Hindawi
Security and Communication Networks
Volume 2023, Article ID 5573310, 30 pages
https://doi.org/10.1155/2023/5573310

Research Article

Towards an Improved Taxonomy of Attacks Related to Digital Identities and Identity Management Systems

Daniela Pöhn and Wolfgang Hommel

Universität der Bundeswehr München, RI CODE, 85577 Neubiberg, Germany

Correspondence should be addressed to Daniela Pöhn; daniela.poehn@unibw.de

Received 13 December 2022; Revised 23 January 2023; Accepted 20 April 2023; Published 19 June 2023

Academic Editor: Wojciech Mazurczyk

Digital transformation with the adoption of cloud technologies, outsourcing, and working-from-home possibilities permits flexibility for organizations and persons. At the same time, it makes it more difficult to secure the IT infrastructure as the IT team needs to keep track of who is accessing what data from where and when on which device. With these changes, identity management as a key element of security becomes more important. Identity management relates to the technologies and policies for the identification, authentication, and authorization of users (humans and devices) in computer networks. Due to the diversity of identity management (i.e., models, protocols, and implementations), different requirements, problems, and attack vectors need to be taken into account. In order to secure identity management systems with their identities, a systematic approach is required. In this article, we propose the improved framework Taxonomy for Identity Management related to Attacks (TaxIdMA). The purpose of TaxIdMA is to classify existing attacks, attack vectors, and vulnerabilities associated with system identities, identity management systems, and end-user identities. In addition, the background of these attacks can be described in a structured and systematic way. The taxonomy is applied to the Internet of Things and self-sovereign identities. It is enhanced by a description language for threat intelligence sharing. Last but not least, TaxIdMA is evaluated and improved based on expert interviews, statistics, and discussions. This step enables broader applicability and level of detail at the same time. The combination of TaxIdMA, which allows a structured way to outline attacks and is applicable to different scenarios, and a description language for threat intelligence helps to improve the security identity management systems and processes.

1. Introduction

Credential theft and social engineering are the most frequent attacks that organizations are facing [1]. With valid credentials, miscreants can start their attacks on organizations or sell them for financial purposes. The difficulties often begin with password management: many accounts require secure passwords. While a password manager helps to generate and remember passwords, not all persons use them effectively or at all [2–4]. Therefore, weak passwords such as 123456, qwertz, and password are common. These are included in wordlists with rockyou.txt [5] (14,341,564 unique passwords used in 32,603,388 accounts) being the best known. The password list of John [6] is typically applied during cracking, while brutespray [7] with its wordlist automates brute-forcing based on the Network Mapper (nmap) output. In consequence, attackers can easily break them. Even if the users apply passwords with high entropy, they might be reused for several platforms [8], enabling credential stuffing attacks if one such system is compromised or the password is stolen otherwise [9]. In addition, social engineering does not target the storage or complexity of passwords but the human element. This shows that credentials and, thereby, identity management (IdM) are core elements for security in a network.

While these user identities seem to be an easy target, identity management systems (IdMS), which store and manage the identities of an organization, can be targeted in more serious attacks as shown by the SolarWinds incident [10–12]. With access to an identity management system,

which serves as a central identity repository, attackers also have access to any resource (service, computer, printer, etc.) [13]. The consequences are complex, ranging from lost data and compromised accounts to financial loss. As a result, identity management systems need to be secured and well-protected. Typical defense mechanisms are strong password policies, usage of password managers, enforcement of multi-factor authentication, privileged access management, and training. Depending on the implemented identity management system, specific defense mechanisms and configurations may be applied. According to the Purple Knight Report 2022 [14], organizations have problems correctly securing Microsoft Active Directory (AD) as one of the most prominent identity management systems.

In order to systematically analyze and evaluate attacks, attack vectors, and vulnerabilities, a structured approach is required. In this context, taxonomies provide an overview of these complex systems and, thereby, possible attacks. Such a systematic approach helps to enhance the current situation by identifying gaps and providing guidelines for new security mechanisms. To the best of our knowledge, although several taxonomies and categorizations have been proposed and some case studies on specific attacks have been published, only our previous work [15] is a taxonomy on attacks targeting identity management. In consequence, we propose an improved taxonomy framework for attacks related to identities and identity management systems, TaxIdMA. This framework consists of (1) a background description, (2) taxonomies for attacks on end-user identities, system identities, and identity management systems, and (3) application on Internet of Things (IoT) identities and self-sovereign identities (SSI). In order to exchange information about these attacks, an extension to the description language Structured Threat Information Expression (STIX) [16] is proposed.

This article extends [15] by a background description, improved TaxIdMA taxonomies, the addition of IoT and SSI, and an enhanced evaluation of the related work and TaxIdMA. Last but not least, an extension of the description language STIX for exchanging attack information related to identity management is proposed. As a result, the contribution of the article is multi-fold: (1) an improved taxonomy framework for attacks on identities and identity management systems; (2) an extended evaluation of related work; (3) an extended evaluation of TaxIdMA; and (4) an extension of the description language STIX based on TaxIdMA.

The remainder of this article is as follows. First, the background of identity management is summarized, followed by a broad discussion of various aspects of related work. Then, the methodology to establish and verify the taxonomy framework is outlined. The methodology includes information about the changes from the previous to the current version of TaxIdMA. This is followed by TaxIdMA, the taxonomy framework for attacks with background, attacks on end-user, system identities, and identity management systems. TaxIdMA is then applied to the areas of IoT and SSI. This enhanced version of TaxIdMA is evaluated by expert interviews and statistical information. Based on TaxIdMA, an extension of the description language STIX to exchange information related to identity management is proposed. Both aspects, TaxIdMA and description language, are discussed in the following section. Last but not least, a summary and an outlook on future work are given.

2. Background

Identity management is the organizational and technical process for registering and authorizing access rights during enrollment and authentication as well as controlling identities based on previously authorized access rights. Identity management is described by accessing a service from the user's perspective, followed by centralized, federated, and user-centric identity management, and concluded with issues related to identity management.

2.1. End-Users. In order to access different services, users first need to register. Users typically add personal information, the so-called attributes. Then, users can authenticate and get authorized to access the requested services. Authentication is often password-based, though other authentication methods from the categories of knowledge, possession, and biometrics can be applied as well. With an increasing number of services, users tend to forget their credentials. This frequently results in the reuse of passwords across several accounts, which reduces security. In contrast, users could use password managers to store and generate passwords for multiple accounts. To improve security, multi-factor authentication (MFA) [17] might be implemented. This means that at least two different and independent methods are required. A more usable version is risk-based authentication (RBA) [18], where additional factors are requested depending on risk and the user's situation. If one authentication method is (temporarily) unavailable, predefined fallback mechanisms, such as security questions and e-mail links, come into play [19].

2.2. Local Identity Management. Windows accounts can be categorized as the user, administrator, and system. Administrator accounts generally have higher permissions than user accounts. They have full control of the files, directories, services, and other resources on the local computer. At the same time, they are able to manage accounts, rights, and permissions. On the other hand, users are more restricted in their rights. Depending on roles among other things, their permissions vary. In an illicitly configured network, a user could theoretically have more or less the same permissions as an administrator [20]. A similar system exists for Linux, where the highest privileges come with the user type root. When installing services on Linux, they typically come with a corresponding user. For example, web services and PHP often use www-data in the group www-data. Those service users have limited permissions due to security reasons.

A pluggable authentication module (PAM) [21] is a mechanism to integrate multiple authentication possibilities. Thereby, PAM allows programs to reuse these schemes instead of requiring each developer to write their own method. For example, Linux PAM is a suite of libraries that

allow system administrators to configure authentication methods, such as local passwords and lightweight directory access protocol (LDAP), for their users. PAM can be used to streamline local identity management.

2.3. Centralized Identity Management. Identity management allows users to access different services. Thereby, the security of the services is tightly tied to it. In organizations, typically an identity management system is operated. The introduction of LDAP [22] started the first evolution of identity management towards a central system. LDAP maintains and shares directory information services, such as users, networks, services, and applications. Popular implementations include OpenLDAP and Microsoft AD, which combine LDAP with the Kerberos protocol. Typical issues with AD [23] can be boiled down to privileged account activity, login failures, and remote logins. As shown in the introduction, properly securing AD is not an easy task. With single sign-on (SSO) running, the user has to log in only once to access several services. Identity management can also be operated on cloud services [24].

2.4. Federated Identity Management. As organizations tend to cooperate, there are two main possibilities related to identity management: (1) duplicate the accounts and (2) implement federated identity management (FIM). FIM [25] allows users to utilize their home organizations' credentials to sign in to other services within the trust boundaries of the federation. It thereby uses centralized identity management as the main source. In consequence, users only have to remember the credentials for their accounts at their home organizations. At the same time, security incidents may have a bigger impact. Two main FIM directions are used in practice: (1) Security Assertion Markup Language (SAML) [26] and (2) Open Authorization (OAuth) 2.0 [27] for authorization with OpenID Connect (OIDC) [28] for authentication. OAuth and OIDC can be combined but may run on their own. Typical use cases include research and education and eID federations [29] (SAML) resp. commercial web services (OAuth and OIDC). Both directions with the protocols, implementations, and configurations have different security issues though [30–35].

2.5. User-Centric Identity Management. In parallel, several user-centric identity management approaches were proposed and introduced, in order to give users more control over their data. One protocol is User Managed Access (UMA) [36–38], which is built upon OAuth. With SSI [39, 40], the research direction gained momentum. In contrast to traditional identity management, the user has full control over their data, which is issued by issuers, formerly home organizations, in form of verifiable credentials. These are stored in the user's wallet and can be rearranged as verifiable presentations to holders, which offer services. Further information is stored decentralized, for example, by the use of blockchain. So far, Naik et al. [41] published the only approach to systematically evaluate the security of SSI. Although this is a systematic approach, further attack vectors are possible, such as obtaining administrator credentials by leaks and configuration issues.

2.6. Issues with Identity Management. As shown by the user side, not only do organizations operate identity management for their employees and cooperation, but also for different purposes, such as customer identity management. For web services, the identity data are often stored in databases, but also other forms of management are possible. Identity management for IoT devices might be used in parallel, leading to a multitude of identity management systems within the identity models [42]. This makes it harder to configure and secure the systems correctly.

2.7. Summary. When we look at the aforementioned areas of identity management, it becomes clear that involved entities, protocols with their implementations, technical requirements, and managed identities are different. For this reason, the improved taxonomy must allow the inclusion of all the heterogeneous aspects to categorize attacks systematically without excluding relevant information.

3. Related Work

In this section, related work towards attack categories and generic as well as specific attack taxonomies is discussed. To find the generic approaches, we used the search terms "(taxonomy OR categorization OR classification) AND (attack OR threat OR security)". For the specific attack taxonomies, we added AND identity. We applied these search terms at ACM, IEEE, Springer Link, USENIX, and MDPI. We excluded posters and short papers as well as publications, which apply taxonomies. This is enhanced by a description of related work on attacks on identity management and specific application. Here, we used the search terms "(threat OR attack) AND (identity OR "Internet of things" OR "self-sovereign identity")". In addition, threat information-sharing approaches for both, languages and platforms, are evaluated. The corresponding search term is ""threat information" AND sharing". Last but not least, the limitations of related work are described.

3.1. Attack Categories. Several community-driven and commercial approaches categorize and list attacks [43]. For example, the Common Weakness Enumeration (CWE) by MITRE [44] is a community-driven list of software and hardware weaknesses, which is applied as a common language for weakness identification, mitigation, and prevention. This includes weaknesses in identity management, such as different types of improper access controls ranging from Hypertext Transfer Protocol (HTTP) cookies to on-chip hardware issues. MITRE ATT&CK [45] details numerous attack methods during the cyber kill chain, also called the attack lifecycle [46]. For example, during reconnaissance, information is gathered through phishing and searches. The initial access includes phishing and the usage

of valid accounts. Thereby, several identity-related methods are matched to the lifecycle. The Common Attack Pattern Enumeration and Classification (CAPEC) [47] describes attack patterns based on software design patterns. In the area of identity management, the subvert of access control comprises, for example, authentication abuse and bypass as well as physical theft. Even though these design patterns are important, not all attacks are based on them. The Open Web Application Security Project (OWASP) [48] publishes several top 10 lists and cheat sheets for typical problems, including error messages during login among others. Although these guidelines are relevant during configuration and improvements, they do not comprise all areas of identity management. Nonetheless, several aspects of these attack categories are taken into consideration while designing TaxIdMA.

3.2. Attack Taxonomies. Taxonomies are categorizations or classifications in mostly hierarchical order. Items are thereby arranged in groups or types. This can be used to organize and index knowledge. Originally from biology, the categorization is applied in different fields, including computer science.

3.2.1. Generic Attack Taxonomies. Different taxonomies related to attacks were proposed so far. Igure and Williams [49] analyzed a multitude of taxonomies published from 1974 until 2006. Based on their findings, the authors proposed a taxonomy of attacks and vulnerabilities in computer systems. Although the authors included numerous approaches, the resulting taxonomy is a generic attack taxonomy. As a consequence, it is not focused on a specific area. Chapman et al. [50] proposed a 3-tier taxonomy, which describes the effects of cyberattacks. The authors thereby reported stages ranging from no access over user access to root access. In consequence, they specified different levels of permissions an attacker can gain. These levels may depend on the operating system (OS). In addition, the approach is unclear in some cases, such as service users like www-data. Derbyshire et al. [51] evaluated different well-known taxonomies based on predefined criteria and selected real-world attacks. The authors concluded that CAPEC outperforms other taxonomies, although several taxonomies do not include humans. As a result, TaxIdMA needs to include human elements. Cho et al. [46] explored different cyber kill chain models. Based on their evaluation, the authors proposed a new model. Haber and Rolls summarized typical identity attack vectors in practice [52]. The cyber kill chain is a structured way to explain the stage of an attack and, therefore, should be included in the TaxIdMA.

3.2.2. Specific Attack Taxonomies. Other authors focused their taxonomies on a specific aspect. Habiba et al. [53] proposed a taxonomy related to cloud IdMS security issues. The authors first outlined the different identity management systems, before describing related security challenges and known attacks. These include brute-force attacks, cookie-replay attacks, data tampering attacks, eavesdropping, the elevation of privilege, identity theft, and phishing attacks. Although these attacks are relevant for identity management (identity management systems and end-users), they are limited to attacks targeting cloud IdMS, which were known at the time the approach was published. Klaper and Hovy [54] established a taxonomy with cybersecurity topics. These basic topics were then linked to relevant educational or research material. Thereby, the authors noticed gaps in the study curriculum. Different description languages are used to categorize and exchange threat information. Based on a literature review, Burger et al. [55] proposed a taxonomy related to the exchange of cyber threat intelligence information. The authors used a layered model with the 5W's, intelligence, indicators, session, and transport. Within the category of the session, the authors differentiated authentication, authorization, and permissions. Although many aspects are relevant for attacks on identity management, the proposed taxonomy is rather generic. Husseis et al. [56] regarded potential threats affecting biometric systems, while Mamchenko and Sabanov [57] explored USB-based attacks. Hollick et al. [58] described a taxonomy and attacker model for secure routing protocols. Chaipa et al. [59] proposed a taxonomy of insider threats. These taxonomies are focused on a specific aspect and, therefore, are not suitable for identity management. Nonetheless, useful aspects, such as attack types, are repurposed for our taxonomy framework.

3.2.3. IoT Attack Taxonomies. Several IoT attack taxonomies are published. Alsamani and Lahza [60] proposed an IoT taxonomy concerning security and privacy threats. The taxonomy consists of three dimensions, not covering the whole aspect. Nawir et al. [61] also presented a security taxonomy, which includes some categories, but is already outdated. Khanam et al. [62] outlined several security challenges. Based on the review, the authors designed an attack taxonomy and corresponding countermeasures. The authors thereby used the layers application, network, physical, and multi. Although several attacks are outlined, the taxonomy is rather simple. Neshenko et al. [63] described an extensive survey on IoT vulnerabilities. The authors differentiated the layers of devices, software, and network. Similarly, Wüstrich et al. [64] proposed a simple naming scheme for IoT threat, which was used for a work-in-progress taxonomy. Rizvi et al. [65] differentiated architecture, threat vector, trust, and compliance in their taxonomy. The terminology is not aligned with the one in the field. Trust is according to the authors related to privacy, availability, and reliability, which might be the case for end-users, but not (only) for other entities. Shasha et al. [66] used simple differentiations in their taxonomy, such as physical, nearby, and remote, not taking all aspects into account.

Other authors established a taxonomy based on their survey results. Williams et al. [67] conducted a survey to classify security features and threats in IoT devices. The authors used a simple list of seven items, which they call taxonomy. In consequence, they do not include all issues. Similarly, Squillace and Bantan [68] conducted a study with

limited results. Xenofontos et al. [69] proposed an attack taxonomy for IoT and studied different cases of IoT insecurity. Although the case study is extensive, the taxonomy is comparably simple. In consequence, several aspects can be adapted, though none of these IoT attack taxonomies are sufficient to describe attacks on identities related to IoT. Nonetheless, they did not propose a taxonomy.

Several approaches focus on specific aspects. Taivalsaari and Mikkonen [70] proposed a taxonomy related to IoT client security, which is one aspect of IoT security. Auliar and Bekaroo [71] focused on IoT security taxonomy related to the Mirai botnet, whereas El-hajj et al. [72] analyzed the security of IoT authentication in form of a taxonomy. Lounis and Zulkernine [73] proposed a taxonomy related to the security of short-range wireless technology for IoT devices. Boujezza et al. [74] established a taxonomy related to identity management for the IoT environment, which is already outdated. Although Bikos and Kumar [75] used well-defined layers of application, middleware, access gateway, and edge technology, they mainly focused on the usage of blockchain for IoT. Berger et al. [76] focused on resilience for IoT devices. Alsubaei et al. [77] proposed a taxonomy related to the security of medical IoT devices. Their differentiation is mainly on availability, integrity, and confidentiality as well as a few layers.

3.3. Attacks on Identity Management. As shown, different attacks on identity management are possible. Fritsch [13] identified identity management as a target in cyberwar. Our previous work [15] proposes a first taxonomy on attacks. First, we study generic cases and then detail specific areas of identity management.

3.3.1. Case Study of Attacks. Several authors focused on attacks related to digital identities. Redding et al. [78] analyzed the Parler data breach, which used massive application programming interface (API) scraping of Parler's servers. This was possible as Parler failed to implement authentication on calls made to the platform's API correctly. In a further step, the attackers uncovered credentials due to insufficient security measures. Similarly, Gibson et al. [79] described the LinkedIn data breach by massive API scraping in 2021. Also here, failed implementation of authentication and authorization for API calls was one of the reasons. Qian et al. [80] analyzed the SocialArks data breach resulting from a brute-force web login attack. Elasticsearch does not have enabled authentication by default, which was one of the problems in this incident. In the next step, the attackers got superuser permissions. Nguyen Ba Minh et al. [81] described the case of the Canva data breach, where the attacker GnosticPlayers was able to obtain data from 139 million users by credential stuffing and credential cracking.

Other attacks are more sophisticated. Rizkallah et al. [82] focused on the BlueToad case. It is unclear how the attacker got hold of the unchangeable UDIDs of Apple. Most likely, Apple shared the unencrypted unique device identifiers (UDIDs) with companies or applications, which then store them in their databases. Attackers may be able to steal them if weak security policies are applied. Pitney et al. [83] systematically reviewed the 2021 Microsoft Exchange data breach exploiting four different zero-day vulnerabilities. The attack methodology includes server-side request forgery, deserialization vulnerability, first file write vulnerability, and second file write vulnerability. As patches were not timely installed, this data breach impacted several organizations. Nadjar et al. [84] analyzed the case of the multi-vector data breach on Astoria, where confidential user data were exploited by MySQL and PHP-based vulnerabilities in a popular data management tool. After a data import request, the attackers were able to access a PHP file and obtain the admin credentials. This then led to data exfiltration. Faircloth et al. [85] described the brute-force attack on T-Mobile leading to subscriber identity module (SIM) hijacking and identity theft. The attacker used a dictionary attack, rainbow table attack, guessing attack, and spidering. Motero et al. [86] utilized a practical survey to describe attacks on Kerberos authentication protocols. The authors analyzed overpass the hash, pass the ticket, golden ticket, silver ticket, Kerberoasting, unrestricted delegation attacks, restricted delegation attacks, resource-based restricted delegation attacks, and Kerberos bronze bit attacks. All these attack descriptions are included in TaxIdMA.

3.3.2. Attacks on Specific Areas. Other authors focused on specific applications. Naik et al. [41] proposed an attack tree for SSI. Anita and Vijayalakshmi [87] and Saad et al. [88] regarded blockchain (used among others for SSI) security based on surveys. Al-Khurafi et al. [89] described the security of web applications based on a survey. The security of web applications is relevant to the security of digital identities. Gaikwad and Ragha [90] focused on the mitigation of attacks on authenticating identities in ad hoc networks, while Sharma and Singh [91] described detection techniques related to it. Bahri [92] outlined identity-related threats in online social networks. Based on a survey, Gupta et al. [93] categorized social engineering attacks with a focus on phishing attacks, where information on digital identities is stolen. Qin et al. [94] addressed false identity attacks in peer-to-peer networks. Karunanayake et al. [95] categorized deanonymization attacks on the Tor network. Similarly, Erdin et al. [96] considered finding hidden users based on a survey. Mavoungou et al. [97] provided a survey on threats and attacks on mobile networks, where, for example, devices have identities. Briones et al. [98] showed identity theft in a Wi-Fi setting through a case study. Mei et al. [99] published a survey on advanced persistent threats (APTs), where digital identities were stolen among other things.

Further authors used the information for their proposals. Barona and Mary Anita [100] summarized data breach challenges in cloud computing security including identity management. These comprise data breaches, account or service traffic hijacking, insecure interfaces and APIs, denial of service (DoS), malicious insiders, abuse of cloud services, and shared technology vulnerabilities. Fang et al. [101] analyzed data breaches in underground forums, whereas Subramanian et al. [102] proposed a model to predict cyber

hacking breaches. Information from the specific applications and data breach challenges were considered as input. General attacks on identity management were summarized by Haber and Rolls [52]. Further attacks are described towards blockchains and wallets (see, e.g., [103]), though not for SSI.

3.4. Threat Information Sharing. The information about the previously described threats can be shared by (1) a systematic language and (2) a sharing platform. One well-known language is STIX [16], which specifies attack pattern, campaign, course of action, grouping, identity, indicator, infrastructure, intrusion set, location, malware, malware analysis, note, observed data, opinion, report, threat actor, tool, and vulnerability. Identity has the properties name, description, roles, identity_class, sectors, and contact_information and might have relationships. In addition, suspicious action at user account objects can be outlined. Thereby, several attacks can be specified. Ussath et al. [104] extended STIX to support complex patterns, whereas Vielberth et al. [105] added human-as-a-security-sensor. For identity management, more information might be needed. The Trusted Automated eXchange of Intelligence Information (TAXII) [106] framework is an application layer protocol for the communication of cyber threat information in a simple and scalable manner and it relates to STIX. Open Indicators of Compromise (OpenIOC) [107] apply schemes and specific terms to describe metadata, criteria, and parameters. This shows that the threat information description is not suitable for identity management. Incident Object Description Exchange Format (IODEF) [108] is an incident object description exchange format representing computer security information exchanged between computer security response teams. It is based on [109–111]. The format includes incident ID, related activities, detection time, start and end time, report time, description, assessment, method, contact, event data, history, and additional data. Thereby, it can generally be used. A more detailed description format though would help identity management.

Burger et al. [55] analyzed ontologies for sharing threats, such as OpenIOC, STIX, and IODEF, and proposed their own taxonomy. Stillions [112] described a detection maturity level model (DML), which was extended in [113] to present cyber threats. It thereby specifies the attacker's identity, goals, strategy, tactics, techniques, procedures, and tools, as well as traces of the attack execution. Pahlevan et al. [114] extended the TAXII framework for distributed ledger technologies. Mavroeidis and Bromander [115] analyzed taxonomies, ontologies, and standards for cyber threat sharing. The authors concluded that there is no existing ontology which can be used within cyber threat intelligence as the existing ones mainly lack expressiveness and do not cover all relevant data and information. Zibak and Simpson [116] explored the benefits and barriers of threat information sharing, while Stojkovski et al. [117] analyzed the user experience. Bromander et al. [118] proposed a new data model for the exchange, whereas Mavroeidis et al. [119] argued to improve current ontologies by commonly agreed-upon controlled vocabulary. This shows that work is still needed. As we notice that detailed information is missing regarding identity management, this conclusion is especially true for identity management.

One possible sharing platform is the Malware Information Sharing Platform (MISP) [120]. Another open source platform is Open Cyber Threat Intelligence (OpenCTI) [121], which allows organizations to manage their cyber threat intelligence knowledge and observables. OpenCTI's knowledge schema is based on the STIX standard. The tool can be integrated with others, such as MISP and TheHive. In contrast, TheHive [122] is a security incident response platform, which can make use of MISP.

3.5. Limitations of Current Approaches. Although several attack taxonomies and categorizations exist, none focus on identity management. As a result, a taxonomy for attacks related to identities and identity management systems is still missing. TaxIdMA [15] is a first approach but requires further work. Elements of the related work (taxonomies, case studies of attacks, etc.) can be used as a basis for a holistic taxonomy resp. an improved TaxIdMA. This taxonomy can be enhanced by threat information-sharing language, which needs to be extended for the purpose of identity management.

4. Methodology

This section describes the methodology used to design the taxonomy framework. First, criteria for evaluation are established before the steps towards TaxIdMA with its previous version, limitations, and the improved version are outlined. Next, design decisions are justified and the naming convention is specified. The glossary defines the terms used in this article. Last but not least, the limitations are summarized.

4.1. Criteria for Evaluation. A taxonomy organizes the concepts hierarchically, while each concept includes a short description and further information. Thereby, a taxonomy can help to define and clarify a specific topic [123]. Before building a new resp. improving a taxonomy or taxonomy framework, criteria have to be determined for judging its merits [124, 125]. For this article, the following criteria are selected to judge the effectiveness.

(1) Completeness/exhaustibility: All objects are contained in the taxonomy.

(2) Comprehensiveness: The taxonomy is understandable for experts in the field. If the taxonomy is understandable for novices in the field, this would be beneficial.

(3) Well defined: The terminology is established in the field, meaning there is no confusion as to what is meant.

(4) Unambiguousness: The categories are clearly defined, ensuring there exists no confusion.

(5) Mutual exclusivity: Categories do not overlap and thereby prevent ambiguities.

(6) Replicability: Repeated attempts at classification result in the same taxonomy classes.

(7) Versatility: There is a clear process for adding new items and updating the taxonomy.

4.2. Steps towards TaxIdMA. This section outlines the steps toward the taxonomies and their iterations. First, the iterations of the previous version are summarized, before the limitations are described. This leads to the iterations for the current version. Thereby, the rationale behind the choice of the taxonomies of TaxIdMA is presented.

4.2.1. Previous Version. The first and hence previous version of TaxIdMA [15] was generated through a regression manner by the abstraction of knowledge.

(1) First, all related information was gathered in one taxonomy and extended step by step while including information from attacks, taxonomies, and other related work. The items were grouped by known categories and found similarities in properties.

(2) With the growing complexity, ways to structure it more clearly were explored. This first resulted in two taxonomies: end-users and identity management systems.

(3) By regarding both so-designed taxonomies, many similarities were noticed. If these were nonchangeable during the attack, they were separated in an attack background. Thereby, the attack background can be used together with arbitrary taxonomies to explain an attack in detail. In addition, the terminology, notion, and structure were aligned.

(4) While including further items based on a literature review, the importance of system identities became clearer, adding another taxonomy.

(5) The proposed taxonomies were improved by discussions with experts and the application of selected real-world examples.

(6) Last but not least, TaxIdMA was evaluated based on real-world examples and a discussion.

Thereby, the first version of TaxIdMA consisted of the taxonomies' attack background, system identities, identity management systems, and end-user identities.

(i) Attack background: The taxonomy on attack background describes the background of all attacks involving identities and is constant during the attack cycle, which can involve several identities. Categories, where the values may vary either depending on the attack type or during the attack cycle, are included in the more specific taxonomies. Thereby, the attack background is used in every description, whereas the further taxonomies depend on the use case.

(ii) System identities: During the cyber kill chain, the attacker typically uses several identities, which are described in the related taxonomy. If the attacker utilizes multiple identities, then the taxonomy can be applied to each of these identities.

(iii) Identity management systems: Depending on the motivation of the attacker, gaining access to the identity management system may be one goal as all accounts (human, devices, etc.) are managed there. As a consequence, the categorization of these attacks can be made by the taxonomy of identity management systems. If an organization operates several identity management systems, which are compromised during an attack, for each system the taxonomy should be applied. With the outsourcing of services including identity management, several entities may be involved. As a result, the taxonomy can be applied to all entities.

(iv) End-user identities: While gaining access to an identity management system requires additional effort, attacks on end-user identities are usually with less time effort and less financial gain. Due to the scalability, a financial profit can be made. Therefore, another taxonomy describes these attacks.

Considering that an attacker may exploit various identities and identity management systems, several up to all specific taxonomies can once or multiple times be applied in a stepwise way. For example, a spear-phishing attack targets an employee. This is possible due to an identity leak for a service the employee typically uses (end-user identities). With the spear-phishing attack, the employee installs malware, which gives the attackers access to the computer (system/service identities). As the identity management systems were not patched recently, the attackers can attack it after some additional steps (identity management systems). In this example, all taxonomies can be utilized to systematically describe the attack. The direction of the description is not predefined and can be either from start to end or vice versa. The attack background generally outlines the attack.

4.2.2. Limitations of the Previous Version. While the first version of TaxIdMA was also the first step towards a taxonomy framework related to identities, it had several shortcomings.

(1) Not all items were unambiguous as social engineering attacks can, for example, apply hardware attacks. As a result, the human element had to be separated. This was done by simplifying the type of attack.

(2) The degree of detail varies between the taxonomies and not all information was included in every taxonomy. In consequence, streamlining items and terminology was required.

(3) In order to reuse the taxonomies for incident handling, the naming convention needed to be clearly defined.

(4) Although the first version was evaluated based on real-world examples, further validation has improved the outcome. In addition, input from further researchers was not actively sought originally.

(5) As suggested in its future work section, additional taxonomies related to IoT and SSI might be needed. As SSI is a completely different identity management model, it requires its own taxonomy. Furthermore, IoT devices have limitations, which should be included in the taxonomy. Both applications are used to explain the way how the taxonomies are derived.

4.2.3. Improved Version. The improved version described in the following sections is built upon the first version and improved in a stepwise way by expert interviews and a literature review.

(1) The first version is used as a basis.

(2) By expert interviews and a wider literature review, the given taxonomies are improved and better structured.

(3) To comply with STIX, the name system identity is changed to service identity.

(4) In order to provide an easier way to reference categories and elements, a naming convention is established.

(5) By further discussions and interviews, additional taxonomies are added: IoT devices and the new research direction SSI.

(6) Last but not least, TaxIdMA with its taxonomies is evaluated based on expert interviews, the application of real-world examples, and related work.

In consequence, the improved version of TaxIdMA includes the following applications. The methodology for these taxonomy applications is described in the corresponding sections.

(i) Internet of Things: IoT is a technology originating from the field of sensor networks. IoT devices can collect, process, and exchange data via a data communication network. In order to identify objects and describe the relationships with owners and other objects, several methods are applied and new ones are proposed (see, for example, [126–130]). To keep up with the technological progress and satisfy the diverse options, a new taxonomy is established.

(ii) Self-sovereign identities: Self-sovereign identities are an approach to digital identities that gives individuals control over the information they use to prove who they are to services on the Internet. The research direction obtains momentum with the new version of the electronic IDentification, Authentication, and trust Services (eIDAS) regulation [131, 132]. As self-sovereign identity is different from traditional identity management [133], at least from the entity and layer perspectives, it is best described in its own taxonomy.

4.3. Justification of Taxonomy Design Decisions. In this section, we give reasons for modifying, disregarding, and applying related work for resp. to TaxIdMA.

(1) Terminology: The previous terminology was based on established terms in the field. Although this is relevant for understanding, it does not reflect the possibility to use the taxonomy for threat intelligence sharing. Therefore, especially STIX terminology was taken into account while improving TaxIdMA. One example is the renaming from system identities to service identities.

(2) Level of detail: STIX especially details the attacker, which is adapted to add further information. The same applies to attack types, which are enhanced by Habiba et al. [53]. Windows integrity levels are omitted as they focus only on Windows systems.

(3) Categories: In addition, related work is used to describe attack types. The categories though do not clearly distinguish between attacks with and attacks without social engineering. Social engineering is one option, though it could be combined with other attack types. As a result, current categorizations are dropped. In order to provide information about the device, this item is added to the service identity taxonomy. Here, it is more relevant than other taxonomies, where it is combined with the location. With the chosen categories, not all combinations might be possible. Nonetheless, this approach was selected as it may provide more information. For example, unusual combinations are included and information is not redundant.

(4) Extendibility: Due to the different natures of SSI and IoT, these applications are added. A key element of taxonomies is extendibility. In order to provide guidance on extendibility, the steps towards these new taxonomies are described in more detail in the corresponding sections.

4.4. Naming Convention. The elements of the taxonomy are enumerated using the convention [T].[C].[I].n.

(i) T: Each taxonomy has a unique name with an abbreviation consisting of two resp. three letters — Background (BG), Service Identities (SI), Identity Management Systems (IMS), End-Users (UE), Internet of Things (IoT), Self-Sovereign Identities (SSI), and Web Application (WA). Thereby, two letters are the standard use case, while known abbreviations are applied.

(ii) C: The categories also have a one-letter abbreviation — Attacker (A), Target (T), Identity (I), and Attack (K).

(iii) I: This is followed by another abbreviation for the items—Type (T), Capabilities (C), Identity (I), Permissions (P), Authenticity (A), Delivery (D), Results (R), and Impact (M).

(iv) n: The leaves are enumerated. Sub-leaves are added by a dot and additional number. Further leaves are added accordingly if necessary. The only exception is Others (0) for better extendability.

For example, to describe the impostor authenticity of the attacker identity in the attack background, the following notion can be used: BG.I.A.1. The naming convention is practically shown in the background in Figure 1.

The naming of the taxonomy follows a clear structure. First, the type of the category is outlined. Then, the category is detailed. The name consists of one word, besides well-established terminologies, such as resource development or privilege escalation. In consequence, the different words can be combined. BG.I.A.1 can be named "Background Identity Authenticity Impostor".

4.5. Glossary. In the following, definitions for the terms used within the taxonomies are given. These definitions are based on [15] and related work.

(i) Attack: The use of an exploit by an adversary to take advantage of a weakness with the intent to achieve a negative impact.

(1) Category: Targeted weakness of identity management.
(2) Delivery: Way of conveying the attack.
(3) Impact: Loss or the consequences which are incurring (effects) due to the attack.
(4) Pattern: Description of the methodology used by the adversaries to exploit weaknesses.
(5) Results: Direct consequences (final product) of an attack.
(6) Type: Classification of the attack.
(7) Vector: Specific path, method, or scenario exploited.
(8) Vulnerability: Vulnerability resp. vulnerabilities used in the attack.

(ii) Attacker: Someone who explores methods for breaching weaknesses in a computer system or network.

(1) Capabilities: Expertise or the ability of the attacker to reach the goal.
(2) Type: Attributes of the attacker.

(iii) Identity: Digital identity used during the attack.

(1) Amount: Quantity of targeted identities.
(2) Authenticity: Attribution of the attacker towards the system during the attack.
(3) Completeness: State or condition of being complete concerning the identity control takeover.
(4) Directness: State of direction of targeting.
(5) Lifecycle: Stage of attack lifecycle, also known as cyber kill chain [45, 46].
(6) Permissions: Authorization of the overtaken digital identity.
(7) Timeliness: State and duration of being timely concerning the identity control takeover.
(8) Type: Type of digital identity used during the attack.

(iv) Target: A goal designated for an attack.

(1) Characteristics: Characteristics of the target, which have consequences on attack vectors and impact.
(2) Device: Device of the attacked target.
(3) Domain: Area of application of the target, similar to the sector, but in a broader sense.
(4) Level: Target position in the system stack.
(5) Location: Particular place in the physical space of the target in relation to the attacker.
(6) Identity: Position of the target related to the attacker.
(7) Sector: The area of industry the target is in.
(8) Type: Characteristics of the target.

(v) Type: A grouping based on shared characteristics.

4.6. Limitations. Although this improved TaxIdMA explains the design and iterations of the taxonomies, it uses the terminology of the research area, which requires basic knowledge. As a consequence, even though the structure should be clear, not all items may be known to novices. This article cannot provide further guidance in form of a tutorial. Instead, a web repository would be needed. As identity management is changing, further taxonomies might be needed in the future. Although we evaluate TaxIdMA on a wider basis, not all aspects might be discovered in this version.

5. TaxIdMA: Taxonomy on Attacks

This section describes the taxonomy framework TaxIdMA, which consists of taxonomies related to the attack background, service identities, identity management systems, and end-user identities. The background is constant during the attack cycle. In consequence, the taxonomy on the attack background is applied to all attacks and vulnerabilities. The taxonomies on service identities, identity management systems, and end-user identities further detail the attack resp. vulnerability. An attacker typically applies several service identities during the attack lifecycle, which is described in the related taxonomy. For multiple identities, the taxonomy is applied several times. Identity management systems can pose an interesting goal of an attack, as shown by the SolarWinds Orion attack. The related taxonomy can be used for all involved entities in a cross-organizational system. Last but not least, attacks on end-user identities are categorized according to the taxonomy as they are the goal in broader-scale attacks such as phishing or selected attacks, like spear-phishing. The outlined taxonomies can be applied in a stepwise way.

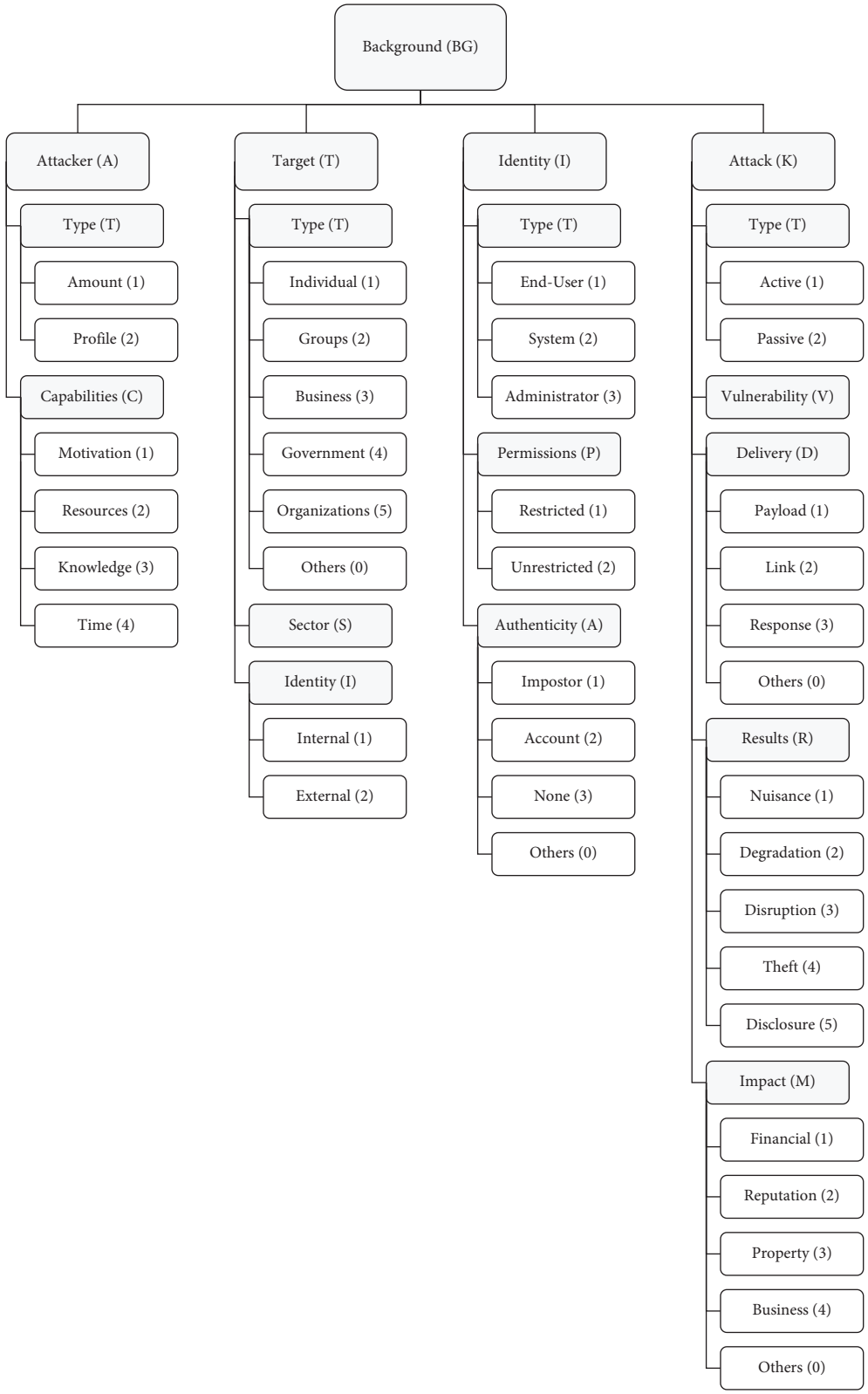

Figure 1: Taxonomy for attack background.

5.1. Attack Background. The attack background taxonomy describes the background of the attack, detailed by the following specific attack taxonomies. It is categorized by the attacker, target, attack identity, and the attack itself, as outlined in Figure 1.

5.1.1. Attacker. The attacker is someone who explores methods for breaching weaknesses in a computer system or network. They are detailed by type and capabilities [134].

(i) Type: The type of attacker describes the position and their profiles.
  (1) Amount: The amount specifies the number of persons involved, ranging from individual to small and big groups resp. organizations.
  (2) Profile: The amount partly relates to the profile. According to STIX, this can be activist, competitor, crime syndicate, criminal, hacker, inside accidental, insider disgruntled, nation state, sensationalist, spy, terrorist, and unknown. As attacks can be started by script kiddies and other less skilled persons, these should be added.

(ii) Capabilities: The expertise or ability of the attacker to reach the goal. The capabilities are characterized by motivation, resources, knowledge, and time. These impact the severity of the attack. The capabilities partly relate to the attacker type.
  (1) Motivation: According to STIX, motivation can be described as accidental, coercion, dominance, ideology, notoriety, organizational gain, personal gain, personal satisfaction, revenge, and unpredictable.
  (2) Resources: Depending on the resources, different attacks are possible. For example, an individual would probably use scripts found online or at Metasploit to exploit, whereas state-sponsored actors might use external sources to implement the malware.
  (3) Knowledge: The sophistication, as STIX calls the knowledge, ranges from none to minimal, intermediate, advanced, expert, innovator, and strategic.
  (4) Time: Time is an important resource, as, for example, scans and brute-force attacks may be extended over a longer time period with the hope of not being noticed by the monitoring system. Therefore, little, medium, and much are possible items.

5.1.2. Target. It is the goal designated for an attack, described by identity, type, and sector [135, 136].

(i) Type: Attacks focus on different targets, ranging from individuals, groups, businesses, governments, and organizations to other types.

(ii) Sector: These types can be grouped into sectors by applying the notion of STIX.

(iii) Identity: The identity describes the position of the target related to the attacker and can be further detailed by their roles internal (for example, executives, employees, administrators, and contractors) resp. external (for example, partners, customers, trusted third parties, competitors, and strangers).

5.1.3. Identity. Identity outlines the digital identity resp. identities used during the attack with their permissions [50] and authenticity.

(i) Type: The role of the digital identity in use by the attacker, i.e., end-user, system, or administrator [46].

(ii) Permissions: Identities come with permissions according to roles and functions, ranging from restricted to unrestricted [50]. In consequence, permissions describe the authorization the overtaken identity has at the expressed moment.

(iii) Authenticity: The authenticity specifies the authenticity of the attacker towards the system during the attack. The type of identity has one of the following authenticities: impostor (for example, during phishing attacks), the authenticity of a new or compromised account (for example, if successfully attacking a web server or the attacker is able to create a new account), none, or others. The authenticity hence describes one added human element [51].

5.1.4. Attack. The attack is categorized by type, delivery, results, and impact to comply with [135, 136].

(i) Type: The type characterizes the threat. Active attacks include social engineering, physical attacks, and web attacks among others. Passive attacks describe eavesdropping and other passive methods.

(ii) Vulnerability: The actual vulnerability exploited by the attacker [49]. This inherently relates to criticality.

(iii) Delivery: This explains the way of delivering the attack, ranging from payloads (for example, a reverse shell), links (for example, phishing links), and responses (for example, server or e-mail responses) to others (for example, physical) [137].

(iv) Results: The direct consequences of an attack, ranging from nuisance and degradation at the lower end to disruption, theft, and disclosure.

(v) Impact: The loss or the consequences which are incurred due to the attack. This includes financial, reputation, property, business, and others.

5.2. Service Identities. During attacks targeting servers among others, attackers typically use different identities. In order to categorize these, the following taxonomy (see Figure 2) further details target, identity, and attack.

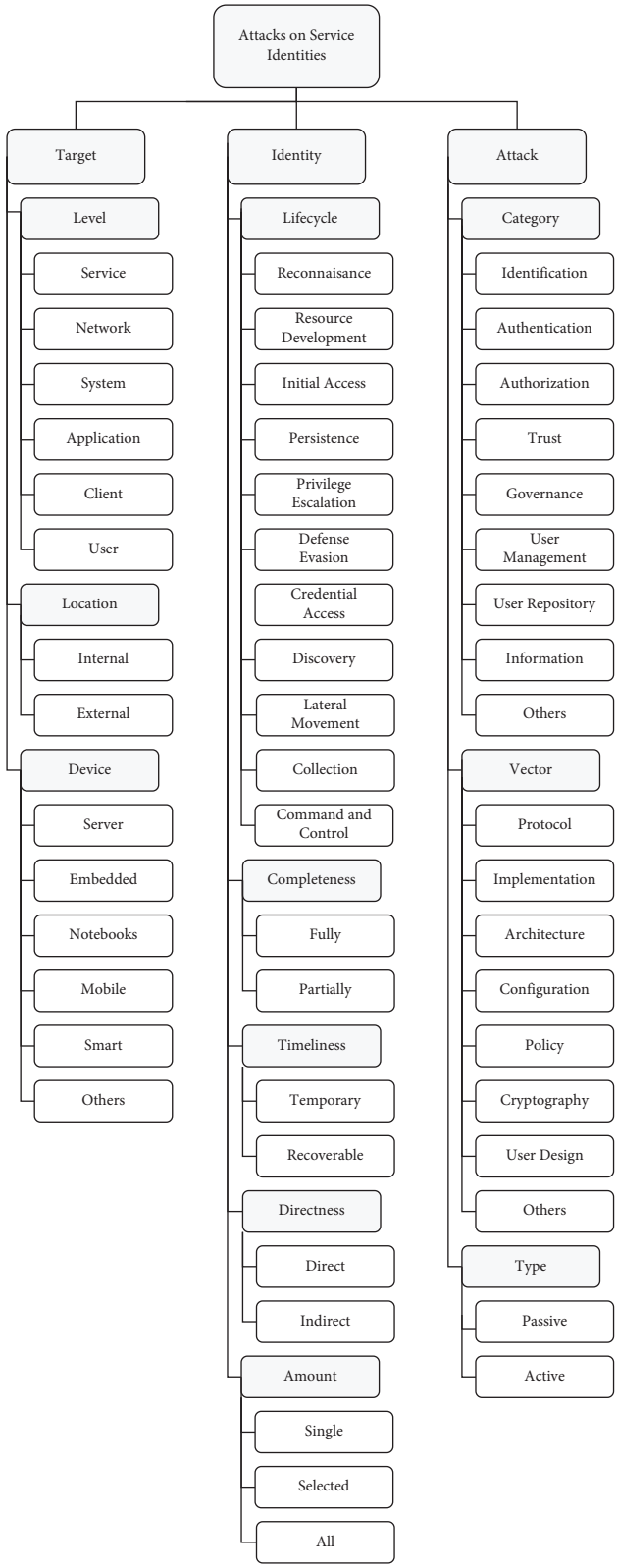

Figure 2: Taxonomy for attacks using service identities.

5.2.1. Target. The target specifies the target of the attack. This information is an addition to the attack background.

(i) Level: Level describes the target level in the system stack. As identities appear on different levels, all these levels can be targeted. This includes a service, network, system with cryptography and hardware, an application with a server (for example, database, storage, web, and e-mail), and a client as well as a user [138]. The degree of detail varies from taxonomy and taxonomy and, therefore, is included in each taxonomy besides background.

(ii) Location: The physical location of the target is categorized here. The location of the target in relation to the attacker may vary, from local/internal to external, for example, a trusted third party [53].

(iii) Device: The device specifies the location of the targeted device, as it is more relevant in this context.

5.2.2. Identity. The identity categorizes lifecycle, completeness, timeliness, directness, and amount.

(i) Lifecycle: The stage of the attack lifecycle, that is, cyber kill chain [45, 46].

(ii) Completeness: The completeness of identity takeover, i.e., fully or partly.

(iii) Timeliness: The timeliness of identity takeover, i.e., definitely temporary or recoverable.

(iv) Directness: The direction of targeting, i.e., directly or indirectly.

(v) Amount: The amount of targeted identities. While applying different identities during the attack lifecycle, the amount is most likely single or selected identities.

5.2.3. Attack. The attack is described by category, vector, and type.

(i) Category: The targeted weakness of identity management, i.e., identification, authentication, authorization, trust, governance, user management, user repository, information, or others [47]. This includes the identity lifecycle by governance (request, provisioning, and de-provisioning) and identification, authentication, and authorization (operation).

(ii) Vector: The vector specifies the path, method, or scenario exploited. This can range from protocol, implementation, architecture, configuration, policy, and cryptography to user design and others.

(iii) Type: The type further details the attack, i.e., passive or active. Both include further attacks, such as probing, scanning, bypassing, eavesdropping, and modifying [57].

5.3. Identity Management Systems. Due to the reason that identity management systems manage all identities (for example, humans, devices, and services) in an organization, they pose an interesting goal. Figure 3 outlines the importance of the location in the diverse setting. Target, identity, and attack are explained in the following.

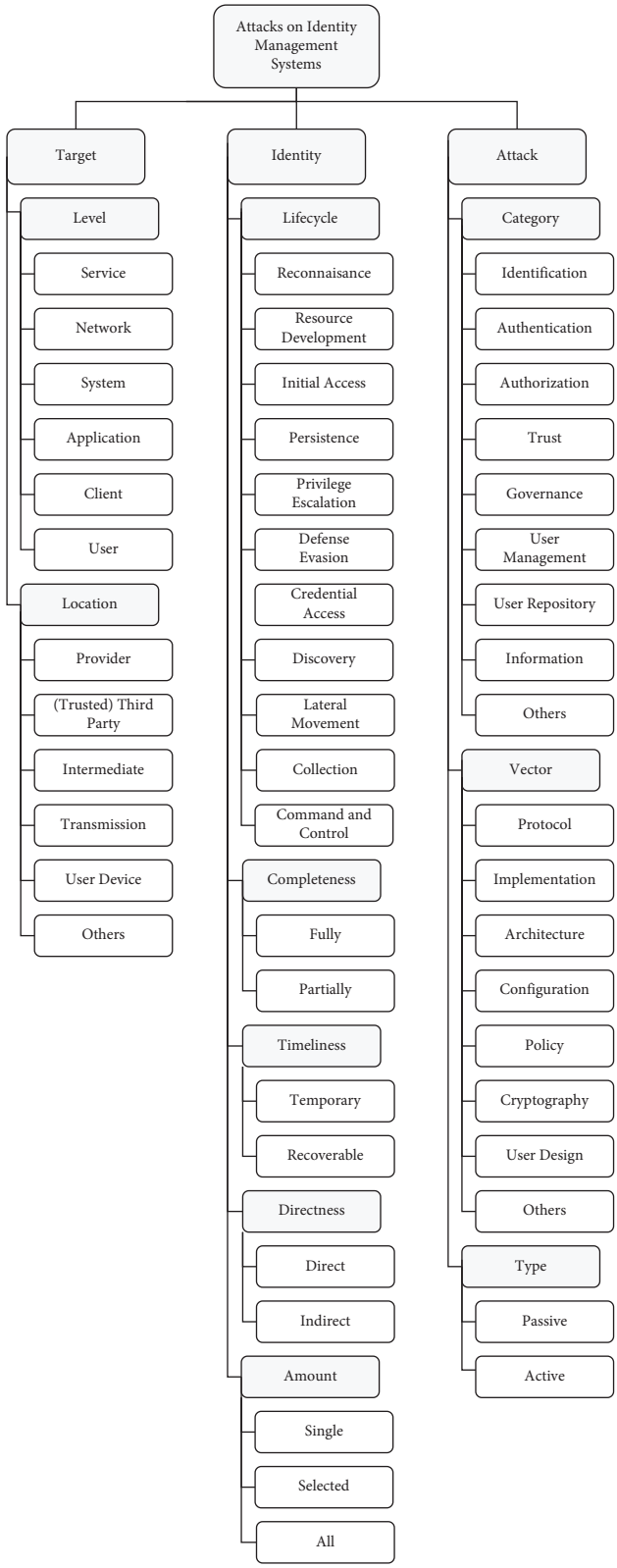

Figure 3: Taxonomy for attacks on identity management systems.

5.3.1. Target. The target is detailed by level and location.

(i) Level: The level is similar to the one in service identities [138] shown above and includes service, network, system, application, client, and user.

(ii) Location: Identity management systems can be cross-organizational and operated in a cloud environment by other entities. As a result, the location is either internal or external and according to [53] diverse with (identity/service) provider, (trusted) third party, intermediate, transmission, and user device as well as others. The device is not relevant for identity management systems in contrast to service identities.

5.3.2. Identity. The identity is described by the lifecycle, completeness, timeliness, directness, and amount.

(i) Lifecycle: The attack can involve or target the identity management system at different stages of the lifecycle [45, 46]. These include, according to MITRE ATT&CK, reconnaissance, resource development, initial access, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, and command and control.

(ii) Completeness: An identity management system can partly or fully be taken over, as shown with silver and golden tickets for AD [139].

(iii) Timeliness: The timeliness is either temporary or recoverable, whereas recoverable is standard for an identity management system.

(iv) Directness: The attacker can either directly or indirectly target the identity management system.

(v) Amount: An attacker can overtake single, selected, or all accounts. The amount might increase during the attack.

5.3.3. Attack. An attack is outlined by category, vector, and type. This category is similar to service identities.

(i) Category: The taxonomy applies the category of attacks in [47]—identification, authentication, authorization, trust, governance, user management, user repository, and information as well as others.

(ii) Vector: The attack vector is divided into the items protocol, implementation, architecture, policy, cryptography, user design, and others. Two examples of implementation are shown next. The implementation of AD had the vulnerabilities MS17-010 Eternal Blue [140] and MS16-032 [141] in earlier versions. The AD implementation of Kerberos could be used for Pass-the-Hash [142] and Kerberoasting [143] attacks. The configuration can be a source as well. The configuration of AD has pitfalls, grouped into accounts (for example, password in comments), groups (for example, built-in groups and unlimited groups), and delegation. Some implementations of LDAP are vulnerable to enumeration by misconfiguration. With identity management systems exposed to the web, API security becomes important.

(iii) Type: The type of attack, or technique at MITRE ATT&CK, describes the sort of attack, which is either passive or active and can be further detailed in the leaves.

5.4. End-User Identities. The end-user identity taxonomy focuses on user identities, which are typically targeted in large-scale attacks. While an individual digital identity has little financial value (which varies between the identity types), the amount of acquired accounts makes these types of attacks interesting for attackers. In consequence, the taxonomy as shown in Figure 4 includes additional identity types. The type of attack is concretized by the inclusion of an additional pattern.

5.4.1. Target. The target user limits the possibilities.

(i) Level: User identities appear on the levels of system, application, client, and user.

(ii) Location: User identities are stored in databases and identity management systems mainly. Furthermore, users may store them directly or indirectly on devices. As a result, the same locations are possible with (identity/service) provider, (trusted) third party, intermediate, transmission, user device, and others.

5.4.2. Identity. The identity is described by type, completeness, timeliness, directness, and amount.

(i) Type: Typical identity types contain information resp. accounts about financial information, such as credit card (including child credit card history) and bank; employment (according to STIX, this may be LDAP, OpenID, remote authentication dial-in user service (RADIUS), UNIX, or Windows local/domain); state-related information such as tax, eID, and social security number; phone; insurance including healthcare; online social networks (for example, Facebook, Twitter, Skype, and Instagram); online shopping; and others.

(ii) Completeness: Completeness is divided into full (for example, phishing) and partial (for example, session hijacking) takeover.

(iii) Timeliness: Timeliness is defined as either temporary (for example, session hijacking) or recoverable (for example, phishing).

(iv) Directness: The attack can either be direct (for example, phishing) or indirect (for example, supply chain attack).

(v) Amount: The amount ranges from single to selected and all.

5.4.3. Attack. The attack is specified by type and pattern.

(i) Type: The attack type contains the same categories as the already described taxonomies. Typical attacks towards identities are outlined. This includes brute-force attacks and social engineering, which could be further detailed. Brute-force includes OSINT-based, hybrid, password spraying, credential stuffing, dictionary, and rainbow table. Another type is web attacks with cookie replay and other types of session hijacking among others.

(ii) Pattern: The pattern describes the methodology applied by the adversaries. The attack pattern contains identity theft, identity manipulation, and deanonymization. Identity theft is further divided into new account fraud (for example, existing profile cloning attack) and account takeover (for example, by account recovery exploit), which can be combined. The category of pattern relates to CAPEC, CWE, and OWASP.

6. Application of TaxIdMA on Specific Areas

TaxIdMA is a rather generic taxonomy framework related to attacks on identities and identity management systems. Specific areas may have customized properties as indicated in [15]. We outlined two of them, IoT and SSI, which have partly different properties. In consequence, we describe TaxIdMA for IoT and SSI in the following.

6.1. Internet of Things. IoT describes physical objects with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems. In the consumer market, IoT technology is contained in the concept of smart homes. Otherwise, IoT is used in healthcare systems, industry, and many more.

6.1.1. Methodology. In order to classify IoT, we use the search terms "(iot OR "Internet of things) AND (taxonomy OR categorization OR classification OR vulnerability)" at IEEE, ACM, USENIX, MDPI, and Springer Link. The results are evaluated in accordance with the search term and then further processed to extract the important aspects. If several approaches contradict, the average proposal is used. In addition, unstructured interviews with experts in the IoT area help to further detail certain characteristics. The thereby extracted characteristics are then compared with the taxonomies of TaxIdMA. If IoT differs in a certain aspect, then the corresponding characteristic is added.

6.1.2. Application of TaxIdMA on Internet of Things. IoT architectures consist of IoT devices, maybe gateways, network structures, and central systems for administration and processing that might be in the cloud to allow the IoT devices to communicate with each other. Thereby, IoT architectures consist of different layers. These may depend on the actually applied protocols. Based on [69, 77], we summarize them as infrastructure (sensors, gateways, and other devices, but also central units), communication (connectivity between the elements, for example, with 5G, Wi-Fi, Bluetooth, and low-power wide-area networks (LPWANs) [73]), routing, service (application), a client (for end-users), and others. These

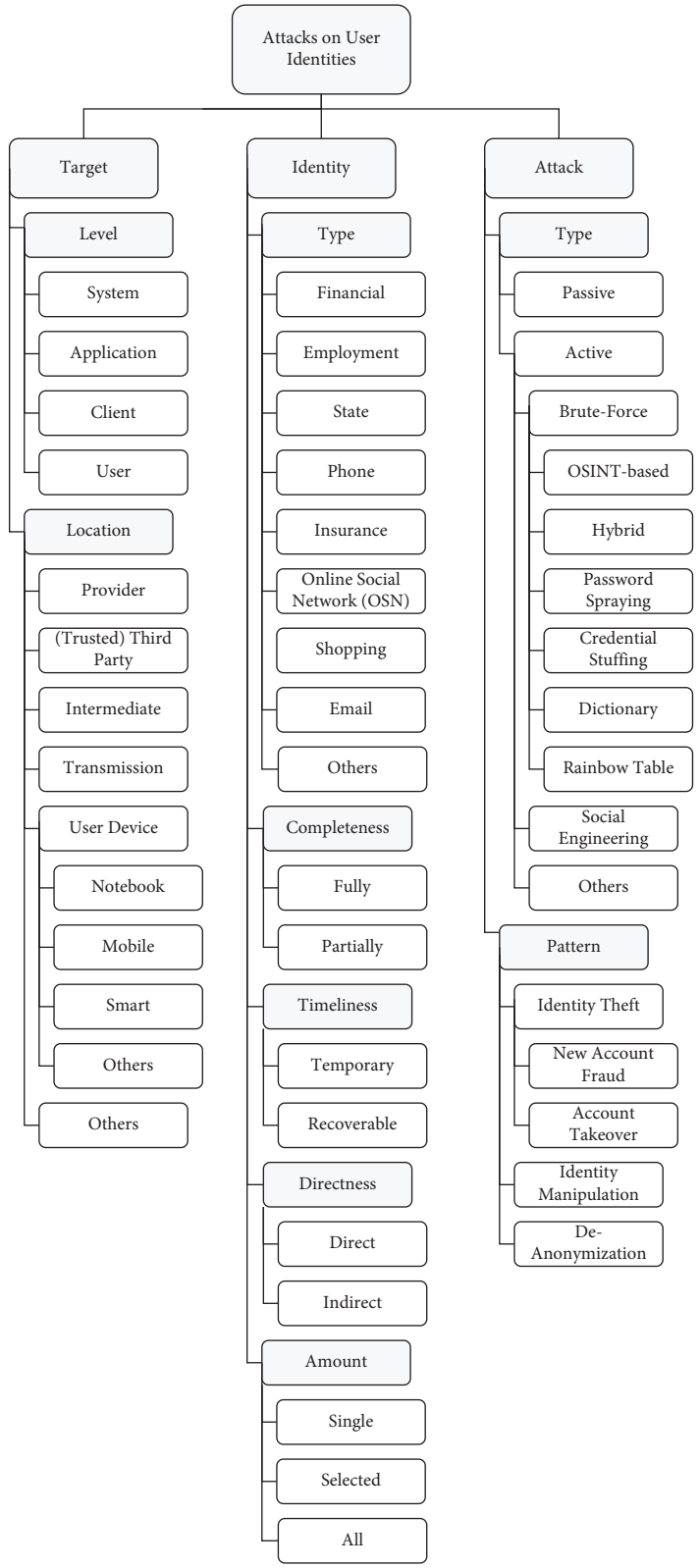

Figure 4: Taxonomy for attacks on end-user identities.

layers support IoT devices to collect and process data. With these layers, we also notice various identities: all the devices, users, but also applications, and maybe data. As this architecture goes beyond the ISO/OSI model to include the transformation of data into usable information, the layers are adapted in the taxonomy. In consequence, the object characteristics differ, ranging from automation and intelligence to storage and processing [60]. Due to the different

infrastructures, other attacks are possible, such as tag cloning, sensor tracking, rogue access, and tampering [62–64, 77]. In addition, the attacks at least partly depend on the location (inside vs. outside) and the domain (healthcare, transport, smart homes, robotics, etc.) [61]. The security countermeasures may differ from the type of IoT device. For example, industrial and commercial devices might have more countermeasures than consumer devices, although this is subject to the actual device [69]. The attacks again have various consequences, up to life-threatening situations.

In consequence, the taxonomies on the attack background and service identities are adapted as follows. Again, the background generally describes the attack, whereas the other taxonomies specify the attack in more detail. This includes attacks on the communication layer. The taxonomy for attacks on user identities typically uses the identity type others, as IoT devices are concerned. As shown by Wüstrich et al. [64], the typical attack vectors apply here. Regarding identity management systems, the identity type (for example, human, device, and application) could be included. Otherwise, these two taxonomies remain the same.

(1) Attack Background The background, as shown in Figure 5, applies the terminology of the IoT area and is adapted as follows.
   (i) Attacker: Nothing is changed.
   (ii) Target: The target type uses the terminology, i.e., consumer instead of individual, industry instead of business, and commercial instead of groups [69]. Consumer goods target end-user applications including personal devices (for example, cameras, smartphones, and refrigerators). Commercial IoT devices refer to the resources utilized by enterprises and bigger infrastructures. They could be used with an additional security layer for industry, government, and other organizations. Industrial IoT includes sensors, actuators, controllers, industrial assets, remote telemetry, monitoring, and management systems for mission-critical architectures. The sector is changed into a domain, which features the most important areas of smart home, healthcare, transportation (for example, vehicles), and Industry 4.0 [61].
   (iii) Identity: The type includes the division into sensor, device, and system. The differentiation between a device and a sensor determines the place of change. As an example, a sensor could be replaced, resulting in different data, while the device stays the same. Furthermore, the locations producer, consumer, and intermediate are added [69].
   (iv) Attack: Nothing is changed.

(2) Service Identity Service identities (sensors, gateways, etc.) are adapted according to the literature (see Figure 6).
   (i) Target: The target level features the levels (i.e., physical, logical, and application) summarized above according to the literature [69, 77]. These can be further detailed if required. Depending on the target level, other attacks are possible, for example, jamming, cloning, and tampering on the physical layer and exhaustion and unfairness at data link, resp. spoofing, sinkholes, Sybil attacks, wormholes, clone IDs, and more on the network. Applications can be attacked by malware, flooding, and code injection, among others. The location (internal resp. external) is not as important in IoT settings as in others, whereas indoor and outdoor would be more interesting and could be added [61]. The devices reflect the IoT environment with gateways and sensors among others. It is decided to keep both characteristics separately to allow a finer grade of detail. In addition, the characteristics of the target are outlined, i.e., automation, intelligence, storage, sensing, processing, and others [60].
   (ii) Identity: The identity is not changed.
   (iii) Attack: The attack category is adapted accordingly, i.e., management instead of user management and the omission of user repository. Trust attacks in the IoT environment include, for example, Sybil attacks, bad-mouthing, ballot stuffing, denial of service, black holes, and on-offs[143].

6.2. Self-Sovereign Identities. Self-sovereign identity is an approach that gives users control over their information in a decentralized setting. Thereby, the users can provide user information they received from their home organizations to service providers independently.

6.2.1. Methodology. In order to classify SSI, we search for "(attack OR security OR vulnerability) AND (ssi OR "self-sovereign identity" OR "self-sovereign identities")" and elements (wallet, blockchain, and distributed ledger technologies) at IEEE, ACM, USENIX, MDPI, and Springer Link. We then regard the content for relevance and include the elements accordingly. Based on the literature review and expert interviews, we detail categories and align them in the taxonomy framework accordingly.

6.2.2. Adaption for SSI. The SSI architecture comprises the entities issuer, holder, and verifier, which use a decentralized system such as blockchain to store data [145]. Further important components are the wallet of the holder, typically on a smartphone, and software agents and network nodes. The issuer verifies the credentials of the holder, which are then stored in the wallet. The holder can present verifiable presentations depending on the information the verifier requests. Basic information about the entities among others is stored in a decentralized way. This might be blockchain as a form of decentralized ledger technology. One application for blockchain is cryptocurrencies such as Bitcoin, where more attack vectors are known [146–154]. Consensus and

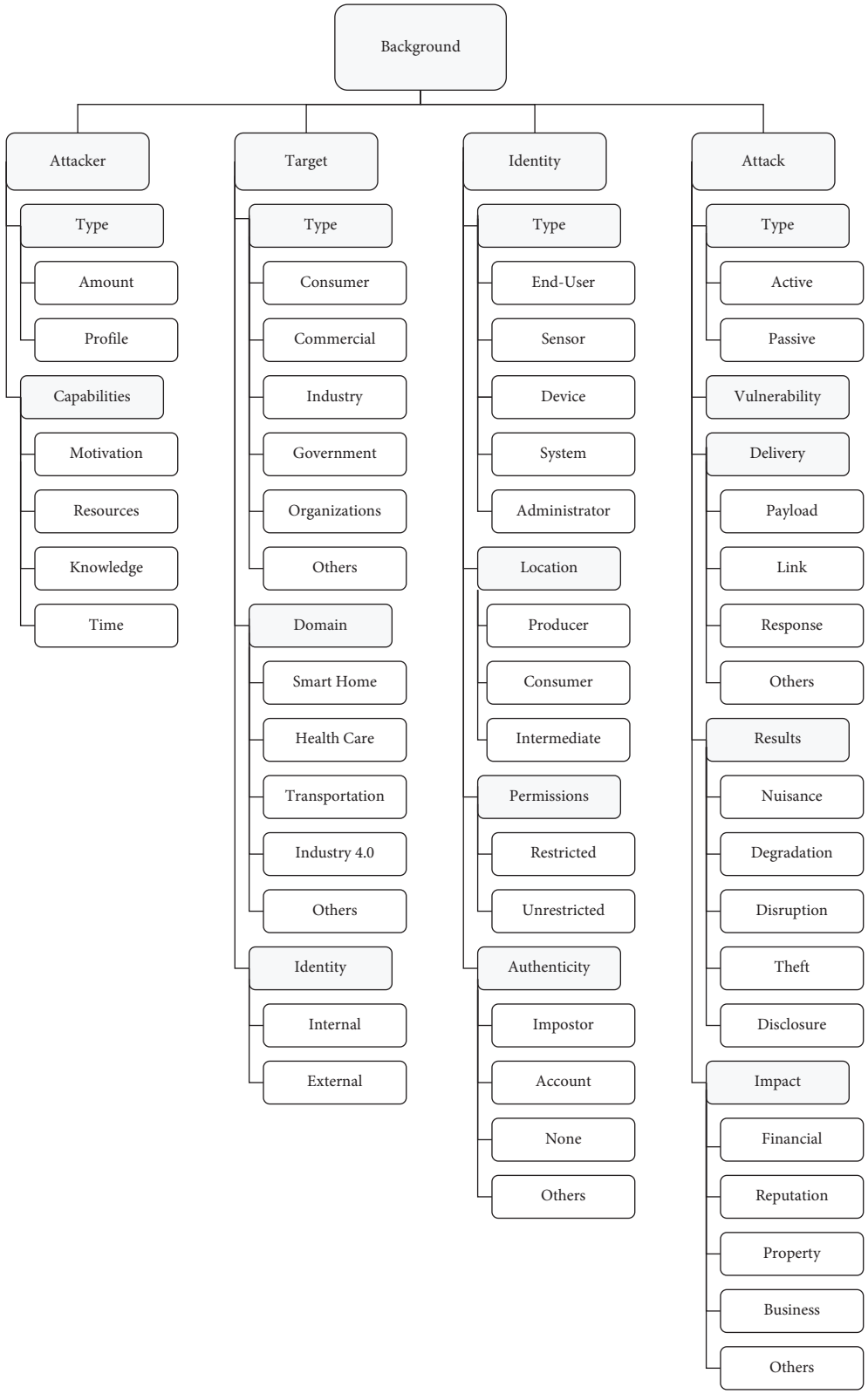

Figure 5: Taxonomy for IoT attack background.

ledger-based attacks are possible, such as Finney attack, race attack, and 51% attack, resulting in double-spending. If no central authority is introduced, Sybil attacks, eclipse attacks, denial of service attacks, and routing attacks might be possible. Regarding issuer and verifier, fake resp. compromised entities, fake identity attacks, and identity theft attacks are relevant. Another interesting target is the holder with the wallet, which could be compromised by malware, physical

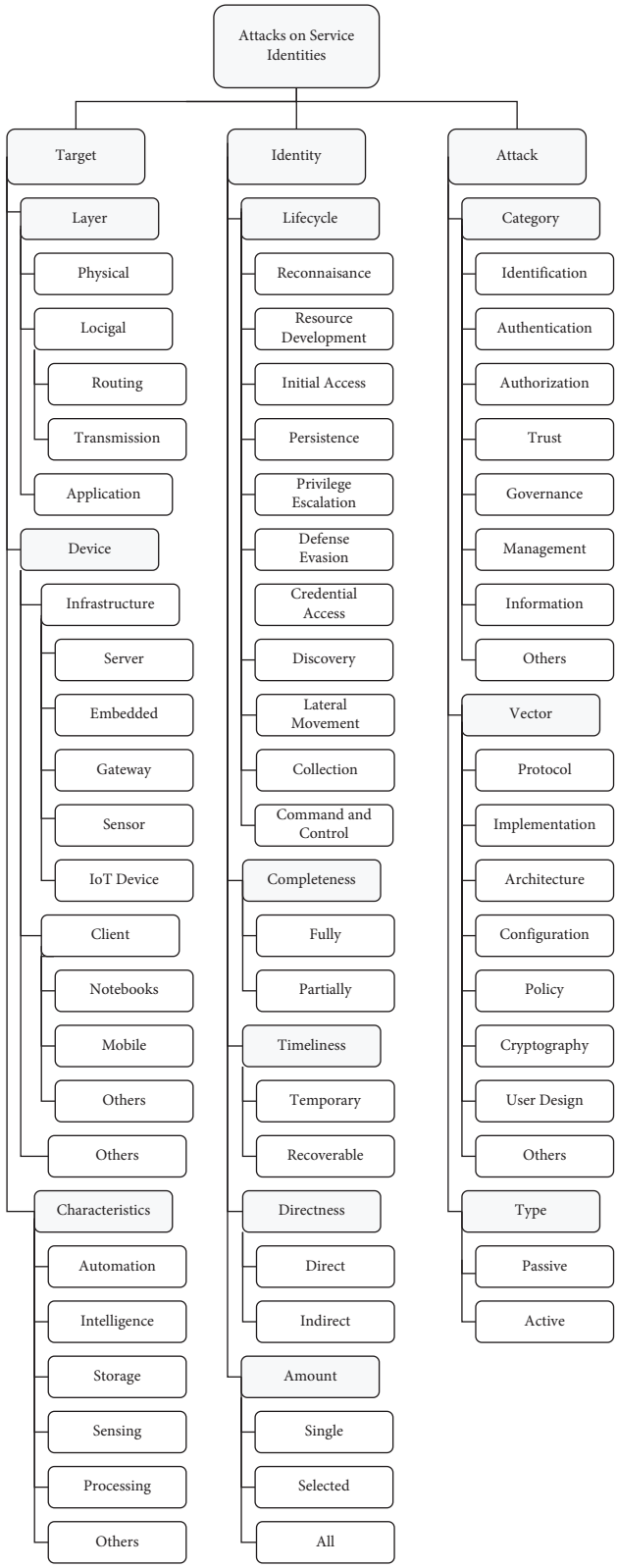

Figure 6: Taxonomy for attack on IoT service identity.

access, social engineering, and other forms of malicious actions. More approaches are known for cryptocurrencies [103, 155–157]. In consequence, Naik et al. [41] determined software agents, network nodes, and data stores (wallets) as assets. The authors outlined faking identity attacks, identity theft attacks, and distributed denial of service attacks as potential attacks on SSI systems. These attacks are then further detailed by attack trees.

Different attacks are possible due to the usage of decentralized storage and protocols. In consequence, the main difference is the target within the taxonomies on end-user identities, identity management systems, and service identities. Especially the items of level and location are adapted (differ from the foundational one) as follows, utilizing standardized terms [145].

(i) Level: Service, Network (i.e., normal or decentralized), System (Server, Client), Wallet, Agent, User, and Others.

(ii) Location: Issuer, Holder, Verifier, TTP, Decentralized Storage (for example, distributed ledger technologies such as blockchain), User Device, Transmission, and Others.

The identities do not change as they could be issued to the user. For example, they have the e-mail address user@provider.com. Even though the holder possesses the user device, the importance of the device (typically a smartphone) is emphasized with the addition of both. Due to the fact that self-sovereign identity gives the user full control over their identities, this is justifiable. Here, especially attacks focusing on the user such as social engineering can be possible. The adapted taxonomy is shown in Figure 7 for end-user identities in the SSI environment.

7. Evaluation

The evaluation is three-fold. First, we apply typical threats and talk about statistics concerning identity management. Following this, we evaluate TaxIdMA based on the established requirements. Last but not least, we summarize the expert interviews and their results.

7.1. Application on Typical Threats. According to Symantec [158], targeted attacks are on the rise, whereas 65% of groups use spear phishing as the primary infection vector and 96% of groups' primary motivation continues to be intelligence gathering. The ENISA threat report 2022 [159] describes that new forms of phishing arise such as spear-phishing, whaling, smishing, and vishing. In consequence, information on the web and social engineering are important ways to receive information. According to the Federal Trade Commission [160], identity theft is rising since 2001 from 0.33 million to 5.7 million in 2021 in the U.S. Government documents or benefit frauds are on the top with 396,012 complaints, followed by credit card fraud (389,845) and identity theft (377,203). Further top identity thefts are loan or lease fraud (192,967), bank fraud (124,497), employment or tax-related fraud (111,755), and phone or utilities fraud (88,842) in 2021. Scammers typically engage by phone (646,440), text (378,119), e-mail (264,069), website or apps (180,114), social media (159,458), others (115,730), mail (43,915), and online ad or pop-up (36,731). According to Ernst & Young (EY)

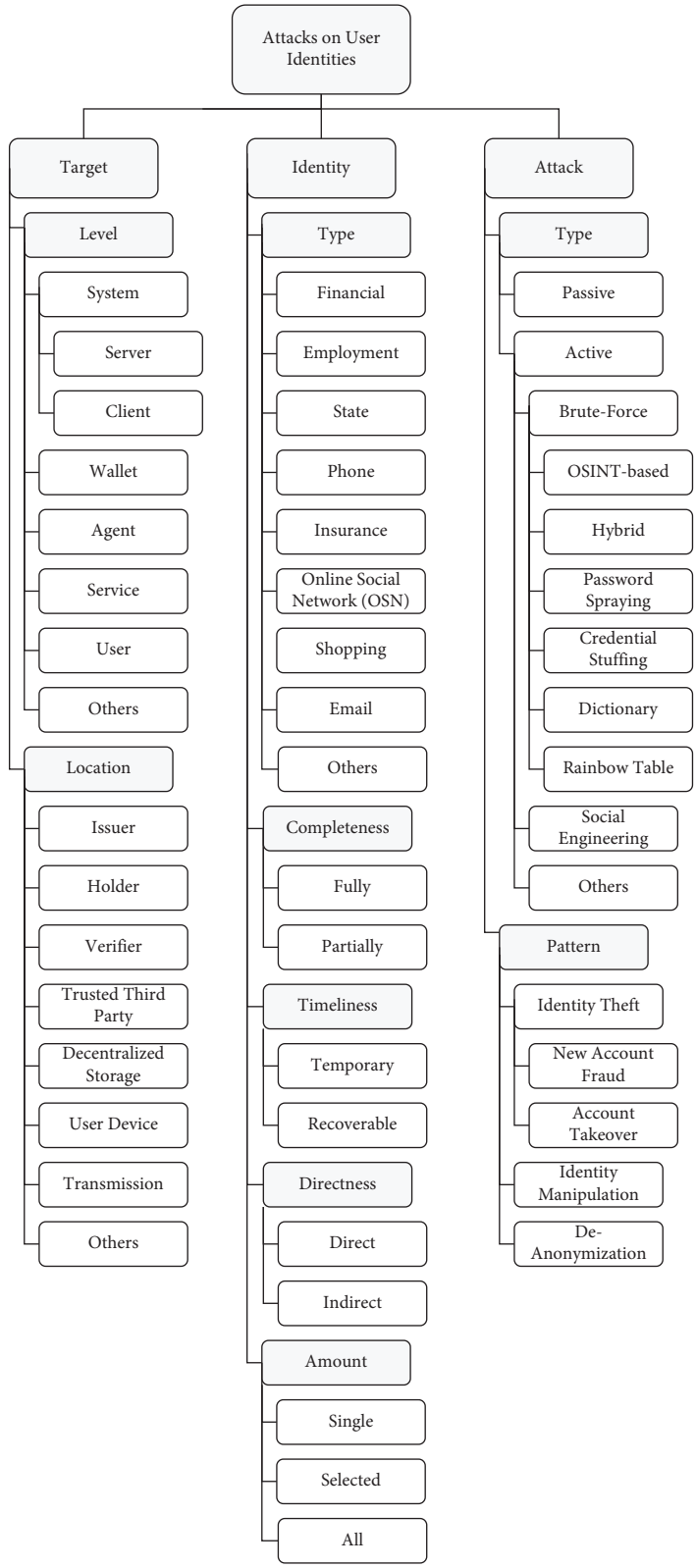

Figure 7: Taxonomy for attacks on end-user identities at self-sovereign identities.

Security Survey 2018-19 [161], the top ten most valuable kinds of information to cyber criminals are customer information (17%), financial information (12%), strategic plans (12%), board member information (11%), customer passwords (11%), research and development information (9%), merger and acquisition information (8%), intellectual

property (6%), non-patented IP (5%), and supplier information (5%). Identity theft is used during all stages of the attack lifecycle. According to ENISA [160, 162, 163], brands such as Microsoft and Amazon are often impersonated. The top data types lost in 2019 are e-mail (65%), password (59%), name (26%), miscellaneous (18%), address (13%), credit card (12%), and account (10%). EY [161] summarizes the top 10 biggest cyber threats to organizations as phishing (22%), malware (20%), cyberattacks to disrupt (13%), cyberattacks to steal money (12%), fraud (10%), cyberattacks to steal IP (8%), spam (6%), internal attacks (5%), natural disasters (2%), and espionage (2%).

Regarding the OWASP Top Ten [164], we notice that broken access control is the top web application security risk. This is followed by cryptographic failures, injection, insecure design, security misconfiguration, and vulnerable and outdated components. The seventh item is identification and authentication failures, previously called broken authentication. Software and data integrity failures, security logging and monitoring failures, and server-side request forgery are also included. Thereby, we notice the importance of authentication and access control. This is not only the case at standard online services but also for IoT environments as noticed by IIoT World [165].

In order to take over the credentials of an employee, an attacker might first look at third-party breaches, where actors share datasets publicly or in private. These could be gained from insiders, phished credentials, malware, and otherwise stolen credentials. Based on the dataset, attackers may attempt to compromise the login. If the attacker has a password list, they could try brute-force attempts, password spraying, and password reuse. If the passwords are hashed, then cracking may be successful in the case that the hash algorithm is insecure and respectively or no salt was added. MFA can be applied to increase security if the factors are independent. Typical methods include e-mail, SMS, and software and hardware code. If the attacker has the original password and MFA is enabled, then further factors need to be bypassed. The bypass attempts depend on the actual deployed MFA and system behind. By finding flaws in the technology underpinning the MFA solution, MFA can be circumvented. This may include compromising the encryption of the secrets, finding patterns, and hijacking name spaces. Again, there is the human element with social engineering. Furthermore, the network session could be hijacked. E-mail MFA can be bypassed by e-mail (such as O365 mailbox via Exchange Web Services (EWS)) compromise, physical threat, social engineering, and extortion via harassment. For SMS, SIM swapping is an additional attack vector. Social engineering, extortion via harassment, token theft, and physical threat also apply to software and hardware MFA code. Other vectors are the discovery of vulnerabilities by scanning the domain, IP addresses, ports, and services. If a vulnerability is discovered, it might be exploited using an exploit with a customized payload, which is delivered to the victim. Such exploitation results in the initial access to the infrastructure. If the attackers are successful in bypassing the employee's credentials or exploiting the infrastructure, they could access the portal or services and compromise the account. Thereby, further actions such as execution and privilege escalation might be possible [166]. In consequence, the end-user credentials are important here, although other means might be used.

Regarding our taxonomy, we see the following.

(i) Target: At least for the first factor, the target level is often the user (i.e., social engineering and other password attacks). With MFA, it could not only be user's device but also the underlying infrastructure and network.

(ii) Identity: The identity type is employment with direct and complete takeover until recovery. The amount can be everything from single to all, although single or selected is most likely.

(iii) Attack: The attack type is most likely active with the pattern of identity theft. If MFA is enabled, then two types are required to compromise the account. The exact type depends on the attack path.

The Identity Defined Security Alliance (IDSA) trend report for 2022 [167] outlines that inadequately managed privileges (36%), excessive privileges (21%), and compromised privileged identities (23%) result in breaches. Acquired privileged accounts shorten the attack lifecycle to access sensitive data. Nonetheless, further identities can be used in attacks, especially if the number of identities in organizations is increasing due to the adoption of more cloud applications, third-party relationships, machine identities, and further reasons. Although employees are most likely to be attacked successfully and have the biggest business impact, many organizations have business customers, third parties, consumers, and machine identities. According to IDSA, 84% experienced an identity-related breach in the past year. The number of incidents targeting the identity management system is though not known to the authors. At least in the SolarWinds Orion attack, they were used. In consequence, these can be characterized by TaxIdMA.

7.2. Expert Interviews. In order to improve and quantitatively evaluate TaxIdMA, we conducted semi-structured interviews with experts in identity management, IoT, and SSI. The interviews were in accordance with the ethics board and their guidelines.

7.2.1. Methodology. The experts were selected on the basis of their competence in the fields. Such competence was assumed on the basis of the following main criteria for inclusion: that the experts should be working in the field for at least one or several years with at least either projects or publications related to their work. For example, a person working in research on the topic of SSI for seven years is considered fitting. The selection of the experts was performed on the authors' personal experience and the advice of other experts. In order to obtain the six experts, we had to contact twelve experts in all. The experts did not get any compensation.

The interviews were performed either in person or virtually via a conference system. The interview language was German ($N = 5$) or English ($N = 1$), according to the preference of the participants. Interviews took place in November resp. December 2022 and lasted an average of 30 minutes. The first part of the semi-structured interviews was dedicated to the specific area of expertise (description of the area and the related threats and attacks). Then, the corresponding taxonomy resp. taxonomies were shown and explained with the text of this article, leading to a discussion about the correctness (general understanding, division of the taxonomies, the related categories and their items, and completeness). The third and last part of the interview focused on specific aspects of the taxonomy and the field of expertise (corresponding taxonomies, again threats and attacks, and possible improvements). The transcripts were analyzed, discussed, and collated. Here, we used Delphi panels to discuss and collate the comments.

7.2.2. Results. In the following, the results of the expert interviews are summarized.

(i) TaxIdMA: Before improving TaxIdMA, comments from the presentation of [15] were noted. In addition, a semi-structured interview with two experts was conducted to receive further input for the improved version. The focus was on the correctness, completeness, and understandability of TaxIdMA. Last but not least, typical attack vectors and vulnerabilities were discussed and categorized by TaxIdMA during the interviews. The feedback was incorporated into the new version of TaxIdMA, which was discussed with five experts (two from the previous round and three new experts) in semi-structured interviews. Here, TaxIdMA was structured and detailed to the satisfaction of the experts and no further iterations were needed.

(ii) IoT: In order to establish a first version of the taxonomy for the IoT environment, related work was analyzed and an expert was interviewed about the potential adaption of TaxIdMA for IoT and different attack vectors and problems with IoT. This was accompanied by another extended literature review, leading to the first version of the taxonomy. The application of the taxonomies was then evaluated by one expert for correctness, completeness, and understandability. While the taxonomy on the background stayed the same, the description was extended by further explanations. The taxonomy of IoT service identities was changed as follows: target layer and device were separated to provide more information and flexibility. This improved taxonomy version was then evaluated by four experts. At this point, the adaption gained the approval of the experts.

(iii) SSI: A first version of the taxonomy was designed based on the literature review and knowledge of the authors. This version of the taxonomy was then discussed with three experts in semi-structured interviews. In the interviews, the experts were fine with the adaptation for SSI. In addition, one expert suggested providing detailed security analysis of SSI as this is currently missing. Due to the scope of the article, we plan to conduct such an analysis in future work.

7.3. Requirements. For TaxIdMA, seven criteria were previously selected to judge the effectiveness. We discuss their fulfillment in the following.

(1) Completeness/exhaustibility: All objects identified by the authors are contained in the taxonomy. There might be objects missed out.

(2) Comprehensiveness: As TaxIdMA reuses established terminology and groupings, the taxonomies are understandable for experts in the fields. For novices, further material in form of guidelines and more detailed descriptions would be necessary.

(3) Well defined: The terminology is established in the field. In contrast to the original version, some terminology was adapted from STIX, helping to apply TaxIdMA in threat intelligence sharing. As a result, there should be no confusion.

(4) Unambiguousness: The categories are clearly defined by the glossary.

(5) Mutual exclusivity: In contrast to the original taxonomies, some categories were defined in more detail resp. in less detail, leading to categories not overlapping. Some categories depend though on each other, for example, target level and location. This is needed as further items could be chosen.

(6) Replicability: Although different elements of the taxonomies could be grouped differently, the process to derive the so-described taxonomies is outlined, which could result in replicability. With IoT and SSI and the same authors, the same taxonomy classes were used. In consequence, the replicability is at least partly fulfilled.

(7) Versatility: The process for updating the original TaxIdMA and adapting the taxonomy framework for IoT and SSI was described in a step-by-step way. Thereby, TaxIdMA is versatile.

8. STIX for Identities

STIX is a well-known language and serialization format to exchange cyber threat intelligence related to all aspects of suspicion, compromise, and attribution. It consists of 18 STIX Domain Objects (SDOs), ranging from attack pattern to vulnerability, and two STIX Relationship Objects (SROs), i.e., relationship and sighting. Thereby, different attacks are describable in a structured way and this information can be shared. STIX can be extended as long as existing standardized objects or properties are not redefined. The three ways STIX proposes are (1) define one or more new STIX

object types; (2) define additional properties for an existing STIX object type as a nested property extension to represent sub-components or modules; and (3) define additional properties for an existing STIX object type at the object's top level, representing properties that form an inherent part of the definition of an object type. When defining a new STIX object, all common properties associated with that type of object must be included in the schema or definition. In addition, extensions must follow all conformance requirements for that object type. Last but not least, the extension property must be included. TaxIdMA is a taxonomy framework for describing attacks related to identity and identity management. In order to combine both approaches, ways for integration and extension are discussed in this section. The extension should be called taxidma v2 with a corresponding ID and will be part of a repository with additional information.

8.1. Integration of TaxIdMA into STIX. By the usage of the SDOs attack pattern, campaign, course of action, grouping, identity, indicator, infrastructure, intrusion set, location, malware, malware analysis, note, observed data, opinion, report, threat actor, tool, and vulnerability, the threats are described. Most aspects of TaxIdMA can be incorporated without any problems due to the same or similar terminology. While TaxIdMA concentrates on attacks, the course of action describes countermeasures, which will be future work. With grouping, STIX objects can be shared. Infrastructure further describes the infrastructure of the attackers. The intrusion set groups the adversarial behaviors and resources with common properties. The location represents the geographical location of either attacker or target and so on. STIX uses attack lifecycles, which are part of TaxIdMA.

8.2. Extending STIX for TaxIdMA. Specific SDOs and SROs can be extended by the information specified with TaxIdMA.

8.2.1. Attack Pattern. STIX uses type and name (both required) as well as the optional external_reference, description, aliases, and kill_chain_phases as properties. In consequence, the attack pattern relates to malware, identity, location, vulnerability, and tool. A reverse relationship exists with indicator, course of action, campaign, intrusion set, malware, and threat actor. Regarding TaxIdMA, the kill chain phases can be reused, while TaxIdMA can be given as the external reference. The attack pattern of user identities could extend STIX with identity_pattern. In addition, attack_type should be given.

8.2.2. Campaign. STIX applies type, name (both required), description, aliases, first_seen, last_seen, and objective (all optional). Thereby, the campaign relates to the items intrusion set, threat actor, infrastructure, location, identity, vulnerability, attack pattern, malware, and tool. TaxIdMA uses several to all taxonomies to describe attacks. Thereby, a reference to the different attacks and attack patterns should be included.

8.2.3. Identity. STIX requires the properties type and name. In addition, description, roles, identity_class, and contact_information are optional properties. Identity is located at a location, whereas attack pattern, campaign, intrusion set, malware, threat actor, and tool target identities. Hence, a threat actor may impersonate an identity. Here, a reference to the user account with privileges is missing. The properties completeness, timeliness, directness, amount resp. a list of user accounts, and authenticity can be added.

8.2.4. Incident. Incident is currently a stub in STIX 2.1, i.e., it is included to support basic use cases but does not contain properties to represent metadata about incidents. Future versions should include these capabilities. Currently, type and name are required if used and description is optional. It could be utilized to combine aspects of the different taxonomies of TaxIdMA.

8.2.5. Indicator. The indicator in STIX contains a pattern that can be used to detect suspicious or malicious activities. Required properties are type, pattern, pattern_type, and valid_from. Optional properties are name, description, indicator_types, pattern_version, valid_until, and kill_chain_phases. The indicator indicates attack pattern, campaign, infrastructure, intrusion set, malware, threat actor, and tool and is based on observed data. The course of action investigates and mitigates indicators. The TaxIdMA attack_category could be used to further specify the indicator or extend the pattern.

8.2.6. Intrusion Set. The STIX intrusion set is a grouped set of adversarial behaviors and resources with common properties. It consists of the required properties type and name and the optional properties description, aliases, first_seen, last_seen, goals, resource_level, primary_motivation, and secondary_motivation. The intrusion set is attributed to threat actor, compromises/hosts/owns infrastructure, originates from a location, targets identity, location, and vulnerability, and uses attack pattern, infrastructure, malware, and tool. Regarding TaxIdMA, capabilities, impact, and results could be added.

8.2.7. STIX Cyber-Observable Objects. The cyber-observable objects describe observations such as artifacts, autonomous systems, directories, e-mail addresses, and more. Related to identities, social engineering and OSINT are important methods for the first steps within the attack lifecycle. In consequence, they are added with type, value, and description and are related to identity and location.

8.2.8. STIX Vocabulary. The account type in STIX can have the values facebook, ldap, nis, openid, radius, skype, tacacs, twitter, unix, windows-local, and windows-domain. Further social media accounts, Microsoft, Linux, IoT, mobile devices, etc. are missing and can be added when applying the STIX notation. Infrastructure uses phishing, but neither

other types of social engineering nor other devices such as IoT devices and user devices are currently included.

8.3. Adding Categories for TaxIdMA to STIX. In addition, further information systematically collected with TaxIdMA is added to STIX by introducing the following new categories.

8.3.1. Targeted Organization. In order to describe the targeted organization when sharing the threat information, type, name (both required), sector, domain, description, and size are applied.

8.3.2. Device. To specify the targeted device, type, name (both required), level, location, and device_category are included.

8.3.3. Identity Management Category. If identity management is the goal, a further category can be used. This category further specifies the cyber-observable object software. The properties type and name are required, whereas description, vendor, protocol, version, indicator, cpe, swid, languages, and kill_chain_phase are optional.

9. Discussion

During the design of TaxIdMA and its STIX extension, several iterations were made. These are partly described in the steps towards TaxIdMA. Both TaxIdMA and STIX were discussed with several experts in semi-structured interviews.

9.1. TaxIdMA. TaxIdMA should fulfill the stated requirements. While the previous version was mostly clear and unambiguous, the current version tries to combat these issues through the outlined changes, which are described in detail in the appendix. Although we discussed TaxIdMA with experts, more experts and real-world attacks could be included to evaluate TaxIdMA extensively. In order to adjust to SSI and IoT, applications of TaxIdMA were designed. Nonetheless, attacks and identity management progress, leading to new changes in the future.

9.2. STIX. By extending STIX with TaxIdMA, the systematic description of attacks can be used to share information about the threat with other entities. The extension of STIX was discussed with and improved by experts at the institution. To further evaluate STIX, expert interviews and the application of real-world attacks are necessary. Last but not least, the extension should be tested in an implementation.

9.3. Open Challenges. TaxIdMA and the extension of STIX provide a step towards the shift to identities. Further steps are needed. One object of STIX is the course of action, describing countermeasures. While TaxIdMA categorizes attacks, defense mechanisms are still missing. Although the taxonomy for SSI describes several attack vectors, it is not a detailed security analysis, which we plan in future work.

10. Conclusion and Outlook

Identities and thereby identity management are important elements of all IT services as everyone and everything has a digital identity for authentication. In consequence, they are essential for IT security. In order to systematically describe attacks and vulnerabilities related to identities and identity management systems, the taxonomy framework TaxIdMA in a revised version was proposed. TaxIdMA consists of four main taxonomies: attack background and the more specific attacks on service identities, end-user identities, and identity management systems. In the improved version, we incorporated input from experts and related work and included a naming convention. In order to improve the previous version, an application on IoT and SSI was introduced. Further adjustments help to clearly specify attacks while keeping the taxonomies as flexible as possible. By describing the iterations towards a taxonomy, future additions are made possible. TaxIdMA is evaluated based on statistics, the application of real-world examples, requirements, and expert interviews. TaxIdMA is accompanied by an extension for STIX to enable the sharing of threat intelligence related to identity management. Thereby, TaxIdMA and STIX work together to increase security. Last but not least, the new version of TaxIdMA is being discussed.

As identity management and attacks resp. threats progress, TaxIdMA will regularly be reevaluated. In future work, we plan to analyze more attacks and common problems and provide a tutorial to better explain TaxIdMA. This tutorial will be published together with STIX in a repository. As shown in the literature review, approaches focusing on the security of SSI are rare. In consequence, we want to analyze threat vectors of SSI in more detail and compare different architectures. Last but not least, defense mechanisms will be grouped in an additional taxonomy framework, which is then mapped to TaxIdMA.

Appendix

Changes to the Taxonomy

The changes target the following issues.

(i) *Attack Background*

(1) Attacker: The position within the attacker type is omitted for clarity as it partly overlapped with the target identity.
(2) Target: According to the literature, the sector is added to the background of the target, while the target type person is changed to individual to suit STIX terminology. The target type group is appended to comply with STIX. Class is though omitted as no benefit was seen.
(3) Identity: The identity type is changed to comply with typical user levels. In authenticity, temporary is removed as it is nonetheless an account.
(4) Attack: The attack type is changed to active and passive as although physical, active, passive,

offline, and social engineering are typical categories in various taxonomies, they can be combined. For example, a social engineering attack could use physical means. Therefore, the lowest common denominator is chosen. Active attacks though can be further specified. The impact notion is streamlined to fit into one word. In addition, vulnerability is introduced to further detail the background of the attack.

(ii) *Service Identities*. Name changed from system to service.

(1) Target: The location of the target is simplified by only differentiating between internal and external. Furthermore, the corresponding device of the target is added.
(2) Identity: The item until recovery in timeliness is changed to recoverable to reduce the number of words in this item. The word multiple in amount is modified to all, in order to clearly differentiate to selected.
(3) Attack: In both category and pattern, the item others is included. In addition, type is introduced to further specify the attack.

(iii) *Identity Management Systems*

(1) Target: The target locations' trusted third party and third party are combined as the difference between them is minimal. In addition, the user is changed to the user's device to further specify the location.
(2) Identity: The item until recovery in timeliness is modified to recoverable to reduce the number of words in this item. The word multiple in amount is alternated to all, in order to clearly differentiate to selected.
(3) Attack: In both category and pattern, the item others is included. In addition, type is introduced to further specify the attack.

(iv) *User Identities*

(1) Target: The target locations' trusted third party and third party are merged due to minimal differences. In addition, the user is transformed into the user device to further detail the location.
(2) Identity: The identity types are rearranged, for example, bank and credit card combined into financial and the missing eID and tax transitioned to state, which could include social security number in the U.S. In addition, the identity type e-mail is added.
(3) Attack: The attack type is adapted according to the attack background.

Data Availability

The expert interview data used to support the findings of this study have not been made available because of expert requests not to publish details for privacy reasons.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This article extends [15] as stated in the introduction. This work was partly funded by the Bavarian Ministry for Digital Affairs (project no. DISPUT/STMD-B3-4140-1-4). The authors alone are responsible for the content of the paper.

References

[1] Ponemon Institute, "Cybersecurity in the remote work era: a global risk report," Technical Report, Ponemon Institute, Traverse, MI, USA, 2020.
[2] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, "Why Older Adults (Don't) Use Password Managers," in *Proceedings of the 30th USENIX Security Symposium (USENIX Security)*, Berkeley, CA, USA, August 2021.
[3] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," in *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*, pp. 319–338, Berkeley, CA, USA, August 2019.
[4] P. Mayer, C. W. Munyendo, M. L. Mazurek, and A. J. Aviv, "Why Users (Don't) Use Password Managers at a Large Educational Institution," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security)*, pp. 1849–1866, Berkley, CA, USA, August 2022.
[5] Kaggle, "Common Password List (rockyou.txt)," 2021, https://www.kaggle.com/datasets/wjburns/common-password-list-rockyoutxt.
[6] OffSec Services, "John," 2022, https://www.kali.org/tools/john/.
[7] OffSec Services, "Brutespray," 2022, https://www.kali.org/tools/brutespray/.
[8] E. Stobert and R. Biddle, "The Password Life Cycle," *ACM Trans. Priv. Secur*, vol. 21, no. 3, pp. 1–32, 2018.
[9] S. Sahin and F. Li, "Don't Forget the Stuffing! Revisiting the Security Impact of Typo-Tolerant Password Authentication," in *Proceedings of the SIGSAC Conference On Computer And Communications Security (CCS)*, pp. 252–270, Association for Computing Machinery, New York, NY, USA, November 2021.
[10] J. Arquilla and M. Guzdial, "The SolarWinds Hack, and a Grand Challenge for CS Education," *Communications of the ACM*, vol. 64, no. 4, pp. 6-7, 2021.
[11] S. Peisert, B. Schneier, H. Okhravi et al., "Perspectives on the SolarWinds Incident," *IEEE Security & Privacy*, vol. 19, no. 2, pp. 7–13, 2021.
[12] L. Sterle and S. Bhunia, "On SolarWinds Orion Platform Security Breach," in *Proceedings of the SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, pp. 636–641, IEEE, New York, NY, USA, October 2021.
[13] L. Fritsch, "Identity management as a target in cyberwar," in *Proceedings of the Open Identity Summit (OIS)*, H. Roßnagel, C. H. Schunck, S. Mödersheim, and D. Hühnlein, Eds., GI, Bonn, Germany, pp. 61–70, April 2020.
[14] Purple Knights Security, "Purple Knight Report 2022 – facing the unknown: uncovering & addressing systemic

active directory security failures," Technical Report, Purple Knights Security, Hoboken, NJ, USA, 2022.

[15] D. Pöhn and W. Hommel, "TaxIdMA: Towards a Taxonomy for Attacks Related to Identities," in *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES)*, Association for Computing Machinery, New York, NY, USA, August 2022.

[16] OASIS Cyber Threat Intelligence Technical Committee, "Introduction to STIX," 2022, https://oasis-open.github.io/cti-documentation/stix/intro.html.

[17] A. Henricks and H. Kettani, "On Data Protection Using Multi-Factor Authentication," in *Proceedings of the 2019 International Conference on Information System and System Management ISSM 2019*, pp. 1–4, Association for Computing Machinery, New York, NY, USA, October 2020.

[18] S. Wiefling, P. R. Jørgensen, S. Thunem, and L. L. Iacono, "Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service," *ACM Trans. Priv. Secur*, vol. 26, no. 1, pp. 1–36, 2022.

[19] A. Hang, A. De Luca, E. von Zezschwitz, M. Demmler, and H. Hussmann, "Locked Your Phone? Buy a New One? From Tales of Fallback Authentication on Smartphones to Actual Concepts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pp. 295–305, Association for Computing Machinery, New York, NY, USA, August 2015.

[20] S. Motiee, K. Hawkey, and K. Beznosov, "Do Windows Users Follow the Principle of Least Privilege? Investigating User Account Control Practices," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, October 2010.

[21] V. Samar, "Unified Login with Pluggable Authentication Modules (PAM)," in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pp. 1–10, Association for Computing Machinery, New York, NY, USA, June 1996.

[22] M. A. Qadeer, M. Salim, and M. S. Akhtar, "Profile Management and Authentication Using LDAP," in *Proceedings of the International Conference on Computer Engineering and Technology (ICCET)*, pp. 247–251, IEEE, New York, NY, USA, January 2009.

[23] D. Lowe, *Managing Windows User Accounts*, Microsoft Corporation, Washington, DC, USA, 2020.

[24] A. Kostopoulos, E. Sfakianakis, I. Chochliouros et al., "Towards the Adoption of Secure Cloud Identity Services," in *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES)*, pp. 1–90, ACM, New York, NY, USA, August 2017.

[25] E. Maler and D. Reed, "The Venn of Identity: Options and Issues in Federated Identity Management," *IEEE Security and Privacy Magazine*, vol. 6, no. 2, pp. 16–23, 2008.

[26] N. Ragouzis, J. Hughes, R. Philpott, and E. Maler, "Security Assertion Markup Language (SAML) V2.0 Technical Overview," Technical report, OASIS, New York, NY, USA, 2008.

[27] D. Hardt, "The OAuth 2.0 authorization framework," 2012, http://www.rfc-editor.org/rfc/rfc6749.txt.

[28] N. Sakimura, J. Bradley, M. B. Jones, B. de Medeiros, and C. Mortimore, "OpenID Connect Core 1.0," Technical report, Open ID Foundation, San Ramon, CA, USA, 2014.

[29] D. Berbecaru, A. Lioy, and C. Cameroni, "Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure," *Information*, vol. 10, no. 6, p. 210, 2019.

[30] C. Mainka, V. Mladenov, J. Schwenk, and T. Wich. "SoK, "Single Sign-On Security — An Evaluation of OpenID Connect," in *Proceedings of the European Symposium on Security and Privacy (EuroS&P)*, pp. 251–266, IEEE, New York, NY, USA, August 2017.

[31] V. Mladenov and C. Mainka, "OpenID Connect Security Considerations," Technical report, Ruhr Universität Bochum, Bochum, Germany, 2017.

[32] D. Fett, R. Küsters, and G. Schmitz, "A Comprehensive Formal Security Analysis of OAuth 2.0," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1204–1215, Association for Computing Machinery, New York, NY, USA, October 2016.

[33] T. Lodderstedt, J. Bradley, A. Labunets, and D. Fett, "OAuth 2.0 Security Best Current Practice," 2020, http://www.ietf.org/internet-drafts/draft-ietf-oauth-security-topics-16.txt.

[34] T. Lodderstedt, M. McGloin, and P. Hunt, *OAuth 2.0 Threat Model and Security Considerations*, RFC Editor, Marina del Rey, CA, USA, 2013.

[35] F. Hirsch, R. Philpott, and E. Maler, "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0," Technical Report, OASIS, New York, NY, USA, 2005.

[36] E. Maler, M. Machulak, and J. Richer, *User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization*, Kantara Specification, Herndon, VA, USA, 2018.

[37] E. Maler, M. Machulak, and J. Richer, *Federated Authorization for User-Managed Access (UMA 2.0)*, Kantara Specification, Herndon, VA, USA, 2017.

[38] M. P. Machulak, E. L. Maler, D. Catalano, and A. van. Moorsel, "User-Managed Access to Web Resources," in *Proceedings of the 6th Workshop on Digital Identity Management (DIM)*, pp. 35–44, Association for Computing Machinery, New York, NY, USA, August 2010.

[39] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019.

[40] K. C. Toth and A. Anderson-Priddy, "Self-Sovereign Digital Identity: A Paradigm Shift for Identity," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 17–27, 2019.

[41] N. Naik, P. Grace, and P. Jenkins, "An Attack Tree Based Risk Analysis Method for Investigating Attacks and Facilitating Their Mitigations in Self-Sovereign Identity," in *Proceedings of the Symposium Series on Computational Intelligence (SSCI)*, pp. 1–8, IEEE, New York, NY, USA, December 2021.

[42] H. L'Amrani, B. E. Berroukech, Y. El Bouzekri Idrissi, and R. Ajhoun, "Identity management systems: Laws of identity for models evaluation," in *Proceedings of the 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, pp. 736–740, IEEE, New York, NY, USA, October 2016.

[43] B. Martin, "Common Vulnerabilities Enumeration (CVE), Common Weakness Enumeration (CWE), and Common Quality Enumeration (CQE): Attempting to Systematically Catalog the Safety and Security Challenges for Modern, Networked, Software-Intensive Systems," *Ada Lett*, vol. 38, no. 2, pp. 9–42, 2019.

[44] MITRE Corporation, "CWE – Common Weakness Enumeration," 2022, https://cwe.mitre.org.

[45] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT&CK: Design and Philosophy," Report, The MITRE Corporation, McLean, VI, USA, 2020.

[46] S. Cho, I. Han, and H. Jeong, "Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture," in *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, pp. 1–8, IEEE, New York, NY, USA, January 2018.

[47] MITRE Corporation, "CAPEC – Common Attack Pattern Enumeration and Classification," 2022, https://capec.mitre.org.

[48] OWASP, "Projects," 2022, https://owasp.org/projects/.

[49] V. M. Igure and R. D. Williams, "Taxonomies of Attacks and Vulnerabilities in Computer Systems," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 1, pp. 6–19, 2008.

[50] I. M. Chapman, S. P. Leblanc, and A. Partington, "Taxonomy of Cyber Attacks and Simulation of Their Effects," in *Proceedings of the Military Modeling & Simulation Symposium (MMS)*, pp. 73–80, Society for Computer Simulation International, San Diego, CA, USA, August 2011.

[51] R. Derbyshire, B. Green, D. Prince, A. Mauthe, and D. Hutchison, "An Analysis of Cyber Security Attack Taxonomies," in *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 153–161, New York, NY, USA, June 2018.

[52] M. J. Haber and D. Rolls, *Identity Attack Vectors*, Apress, New York, NY, USA, 2020.

[53] U. Habiba, R. Masood, M. A. Shibli, and M. A. Niazi, "Cloud identity management security issues & solutions: a taxonomy," *Complex Adaptive Systems Modeling*, vol. 2, no. 1, p. 5, 2014.

[54] D. Klaper and E. Hovy, "A Taxonomy and a Knowledge Portal for Cybersecurity," in *Proceedings of the 15th Annual International Conference on Digital Government Research (DG-O)*, pp. 79–85, ACM, New York, NY, USA, March 2014.

[55] E. W. Burger, M. D. Goodman, P. Kampanakis, J. Squillace, and M. Bantan, "Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies," in *Proceedings of the Workshop on Information Sharing & Collaborative Security (WISCS)*, pp. 51–60, ACM, New York, NY, USA, August 2014.

[56] A. Husseis, J. Liu-Jimenez, I. Goicoechea-Telleria, and R. Sanchez-Reillo, "A Survey in Presentation Attack and Presentation Attack Detection," in *Proceedings of the International Carnahan Conference on Security Technology (ICCST)*, pp. 1–13, IEEE, New York, NY, USA, December 2019.

[57] M. Mamchenko and A. Sabanov, "Exploring the Taxonomy of USB-Based Attacks," in *Proceedings of the 12th International Conference Management of Large-Scale System Development (MLSD)*, pp. 1–4, IEEE, New York, NY, USA, January 2019.

[58] M. Hollick, C. Nita-Rotaru, P. Papadimitratos, A. Perrig, and S. Schmid, "Toward a Taxonomy and Attacker Model for Secure Routing Protocols," *SIGCOMM Comput. Commun. Rev.*vol. 47, no. 1, pp. 43–48, 2017.

[59] S. Chaipa, E. K. Ngassam, and S. Singh, "Towards a New Taxonomy of Insider Threats," in *Proceedings of the IST-Africa Conference (IST-Africa)*, pp. 1–10, IEEE, New York, NY, USA, June 2022.

[60] B. Alsamani and H. Lahza, "A taxonomy of IoT: Security and privacy threats," in *Proceedings of the International Conference on Information and Computer Technologies (ICICT)*, pp. 72–77, IEEE, New York, NY, USA, August 2018.

[61] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in *Proceedings of the 3rd International Conference on Electronic Design (ICED)*, pp. 321–326, IEEE, New York, NY, USA, May 2016.

[62] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020.

[63] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[64] L. Wüstrich, M.-O. Pahl, and S. Liebald, "Towards an Extensible IoT Security Taxonomy," in *Proceedings of the IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–6, IEEE, New York, NY, USA, February 2020.

[65] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, pp. 163–168, IEEE, New York, NY, USA, October 2018.

[66] S. Shasha, M. Mahmoud, M. Mannan, and A. Youssef, "Playing With Danger: A Taxonomy and Evaluation of Threats to Smart Toys," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2986–3002, 2019.

[67] P. Williams, P. Rojas, and M. Bayoumi, "Security Taxonomy in IoT – A Survey," in *Proceedings of the 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 560–565, IEEE, New York, NY, USA, July 2019.

[68] J. Squillace and M. Bantan, "A Taxonomy of Privacy, Trust, and Security Breach Incidents of Internet-of-Things Linked to F(M).A.A.N.G. Corporations," in *Proceedings of the World AI IoT Congress (AIIoT)*, pp. 591–596, IEEE, New York, NY, USA, August 2022.

[69] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K. K. R. Choo, "Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 199–221, 2022.

[70] A. Taivalsaari and T. Mikkonen, "A Taxonomy of IoT Client Architectures," *IEEE Software*, vol. 35, no. 3, pp. 83–88, 2018.

[71] R. B. Auliar and G. Bekaroo, "Security in IoT-based Smart Homes: A Taxonomy Study of Detection Methods of Mirai Malware and Countermeasures," in *Proceedings of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1–6, IEEE, New York, NY, USA, January 2021.

[72] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Taxonomy of authentication techniques in Internet of Things (IoT)," in *Proceedings of the 15th Student Conference on Research and Development (SCOReD)*, pp. 67–71, IEEE, New York, NY, USA, August 2017.

[73] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," *IEEE Access*, vol. 8, pp. 88892–88932, 2020.

[74] H. Boujezza, M. Al-Mufti, H. K. Ben Ayed, and L. Saidane, "A taxonomy of identities management systems in IOT," in *Proceedings of the IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1–8, IEEE, New York, NY, USA, November 2015.

[75] A. N. Bikos and S. A. P. Kumar, "Securing Digital Ledger Technologies-Enabled IoT Devices: Taxonomy, Challenges, and Solutions," *IEEE Access*, vol. 10, pp. 46238–46254, 2022.

[76] C. Berger, P. Eichhammer, H. P. Reiser, J. Domaschka, F. J. Hauck, and G. Habiger, "A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms," *ACM Computing Surveys*, vol. 54, no. 7, pp. 1–39, September 2021.

[77] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the internet of medical things: Taxonomy and risk assessment," in *Proceedings of the 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 112–120, IEEE, New York, NY, USA, December 2017.

[78] D. Redding, A. Jian, and S. Bhunia, "A Case Study of Massive API Scrapping: Parler Data Breach After the Capitol Riot," in *Proceedings of the 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–7, IEEE, New York, NY, USA, January 2022.

[79] B. Gibson, T. Spencer, D. Lewis, and S. Bhunia, "Vulnerability in massive api scraping: 2021 linkedin data breach," in *Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 777–782, IEEE, New York, NY, USA, January 2021.

[80] J. Qian, Z. Gan, J. Zhang, and S. Bhunia, "Analyzing SocialArks Data Leak - A Brute Force Web Login Attack," in *Proceedings of the 4th International Conference on Computer Communication and the Internet (ICCCI)*, pp. 21–27, IEEE, New York, NY, USA, December 2022.

[81] H. Nguyen Ba Minh, J. Bennett, M. Gallagher, and S. Bhunia, "A Case Study of Credential Stuffing Attack: Canva Data Breach," in *Proceedings of the International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 735–740, IEEE, New York, NY, USA, November 2021.

[82] L. Rizkallah, N. Potter, K. Reed, D. Reynolds, M. Salman, and S. Bhunia, "Red Toad, Blue Toad, Hacked Toad?" in *Proceedings of the World AI IoT Congress (AIIoT)*, pp. 379–386, IEEE, New York, NY, USA, December 2022.

[83] A. Pitney, S. Penrod, M. Foraker, and S. Bhunia, "A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities," in *Proceedings of the 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, IEEE, New York, NY, USA, August 2022.

[84] J. Nadjar, Y. Liu, J. Salinas, and S. Bhunia, "A Case Study on the Multi-Vector Data Breach on Astoria," in *Proceedings of the 4th International Conference on Computer Communication and the Internet (ICCCI)*, pp. 51–57, IEEE, New York, NY, USA, November 2022.

[85] C. Faircloth, G. Hartzell, N. Callahan, and S. Bhunia, "A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft," in *Proceedings of the World AI IoT Congress (AIIoT)*, pp. 501–507, IEEE, New York, NY, USA, August 2022.

[86] C. D. Motero, J. R. B. Higuera, J. B. Higuera, J. A. S. Montalvo, and N. G. Gomez, "On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey," *IEEE Access*, vol. 9, pp. 109289–109319, 2021.

[87] N. Anita and M. Vijayalakshmi, "Blockchain Security Attack: A Brief Survey," in *Proceedings of the 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, IEEE, New York, NY, USA, January 2019.

[88] M. Saad, J. Spaulding, L. Njilla et al., "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[89] O. B. Al-Khurafi and M. A. Al-Ahmad, "Survey of Web Application Vulnerability Attacks," in *Proceedings of the 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pp. 154–158, IEEE, New York, NY, USA, October 2015.

[90] V. Gaikwad and L. Ragha, "Mitigation of attack on authenticating identities in ad-hoc network," in *Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 1027–1032, IEEE, New York, NY, USA, November 2017.

[91] T. Sharma and L. Singh, "A detection technique for identity based attacks in clustered mobile ad-hoc networks," in *Proceedings of the International Conference on Advances in Computer Engineering and Applications (ICACEA)*, pp. 893–898, IEEE, New York, NY, USA, November 2015.

[92] L. Bahri, "Identity Related Threats, Vulnerabilities and Risk Mitigation in Online Social Networks: A Tutorial," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 2603–2605, Association for Computing Machinery, New York, NY, USA, December 2017.

[93] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *Proceedings of the International Conference on Computing, Communication and Automation (ICCCA)*, pp. 537–540, IEEE, New York, NY, USA, February 2016.

[94] S. Qin, M. C. Silaghi, T. Matsui, M. Yokoo, and K. Hirayama, "Addressing False Identity Attacks in Action-Based P2P Social Networks with an Open Census," in *Proceedings of the IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, pp. 50–57, IEEE Computer Society, New York, NY, USA, March 2013.

[95] I. Karunanayake, N. Ahmed, R. Malaney, R. Islam, and S. K. Jha, "De-Anonymisation Attacks on Tor: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2324–2350, 2021.

[96] E. Erdin, C. Zachor, and M. H. Gunes, "How to Find Hidden Users: A Survey of Attacks on Anonymity Networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2296–2316, 2015.

[97] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on Threats and Attacks on Mobile Networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[98] J. M. Briones, M. A. Coronel, and P. Chavez-Burbano, "Case of study: Identity theft in a university WLAN Evil twin and cloned authentication web interface," in *Proceedings of the World Congress on Computer and Information Technology (WCCIT)*, pp. 1–4, IEEE, New York, NY, USA, January 2013.

[99] Y. Mei, W. Han, S. Li, and X. Wu, "A Survey of Advanced Persistent Threats Attack and Defense," in *Proceedings of the 6th International Conference on Data Science in Cyberspace (DSC)*, pp. 608–613, IEEE, New York, NY, USA, February 2021.

[100] R. Barona and E. A. Mary Anita, "A survey on data breach challenges in cloud computing security: issues and threats," in *Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, pp. 1–8, IEEE, New York, NY, USA, 2017.

[101] Y. Fang, Y. Guo, C. Huang, and L. Liu, "Analyzing and Identifying Data Breaches in Underground Forums," *IEEE Access*, vol. 7, pp. 48770–48777, 2019.

[102] R. R. Subramanian, R. Avula, P. S. Surya, and B. Pranay, "Modeling and predicting cyber hacking breaches," in *Proceedings of the 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 288–293, IEEE, New York, NY, USA, December 2021.

[103] F. Aiolli, M. Conti, A. Gangwal, and M. Polato, "Mind Your Wallet's Privacy: Identifying Bitcoin Wallet Apps and User's Actions through Network Traffic Analysis," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (SAC)*, pp. 1484–1491, Association for Computing Machinery, New York, NY, USA, January 2019.

[104] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, "Pushing the limits of cyber threat intelligence: Extending stix to support complex patterns," in *Information Technology: New Generations*, S. Latifi, Ed., pp. 213–225, Springer International Publishing, Cham, Switzerland, 2016.

[105] M. Vielberth, F. Menges, and G. Pernul, "Human-as-a-security-sensor for harvesting threat intelligence," *Cybersecurity*, vol. 2, no. 1, p. 23, 2019.

[106] OASIS Cyber Threat Intelligence TC, *TAXII Version 2.1"*, OASIS, New York, NY, USA, 2021.

[107] FireEye, "OpenIOC 1.1 DRAFT – README," 2020, https://github.com/fireeye/OpenIOC_1.1.

[108] SECEF, "IODEF Introduction," 2022, https://www.secef.net/secef/iodef/iodef-introduction/.

[109] J. Meijer, R. Danyliw, and Y. Demchenko, "The Incident Object Description Exchange Format," 2007, https://www.rfc-editor.org/info/rfc5070.

[110] B. Trammell, "Expert Review for Incident Object Description Exchange Format (IODEF) Extensions in IANA XML Registry," 2012, https://www.rfc-editor.org/info/rfc6685.

[111] T. Takahashi, K. Landfield, and Y. Kadobayashi, "An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information". RFC 7203," 2014, https://www.rfc-editor.org/info/rfc7203.

[112] R. Stillions, "The DML model," 2014, https://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html.

[113] S. Bromander, A. Jøsang, and M. Eian, "Semantic Cyberthreat Modelling," in *Proceedings of the Semantic Technology for Intelligence, Defense, and Security (STIDS)*, pp. 74–78, CEUR Workshop, Aachen, Germany, January 2016.

[114] M. Pahlevan, A. Voulkidis, and T.-H. Velivassaki, "Secure Exchange of Cyber Threat Intelligence Using TAXII and Distributed Ledger Technologies - Application for Electrical Power and Energy System," in *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES)*, Association for Computing Machinery, New York, NY, USA, November 2021.

[115] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," in *Proceedings of the European Intelligence and Security Informatics Conference (EISIC)*, pp. 91–98, IEEE, New York, NY, USA, October 2017.

[116] A. Zibak and A. Simpson, "Cyber Threat Information Sharing: Perceived Benefits and Barriers," in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES)*, Association for Computing Machinery, New York, NY, USA, January 2019.

[117] B. Stojkovski, G. Lenzini, V. Koenig, and S. Rivas, "What's in a Cyber Threat Intelligence Sharing Platform? A Mixed-Methods User Experience Investigation of MISP," in *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pp. 385–398, Association for Computing Machinery, New York, NY, USA, December 2021.

[118] S. Bromander, M. Swimmer, L. P. Muller et al., "Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange," *Digital Threats*, vol. 3, no. 1, pp. 1–22, 2021.

[119] V. Mavroeidis, H. Ryan, T. Casey, and A. Jesang, "Threat Actor Type Inference and Characterization within Cyber Threat Intelligence," in *Proceedings of the 13th International Conference on Cyber Conflict (CyCon)*, pp. 327–352, IEEE, New York, NY, USA, May 2021.

[120] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform," in *Proceedings of the Workshop on Information Sharing and Collaborative Security (WISCS)*, pp. 49–56, Association for Computing Machinery, New York, NY, USA, February 2016.

[121] OpenCTI Platform, "OpenCTI," 2022, https://github.com/OpenCTI-Platform/opencti.

[122] N. Adouani, T. Franco, and J. Leonard, "TheHive," 2022, https://github.com/TheHive-Project/TheHive.

[123] S. Wendzel, L. Caviglione, and W. Mazurczyk, "Avoiding research tribal wars using taxonomies," *IEEE Computer*, vol. 56, no. 1, 2023.

[124] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi, "A taxonomy of computer program security flaws," *ACM Computing Surveys*, vol. 26, no. 3, pp. 211–254, 1994.

[125] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pp. 154–163, New York, NY, USA, November 1997.

[126] M. J. M. Al-Saadi and M. Ilyas, "Identity Management Approach in Internet of Things (IoT)," in *Proceedings of the 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 1–6, IEEE, New York, NY, USA, December 2020.

[127] B. Zhao, P. Zhao, and P. Fan, "ePUF: A lightweight double identity verification in IoT," *Tsinghua Science and Technology*, vol. 25, no. 5, pp. 625–635, 2020.

[128] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, and Z. Cui, "Distributed, Secure, Self-Sovereign Identity for IoT Devices," in *Proceedings of the 6th World Forum on Internet of Things (WF-IoT)*, pp. 1–6, IEEE, New York, NY, USA, December 2020.

[129] H. Ning, Z. Zhen, F. Shi, and M. Daneshmand, "A Survey of Identity Modeling and Identity Addressing in Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4697–4710, 2020.

[130] B. B. Gupta, A. Gaurav, K. T. Chui, and C.-H. Hsu, "Identity-Based Authentication Technique for IoT Devices," in *Proceedings of the International Conference on Consumer Electronics (ICCE)*, vol. 4, p. 1, IEEE, New York, NY, USA, May 2022.

[131] S. Lips, N. Vinogradova, R. Krimmer, and D. Draheim, "Re-Shaping the EU Digital Identity Framework," in *Proceedings of the 23rd Annual International Conference on Digital Government Research (dg.O)*, pp. 13–21, Association for Computing Machinery, New York, NY, USA, August 2022.

[132] A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, and S. Ranise. "SoK, "A Survey on Technological Trends for (Pre)Notified EIDAS Electronic Identity Schemes," in *Proceedings of the*

17th International Conference on Availability, Reliability and Security (ARES), Association for Computing Machinery, New York, NY, USA, December 2022.

[133] Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović, and M. Turkanović, "Towards the Classification of Self-Sovereign Identity Properties," *IEEE Access*, vol. 10, pp. 88306–88329, 2022.

[134] S. Chng, H. Y. Lu, A. Kumar, and D. Yau, "Hacker types, motivations and strategies: A comprehensive framework," *Computers in Human Behavior Reports*, vol. 5, Article ID 100167, 2022.

[135] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security*, vol. 24, no. 1, pp. 31–43, 2005.

[136] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: A Cyber Attack Taxonomy," in *Proceedings of the 9th Annual Symposium on Information Assurance (ASIA)*, pp. 2–12, New York, NY, USA, June 2014.

[137] R. Heartfield and G. Loukas, "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks," *ACM Computing Surveys*, vol. 48, no. 3, pp. 1–39, 2015.

[138] Federal Office for Information Security, *IT-Grundschutz-Compendium*, Bonn, Germany, 2021.

[139] MITRE, "Steal or Forge Kerberos Tickets," 2022, https://attack.mitre.org/techniques/T1558/.

[140] Microsoft, "Microsoft Security Bulletin MS17-010-Critical," 2022, https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

[141] Microsoft, "Microsoft Security Bulletin MS16-032-Important," 2022, https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-032.

[142] MITRE, "Steal or Forge Kerberos Tickets," 2022, https://attack.mitre.org/techniques/T1550/002/.

[143] MITRE, "Steal or Forge Kerberos Tickets: Kerberoasting," 2022, https://attack.mitre.org/techniques/T1558/003/.

[144] K. I. Ahmed, M. Tahir, and S. L. Lau, "Trust Management for IoT Security: Taxonomy and Future Research Directions," in *Proceedings of the Conference on Application, Information and Network Security (AINS)*, pp. 26–31, IEEE, New York, NY, USA, December 2020.

[145] N. Naik and P. Jenkins, "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology," in *Proceedings of the 8th International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pp. 90–95, IEEE, New York, NY, USA, November 2020.

[146] X. Chen, Z. Wei, X. Jia, P. Zheng, M. Han, and X. Yang, "Current Status and Prospects of Blockchain Security Standardization," in *Proceedings of the 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 24–29, IEEE, New York, NY, USA, January 2022.

[147] P. R. Nair and D. R Dorai, "Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pp. 279–283, IEEE, New York, NY, USA, May 2021.

[148] S. Sharma and K. Shah, "Exploring Security Threats on Blockchain Technology along with possible Remedies," in *Proceedings of the 7th International conference for Convergence in Technology (I2CT)*, pp. 1–4, IEEE, New York, NY, USA, February 2022.

[149] B. Putz and G. Pernul, "Detecting Blockchain Security Threats," in *Proceedings of the International Conference on Blockchain (Blockchain)*, pp. 313–320, IEEE, New York, NY, USA, April 2020.

[150] T. Ameen, S. Sankagiri, and B. Hajek, "Blockchain Security When Messages Are Lost," in *Proceedings of the Workshop on Developments in Consensus (ConsensusDay)*, pp. 1–14, Association for Computing Machinery, New York, NY, USA, December 2022.

[151] A. Lewis-Pye and T. Roughgarden, "How Does Blockchain Security Dictate Blockchain Implementation?" in *Proceedings of the SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 1006–1019, Association for Computing Machinery, New York, NY, USA, October 2021.

[152] G. Karame, "On the Security and Scalability of Bitcoin's Blockchain," in *Proceedings of the SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 1861-1862, Association for Computing Machinery, New York, NY, USA, November 2016.

[153] N. Amiet, "Blockchain Vulnerabilities in Practice," *Digital Threats*, vol. 2, no. 2, pp. 1–7, 2021.

[154] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp. 1–34, July 2019.

[155] A. Davenport and S. Shetty, "Modeling Threat of Leaking Private Keys from Air-Gapped Blockchain Wallets," in *Proceedings of the International Smart Cities Conference (ISC2)*, pp. 9–13, IEEE, New York, NY, USA, January 2019.

[156] M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets," in *Proceedings of the International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1308–1316, IEEE, New York, NY, USA, May 2018.

[157] Y. Hu, S. Wang, G.-H. Tu et al., "Security Threats from Bitcoin Wallet Smartphone Applications: Vulnerabilities, Attacks, and Countermeasures," in *Proceedings of the 11th Conference on Data and Application Security and Privacy (CODASPY)*, pp. 89–100, Association for Computing Machinery, New York, NY, USA, September 2021.

[158] Symantec, "Internet Security Threat Report," Technical report, Symantec, Tempe, AR, USA, 2019.

[159] ENISA, "ENISA Threat Landscape," Technical report, ENISA, Athens, Greece, 2022.

[160] Federal Trade Commission, "Consumer Sentinel Network Data Book 2021," Technical report, Federal Trade Commission, Washington, DC, USA, 2022.

[161] EY, "Is cybersecurity about more than protection? – EY Global Information Security Survey 2018-19," Technical report, EY, Washington, DC, USA, 2018.
[162] ENISA, "Identity Theft - ENISA Threat Landscape," Technical report, ENISA, Athens, Greece, 2020.
[163] ENISA, "Data Breach - ENISA Threat Landscape," Technical report, ENISA, Athens, Greece, 2020.
[164] OWASP Top Ten, 2022,https://owasp.org/www-project-top-ten/.
[165] IIoT World, "An Overview of the IoT Security Market Report 2017-2022," 2022, https://iiot-world.com/reports/an-overview-of-the-iot-security-market-report-2017-2022/.
[166] Curated Intel, "Initial-Access-Broker-Landscape," 2021, https://github.com/curated-intel/Initial-Access-Broker-Landscape.
[167] Identity Defined Security Alliance, "2022 Trends in Securing Digital Identities," Technical report, IDSA, New Delhi, India, 2022.