TaxIdMA: Towards a Taxonomy for Attacks related to Identities

Daniela Pöhn

Wolfgang Hommel daniela.poehn@unibw.de wolfgang.hommel@unibw.de Universität der Bundeswehr München, RI CODE Munich, Germany

ABSTRACT

Identity management refers to the technology and policies for the identification, authentication, and authorization of users in computer networks. Identity management is therefore fundamental to today's IT ecosystem. At the same time, identity management systems, where digital identities are managed, pose an attractive target for attacks. With the heterogeneity of identity management systems, every type (i. e., models, protocols, implementations) has different requirements, typical problems, and hence attack vectors. In order to provide a systematic and categorized overview, the framework Taxonomy for Identity Management Attacks (TaxIdMA) for attacks related to identities is proposed. The purpose of this framework is to classify existing attacks associated with system identities, identity management systems, and end-user identities as well as the background using an extensible structure from a scientific perspective. The taxonomy is then evaluated with eight real-world attacks resp. vulnerabilities. This analysis shows the capability of the proposed taxonomy framework TaxIdMA in describing and categorizing these attacks.

CCS CONCEPTS

• Security and privacy \rightarrow Security services.

KEYWORDS

identity, identity management, taxonomy, categorization, attack, vulnerability

ACM Reference Format:

Daniela Pöhn and Wolfgang Hommel. 2022. TaxIdMA: Towards a Taxonomy for Attacks related to Identities. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3538969. 3544430

1 INTRODUCTION

In order to provide access to several different services, organizations operate identity management systems (IdMS). These systems manage users with their digital identities, associated user information, i. e., attributes, authentication methods, and permissions. One often used IdMS is Microsoft Active Directory (AD), which does not only manage users but also devices. These systems typically come with other mature technologies including single sign-on and role-based access control. Attacks targeting identities often focus on IdMS as the central source of truth [12]. However, security among other things relies on the correct setup and configuration. According to the Purple Knight Report 2022 [25], organizations scored an average of 68% across five AD security categories, while large organizations achieved an even lower rating. This shows that organizations are challenged by securing AD, especially in larger environments. As industries move forward with outsourcing, the reliance on the correct implementation of processes and human factors becomes more problematic.

In addition, users can enable as well as be the target of attacks. For example, users tend to reuse or create simple passwords [27]. Consequently, different brute-force attacks such as credential stuffing are possible, resulting in account takeover and, thereby, the loss of personal data. Last but not least, identities are used in every system, e. g., to run a web service. These identities are misused by attackers during the attack life cycle [28]. This demonstrates that identities are an important part of IT and, thereby, IT security. In this context, taxonomies provide an overview of the systems and different possibilities. Such a systematic approach helps to identify gaps, improve the current situation, and provide a guideline for establishing new security measures.

The contribution of the paper focuses on Taxonomy for Identity Management Attacks (TaxIdMA), which is a novel taxonomy framework for attacks related to identities. The following taxonomies are proposed: i) attack background, ii) attacks involving system identities, iii) attacks on IdMS, and iv) attacks on end-user identities. The taxonomy on the attack background describes the general setting of an account. The other taxonomies detail attacks and can be combined to categorize the different steps within an attack life cycle. Thereby, the taxonomies classify various attacks in greater detail than existing generic taxonomies. This can help to, e. g., improve the security of identities and systems, analyze incidents, and design new approaches. TaxIdMA is then evaluated based on eight real-world examples.

The remainder of the paper is as follows: Section 2 discusses existing taxonomies and categorizations. Section 3 describes the proposed taxonomies of TaxIdMA. Section 4 evaluates the proposed taxonomies by applying real-world examples. Based on the evaluation, Section 5 discusses the benefits and limits of the taxonomies. Last but not least, Section 6 concludes the paper and gives an outlook on future work.

ARES 2022, August 23-26, 2022, Vienna, Austria

^{© 2022} Copyright held by the owner/author(s). Publication rights licensed to ACM. This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria, https://doi.org/10.1145/3538969.3544430.*

2 RELATED WORK

Different criteria and taxonomies group incidents involving identities. Common Weakness Enumeration (CWE) by MITRE [22] is a community-developed list of software and hardware weaknesses. This list serves as a common language for weakness identification, mitigation, and prevention efforts. The research concept of improper access control includes, e.g., different types of improper access controls ranging from Hypertext Transfer Protocol (HTTP) cookies to on-chip hardware issues. Other categories also contain weaknesses related to identity management. Common Attack Pattern Enumerations and Classifications (CAPEC) [21] relates to CWE and Common Vulnerabilities and Exposures (CVE). Here, attack patterns are based on software design patterns. Subvert of access control includes, e.g., authentication abuse and bypass as well as physical theft, without including all issues related to it. Further categorizations have a section about identity management without going into details. Open Web Application Security Project (OWASP) [24] publishes top 10 lists and cheat sheets for typical problems.

Igure and Williams [17] analyze taxonomies published from 1974 until 2006 resulting in a taxonomy of attacks and vulnerabilities in computer systems. Even though the authors include numerous approaches, the proposed taxonomy is generic as it is not focused on a specific security area. Chapman et al. [3] propose a 3-tier taxonomy to describe the effects of cyber attacks, ranging from no access to user access to root access requirements. The authors thereby characterize the different levels of permissions an attacker gained. Nevertheless, it is unclear whether service users like www-data are included in user access or nowhere. Derbyshire et al. [8] evaluate different taxonomies based on a criteria set and real-world attacks. CAPEC outperforms the other taxonomies, though the different versions and criteria might be challenging. Furthermore, the authors notice that several taxonomies do not include human elements. Cho et al. [5] explore cyber kill chain models resulting in a new model to evaluate cyber situation awareness. Other taxonomies have a specific focus. Habiba et al. [13] propose a taxonomy for security issues related to cloud IdMS. Klaper and Hovy [18] create a basic taxonomy with cybersecurity topics linked to relevant educational or research material. Burger et al. [2] suggest a cyber threat intelligence information exchange taxonomy. Husseis et al. [16] provide a review of potential threats affecting biometric systems. Williams et al. [30] classify security features in Internet of Things (IoT) devices.

As a result, a holistic taxonomy for attacks related to identities is still missing.

3 TAXIDMA

In this section, the framework TaxIdMA with its taxonomies is described. A taxonomy organizes its concepts hierarchically by following these ideal properties [19, 20]: i) mutually exclusive categorization, i. e., no overlapping, ii) clear and unambiguous classification criteria, and iii) comprehensible, useful, and compliant with established terminology. TaxIdMA was generated through a regression manner – abstraction of knowledge from existing taxonomies, other related approaches, and known attacks. During the design, attention was paid to the complete coverage of all necessary factors

of the attacks. The goal of TaxIdMA is to categorize all steps of an attack related to identities.

TaxIdMA consists of the taxonomies attack background, system identities, identity management systems, and end-user identities. It uses the definitions summarized in Appendix A.1. The taxonomy on attack background, described in Section 3.1, can be used for all attacks involving identities as it outlines the background of the attack. The background is constant during the attack cycle, which can involve several identities. Categories with unmodified values are grouped there; categories, where the values may vary either depending on the attack type or during the attack cycle are listed in the following taxonomies. The taxonomies on system identities, identity management systems, and end-user identities further detail the attack. During the attack cycle, the attacker typically reuses system identities. This circumstance is described in the related taxonomy, see Section 3.2. If multiple system identities are utilized, the taxonomy can be applied several times. One major goal of attacks are IdMSs, as all accounts are managed there. Hence, it is described in another taxonomy. With the outsourcing of services including IdMS, several entities may be involved. A categorization of the steps towards an attack is shown in the according taxonomy in Section 3.3. Last but not least, another kind of attack targets enduser identities, either in rather selected attacks, like spear-phishing, or in massive attacks, e.g. broader-scale phishing. As they focus on end-users and not organizations, another taxonomy is established in Section 3.4.

Considering that an attacker may exploit various identities, several up to all taxonomies can be applied in a stepwise way. For example, a spear-phishing attack targets an employee with the help of an identity leak for a service the employee uses, dropping malware, which then gives access to a system identity with the ultimate goal of the IdMS. In this example, all taxonomies are utilized to systematically describe the attack, either from the start to the end or vise versa.

3.1 Attack Background

The attack background taxonomy, shown in Figure 1, is categorized by the attacker, target, attack identity, and the attack itself. It describes the background of the attack, detailed by the different attack taxonomies in the following sections.

Attacker: Someone who explores methods for breaching weaknesses in a computer system or network. The attacker is detailed by type and capabilities [4].

- *Type*: The type of attacker describes the position (i. e., internal or external), the number of involved persons (amount), and their profiles (single or groups such as cybercriminals or state-sponsored hackers).
- Capabilities: Expertise or ability of the attacker to reach the goal. The capabilities are characterized by motivation, resources, knowledge, and time. Determined by the capabilities, the severity of the attack varies.

Target: A goal designated for an attack. The target is described by identity, type, and sector [14, 26].

• *Type:* Attacks focus on different targets, ranging from single persons, businesses, governments, and organizations to other types. These can be grouped into sectors.

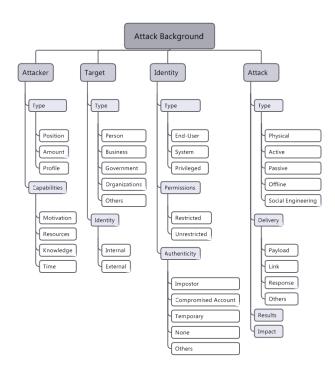


Figure 1: Taxonomy for attack background

• *Identity:* The identity describes the position of the target related to the attacker and can be further detailed by their roles. The identity of the target is either internal or external. Internal can be characterized by the various types of identities, which have different permissions. As an example, executive, employee, administrator, and contractor are named. External contains partner, customer, trusted third party, and stranger.

Identity: Digital identity used during the attack with permissions [3] and authenticity.

- *Type:* Type of digital identity, i. e., end-user, system, and privileged [5]. In the beginning, the attacker typically has no identity.
- *Permissions*: Permissions (authorization) the overtaken identity and, therefore, the attacker has at the described moment. Identities come with permissions according to roles and functions, ranging from restricted to unrestricted [3].
- *Authenticity*: The authenticity of the attacker towards the system during the attack. The type of identity has one of the following authenticities: impostor (e.g., during phishing attacks), the authenticity of the compromised account (e.g., during a system attack), a temporary authenticity (e.g., if the attacker has the possibility to create accounts), none, or others. The authenticity was added to describe the human element [8].

Attack: The use of an exploit by an adversary to take advantage of a weakness with the intent to achieve a negative impact. The attack is described by type, delivery, results, and impact [14, 26].

- *Type:* Characterization of the threat similar to CAPEC. Physical attacks contain, e. g., theft. Active attacks can again be divided and include, e. g., identity theft and interruptive attacks ((distributed) denial of service). Passive attacks describe eavesdropping and other passive methods. Offline attacks comprise of cracking attacks, password speculations, and crypto analyses. Last but not least, social engineering is named, which may include other types, e. g., passive (research), active (actual attack), and physical (e. g., tailgating). Even though it may contradict the outline, it was added to include human elements [8].
- *Delivery:* Way of delivering the attack. This consists of payloads (e.g., a reverse shell), links (e.g., phishing links), responses (e.g., server or email responses), and others (e.g., physical) [15].
- *Results:* Direct consequences of an attack, ranging from nuisance, degradation, and disruption to disabling, theft, and disclosure.
- *Impact*: Loss or the consequences which are incurring due to the attack. For example, business disruption, intellectual property loss, customer information loss, reputation loss, and financial loss. Further details of results and impact were intentionally left out of the figure for clarity and can be seen in Figure 7 in Appendix A.2.

3.2 System Identities

The system identities taxonomy is relevant during almost all attacks (besides denial of service and eavesdropping), because attackers take over different digital identities to progress towards their goal. As shown in Figure 2, the taxonomy further details target, identity, and attack.

Target: In accordance with the taxonomy of the attack background, the target is further specified.

- *Level:* Target level in the system stack. Identities appear on different levels: service, network, system with cryptography and hardware, applications with server (database, storage, web, email, etc.) and client as well as user [11]. As the level varies across the taxonomies, it is detailed within the specific taxonomies. Even though the differences in the presented taxonomies are rather small, extensions may require other levels.
- *Location:* Physical location of the target. With outsourcing and cloud infrastructures, the location of the target in relation to the attacker may vary, from local to external, e.g., a trusted third party. [13]

Identity: The identity category details lifecycle, completeness, timeliness, directness, and amount.

- *Lifecycle:* Stage of the attack lifecycle, also known as cyber kill chain [5, 28].
- *Completeness:* Completeness of identity control takeover, i. e., fully or partly.
- *Timeliness:* Timeliness of identity control takeover, i. e., definitely temporary or until recovery.
- Directness: Direction of targeting, i. e., directly or indirectly.
- *Amount*: Amount of targeted identities. With system identities, single or selected identities are typically under the

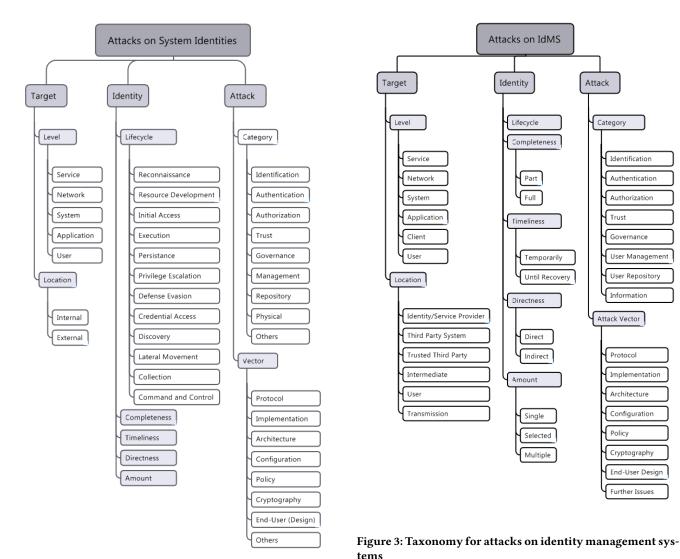


Figure 2: Taxonomy for attacks using system identities

control of the attacker. This may change within the following taxonomies, where multiple identities can be gained. The latter values were left out of the figure for clarity and can be found in Figure 8 in Appendix A.2.

Attack: The attack is described by category and vector.

- *Category:* Targeted weakness of identity management, i. e., identification, authentication, authorization, trust, governance, user management, user repository, physical or others [21].
- *Vector:* Specific path, method, or scenario exploited. This can be protocol, implementation, architecture, configuration, policy, cryptography, end-user design, and others.

3.3 Identity Management Systems

IdMSs are an important goal during attacks. As shown in Figure 3, the location within targets contains more entities as IdMS may be used in cooperation with third parties. In addition, the attack vector is further divided and several examples are explained.

Target: The target is detailed by level and location.

- *Level*: The level is similar to the taxonomy for system identities [11], shown above.
- *Location:* As IdMS can be used across organizations (e.g., cross-organization IdM, IdM-as-a-Service), identity provider resp. service provider, third party system, trusted third party, intermediate, end-users, and transmission are possible [13].

Identity: Similarly to the taxonomy for system identities, the identity is described by the lifecycle, completeness, timeliness, directness, and amount.

- *Lifecycle:* The attack can involve the IdMS in different stages within the lifecycle, even though the IdMS is typically the first main target [5, 28]. The lifecycle is intentionally left out and shown in Figure 9 in Appendix A.2.
- *Completeness:* An identity and IdMS can partly or fully be taken over, see, e.g., silver tickets for AD.
- *Timeliness:* The timeliness can differ, although until recovery is standard for IdMS.
- Directness: An attack can either be direct or indirect.
- Amount: Typically, the number of targeted accounts is multiple, though it could be selected or single. The amount may increase during the attack.

Attack: An attack is detailed by category and vector. The vector is use case-specific and explained in the following.

- *Category:* Similarly to system identities, the IdMS taxonomy uses a category of attacks [21]. This can include identification, authentication, authorization, trust, governance, user management, user repository, and information.
- *Vector:* The attack groups are further divided into protocol, implementation, architecture, policy, cryptography, end-user design, and further issues. Following are two examples for implementation and configuration. The implementation of AD had vulnerabilities including MS17-010 Eternal Blue and MS16-032 in earlier versions. The AD implementation of Kerberos could be used for Pass-the-Hash and Kerberoasting. The configuration of AD has several pitfalls, grouped into account (e. g., password in comments), group (e. g., built-in groups and unlimited groups), and delegation. Depending on, for example, the configuration of the Lightweight Directory Access Protocol (LDAP) implementation or finger, enumeration is possible.

3.4 End-User Identities

The end-user identities taxonomy is shown in Figure 4. It focuses on end-user identities, which are attacked, either directly or indirectly. While an individual digital identity has little financial value, the amount makes these types of attacks powerful. Hence, the taxonomy includes additional identity types, while the number of targeted identities is mostly multiple. The type of attack is concretized, while an additional pattern is included. The attack pattern further details and describes the purpose of the attack.

Target: The target end-user limits the possibilities of type and identity. Instead, level and location are added.

- *Level:* End-user identities appear on fewer levels: system, application, client, and user.
- *Location:* As identities are stored in databases and IdMS, the same locations are possible: identity resp. service provider, trusted third party, third party, intermediate, transmission, end-user, and others.

Identity: With the focus on end-users, the type shifts.

• *Type:* The identity type related to end-users is different from the types described above. Typical types contain information resp. accounts about credit card (including child credit card history), employment, tax, phone, bank, online social networks, online shopping, and other accounts.

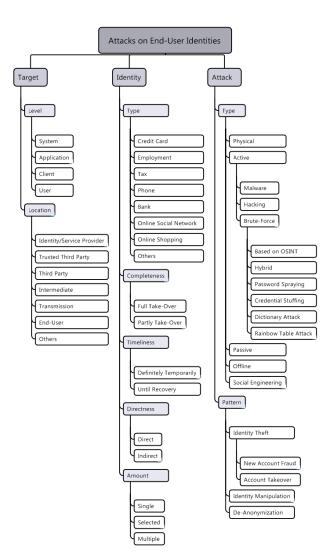


Figure 4: Taxonomy for attacks on end-user identities

- *Completeness:* Completeness is divided into full and partial take-over. Partial take-over is, e.g., possible during session hijacking.
- *Timeliness:* Timeliness is defined as either definitely temporarily or until recovery. The session is hijacked as long as the session exists. Therefore, the timeliness of the example is temporarily.
- Directness: The attack can either be direct or indirect.
- *Amount:* While the data from one end-user identity is cheap, the number of compromised accounts makes attacks valuable. Nevertheless, the attacker may target selected and single identities as well.

Attack: Also here, the types change and patterns further define the attack.

- *Type:* The attack type contains the same categories as the taxonomies beforehand. Passive may be the underground economy, open-source intelligence (OSINT), eavesdropping, and cracking. Physical especially focuses on things and devices. Another category is social engineering such as phishing. Within active attacks, malware (e.g., keylogger), hacking, and brute force are possible. Brute force related to identities includes password spraying, credential stuffing, dictionary attacks, rainbow table attacks, attacks based on OSINT information, and hybrid mode. [21]
- *Pattern:* Description of the methodology used by the adversaries to exploit weaknesses. The attack pattern consists of identity theft, identity manipulation, and de-anonymization. Identity theft is further divided into new account fraud (e.g., existing profile cloning attack) and account takeover. Both can be combined. This category relates to CAPEC, CWE, and OWASP.

4 EVALUATION OF TAXIDMA

In this section, the taxonomy framework TaxIdMA is evaluated. First, the applied methodology is described, followed by the evaluation.

4.1 Methodology

In order to analyze TaxIdMA, we apply eight real-world examples. These include one vulnerability, a smartphone app, and an advanced persistent threat, which is at the same time a supply chain attack. The examples were selected so that they are as diverse and up-to-date as possible. There is one exception: Celebgate already happened in 2014. Nevertheless, it can be categorized. All selection criteria are shown in Table 1.

4.2 Evaluation

First, the vulnerability or incident is described, followed by the categorization of the background. Last but not least, the mapping to the detailed taxonomy is explained. The first example, Zoom ZSB-22004, additionally highlights the categorization in the respective taxonomies.

4.2.1 Zoom ZSB-22004. Zoom revealed the local privilege escalation vulnerability ZSB-22004 (Common Vulnerabilities and Exposures (CVE)-2022-22782) in April 2022 with a high Common Vulnerability Scoring System (CVSS) score of 7.9. During the installer repair operation, malicious actors could utilize the vulnerability for further actions. [23]

First, the attack background is described based on Figure 5. As it is a vulnerability, the categories "Attacker" and "Target" cannot be further specified. For the category "Identity", the following values are selected: The *type* end-user identity with limited *permissions* is used. The attacker's *authenticity* can either be the end-user itself or utilize the compromised account. Within the category "Attack", we see the following: The attack has the *type* active and might be helped with social engineering. The *delivery* depends on the actual attack and is either payload or others. The *result* is at least escalated privileges, while the *impact* varies.

As the vulnerability can be used to escalate privileges at an enduser system, we select the taxonomy related to system identities

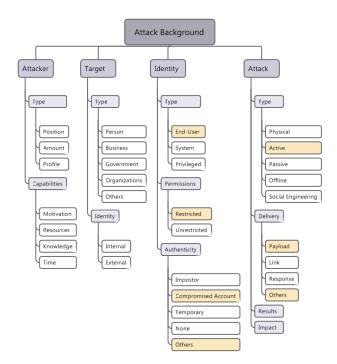


Figure 5: Categorization of Zoom ZSB-22004 based on the taxonomy for attack background

shown in Figure 6. For the category "Target", we detail our description with the following: The vulnerability affects the application *level* and could have consequences on the *location*, which is either internal or external. The vulnerability may have the following "Identity": It is used during privilege escalation within the *lifecycle*. If the attacker manages to establish persistent access, then the *completeness* and *timeliness* are given, otherwise not. The *amount* is single to selected and the identities have the *directness* directly. Last but not least, the category "Attack" is specified. The attack targets the *category* authorization and uses the *vector* implementation of Zoom.

4.2.2 VirusTotal. VirusTotal is a web application with more than 70 antivirus scanners that scan files and Uniform Resource Locators (URLs) sent by users. Researchers of the CySource Team [7] used the platform to upload a payload, which was added to the file's metadata, to the different hosts to perform the scan. When the exiftool on the hosts was utilized, the uploaded payload was actually executed, giving the researchers reverse shells from more than 50 internal hosts with high privileges. Due to the unauthorized access, it was possible to obtain sensitive and critical information, such as tokens and certificates.

The attacker *type* researcher is rather special as they want to play out of interest, typically work in teams, and are mostly outsiders. The *capabilities* were more than script kiddie as they had a specific CVE (CVE-2021-22204) in mind and the knowledge to use it. The target *type* was a selected service hosted by Google, which

	Background	System	IdMS	End-User
Vulnerabilities/Attacks	1/7	1/1	0/3	0/3
APT	1	0	1	0
Supply Chain Attack	1	0	1	0
Web Application/Smartphone	3/1	1/0	0/0	2/1
Computer/Server	1/3	1/0	0/3	0/0
Year	2014-2022	2022	2020, 2022	2014, 2021, 2022
Amount	8	2	3	3

Table 1: Overview of the selected examples used within the evaluation

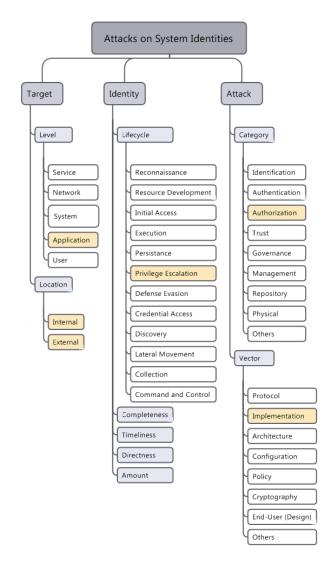


Figure 6: Categorization of Zoom ZSB-22004 based on the taxonomy for attacks using system identities

has the *identity* external. The identity utilized had the *type* enduser, while they gained privileged access. Thereby, they had almost unrestricted *permissions* with the *authenticity* of the compromised account. The attack *type* was active (i. e., hacking), using a payload for *delivery*, which was inserted into the file's metadata. The *result* was the compromise of several servers and the leakage of several sensitive and critical information. The *impact* may be press for the researchers as well as the service.

The target *level* is system via applications and, therefore, has an external *location*. Regarding the *lifecycle*, the initial access was mostly also the privilege escalation, providing privileged access. While the researchers *completely* took control and the *timeliness* is until recovery, the *directness* is indirect as they used the web application to get access. The *amount* of gained identities are multiple. The main *vector* is the implementation of exiftool, although there should be at least a policy in place to update vulnerable software. Probably the configuration (too many permissions) could be improved as well. Hence, the *category* is others.

4.2.3 Solarwinds from FireEye's Point of View. In December 2020, FireEye reported an incident – the first hint of the Solarwinds Hack [6]. A new registered phone of a FireEye user account raised a standard alarm. As it was the second enrolled phone for the user, the person was contacted and asked if it is their new phone. Even though it was a severity zero alert, an attacker tried to register a new device to bypass multi-factor authentication. Throughout investigations, the earliest trace of compromise was on the system with the Solarwinds product Orion. During the first phase of the attack, a backdoor was installed via Orion. In the second phase, this backdoor was actively used to collect domain credentials. The following phase involved the token signature certificates to access Office365. The last phase targeted the red team tools of FireEye. The attack does not solely concentrate on FireEye, but we take the company's point of view.

The attacker (*type*) likely worked in a group with a high degree of *capabilities*. The attack targeted the *type* businesses, but also governments, and other organizations. The attacker had the *identity* externals. During the attack, the attackers gained several identities with the *type* ranging from end-user to privileged. As far as understood, they used compromised accounts with the respective *permissions* and *authenticity*. The attack was of an active *type*, *delivered* by the malicious code. The *result* includes compromised software and networks, while the *impact* is still not fully known.

One goal during the attack was the IdMS. Therefore, the target was *located* at the identity provider for the *level* systems and networks. The takeover was in a later stage of the *lifecycle* with the *timeliness* until recovery, *directness* direct, and *amount* selected accounts. The registration of the new phone focused on authentication. The attack *vector* is others, as the attacker used the supplychain attack with the software update of Orion.

4.2.4 NVIDIA. NVIDIA Corp. had an incident that completely compromised the company's internal systems over a week in February 2022. According to reports, the attackers got hold of an employee's account. The Twitter user vx-underground tweeted that LAPSUS\$ has claimed responsibility, leaking password hashes for NVIDIA employees and NVIDIA's official code signing certificates, indicating other data [29]. According to LAPSUS\$, NVIDIA tried to hack back and ransomed their machines.

The attacker group LAPSUS\$ with certain *capabilities* typically targets the *type* large enterprises, i. e., the *identity* external. The attackers preannounce their attacks and probably use different *types* of identities, such as compromised accounts with varying *permissions* and *authenticity*, during the attack. The attack might have included the *types* hacking and social engineering. As no more information was released, it is difficult to estimate *delivery*. The *results* and *impact* might not fully be visible yet; at least the data was leaked.

The *location* at the target is the identity provider, as the IdMS was involved. Hence, the *amount* of multiple accounts of employees were leaked, resulting in fully *complete* and *timeliness* until recovery. The attack targeted the *category* user management among others. Further categorization is not possible due to the limited information.

4.2.5 ARcare. The US healthcare provider ARcare [1] experienced a data security incident impacting computer systems and temporarily disrupting its services while affecting 345,353 individuals. The investigation concluded in March 2022 that an attacker had access to the ARcare's network over a five-week period. The attack involved a malware infection. No misuse was reported, but the potentially exposed data include names, social security numbers, drivers' licenses or state identification numbers, financial account information, and health information. A health record is worth more than complete credit card information or social security numbers.

The attacker has some *capabilities* to target a specific business, ARcare, (*type*) with probably an external *identity*. As the data was accessed, the gained identity (*authenticity* compromised or temporary account) had enough *permissions*. Therefore, it was likely of the *type* system or privileged. The attack was of an active *type*, maybe *delivery* with payload, and had the *result* of malware infection and data loss. The *impact* was business disruption and may include identity theft, which can have consequences on the business.

Both, system identities and IdMS, can be regarded. We concentrate on the customer data. The target is further detailed with *level* network and system as well as the *location* identity provider. The data was probably one of the goals of the attack and belongs to the *lifecycle* steps credential access resp. data exfiltration. The *amount* multiple access to data was fully (*completeness* and *timeliness*) gained. The attack targeted the *category* user management, though it stays unclear which *vector* enabled the attack.

4.2.6 Celebgate. An attacker managed to phish several targets to gain access to at least 50 Apple's iCloud and 72 Google accounts in

2014, stealing private photos and videos of celebrities. Partly fallback authentication with security questions and guessable answers was exploited. In some cases, the attacker utilized a software program to download the entire content of the target's iCloud backup. [10]

The single attacker (*type*) had the *capability* and the time to write phishing mails and guess security questions with the motivation to steal photos and videos of mainly female celebrities. The attacker used the *authenticity* of the service provider, gaining access to the *type* end-user identities with their *permissions*. The attack *type* was social engineering (and partly brute-force based on OSINT) with the *delivery* mode link, getting to the *result* of stolen data and the *impact* of the publication of several nude photos (though the connection to the publication of the photos was not found).

The target *level* is the user with the *location* identity provider as the data was stored there. The gained identities were accounts for online services (*type*), which were fully gained until recovery (*completeness* and *timeliness*). The attacker *directly* targeted these selected accounts (*amount*). The attack mainly used the *type* social engineering, though brute-force based on OSINT was successful for some accounts. The *pattern* is identity theft with account takeover.

4.2.7 Spotify Credential Stuffing. In February 2021, Bob Diachenko uncovered that Spotify suffered from a second credential stuffing attack involving an estimated hundred thousand accounts [9]. In November 2020, researchers found a misconfigured and open Elasticsearch cloud database containing more than 3,890 million records. Both databases were owned by malicious third parties. The usernames and passwords might be from previously reported breaches or collections of data, which were reused against Spotify accounts.

The attackers have the *capability* to operate Elasticsearch, but not enough to configure it securely. The motivation might be money if they are able to gain access to high-level accounts or sell them in large quantities. The target consists of the *type* persons, i. e., *type* end-users with limited *permissions*. The *authenticities* towards Spotify are the compromised accounts. The attack *type* is active, possible by the *delivery* responses. The attackers got hold of credentials of valid users (*result*), while the *impact* may range from nuisance to financial, depending on the further actions.

The target consists of the *level* end-users where the credentials are stored at the *location* identity provider. The credentials might be used for third parties. The stolen identities are from the *type* online accounts. Each account is *completely* and *directly* taken over until recovery (*timeliness*, e.g., password change and maybe enabling multi-factor authentication). The *type* brute-force (i. e., credential stuffing) attack with the *pattern* of account takeover had the goal to gain the *amount* multiple accounts.

4.2.8 *FlyTrap.* The Android malware FlyTrap spread to more than 10,000 targets through Google Play Store and third-party app marketplaces. According to Zimperium [31], nine bad apps acted as FlyTrap. The targeted users were told to log in with their Facebook accounts to cast their vote or collect a coupon code. The Trojan hijacked the sessions and took over Facebook accounts. The app then got details like Facebook ID, location, email address, IP address, and cookies resp. tokens associated with the Facebook account, before abusing the Facebook account to spread the malware through personal messaging with links to the Trojan.

TaxIdMA: Towards a Taxonomy for Attacks related to Identities

ARES 2022, August 23-26, 2022, Vienna, Austria

The attacker had enough *capabilities* to build these apps and run the associated command and control (C2) server. The exact *type* of attacker is not known. The target *type* is end-users, resulting in the identity *type* end-user identities with restricted access (*permissions*). The *authenticity* of the attacker is an imposter regarding the app and the compromised account when looking at the social engineering techniques used. The attack *type* is active combined with social engineering. The *delivery* was through the app (i. e., others) and link. FlyTrap *resulted* in several overtaken accounts and sessions stored in the command and control server. The *impact* might increase if a vulnerability of the C2 server is exploited.

The attack targeted end-users via applications (*level*). While the identity data is stored at the identity provider (*location*), the data was gained via the aimed users resp. due to third parties. The goal (*type*) was the partly and temporarily take over (*completeness* and *timeliness*) of Facebook social network accounts. The malware *directly* targeted the accounts while the *amount* is multiple. The attack *type* is active malware with the *pattern* account takeover.

5 DISCUSSION

During the design of the taxonomies, several iterations were made. Whereas the background is based on the common description of an attack, the other taxonomies are to a greater extent based on attacks and related work. One evolutionary iteration enabled the description of a stepwise attack, where the background is static while the identities of the attacker and, thereby, taxonomies change. Next, the categories were aligned across all taxonomies. Items, where the values may change, were added to the specific taxonomies, whereas items with static values were appended to the background.

A taxonomy should fulfill the requirements described in Section 3. The categories are mutually exclusive and, therefore, not overlapping. The classification criteria are (mostly) clear and unambiguous. While this is true for involved experts, a to-be-established tutorial may open the taxonomy to a wider audience. In addition, social engineering attacks may combine further attack types. Therefore, another iteration may be needed in the future. The background can be seen as the basis, whereas the other three parts of TaxIdMA detail the taxonomies for the specific use case. If an IdMS is targeted, the system identity taxonomy can be used for the steps beforehand. Depending on the attack, a taxonomy could be used several times to specify the explicit steps. Also here, a tutorial would provide added value for the wider audience. The evaluation showed that categorizing eight real-world and typical attacks is possible without difficulties. In future work, further attacks and typical problems can be analyzed. The taxonomy is comprehensive and uses established terminology in the fields of identity management and cyber security.

Even though the selected examples were easy to categorize and provide more details than existing approaches, the taxonomy is nevertheless rather generic concerning the variants of attacks focusing on AD. IoT devices can be explained by the system and end-user identities, while the management is again IdMS. A taxonomy specifically for IoT may help to show the variations and secure the systems. With the evolution of IT, further parts of the taxonomy may be needed in the future. The proposed TaxIdMA nevertheless provides a solid basis.

6 CONCLUSION AND OUTLOOK

Identity management is essential for the operation of all IT services. At the same time, IdMSs pose important targets for attacks [12]. Therefore, their design, implementation, and configuration are crucial for the secure operation of the infrastructure. In order to provide a common ground, TaxIdMA was established. The taxonomy framework for identity management consists of several taxonomies: general attack background, system identities, IdMS, and end-user identities. The proposed taxonomy framework is a start towards a well-defined taxonomy for attacks focusing on identities. The evaluation of TaxIdMA with eight real-world examples showed that the taxonomy helps to categorize attacks and hence identify critical elements. However, with new developments, TaxIdMA may need improvements and refinements. In future work, we plan to evaluate more attacks and common problems to further detail the taxonomy. A tutorial will make TaxIdMA useful for a wider audience. Last but not least, defense mechanisms will be mapped to the attacks and grouped in a further taxonomy framework.

ACKNOWLEDGMENTS

This work is partly funded by the Bavarian Ministry for Digital Affairs (Project DISPUT/STMD-B3-4140-1-4). The authors alone are responsible for the content of the paper.

REFERENCES

- ARcare. 2022. Notice of Data Privacy Incident. https://www.arcare.net/wpcontent/themes/altitude-pro/security_notice.html accessed January 3, 2023.
- [2] Eric W. Burger, Michael D. Goodman, Panos Kampanakis, and Kevin A. Zhu. 2014. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. In Proc. of the Workshop on Information Sharing & Collaborative Security (WISCS) (Scottsdale, AZ, USA). ACM, 51–60. https://doi.org/10.1145/ 2663876.2663883
- [3] Ian M. Chapman, Sylvain P. Leblanc, and Andrew Partington. 2011. Taxonomy of Cyber Attacks and Simulation of Their Effects. In Proc. of the 2011 Military Modeling & Simulation Symposium (MMS) (Boston, MA, USA). Society for Computer Simulation International, San Diego, CA, USA, 73–80.
- [4] Samuel Chng, Han Yu Lu, Ayush Kumar, and David Yau. 2022. Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports* 5 (2022), 100167. https://doi.org/10.1016/j.chbr.2022.100167
- [5] Sungyoung Cho, Insung Han, Hyunsook Jeong, Jinsoo Kim, Sungmo Koo, Haengrok Oh, and Moosung Park. 2018. Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture. In Proc. of the International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (Glasgow, UK). IEEE, 1–8. https://doi.org/10.1109/CyberSA.2018.8551383
- [6] Cybersecurity & Infrastructure Security Agency. 2021. Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. https://www.cisa.gov/uscert/ncas/ alerts/aa20-352a accessed January 3, 2023.
- [7] CySource Team. 2022. Remote Code Execution via VirusTotal Platform. https: //www.cysrc.com/blog/virus-total-blog/ accessed January 3, 2023.
- [8] Richard Derbyshire, Benjamin Green, Daniel Prince, Andreas Mauthe, and David Hutchison. 2018. An Analysis of Cyber Security Attack Taxonomies. In Proc. of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (London, UK). 153–161. https://doi.org/10.1109/EuroSPW.2018.00028
- Bob Diachenko. 2021. Bob Diachenko on Twitter. https://twitter.com/ mayhemdayone/status/1357319575440875520 accessed January 3, 2023.
- [10] Rebecca Fallon. 2015. Celebgate: Two Methodological Approaches to the 2014 Celebrity Photo Hacks. In Internet Science, Thanassis Tiropanis, Athena Vakali, Laura Sartori, and Pete Burnap (Eds.). Springer International Publishing, 49–60.
- [11] Federal Office for Information Security. 2021. IT-Grundschutz-Compendium. Technical Report.
- [12] Lothar Fritsch. 2020. Identity Management as a target in cyberwar. In Open Identity Summit 2020 (online), Heiko Roßnagel, Christian H. Schunck, Sebastian Mödersheim, and Detlef Hühnlein (Eds.). GI, 61–70. https://doi.org/10.18420/ ois2020_05
- [13] Umme Habiba, Rahat Masood, Muhammad Awais Shibli, and Muaz A. Niazi. 2014. Cloud identity management security issues & solutions: a taxonomy. *Complex*

Pöhn and Hommel

Adaptive Systems Modeling 2, 1 (2014), 5. https://doi.org/10.1186/s40294-014-0005-9

- [14] Simon Hansman and Ray Hunt. 2005. A taxonomy of network and computer attacks. *Computers & Security* 24, 1 (2005), 31–43. https://doi.org/10.1016/j.cose. 2004.06.011
- [15] Ryan Heartfield and George Loukas. 2015. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. ACM Comput. Surv. 48, 3, Article 37 (2015), 39 pages. https://doi.org/10.1145/2835375
- [16] Anas Husseis, Judith Liu-Jimenez, Ines Goicoechea-Telleria, and Raul Sanchez-Reillo. 2019. A Survey in Presentation Attack and Presentation Attack Detection. In Proc. of the International Carnahan Conference on Security Technology (ICCST) (Chennai, India). IEEE, 1–13. https://doi.org/10.1109/CCST.2019.8888436
- [17] Vinay M. Igure and Ronald D. Williams. 2008. Taxonomies of Attacks and Vulnerabilities in Computer Systems. *IEEE Communications Surveys Tutorials* 10, 1 (2008), 6–19. https://doi.org/10.1109/COMST.2008.4483667
- [18] David Klaper and Eduard Hovy. 2014. A Taxonomy and a Knowledge Portal for Cybersecurity. In Proc. of the 15th Annual International Conference on Digital Government Research (DG-O) (Aguascalientes, Mexico). ACM, 79–85. https: //doi.org/10.1145/2612733.2612759
- [19] Carl E. Landwehr, Alan R. Bull, John P. McDermott, and William S. Choi. 1994. A Taxonomy of Computer Program Security Flaws. ACM Comput. Surv. 26, 3 (1994), 211–254. https://doi.org/10.1145/185403.185412
- [20] Ulf Lindqvist and Erland Jonsson. 1997. How to systematically classify computer security intrusions. In Proc. of the IEEE Symposium on Security and Privacy (S&P) (Oakland, CA, USA). 154–163. https://doi.org/10.1109/SECPRI.1997.601330
- [21] MITRE Corporation. 2022. CAPEC Common Attack Pattern Enumeration and Classification. https://capec.mitre.org accessed January 3, 2023.
- [22] MITRE Corporation. 2022. CWE Common Weakness Enumeration. https: //cwe.mitre.org accessed January 3, 2023.
- [23] NIST. 2022. CVE-2022-22782 Detail. https://nvd.nist.gov/vuln/detail/CVE-2022-22782 accessed January 3, 2023.
- [24] OWASP. 2022. Projects. https://owasp.org/projects/ accessed January 3, 2023.
- [25] Purple Knights Security. 2022. Purple Knight Report 2022 Facing the Unknown: Uncovering & Addressing Systemic Active Directory Security Failures. Technical Report.
- [26] Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, and Qishi Wu. 2014. AVOIDIT: A Cyber Attack Taxonomy. In Proc. of the 9th Annual Symposium on Information Assurance (ASIA). 2–12.
- [27] Elizabeth Stobert and Robert Biddle. 2018. The Password Life Cycle. ACM Trans. Priv. Secur. 21, 3, Article 13 (2018), 32 pages. https://doi.org/10.1145/3183341
- [28] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. 2018. Mitre Att&ck: Design and Philosophy. (2018).
- [29] vx-underground. 2022. vx-underground on Twitter. https://twitter.com/ vxunderground/status/1497484483494354946 accessed January 3, 2023.
- [30] Phillip Williams, Pablo Rojas, and Magdy Bayoumi. 2019. Security Taxonomy in IoT – A Survey. In Proc. of the 62nd International Midwest Symposium on Circuits and Systems (MWSCAS) (Dallas, TX, USA). IEEE, 560–565. https://doi.org/10. 1109/MWSCAS.2019.8884913
- [31] Aazim Yaswant. 2021. FlyTrap Android Malware Compromises Thousands of Facebook Accounts. https://blog.zimperium.com/flytrap-android-malwarecompromises-thousands-of-facebook-accounts/ accessed January 3, 2023.

A TAXONOMIES

This appendix defines the terms used in the taxonomies and visualizes the extended taxonomies.

A.1 Definitions

In the following, definitions for the terms used within the taxonomies are given.

- Amount: Quantity of targeted identities.
- Attack: The use of an exploit by an adversary to take advantage of a weakness with the intent to achieve a negative impact.
- Attack Category: Targeted weakness of identity management.
- Attack Pattern: Description of the methodology used by the adversaries to exploit weaknesses.
- Attack Vector: Specific path, method, or scenario exploited.
- Attacker: Someone who explores methods for breaching weaknesses in a computer system or network.
- Authenticity: Attribution of the attacker towards the system during the attack.
- **Capabilities:** Expertise or ability of the attacker to reach the goal.
- **Completeness:** State or condition of being complete concerning the identity control takeover.
- **Delivery:** Way of conveying the attack.
- Directness: State of direction of targeting.
- Identity: Digital identity used during the attack.
- **Impact:** Loss or the consequences which are incurring (effects) due to the attack.
- Lifecycle: Stage of attack lifecycle, also known as cyber kill chain [5, 28].
- **Permissions:** Authorization of the overtaken digital identity.
- Results: Direct consequences (final product) of an attack.
- Target: A goal designated for an attack.
- Target Level: Target position in the system stack.
- **Target Location:** Particular place in physical space of the target.
- Target Identity: Position of the target related to the attacker.
- **Timeliness:** State and duration of being timely concerning the identity control takeover.
- Type: A grouping based on shared characteristics.

A.2 Extended Taxonomies

In the following, the extended taxonomies for attack background (see Figure 7), system identities (see Figure 8), and IdMS (see Figure 9) are shown.

TaxIdMA: Towards a Taxonomy for Attacks related to Identities

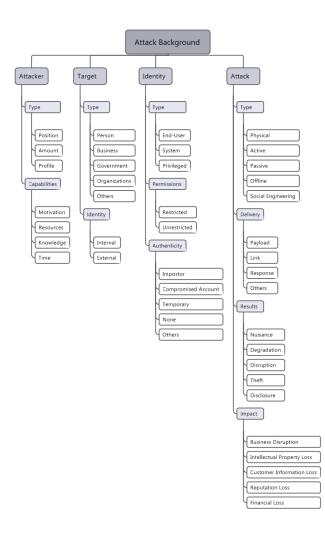


Figure 7: Extended taxonomy for attack background

Pöhn and Hommel

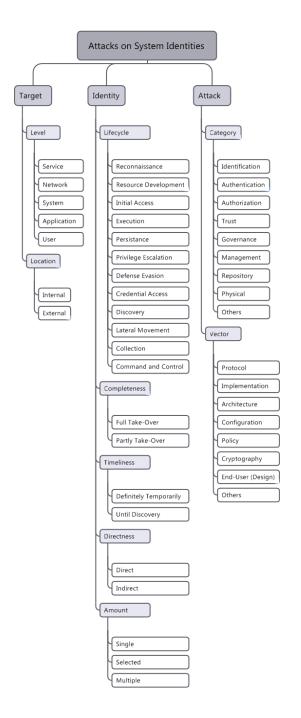


Figure 8: Extended taxonomy for attacks using system identities

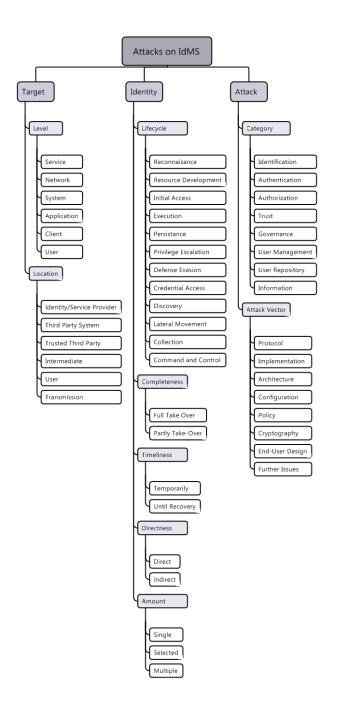


Figure 9: Extended taxonomy for attacks on identity management systems