raven, M., & Grundy, Q. (2017). A health app developer's guide to law and policy: A multi-sector policy analysis. *BMC Medical Informatics and Decision Making*, *17*(1), 1–13. https://doi.org/10.1186/s12911-017-0535-0

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version 0.34 Aug. 10, 2010). *Technical University Dresden*. tech. rep. TU Dresden and ULD Kie. https://doi.org/10.1.1.154.635

Ponemon Institute. (2018). *The State of Cybersecurity in Healthcare Organizations in 2018*.

Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering*, *20*(2), 163–180. https://doi.org/10.1007/s00766-013-0195-2

Seeam, A., Ogbeh, O. S., Guness, S., & Bellekens, X. (2019). Threat Modeling and Security Issues for the Internet of Things. In *2nd International Conference on Next Generation Computing Applications 2019, NextComp 2019 - Proceedings* (pp. 1–8). https://doi.org/10.1109/NEXTCOMP.2019.8883642

Shevchenko, N., Frye, B. R., & Woody, C. (2018). *Threat Modeling for Cyber-Physical System-of-Systems: Methods Evaluation*. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=526365

Shostack, A. (2008). Experiences threat modeling at Microsoft. *CEUR Workshop Proceedings*, *413*, 1–11.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. John Wiley & Sons.

Sion, L., Van Landuyt, D., Yskout, K., & Joosen, W. (2018). SPARTA: Security & Privacy Architecture Through Risk-Driven Threat Assessment. *Proceedings - 2018 IEEE 15th International Conference on Software Architecture Companion, ICSA-C 2018*, 89–92. https://doi.org/10.1109/ICSA-C.2018.00032

Sion, L., Wuyts, K., Yskout, K., Van Landuyt, D., & Joosen, W. (2018). Interaction-Based Privacy Threat Elicitation. *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*, 79–86. https://doi.org/10.1109/EuroSPW.2018.00017

Sion, L., Yskout, K., Van Landuyt, D., & Joosen, W. (2018). Solution-aware data flow diagrams for security threat modeling. In *Proceedings of the ACM Symposium on Applied Computing* (pp. 1425–1432).

https://doi.org/10.1145/3167132.3167285
Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and Privacy in the Medical Internet of Things: A Review. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/5978636
Swiderski, F., & Synder, W. (2004). Threat Modeling. Retrieved March 11, 2016, from https://msdn. microsoft.com/en-us/library/ff648644.aspx
Treacy, C., & McCaffery, F. (2016). Data Security Overview for Medical Mobile Apps Assuring the Confidentiality , Integrity and Availability of Data in Transmission. *International Journal on Advances in Security*, *9*(3 & 4), 146–157.
Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security Fourth Edition*. Boston: Cengage Learning.
Wuyts, K., & Joosen, W. (2015). Tutorial privacy threat modeling: a tutorial, Technical Report (CW Reports), LINDDUN tutorial. Retrieved from https://linddun.org/downloads/LINDDUN_tutorial.pdf%0Ahttps://distrinet.cs.kuleuven.be/software/linddun/downloads/LINDDUN_tutorial.pdf
Wuyts, K., Scandariato, R., & Joosen, W. (2014). Empirical evaluation of a privacy-focused threat modeling methodology. *Journal of Systems and Software*, *96*, 122–138. https://doi.org/10.1016/j.jss.2014.05.075
Wuyts, K., Van Landuyt, D., Hovsepyan, A., & Joosen, W. (2018). Effective and efficient privacy threat modeling through domain refinements. *Proceedings of the ACM Symposium on Applied Computing*, 1175–1178. https://doi.org/10.1145/3167132.3167414.