An Overview and Ontology of Privacy to Preserve Privacy in Ultra-Wideband Networks

Katharina O. E. Müller, Jan von der Assen, Chao Feng, Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland
E-mail: [mueller, vonderassen, cfeng, stiller]@ifi.uzh.ch

***Abstract*—The Internet of Things (IoT) has become increasingly popular due to the growing number of IoT devices and the adoption of numerous communication protocols. With the renewed interest in Ultra-Wideband (UWB) positioning and recent reports on privacy infringements through UWB-enabled spyware, the consideration of privacy in UWB applications has become paramount. Currently, an IoT-centric security database is under development, VarIoT, however, there is no filter for privacy- or protocol-based vulnerabilities, risks, or threats and current UWB literature does not focus on privacy.**

Thus, this work formalizes privacy risks as attack patterns, based on the UWB protocol and presents it in an ontology. The effectiveness of this ontology is exemplified by a case study that receives UWB artifacts as input and derives a set of privacy risks by relying on the presented formalized knowledge graph. By exhibiting the ontology's ability to automatically derive threats for an applied scenario an increased privacy preservation in UWB networks and solutions is reached.

***Index Terms*—privacy, UWB, IoT, ontology, knowledge graph**

I. Introduction

The adoption of Internet of Things (IoT) devices has increased significantly [25] and resulted in a diversified market of non-interoperable devices due to proprietary systems built upon a multitude of communication protocols with varying hardware requirements. Common communication protocols in smart home environments are Bluetooth Low Energy (BLE) and Wi-Fi [18]. However, with the introduction of the Ultra-Wideband (UWB) 802.15.4z amendment and its support from the Fine Ranging (FiRa) Consortium, UWB gains renewed traction for precise and accurate localization of non-smart objects [8].

The latest push by FiRa Consortium partners, such as Apple, NXP, Samsung, and Google, to introduce UWB in personal devices, such as smartphones and tracking tags, is cause for concern from a privacy perspective. Particularly since UWB enables very precise tracking indoors, opening the door for potential user profiling and targeted advertisements, infringes on user privacy in a myriad of ways [1], [25]. For example, with the correct UWB infrastructure and the user carrying a potential tracker with them at all times (their smartphone), a user could be continuously located down to a few centimeters. Consequently, the user can be profiled down to their daily schedule, preferences, routes, and even when they leave their desk at work [1]. Not only does this risk the user's right to privacy, but it also risks the privacy of aggregated personal data, which could be leaked [1], [25] or used to spy on the user, *cf.* recent news concerning AirTag incidents [19]. This showcases a need for further investigation into privacy in UWB and IoT, especially, since privacy is rarely the singular focus of UWB research [2], [29]. The lack of concern for privacy is a crucial gap in current research.

This work fills the privacy gap in current research by laying the theoretical groundwork for a tool to improve the privacy of IoT devices within an IoT environment by providing tailored privacy suggestions based on the network's specific setup and protocols. While existing IoT security and privacy vulnerabilities are provided by databases, such as VARIoT [20], this paper provides a detailed categorization according to the UWB protocol, with a sole focus on privacy. While separating privacy and security into distinct categories, this work provides the following contributions:

- An overview of current work on privacy in UWB
- An ontology-based formalization for privacy attack patterns in UWB
- A knowledge graph that captures domain knowledge on privacy attack patterns relating to UWB

The remainder of this paper is organized as follows. Section II details the UWB technology and key outcomes of privacy-based surveys in UWB and IoT. While Section III provides an overview of privacy risks and threats for the construction of a privacy ontology for UWB, Section IV details the formalization of this scenario and ontology, followed by Section V, which showcases the ontology in a case study. Lastly, Section VI summarizes and outlines next steps.

II. Background and Related Work

Privacy is a complex term to define [9]. According to the National Institute of Standards and Technology (NIST), privacy has three definitions [22]. The first defines privacy as an assurance that both confidentiality and access to information concerning the entity are protected. The second further defines the entity as an individual with a right to "freedom from intrusion into the private life or affairs" [22], especially when infringed upon by the illegal gathering and use of their descriptive data. And the third redefines the entity as a party with the additional right to control its data.

Later, Section III relates to these NIST definitions to varying degrees. Definition three was rarely considered. While none of the presented approaches considered a mathematically formalized definition of privacy, such as of [9], they all agreed that privacy is the confidentiality of an entity's data or data gathered about them as well as the entity's right to know when their data is being gathered [25], which is the definition of privacy considered in this work. Due to the formalization of the threat model in Section IV, the privacy definitions above were categorized into six privacy goals as of [10]: Unobservability, Unlinkability, Transparency, Anonymity, Accountability, and Confidentiality, all of which must be fulfilled to consider a system privacy-preserving.

A. Security and Privacy in IoT

Security and privacy are often considered in tandem [24], [32], hence focusing singularly on privacy without the consideration of security is not possible. If a security vulnerability is uncovered and demonstrates a possible loss of private information, it is also considered a privacy risk [27]. In contrast, a privacy risk is not possible without a security vulnerability. Therefore, this work considers privacy risks a subset of security vulnerabilities.

A privacy risk can be demonstrated by exploiting the security vulnerability, as presented by [33]. The authors showcased three leakage attacks to retrieve the handshake key, owner account, and personal information on the August smart lock system. Utilizing a rooted mobile device, they were able to access the system files, which stored the plaintext data, leverageable to fake an owner by importing the unprotected system files and allowing attackers control over the smart lock, account, and personal information. The unencrypted system files constitute a security vulnerability and a privacy risk since the attacker gained control of the owner's account, allowing access to the August smart lock and the owner's personal information.

B. UWB Protocol

In 2002, the Federal Communications Commission (FCC) defined the high frequency range bands [25] necessary for UWB. Consequentially, the IEEE has introduced UWB standards, including IEEE 802.15.4 Impulse Radio UWB (IR-UWB) to enable highly accurate ranging and positioning [25]. IR-UWB has since seen multiple renewals and amendments, such as IEEE 802.15.4a and IEEE 802.15.4z in 2019, intending to improve ranging performance and Physical Layer security [8].

Thus, UWB is a wideband technology that utilizes a broader spectrum of frequencies, but at lower power and for multiple short bursts [30]. These bursts must stay within the FCC limits of a maximal Power Spectral Density (PSD) of -51.3 dBm/MHz, conversely, requiring multiple pulses across the spectrum to transmit the same amount of data as Bluetooth, with a single signal and its maximum PSD of 33 dBm/MHz. Thus, UWB blends into the noise floor without interfering with other communication protocols, thereby, ensuring it is resistant to interference.

Based on this, UWB presents an interesting basis for research, especially regarding the positioning, tracking, and monitoring of persons in indoor spaces. The hope is that its precision and accuracy in localization will enable more reliable indoor solutions compared to Bluetooth.

C. Related Work: Surveys on Privacy in UWB

This evaluation of surveys on privacy in UWB includes surveys wherein UWB was evaluated with other protocols.

1) Wireless Sensor Networks (WSN): Multiple surveys in the field of wireless networks and WSNs consider UWB in their security overview [14], [27], hence only lightly touching upon privacy concerns. [27] found UWB to utilize three link-layer security levels with no encryption, partial encryption, and full AES-128 communication encryption, with respective levels of data privacy protection. However, [14] deemed UWB secure due to its resistance to multipath effects as well as signal interception and interference, resulting in resistance to jamming attacks. Additionally, [6] focused on the security of the UWB PHY layer and found that it is a superior technology for WSNs, but, privacy, data encryption, and integrity were not fully considered.

2) IoT and Internet of Medical Things (IoMT): The [18] survey paper on research challenges in IoT outlines the need for privacy-preserving mechanisms in IoT, not mentioning protocol-specific solutions. [17] focused on the security of UWB in IoMT and found that it is promising due to its low power consumption and robustness to interference, [32] agreed that the security features were robust, attributing this to the low radiated power and narrow pulses resulting in less attack surface. In contrast, the incompatibility of AES encryption in multichannel mode and the lack of strong and lightweight cryptography algorithms pose a privacy risk to IIoT systems. Finally, [32] determined that interoperability is the core of IIoT security challenges.

3) Localization: The literature focuses extensively on secure localization in UWB. [2] and [29] found that even though privacy is of principal importance, the literature does not cover it sufficiently. [28] and [21] highlighted considerations of UWB standard security with the absence of privacy considerations. Therefore, no clear consensus on the privacy risks in UWB is available today. While many sources praise UWB as a more secure communication protocol, the involved privacy risks are not fully considered or analyzed.

III. Overview of Privacy in UWB

The surveys reviewed in Section II focused on the increase in positioning accuracy and radar-based localization, rather than privacy. Recent research has begun to include privacy considerations, entirely focusing on potential privacy risks of UWB through its continued integration into smart environment solutions. Here, work with the keywords UWB and privacy were considered, focusing on papers from 2017 onward. However, in most cases, privacy was only mentioned rather than analyzed. Thus, only the most pertinent results are presented below.

A. Privacy Interviews

In the 2021 [1] studied three aspects of privacy in UWB-enabled smartphones: *(i)* the perception of privacy, *(ii)* potential privacy concerns, and *(iii)* approaches to address privacy concerns by conducting interviews with experts and users. The expert interviews revealed that the broader bandwidth of UWB results in higher security, as spoofing requires the correct frequency and timing. Nevertheless, it is only a matter of time before UWB insecurities are uncovered.

UWB experts' concerns on surveillance for personal devices include utilizing UWB radar for mapping user surroundings and locating users, who do not wish to be located, as well as tracking and profiling people based on the device's UWB usage. Similarly, a UWB-based infrastructure could intrusively acquire user locations with centimeter accuracy through multiple UWB sensors placed at known locations. Such a pervasive infrastructure could also track the MAC address across time and facilitate targeted advertising. Through the addition of UWB devices to the infrastructure and an increase in users carrying UWB sensors with them, surveillance is more effortless and could be more efficient than BLE in social distancing tracking.

Regarding social privacy risks, the UWB infrastructure interconnects users through the UWB mesh network created. Thus, they might unwittingly locate other users and facilitate stalking of users and social network analysis. On a personal device level, devices share data with unknown devices and users within the same indoor space, such as a clothing store. The device also enables users to locate other users' belongings and track other users' locations with identifiable IDs, constituting an infringement of other users' privacy, especially if they do not wish to be tracked.

On an institutional level, the personal device collects data that might be shared or sold and processed by third parties. Free applications, in particular, often excessively collect user information, wherein they often ask and receive access to data far beyond justification. For example, a tic-tac-toe game would not require location data to function, but might still collect it to sell to other companies. This becomes increasingly dangerous as an aggregation of such data, even though anonymized, could still be used in combination, thus, profiling and deanonymizing users. Creating such an infrastructure can utilize users as free repeaters for faster 5G data rates, localization, profiling, and deanonymization.

B. UWB Localization

Similarly, [25] investigated possibilities to secure UWB ranging and localization in an industrial setting, finding that UWB positioning is not entirely tamper-proof due to security vulnerabilities in the physical layer, MAC layer, and link layer. Due to his focus on industrial applications, privacy was evaluated as comparatively riskless, finding that there are only three possible threats to privacy: a position of partial spoiling, a position of total spoiling, and broken privacy, which could result in privacy issues such as the leaking of industrial secrets.

Thus, local eavesdroppers constitute a privacy risk as they expose localization data, but are internally necessary to monitor the industrial environment. Furthermore, a fully remote privacy leak would only occur due to flaws in the local infrastructure, unrelated to UWB. Ultimately, any active radio device inadvertently broadcasts its rough location and device information, thus, presenting a privacy risk. A flaw improved, but not solved through encryption, since it does not prevent message exchange monitoring, modification, or extraction of physical parameters such as received power, Time-of-Flight, or phase.

Additionally, [7] found multiple security threats to location-based services in IoT. Among the multitude of security threats, two also represent a privacy risk. The first security threat was identity theft due to known IoT device location, thus, representing a privacy risk. Secondly, a trusted network issue can lead to complete control of positioning data, which can then be leaked or misused.

Contrastingly, [31] included privacy as a central aspect of secure UWB-based positioning systems. They agreed with [25] that to preserve privacy, neither the presence nor identity of a device shall be detectable by undesired nearby devices. Two-Way Ranging (TWR) based UWB systems inherently do not fulfill the need for privacy since they actively exchange messages between tags and anchors, revealing both the anchors and the presence of the tag.

Currently, Real-Time Location Systems (RTLS) are moving toward unidirectional communication to avoid revealing the presence of their devices. Upstream RTLS systems rely on a tag sending out periodic polling or broadcast messages to the anchors. Thus, infringing on privacy of tagged devices by continuously revealing their presence. Downstream RTLS systems are more privacy-preserving, as the four anchors sequentially broadcast messages to the tags, while the tags themselves estimate their position, only revealing the anchor's presence.

C. IoMT Communication

[17] surmises that the ZigBee-centric Same-Nonce attack could also be used on UWB to clear the Access Control List, which results in the device sharing its nonce and security key twice. Hence, the eavesdropper could recover device information by XOR-ing two messages, resulting in a loss of privacy of the device's identity and location.

D. Impulse Radio UWB (IR-UWB) Monitoring

IR-UWB is applied as a radar in home environment monitoring [26], fall detection [12], and person counting [16]. Radar functions through one anchor emitting UWB signals and evaluating the returned signal reflections to detect people or a fall within a room. The authors agree that IR-UWB is more privacy-preserving than previous camera-based approaches. Additionally, [26] indicate that IR-UWB radar solutions are only privacy-preserving if the user is not required to wear a wearable sensor that could identify them. Nevertheless, the localization of a specific person among many, and detecting

TABLE I
OVERVIEW OF PRIVACY RISKS IN LITERATURE AND THE THREATENED PRIVACY GOALS

	Attack Pattern			**Technical Details**				**Threatened Privacy Goals**							
		Infrastructure	**Personal Device**	***TWR***	***Radar***	***Downstream***	***Upstream***	***Notice***	***Unobservability***	***Unlinkability***	***Transparency***	***Anonymity***	***Accountability***	***Confidentiality***	**Source**
1	Map user surroundings		●		●			●	●	●	●	●		●	[1]
2	Locate users who may not want to be located		●	●	●		●	●	●	●	●	●		●	[1], [15]
3	Ability to track/profile people based on UWB device usage		●	●			●	●	●	●	●	●		●	[1], [3], [15]
4	Data sharing in a confined space with unknown people		●				●	●	●	●	●			●	[1], [15]
5	Use of UWB to locate other's belongings		●	●				●	●		●				[1]
6	Usage of UWB localization to follow/track people with IDs		●	●			●	●	●	●	●	●		●	[1], [3]
7	Information may be processed by third parties	●	●	●			●	●		●	●	●		●	[1], [3], [15]
8	Excessive data collection without a justifiable reason	●	●	●			●	●	●	●	●		●	●	[1], [15]
9	Aggregation of data across applications		●	●				●	●	●	●	●	●	●	[1], [3]
10	Track people based on location with multiple UWB sensors	●		●			●	●	●		●	●		●	[1], [15]
11	Tracking a MAC address across time	●		●			●	●	●	●	●			●	[1]
12	Intrusive inquiry and targeted advertising	●		●			●	●	●	●	●	●			[1]
13	More devices, naturally leading to easier surveillance	●		●			●	●	●	●	●	●			[1]
14	Social distancing surveillance	●		●	●	●	●			●	●				[1]
15	Stalking users	●	●	●			●	●	●	●	●	●		●	[1]
16	UWB interconnected, with additional users in mesh network	●		●			●	●			●				[1]
17	Social network analysis	●		●			●	●		●		●			[1]
18	Aggregated data and customer profiling	●		●			●	●	●	●	●			●	[1], [15]
19	Deliberate deanonymization	●		●			●	●	●			●		●	[1], [3], [4]
20	Integration with 5G for faster data rates	●		●			●								[1]
21	Identity theft based on IoT location	●	●	●			●	●	●	●	●	●		●	[4], [7]
22	Trusted network issues	●		●		●	●	●						●	[7], [25]
23	Tag spoofing to access unauthorized area or data		●	●	●	●	●				●			●	[25]
24	Position can be approximately seen by an attacker		●	●			●	●	●	●	●	●		●	[25]
25	System-level position accuracy	●		●				●	●	●	●	●		●	[25]
26	Private content read by unauthorized parties			●				●		●	●	●		●	[25]
27	Known presence: continuous broadcasting	●	●	●				●	●			●		●	[31]
28	Known presence: uni-directionally broadcasting to anchor		●				●	●	●			●		●	[31]
29	Decrypted data: wrong access control configuration	●	●	●			●	●	●		●			●	[17]
30	Movement profiling, localization and counting of occupants	●			●		●	●	●	●	●	●		●	[12], [16], [26]

whether they fell, is a privacy risk as it would require a movement profile.

E. Privacy by Design (PBD)

[15] found two privacy issues in an off-the-shelf PBD system: *(a)* the sending of company-related data to a system outside the companies' IT infrastructure results in sharing of internal workflow information of interest to competitors and *(b)* the gathering of tracking data includes the data of nearby peripherals, such as smartphones, meaning the tracking data stored on the cloud server inadvertently includes employee data, which allows for the profiling of employees. It was concluded that these privacy issues stem from the architecture, including a cloud server, and the lack of control and configurability over shared data, which results in sharing of all data, independent of the source. [4] found that linking IoT communications and user identity, can lead to adversarial data modifications and significant health risks.

[3] agrees with [15] and [4] that privacy preservation is not entirely understood, especially since concealing the identity of a user or device does not fully provide privacy. In most cases, the accumulated data stored in a cloud is detailed enough to identify a person or device through analysis and data aggregation. They identified three privacy threats: *(a)* the identity disclosure threat; *(b)* the attribute disclosure threat, which leverages a combination of data from multiple attributes; *(c)* the correlation analysis attack, which tracks, stores, and combines available data to form a user profile.

Overall, this overview here shows that privacy threats exist in UWB. Most authors agree that the focus of current research projects is the accuracy of UWB positioning and effectiveness of localization or monitoring, rather than the privacy of users [1], [15], [25], [34]. Table I, summarizes the aggregated privacy risks and threats as attack patterns; the dot indicates, if the column characteristic applies. Each attack pattern is categorized according to [1]'s types: Infrastructure or Personal Device. The second set of columns describes technical details of the attack pattern, for example, is it based on a UWB Radar localization approach or is it an anchor and tag-based approach with either TWR, Upstream, or downstream communication. The third set of columns considers seven privacy goals, according to [10], indicating whether the attack pattern infringes upon one or more privacy goals, according to the scenarios described in the literature of each individual attack pattern, indicated in the last column. This Table I is the basis for the formalization and privacy ontology in Sections IV and V, thus of key importance for this work.

IV. PRIVACY ONTOLOGY AND KNOWLEDGE GRAPH

Ontologies present an opportunity to represent, communicate and relate gathered knowledge in a standardized formulation, such as the Web Ontology Language (OWL). To

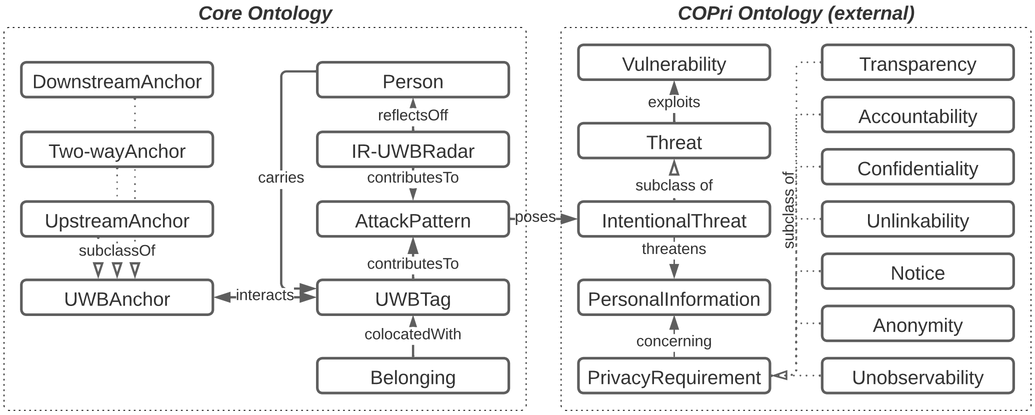


Fig. 1. Privacy Ontology and COPri Ontology

obtain and develop a knowledge graph that represents the relevant concepts, properties, and relationships, of a particular domain of interest, need to be mapped to the basic notions such as classes, properties, and individuals defined in a formal language [13]. This paper follows a well-understood and widely adopted methodology to leverage ontologies for knowledge-engineering [23] to provide a knowledge graph of the previously described findings.

A. Methodology

To develop an ontology enabling the sharing and reuse of domain knowledge, the first key activity is the definition of **competency questions**. Such questions ensure that the scope of an ontology is well-defined, by outlining the types of answers that shall be answered using the formalized knowledge [11]. The goal of the presented ontology is twofold since it *(i)* details the architectural relationships of nodes in UWB networks that are relevant from an adversarial perspective and *(ii)* surfaces privacy threats that may be introduced by integrating these devices. Thus, the following key competency questions are considered for the development of the ontology:

1) What is the role of a device in a certain scenario?
2) Which threats apply to the usage of a device?
3) How do related threats impact privacy goals?

Based on this definition, it becomes apparent that the ontology must be able to **enumerate** key concepts such as privacy requirements, vulnerabilities, threats, and countermeasures. A critical step, to ensure that the knowledge represented by the ontology is not siloed, is the consideration of **existing ontologies**. A core methodology for privacy threats was formalized in the domain of requirements engineering [10]. The *COPri* ontology was implemented in *OWL* and defines relationships between threats, vulnerabilities, and their impact on privacy goals. Furthermore, to relate UWB devices to specific vulnerabilities, the dissemination provided by [20], which captures knowledge about affected products, is vital.

With the key concepts enumerated and knowledge on privacy threats (*cf.* Section III) being acquired, the remainder of the ontology development methodology comprises the definition of the class hierarchy, the addition of properties to the classes and finally, the establishment of instances. The development of the ontology follows a top-down approach, since privacy threats may not only affect instances but broad classes of devices. This ontology comprises two perspectives, the architectural view on UWB technology and its relation to privacy threats. Both areas are codified using *WebVOWL* and described in the subsequent chapters.

B. UWB Ontological Entities

Based on the analysis of UWB technology in the previous chapter, four privacy-relevant architectural scenarios can be derived from the literature. A subset of elements from the *COPri* ontology is reused, starting from a set of privacy goals. In *COPri*, these goals are threatened by *IntentionalThreats*, for which in turn, an *AttackPattern* must exist. Thus, the architectural elements from UWB technology are formalized so that they represent a relation to *AttackPattern*. Although there are no UWB-related vulnerabilities in the *VARIoT* database, the *Vulnerability* class from the related ontology is related as an external entity to an element of the UWB architecture.

The core elements proposed in the ontology have a direct relationship to an *AttackPattern* are *UWB Tags* and *IR-UWB Radars*, since there are no privacy risks without the presence of these elements. While a *Person* may be localized solely by an *IR-UWB Radar*, an *UWB Tag* requires the presence of one or more *UWB Anchors*. Specifically, such anchors are formalized as disjoint subclasses which characterize their communication mode. As such, anchor-based UWB networks may be either *Downstream*, *Upstream* or *Two-Way-Ranging*. UWB-enabled *Smartphones* are represented as a subclass of anchors. Figure 1 presents the core ontology, on which we build the privacy threat knowledge graph.

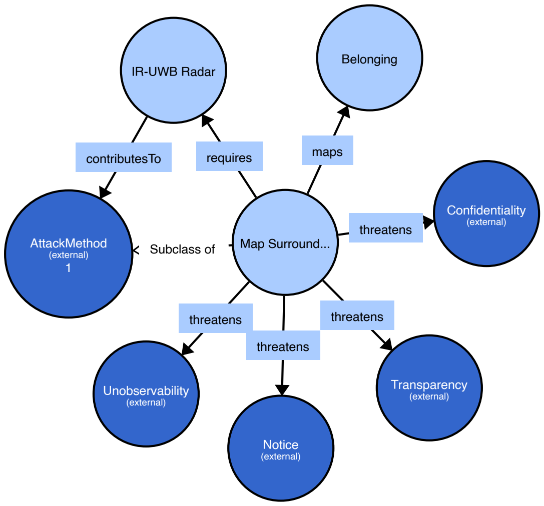


Fig. 2. UWB Attack Pattern AP_1: Map User Surroundings

C. Privacy Threats

With the core ontology formalized, the complete set of threats can be linked to the existing conceptualization, forming a knowledge graph. Formally defined, we can define this knowledge graph KG being a superset of the core ontology CO and the full set of attack patterns AP_1 to AP_{30}, derived from the results of Section III depicted in Table I:

$$KG = (V, E)$$

$$V \in \{CO,\ AP_1,\ AP_2,\ ...\ AP_{29},\ AP_{30}\}$$

Hence, each attack pattern is formalized as an instance of *AttackPattern* that relates to instances of the UWB artifacts and privacy threats. Then, a reasoner can infer, based on a set of available artifacts, which attack methods are applicable.

For each of the 30 privacy threats, it is possible to extrapolate such an attack pattern, for example, as shown in Figure 2, which depicts the attack pattern AP_1. This pattern relates to privacy threat one (see Table I, an IR-UWB Radar based scenario in which the user and their surroundings are involuntarily mapped. This could, for example, be used, to map associates of the user or the time they spent in front of an advertisement. By following the *requires* property, it is apparent that this threat may be introduced when an *IR-UWB Radar* is employed. Specifically, the related privacy goals may be threatened by the introduction of the device. AP_2 requires the same UWB artifacts to localize users without consent.

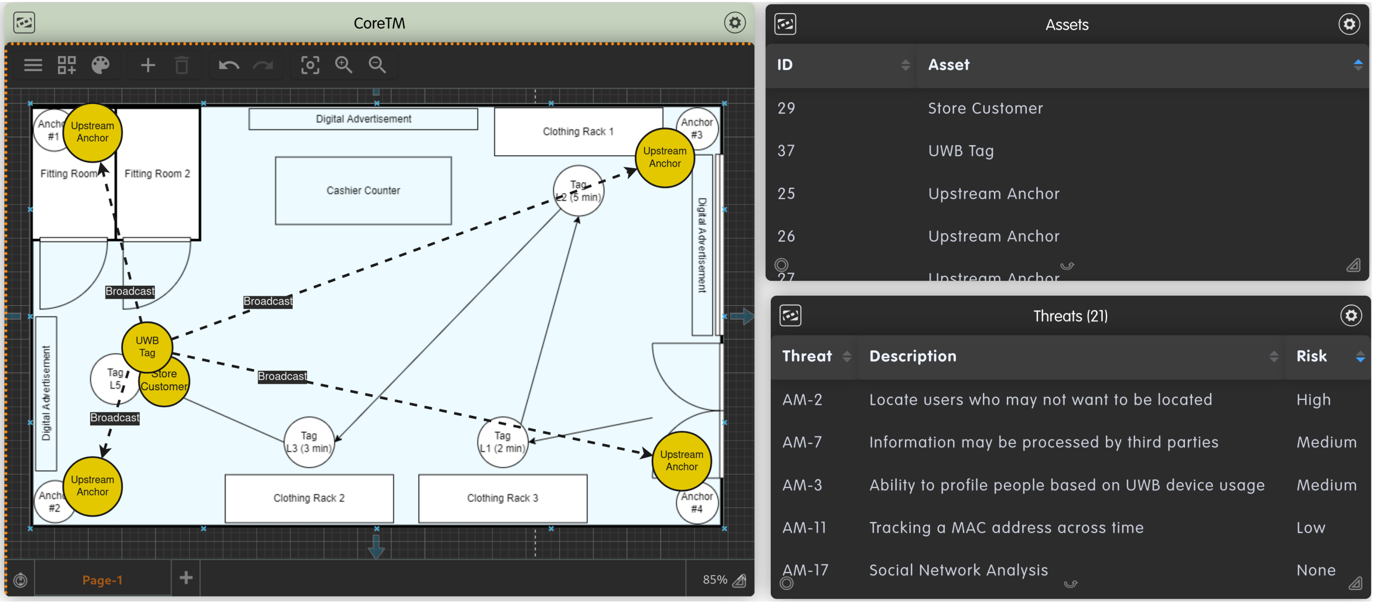
AP_3 introduces the same threat by localizing users. However, here, both a UWB-enabled smartphone and a UWB tag are required for the attack to be plausible. While the previous attacks mapped a user's surroundings or localized them within an area, this attack combines all the gathered data to track the user within a specified space, such as a store or mall. Consequently, noting UWB sensors of other users in proximity, indicating a possible relation between users, or noting a prolonged time spent at a certain store. This tracking can be further expanded upon, by utilizing a full UWB sensor infrastructure across public spaces, wherein a person can be recognized and profiled according to their habits, lifestyle, or schedule. This continuous collection of data across applications and locations would be considered excessive data collection under privacy risk AP_8, data aggregation under AP_9, and cross-location, multi-sensor gathering according to AP_{10}. For example, a person could be going to the same station every day, at 8 am. Additionally, they are recorded going to the bakery every morning and to the grocery store every Friday afternoon. As such, this customer profile highlights a clear preference for baked goods around 8 am, an infringement on privacy as described in AP_{18}. Consequently, this information can be shared and utilized to show bakery advertisements in the train station in the morning, constituting a form of targeted advertising by AP_{12}. While this example might be trivial, it can be expanded to include very specific preferences that are then displayed in front of the public, thus possibly purposely deanonymizing the customer (*cf.* AP_{19}).

V. Case Study: Commercial Privacy Threat Modeling

Assuming that an enterprise already holds a description of an employed architecture leveraging UWB technology, a risk assessment with respect to privacy needs to be conducted in order to argue to upper management that the architecture complies with current information security management standards like the General Data Protection Regulation (GDPR). Thus, a set of privacy threats needs to be derived from purely domain-specific knowledge, which at this point is assumed to be contextualized by an indoor localization system for personalized in-store advertising. An extended knowledge graph can be constructed by *(i)* extracting, *(ii)* contextualizing, and *(iii)* linking domain knowledge (*e.g.*, the currently envisioned architecture of the indoor localization system) with the previously introduced knowledge graph.

By linking a set of facts (*i.e.*, architectural traces) to the knowledge graph, the underlying ontology serves as a semantic anchor to reason about implied knowledge – in this case, the derivation of privacy threats and vulnerabilities. Thus, while the ontology provided in this paper provides entity alignment for UWB privacy threat modeling, the knowledge graph provides specific threat intelligence. To extract the relevant properties, in this case, specific assets leveraging UWB technology, an interactive, collaborative, and visual approach as defined in [5], provides a simple annotation functionality.

Thus, an existing floor plan containing UWB nodes such as anchors and tags is uploaded and the technical elements leveraging UWB technology are annotated with visual elements. Specifically, the architecture employs four static anchors that localize tags carried by users due to their upstream broadcast messages. These annotated elements are then automatically extracted from the underlying XML file and a node can be created in a graph database, effectively linking it to the ontology. *neo4j*, a graph database, provides a convenient way to index and query knowledge bases. After importing the knowledge graph, a list of applicable threats can be obtained



Assets

ID	Asset
29	Store Customer
37	UWB Tag
25	Upstream Anchor
26	Upstream Anchor
27	Upstream Anchor

Threats (21)

Threat	Description	Risk
AM-2	Locate users who may not want to be located	High
AM-7	Information may be processed by third parties	Medium
AM-3	Ability to profile people based on UWB device usage	Medium
AM-11	Tracking a MAC address across time	Low
AM-17	Social Network Analysis	None

Fig. 3. Applying the Knowledge Graph to Automatically Derive Privacy Threats

by querying the graph for *AttackMethod* nodes that are linked to the previously identified assets as follows:

Listing 1. Deriving Threats from the Presence of Artifacts

```
MATCH  (customer:Person)-->(tag:Tag)
       (tag)--(anchor:UpstreamAnchor),
       (anchor)<--(threat:AttackMethod)
RETURN threat.description, threat.id
```

Effectively, the knowledge graph is traversed so that only *AttackMethods* are returned which are directly connected to the usage of an *UpstreamAnchor*. In turn, it is required, that the anchor is connected to a user-associated *UWB Tag*.

Based on this graph traversal, 21 privacy threats are discovered in the database and automatically presented, as shown in Figure 3. These threats may technically apply to the usage of UWB technology in the store. However, only domain experts can judge if there is an underlying risk introduced by the threat. Thus, a domain expert and a solution architect iterate over the identified threats and discuss their applicability in the scenario.

Not all identified threats present themselves as direct risks to the store's business. For example, *AM-17* outlines the threat of performing social network analysis by correlating traffic of multiple tags and their identity. In the context of the store, only one tag is located per user, no personal information is collected, and no correlation to other tags takes place — effectively making the threat unlikely to cause harm from the store's perspective.

On the other hand, other threats, such as the localization of unaware users (*cf. AM-2*) are directly caused by the store and a countermeasure must be implemented. For example, users can be informed about the usage of the technology. Similarly, the risk introduced by having information processed by third parties (*cf. AM-7*) must be mitigated by implementing a data retention policy. Due to the live gathering of data, it is important to avoid implicit deanonymization (*cf. AM-19*), this could be prevented by ensuring that store clerks do not have access to the data and do not get alerts of customers based on time lingered in front of a specified location and ensuring there is no personal identification created or linked to the data.

Thus, based on the threats identified by the application, the ontology is successfully able to derive a set of privacy-related threats by relying on the formalized knowledge graph presented in this paper. Specifically, the privacy threats further explain which privacy goals may be at risk. This is achieved by an explicitly defined and machine-readable specification of the UWB architecture employed, which serves as an input to traverse the graph. Therefore, we can see that based on existing, human-defined user input, the formalization provided in this paper can provide answers to the key competency questions defined in Chapter 1.

VI. Conclusions and Future Work

The literature, as presented in Sections II and III, showed that privacy is currently not the focus of research. This work successfully aggregated UWB privacy risks, necessary to create the first usable UWB protocol-based privacy ontology and adaption in CoreTM, enabling auto-detection of relevant privacy concerns based on the network architecture.

In the case study presented, potential privacy risks were showcased, based on a store's aim to utilize UWB for customized advertising, without infringing on data privacy laws. The uploaded floor plan and marked UWB network artifacts, resulted in 21 extracted and plausible privacy risks.

Once the tool is completed, a positive impact in terms of an increase in privacy awareness can be expected for UWB network applications in a multitude of commercial and research settings, thus, contributing to privacy preservation.

The next step will extend the CoreTM tool by compiling countermeasures to match the extracted attack patterns extracted, enabling a holistic analysis.

References

[1] M. A. Ahmed, “Privacy Issues of Mobile Phone Companies’ Usage of Ultra-Wideband (UWB) Technology: Analysing the use of UWB in Mobile Phones from a Multi-actor Perspective, Magnifying Privacy Concerns and Formulating Guidelines,” Policy and Management, Faculty of Technology, TU Delft, Netherlands, Jul 2021, https://bit.ly/3UjrKA6.

[2] A. Alarifi, A. M. Al-Salman, M. Alsaleh, A. Alnafessah, S. Al-Hadhrami, M. A. Al-Ammar, and H. S. Al-Khalifa, “Ultra Wideband Indoor Positioning Technologies: Analysis and Recent Advances,” *Sensors, Scalable Localization in Wireless Sensor Networks*, Vol. 16, No. 5, pp. 707–743, May 2016.

[3] A. Alrawais, F. Alharbi, M. Almoteri, and S. A. Aljwair, “A Novel Privacy-Preserving Scheme in IoT-Based Social Distancing Technologies,” in *2nd International Conference on Machine Learning Techniques and Data Science (MLDS)*, Zurich, Switzerland, Nov 2021, pp. 237–247.

[4] M. N. Aman, M. H. Basheer, and B. Sikdar, “Data Provenance for IoT with Light Weight Authentication and Privacy Preservation,” *IEEE Internet of Things Journal*, Vol. 6, No. 6, pp. 10 441–10 457, Dec 2019.

[5] J. v. d. Assen, M. F. Franco, C. Killer, E. J. Scheid, and B. Stiller, “CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling,” in *IEEE International Conference on Cyber Security and Resilience*. Virtually, Europe: IEEE, Jul 2022, pp. 1–8.

[6] K. Ayub and V. Zagurskis, “Technology Implications of UWB on Wireless Sensor Network-a Detailed Survey,” *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 7, No. 3, p. 147, Sep 2015.

[7] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, “Robustness, Security and Privacy in Location-based Services for Future IoT: A Survey,” *IEEE Access*, Vol. 5, pp. 8956–8977, Apr 2017.

[8] D. Coppens, A. Shahid, S. Lemey, B. V. Herbruggen, C. Marshall, and E. D. Poorter, “An Overview of UWB Standards and Organizations (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions,” *IEEE Access*, Vol. 10, pp. 70 219–70 241, Jun 2022.

[9] J. Daubert, A. Wiesmaier, and P. Kikiras, “A view on privacy & trust in iot,” London, UK, June 2015, pp. 2665–2670.

[10] M. Gharib, P. Giorgini, and J. Mylopoulos, “COPri v.2 — A Core Ontology for Privacy Requirements,” *Data & Knowledge Engineering*, Vol. 133, p. 101888, May 2021.

[11] M. Grüninger and M. S. Fox, “Methodology for the Design and Evaluation of Ontologies,” 1995.

[12] T. Han, W. Kang, and G. Choi, “IR-UWB Sensor based Fall Detection Method using CNN Algorithm,” *Sensors*, Vol. 20, No. 20, p. 5948, Oct 2020.

[13] P. Hitzler, M. Krötzsch, B. Parsia, P. F. Patel-Schneider, and S. Rudolph, “Web Ontology Language Primer,” *W3C recommendation*, Vol. 27, No. 1, p. 123, 2009.

[14] S. Jaitly, H. Malhotra, and B. Bhushan, “Security Vulnerabilities and Countermeasures against Jamming Attacks in Wireless Sensor Networks: A Survey,” in *2017 International Conference on Computer, Communications and Electronics (Comptelix)*. Jaipur, India: IEEE, Jul 2017, pp. 559–564.

[15] C. Jandl, J. Nurgazina, L. Schöffer, C. Reichl, M. Wagner, and T. Moser, “SensiTrack-a Privacy by Design Concept for Industrial IoT Applications,” in *24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. Zaragoza, Spain: IEEE, Sep 2019, pp. 1782–1789.

[16] G. Ji, C. Lee, and J. Yun, “Counting and localizing occupants using ir-uwb radar and machine learning,” *Journal of the Korea Society of Computer and Information*, Vol. 27, No. 5, pp. 1–9, 2022.

[17] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, “Security in IoMT Communications: A Survey,” *Sensors*, Vol. 20, No. 17, p. 4828, Aug 2020.

[18] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of Things: Vision, Applications and Research Challenges,” *Ad Hoc Networks*, Vol. 10, No. 7, pp. 1497–1516, Sep 2012.

[19] A. Moore, “‘i didn’t want it anywhere near me’: How the apple airtag became a gift to stalkers,” Sep 2022. [Online]. Available: https://www.theguardian.com/technology/2022/sep/05/i-didnt-want-it-anywhere-near-me-how-the-apple-airtag-became-a-gift-to-stalkers

[20] NASK, “VARIoT Database Entry Ontology,” https://bit.ly/3BTrlgo, 2020, last Accessed: Jul 28, 2022.

[21] V. Niemelä, J. Haapola, M. Hämäläinen, and J. Iinatti, “An ultra wideband survey: Global regulations and impulse radio research based on standards,” *IEEE Communications Surveys & Tutorials*, Vol. 19, No. 2, pp. 874–890, 2016.

[22] NIST, “NIST Glossary Privacy Definition,” https://csrc.nist.gov/glossary/term/privacy, Last visit Sep 16, 2022.

[23] N. Noy and D. McGuinness, “Ontology Development 101: A Guide to Creating Your First Ontology,” Stanford Medical Informatics Technical Report SMI-2001-0880, Stanford, USA, Tech. Rep., Mar 2001. [Online]. Available: https://stanford.io/3qOYW4Q

[24] M. M. Ogonji, G. Okeyo, and J. M. Wafula, “Internet of Things: Survey on Security and Privacy,” *Information Security Journal*, Vol. 27, pp. 162–182, Jul 2017.

[25] B. Pestourie, “UWB Secure Ranging and Localization,” Embedded Systems, Université Grenoble Alpes, France, Feb 2021.

[26] S. P. Rana, M. Dey, M. Ghavami, and S. Dudley, “Signature Inspired Home Environments Monitoring System using IR-UWB Technology,” *Sensors*, Vol. 19, No. 2, p. 385, Jan 2019.

[27] D. B. Rawat, G. Yan, B. B. Bista, and V. Chandra, “Wireless Network Security: An Overview,” *Building Next-Generation Converged Networks: Theory and Practice*, Jun 2013.

[28] M. Rytel, A. Felkner, and M. Janiszewski, “Towards a safer internet of things—a survey of iot vulnerability data sources,” *Sensors*, Vol. 20, No. 21, p. 5969, 2020.

[29] W. Sakpere, M. Adeyeye-Oshin, and N. B. Mlitwa, “A State-of-the-Art Survey of Indoor Positioning and Navigation Systems and Technologies,” *South African Computer Journal*, Vol. 29, No. 3, pp. 145–197, Dec 2017.

[30] M. Singh, M. Roeschlin, E. Zalzala, P. Leu, and S. Čapkun, “Security Analysis of IEEE 802.15. 4z/HRP UWB Time-of-Flight Distance Measurement,” in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Abu Dhabi United Arab Emirates, NetworksJun 2021, pp. 227–237.

[31] M. Stocker, B. Großwindhager, C. A. Boano, and K. Römer, “Towards Secure and Scalable UWB-based Positioning Systems,” in *IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. Delhi, India: IEEE, Dec 2020, pp. 247–255.

[32] S. F. Tan and A. Samsudin, “Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey,” *Sensors*, Vol. 21, No. 19, p. 6647, Aug 2021.

[33] M. Ye, N. Jiang, H. Yang, and Q. Yan, “Security Analysis of Internet-of-Things: A Case Study of August Smart Lock,” in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Atlanta, USA, May 2017, pp. 499–504.

[34] F. Zafari, A. Gkelias, and K. K. Leung, “A Survey of Indoor Localization Systems and Technologies,” *IEEE Communications Surveys & Tutorials*, Vol. 21, No. 3, pp. 2568–2599, Apr 2019.