Computer and Information Science; Vol. 7, No. 3; 2014
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Revised Attack Taxonomy for a New Generation of Smart Attacks

Robert Koch[1], Mario Golling[1] & Gabi Dreo Rodosek[1]

[1] Universität der Bundeswehr München, Faculty of Computer Science, D-85577 Neubiberg, Germany

Correspondence: Mario Golling, Universität der Bundeswehr München, Faculty of Computer Science, D-85577 Neubiberg, Germany. Tel: 49-896-004-2255. E-mail: mario.golling@unibw.de

Received: March 31, 2014 Accepted: April 11, 2014 Online Published: July 5, 2014

doi:10.5539/cis.v7n3p18 URL: http://dx.doi.org/10.5539/cis.v7n3p18

Abstract

The last years have seen an unprecedented amount of attacks. Intrusions on IT-Systems are rising constantly - both from a quantitative as well as a qualitative point of view. Well-known examples like the hack of the Sony Playstation Network or the compromise of RSA are just some samples of high-quality attack vectors. Since these Smart Attacks are specifically designed to permeate state of the art technologies, current systems like Intrusion Detection Systems (IDSs) are failing to guarantee an adequate protection. In order to improve the protection, a comprehensive analysis of Smart Attacks needs to be performed to provide a basis against emerging threats.

Following these ideas and inspired by the original definition of the term Advanced Persistent Threat (APT) given by U.S. Department of Defense, this publication starts with defining the terms, primarily the group of Smart Attacks. Thereafter, individual facets of Smart Attacks are presented in more detail, before recent examples are illustrated and classified using these dimensions. Next to this, current taxonomies are presented including their individual shortcomings. Our revised taxonomy is introduced, specifically addressing the latest generation of Smart Attacks. The different classes of our taxonomy are discussed, showing how to address the specifics of sophisticated, modern attacks. Finally, some ideas of addressing Smart Attacks are presented.

Keywords: network security, intrusion detection, taxonomy, smart attack

1. Introduction

During the last years, the number of attacks on IT systems has increased steadily, both from a quantitative as well as a qualitative point of view. Hacks of the Sony Playstation Network, Shanghai Roadway, SK Communications or RSA are just some examples of recent intrusions, reflecting the emerge of a new class of Smart Attack vectors. Recent discovered threats like Uroboros, which sometimes had been active for years before the have been detected (and often only by chance), demonstrate the endangerment by highly sophisticated attacks. These Smart Attacks can also be observed increasingly in case of attacks on critical infrastructures, for example systems of the water supply or the power grid. In contrast to conventional attacks, Smart Attacks include some special features. Among other characteristics, new types of attacks are comparatively complex and novel attacks which are very targeted and thereby able to camouflage themselves very well. As a consequence, state of the art technologies to prevent intrusions are failing to guarantee an adequate protection in this case (e.g., see (Ponemon Institute, 2013)). Even specialized systems, e.g., in the area of Supervisory Control and Data Acquisition (SCADA), are not able to provide the required security level.

In order to improve the protection, a comprehensive analysis of Smart Attacks needs to be performed. Thus, the complex ecosystem with the role of particular elements must be understood to form a basis against this kind of attacks. Following these ideas and inspired by the original definition of the term APT given by the U.S. Department of Defense (DoD), Section 2 starts with defining the terms (Attack, Targeted Attack, Advanced Persistent Threat and Smart Attack). Section 3 illustrates recent examples of Smart Attacks. Based on this, individual facets of Smart Attacks are presented in more detail. Subsequently, recent examples are classified with the use of these dimensions. As a deep understanding of attacks and related techniques is required to be able to identify shortcomings and vulnerabilities on the one hand and possible countermeasures and protection techniques on the other hand, Section 4 gives an overview on related work done in the scope of our publication, focusing on attack taxonomies. Since current attack taxonomies are not able to cope with Smart Attacks, Section 5 contains a revised taxonomy for Smart Attacks using a modified attack classification. Finally, Section 6 concludes our work and gives an overview of further work, providing a digest of tools for next generation

intrusion detection.

2. Definition of Terms

Before going deeper into descriptions about Smart Attacks, within this section, we define the terms used within this publication. This is particularly important, because many of the terms are used differently in various publications, or with a slightly different meaning. As for instance observed by Symantec in 2011, terms such as APT have been overused and sometimes misused by the media (Symantec Corporation, 2011). However, instead of redefining the terms, we want to make use of existing, generally accepted definitions as far as possible.

2.1 Attack

Fundamental to the further understanding of the work is the notion of an attack. According to the Committee on National Security Systems (CNSS) of United States of America, an attack is defined as follows (Committee on National Security Systems, 2010):

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Subsequently, CNSS defines the term cyber-attack in the following way (Committee on National Security Systems, 2010):

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

2.2 Targeted Attack

Since especially Targeted Attacks and APTs are often mixed, it is important to understand the nature of this mounting threat (Symantec Corporation, 2011):

An attack can be considered as targeted if it is intended for a specific person or organization, typically created to evade traditional security defences and frequently makes use of advanced social engineering techniques.

2.3 Advanced Persistent Threat

Today, the term APT is often used for different kinds of highly professional attacks which are more likely Targeted Attacks. APTs have evolved to describe a unique category of Targeted Attacks that are specifically designed to target a particular individual or organization (Symantec Corporation, 2011). APTs are designed to stay below the radar and remain undetected for as long as possible, a characteristic that makes them especially effective, moving quietly and slowly in order to evade detection (Symantec Corporation, 2011). Targeted Attacks and APTs have very much in common. However, not all Targeted Attacks are APTs. For example, the victim may have been selected simply because the attacker was able to exploit information, typically harvested through social networking Web sites.

Having a look at the definition of APT as originally given by the DoD, the major characteristics are as follows (Krypt3ia, 2012):

Advanced: Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques, such as telephone-interception technologies, satellite imaging and Human Intelligence (HUMINT) capabilities. While individual components of the attack may not be classed as particularly “advanced” (e.g., malware components generated from commonly available do-it-yourself malware construction kits, or the use of procured exploit materials), their operators can typically access and develop more advanced tools if required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from “less advanced” threats.

Nation State or Exceedingly Coherent and Supported Actors: APTs usually imply Nation State actors (i.e. spies/proxies for nations seeking to infiltrate and steal data or to manipulate data/supply chains etc.). This can also be non-nation state actors hired by corporations or even in some cases, movements or groups hired for specific operational goals.

Persistent: Operators give priority to a specific task, rather than seeking for financial or other gain. This distinction implies that the attackers are guided by external entities. Targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. This does not mean a barrage of constant attacks and malware updates. In fact, a “low-and-slow” approach is usually more successful. If the operator loses

access to their target they usually will reattempt access, and most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats that only need access to execute a specific task.

Threat: APTs are a threat, because they have both, capability and intent. APT attacks are executed by coordinated, considered human actions, rather than by mindless and automated pieces of code. Operators have a specific objective and are highly skilled, motivated, organized and well-funded.

3. Characteristics of Smart Attacks

Today's security systems are not able to cope with modern and sophisticated attacks (*Smart Attacks*). Although Targeted Attacks and APTs involve numerous aspects, different exploitation vectors, like the level of camouflage, are neglected. In order to develop more capable and efficient defence mechanisms and systems, the nature of today's rising and upcoming threats has to be analysed in detail.

3.1 Methodology

The methodology used within this publication follows a so-called "constructivist process" which is primarily inductive (based on observations, a consolidation of know-how from existing models / related work and technical concepts) and creates a simplified representation of the reality. The taxonomy is hereby created for a class of applications ("generality") and re-uses - as far as possible - other existing models and integrates / extends them ("reutilization"). The construction of the model was performed according to (Fettke & Loos, 2003) and thus involved the following four steps:

Problem Definition: Within the first step, the target domain and the problem that has to be solved (Smart Attacks) was defined.

Requirements Definition: Then an analysis of the problem area (facet of smart attacks) was carried out and a search / survey of existing models / work was performed.

Model Selection: Then these existing models were evaluated accordingly and a selection regarding reusable components did take place.

Model Construction: Finally, in the last phase, by using compositional measures (modifying, changing, completing individual aspects of existing models) as well as genetic measures (explicit measures to complement the overall model), the taxonomy was created.

3.2 Dimensions of Smart Attacks

In contrast to traditional attacks, Smart Attacks have many different facets. Smart Attacks are characterized by the fact that they cover a variety (not necessarily all) of the following dimensions, which we are briefly describing throughout the rest of this subsection:

Targeted: With recourse to the definition of a Targeted Attack introduced in Section 2.2, targeted refers to attacks specifically designed for an individual (person/organization) to withstand respective protective mechanisms. Thus, the attack is not "spread in the wild", but very custom, specifically created for the target that is being attacked. At its best, this can be a malicious program created by a sophisticated attack toolkit, which is able to bypass the security mechanisms of the target. With higher capabilities of the attacker respectively defender, new and specifically designed programs and attack strategies will be generated.

Immune: The term targeted is closely associated with the notion “immune”. In order to be successful with a Targeted Attack, this usually implies overcoming existing protection mechanisms. In the context of IT security, this includes bypassing systems such as intrusion detection / prevention systems (IDPS), firewalls, antivirus systems, and other protective measures.

Persistent: Persistence refers to the ability to remain undetected over a long time. In this regard, one possibility is 'sleeping' malicious software. For instance, a malware (especially when realized as part of the hardware, for example as a backdoor) can be passive for many years, only enabling itself under very special conditions.

One example of a targeted, persistent and immune attack is a specially prepared commercial off-the shelf (COTS) product (such as a Print/Copy/Fax machine with modified firmware), which - besides printing the documents - also sends them via fax to the attacker (after a delaying timer has expired). As modern multi-function printers typically are able to send scans via email, this capability can also be used to exfiltrate data.

Resistant: The last example also introduces the concept of being resistant to new protective measures, e.g., an update of signatures (which are very common in case of IDPSs and antivirus systems). In general, resistance refers to the ability of an attack to withstand against future adverse effects (such as new or improved protective mechanisms).

Camouflaged: As (with regard to the previous example) the data is transmitted by fax instead of using the data network, a detection by traditional IDPSs is rather difficult. This will especially be the case, if the information is not actively sent (i.e. telephone charges may indicate attack traces), but instead with a passive approach (e.g., the system is contacted by the attacker at night and data is transferred in the form of a "fax-demand"; therefore a pull-approach). In such a case, a detection is very difficult and the attack vector is very well camouflaged. Camouflaged corresponds to the attacker's goals to maintain long-term access in order to carry out one specific task and thus refers to the ability of "staying under the radar".

Multilayered: Today, critical systems are (respectively shouldn't be) usually not directly connected to the Internet. Often, such systems can only be reached by overcoming multiple security zones. According to the concept of perimeter security, specific policies are applied for transferring data between networks of different security levels (e.g., the transfer of data between the corporate network and the Internet). In case of high security networks, such a policy may also result in what is often referred to as "air gap", which means, that the two networks like the Intranet and the Internet are physically separated.

However, modern attack vectors have shown, that it is even possible to overcome this air gap. Since there is often still a necessity of a controlled data flow between the secured and the insecure network ("swivel chair interface"), already several examples are known in which the air gap has been overcome. The most prominent example of this is likely to be Stuxnet. There, human behaviour was (once again) the weak point to bridge the air gap, but this can also be done on a technical basis: see the recent discussion about the (theoretical) possibilities of "BadBIOS", the use of audio modulation/demodulation presented by Hanspach et al. and the possibilities to bridge the air gap by technologies of the NSA leaked by the whistleblower Snowden.

Hence, one facet of smart vectors is also that - since they cannot directly attack the target - they operate in a multilayered fashion and first target the perimeter network (the network directly connected to the Internet) and than the separated network.

The example of the attack on Lockheed Martin clearly represents another example of a multilayered attack. Hackers managed to break into the network of Lockheed Martin and some other companies commissioned by the U.S. military. Instead of directly attacking Lockhead Martin (which was likely to be very difficult due to a strong protection), the attack was performed in a combined fashion. First, hackers captured information on SecurID products of crypto specialist RSA. Then in turn, this information was used to attack Lockhead Martin, since they made use of RSA products (Schneier, 2011).

Novel: Using the example of Flame, another facet of Smart Attacks can be illustrated. The Flame espionage malware that infected computers in Iran achieved mathematic breakthroughs that could have been accomplished only by world-class cryptographers (Goodin, 2012). Flame uses a yet unknown MD5 chosen-prefix collision attack. Collision attacks, in which two different sources of plaintext generate identical cryptographic hashes, have long been theorized, but Flame is the first known example of an MD5 collision attack being actively used maliciously in a real-world environment. By that, the malware was able to hijack the Windows Update mechanism (fake servers on the network as well as the corresponding malware appeared to originate from Microsoft). As a consequence, this was used to distribute "patches" (= the malware) to hundreds of millions of customers.

Controllable: Especially in the field of botnets, the ability of a malware to update itself is known. E.g., Zeus comes as a toolkit to build and administer a botnet. It has a control panel that is used to monitor and update patches to the botnet clients. Another example is the Trojan.Zbot that can also be updated by the attacker using the threat's back door capabilities.

Complex: Smart Attacks can exploit several vulnerabilities at the same time, or can consist of multiple attack vectors. This especially doesn't mean that all vulnerabilities are exploited at once, but if one fails, there are fallback possibilities to still exploit the system or keep the malicious code running. See, e.g., the integration of multiple Zero Days in Stuxnet (Falliere, Murchu, & Chien, 2011).

Sophisticated: Sophisticated threats are sophisticated in the sense that they are highly organized and have significant resources at their disposal (e.g., organized cybercrime).

Interdisciplinary: The concept of interdisciplinarity is closely related to the previous dimensions. Interdisciplinary refers to the use of approaches, ways of thinking, or at least methods of different disciplines. An attack on SCADA systems for instance requires experts for the penetration of the computer network as well as those that are able to sabotage control systems of industrial plants. In addition, especially the field of Computer Network Exploitation requires an interdisciplinary approach. HUMINT, for example, is rarely conducted by IT

specialists, but it is an important component of today's attacks. Therefore, social engineers can gather information from a secretary, programmers develop a special kind of attack code while service technicians install a new malicious device into the network of a company.

3.3 Definition of Smart Attacks

Consequently, Smart Attacks are defined as follows:

An attack is considered smart if it is aiming at a single target or a limited target group which is exploited in-depth. The attack is executed via the combined, interdisciplinary exploitation of multiple domains in a camouflaged way where the means and levels of exploitation of the individual domain is below the particular detection respectively suspicion thresholds. Smart Attacks can contain, or be limited to, sleeper exploitations which are (pre-) installed in software or hardware and waiting for a specific time or a trigger for activation.

Within this definition, a limited target group refers to the network(s), system(s) or user(s) of a specific attack target, e.g., one company. *In-depth* corresponds to the implementation of an advanced strategy, also exploiting downstream systems like printers or office PCs for realizing a camouflaged surveillance as well as persistent "implantation" into the network. Exploitation is realized combined or *intradisciplinary*, e.g., by executing slow network scans in parallel to information search at the secretariat. The particular characteristics are described in detail in Table 1 resp. Figure 1.

3.4 Selected Examples of Smart Attacks in the Recent Past

In addition to the examples presented (the RSA attack on Lockheed Martin, Flame and Stuxnet) in particular the trojan "Gauss" will be presented here. As part of its investigations of the 20-MB-Trojan "Flame", security researchers from Kaspersky Lab have encountered a much more widespread cousin: "Gauss". The Trojan horse is believed to have infected tens of thousands of computers in Lebanon, Israel and Palestine. Gauss uses USB sticks to get information about other computers. To this end, it creates a special espionage tool on the portable storage medium, which is executed automatically when plugged into the computer through the so-called LNK vulnerability (if possible). After starting, a variety of information about the system, including running processes, disk drives, and network shares is gathered and stored on the USB drive. An infection of the computer is not carried out. However, on the infected sticks also a RC4 encrypted payload is located that will run only on specific systems. In addition, the malware installs its own font called "Palida Narrow". Some scientists assume that Palida Narrow serves as a "marker", since a website can easily find out if the particular font is installed (therefore, this attribute was used by CrySyS Lab to provide an online Gauss Detector Service). The name "Gauss" comes from the main module; other modules are also named after famous mathematicians. The currently known plugins perform the following functions (GReAT, 2013):

- Intercept browser cookies and passwords
- Harvest and send system configuration data to attackers
- Infect USB sticks with a data stealing module
- List the content of the system drives and folders
- Steal credentials for various banking systems in the Middle East
- Hijack account information for social network, email and IM accounts

Table 1. Summary and classification of recent examples

Classification	Description	RSA Attack on Lockheed Martin	Flame	Stuxnet	Gauss
Targeted	specially designed for an individual (person/ organization)	High	Medium	High	Medium
Immune	overcomes existing protection mechanisms	High	Medium	High	Medium
Persistent	capability to keep functionality over a long period of time (e.g., sleeping malware)	Low	Medium	High	Medium
Resistant	resistant to new protective measures	Low	Medium	High	Medium
Camouflaged	ability of "staying under the radar"	Medium	Medium	High	Medium
Multilayered	overcoming multiple security zones	High	Medium	High	Medium
Novel	yet unknown technique	High	Medium	High	Medium
Controllable	ability of a malware to update itself	Low	Low	Low	Medium
Complex	attack can exploit several vulnerabilities at the same time, or can consist of multiple attack vectors	Low	High	High	Low
Sophisticated	highly organized with significant resources	Medium	High	High	Medium
Interdisciplinary	uses methods of different disciplines	Medium	Medium	High	Medium

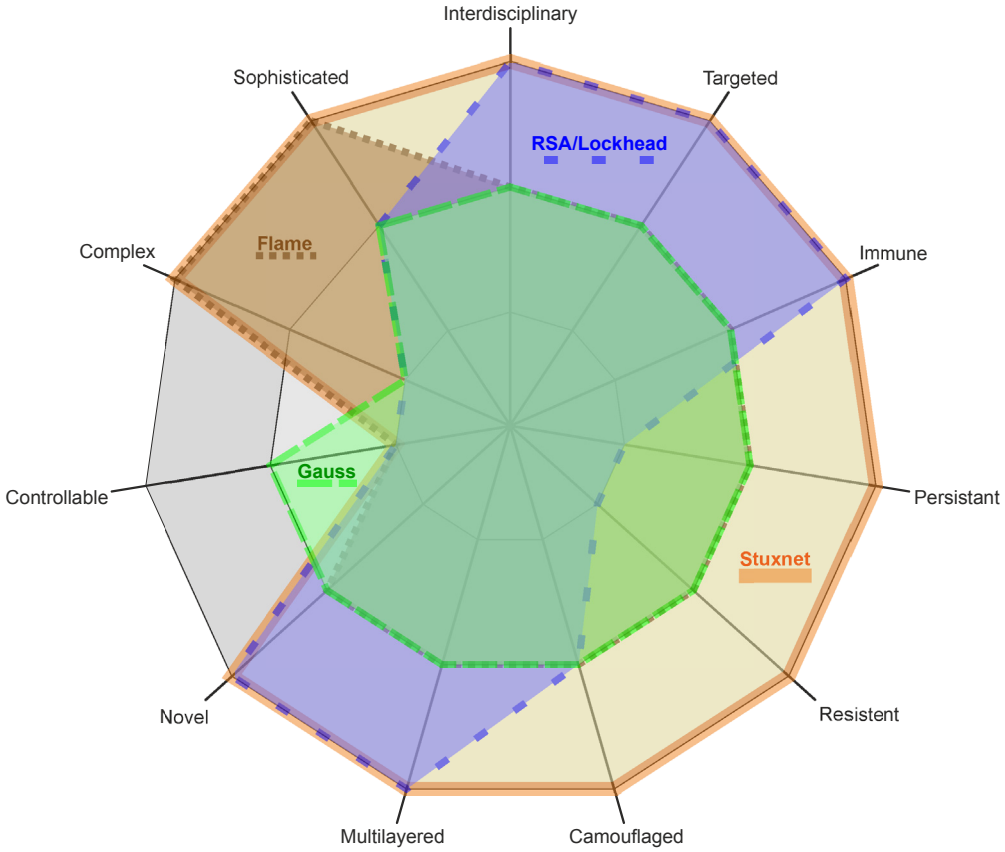

Figure 1. Classification of selected examples of smart attacks

4. Related Work

A deep understanding of attacks and related techniques is required to be able to identify shortcomings and vulnerabilities on the one hand and possible countermeasures and protection techniques on the other hand. Therefore, attacks have been under research for more than thirty years and a lot of publications about attack taxonomies have been published. See Figure 2 for an overview of attack taxonomies.

4.1 Overview of Current Taxonomies

Classifications, also called taxonomies, are the hierarchical structuring of a knowledge field into main groups and subcategories. Based on the allocation of the taxonomy, the nature of the different classes should be understood in detail. By applying them systematically, new weaknesses can be detected. According to Lindqvist and Jonsson, a taxonomy should focus on the following, properties (Lindqvist & Jonsson, 1997):

- The categories are mutually exclusive, there is no overlapping between the categories
- Clear and unambiguous classification criteria. A repeated classification should produce the same results
- Comprehensible and useful
- Comply with established terminology

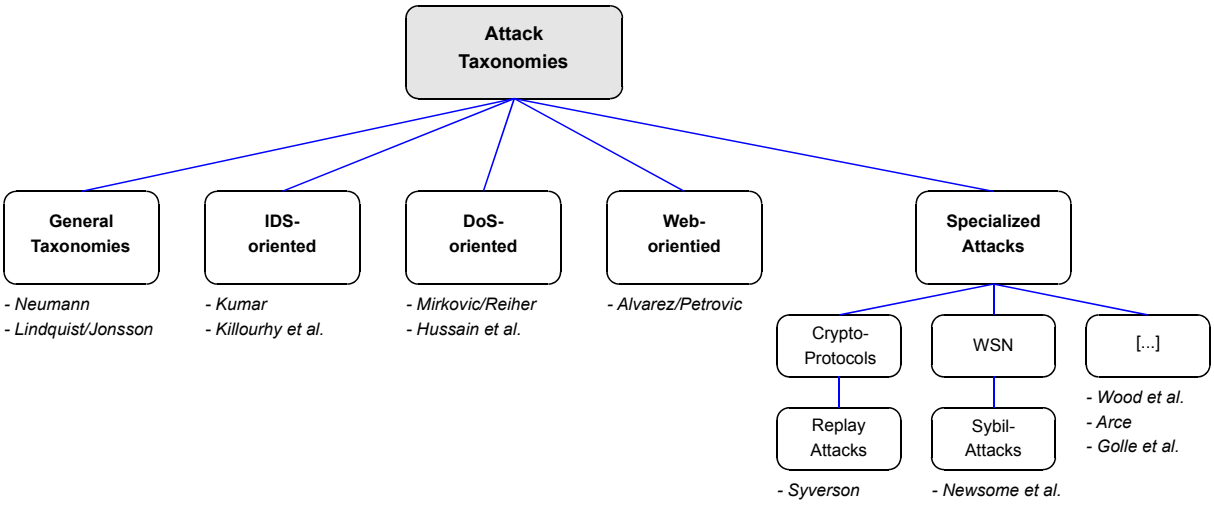

Figure 2. Overview of general and specialized attack taxonomies

Other, slightly different definitions can be found, e.g., see (Lough, 2001) or (Howard & Longstaff, 1998). Anyway, the main requirements for a taxonomy are quite similar everywhere.

The first classifications related to system security were published back in 1976 by Abbott et al. and in 1978 by Bisbey and Hollingworth, focusing on the classification of system flaws. While their taxonomies have some shortcomings (e.g., the classes are not mutually exclusive), the basic concepts have been taken on in later publications (see (Hansman & Hunt, 2005)). Today, numerous approaches for the classification of attacks can be found in the literature. Most often, one-dimensional and hierarchical allocations are used while multi-dimensional ones are quite rare (e.g., Perry and Wallich used two dimensions in 1984; the first dimension was defined by the attacker and the second by the kind of attack; see (Howard, 1997).

Although a lot of taxonomies with keenly different levels of detail have been proposed, none of them has been able to become generally accepted yet. A comprehensive analysis of security-related taxonomies published between 1974 and 2006 was given by Igure and Williams (Igure & Williams, 2008). There, two main groups are built, attack- and vulnerability-related taxonomies. Wrt. the focus on attacks of our publication, Figure 3 shows some examples of available classifications given in the corresponding group. Igure and William conclude that a lot of existing taxonomies are designed for specific areas (e.g., crypto protocols or wireless sensor networks, WSNs), but that they are not applicable in general (because of non-assignable attacks or missing dimensions). For example, Neumann presented a taxonomy based on 26 kinds of attacks which were grouped into nine categories like hardware misuses, bypasses and active misuse. Anyway, because of the lack of a common dimension, it is possible that other attack classes could have been left out (Igure & Williams, 2008). Because of that, Lindquist and Johnson used the attack result for the arrangement of attacks and built three classes, namely exposure, DoS and erroneous output. Another approach is used by Kumar (Kumar, 1995). There, the classes of the taxonomy are built based on the features of signatures (existence, sequence, partial order, duration, interval). While this taxonomy allows the detection of known attacks, an identification of the corresponding vulnerability is not possible. Therefore, the taxonomy can be used for security monitoring, but not for a system analysis (Igure & Williams, 2008). (Almgren, Lundin, & Jonsson, 2003) give a comprehensive overview of further Intrusion Detection System (IDS)-based taxonomies. Numerous other specialized attack taxonomies are available, e.g., focussing on DDoS (Mirkovic & Reiher, 2004), web attacks (Álvarez & Petrović, 2003) or investigating specific attacks like replay attacks or sybil-attacks (e.g., see (Syverson, 1994)).

Having a look on a more general classification of attacks with the idea of respecting their sophistication, a taxonomy can be based on the classification of computer system attacks given by Paulauskas and Garsva (Paulauskas & Garsva, 2006). The authors define 14 classes to describe computer system attacks. Some of the classes are self-explanatory, e.g., the affected layer of the ISO/OSI model, or the type of operating system. Other classes contain, e.g., the attack objective which subsumes for example gaining user or super-user privileges, but also aspects like malicious code execution or security policy violations. Effect type describes the technique or kind of exploited vulnerability, e.g., a virus, a buffer overflow or the use of nonstandard ports. The location of attack subject differentiates “inside local segment”, “between segments” as well as “physical access”, “system user privilege” and “system administration privilege” while the type of object location contains “local system”,

"local network", "global network", "wireless network" and "P2P network". For details about the particular classes as well as the not further described ones, see (Paulauskas & Garsva, 2006).

Based on their model, Paulauskas and Garsva use an attack severity numerical evaluation for enabling an automated data processing of the impact of an attack onto the computer system. The idea behind the numerical evaluation is to provide numbers which represent the respective attack. Based on the numbers, attacks can be grouped or compared with attacks in different networks. This attack description by the objective can be used, e.g., in Snort and by CERT organizations. Paulauskas uses five attack severity levels where level 1 is the most dangerous one. The subclasses of each main class of the computer system attack classification model are assigned to the severity levels, e.g., attack objective has seven subclasses (from "1.1 super-user privilege gain" up to "1.7 security policy violation") where 1.1 to 1.3 are assigned to severity level 1 to 3, 1.4 and 1.5 are assigned to severity level 4 and the remaining two to severity level 5. Anyway, this assignment is not stringent because the subclasses are several times not mutually exclusive: e.g., the class attack objective contains "1.1 super-user privilege gain" and "1.6 malicious code execution". While the first is the aim of an attack, the last is more a technique than an aim: The execution of malicious code is not an end in itself, but tries to exploit some vulnerabilities to gain specific privileges, to manipulate information or to disrupt a service (Denial of Service; DoS). Therefore, neither the subclass of attack objective nor the classes attack objective and effect type are mutually exclusive. This applies to further classes, e.g., the already described class location of attack subject contains items related to the location of the attack source but also items related to the credentials.

4.2 Shortcomings of Current Taxonomies

Most of the available taxonomies can hardly comply with the (ideal) requirements of Lindqvist. While the classification of Paulauskas is designed wrt. applicability and real-world usage, it can be used for a practical application even without fulfilling all requirements of a taxonomy completely. Anyway, having a look at Smart Attacks and classifying them based on these taxonomies, the result does not do justice to the special characteristics of these attacks. For example, while persistence (capability of keeping functionality over a long period of time) and being camouflaged are very important characteristics of Smart Attacks, these aspects get completely lost when applying the taxonomy. Also other taxonomies are not able to cope with sophisticated, modern attack types.

Therefore, we will present an enhancement of the taxonomy of Paulauskas which (i) overcomes the shortcomings within the classes wrt. mutual exclusiveness and completeness and (ii) which respects the special characteristics of sophisticated, modern attacks.

5. Revised Taxonomy for Smart Attacks

To overcome the shortcomings of current classification systems wrt. modern attacks, we present our revised attack taxonomy. Figure 3 gives an overview of the taxonomy.

Our revised taxonomy keeps the idea of "attack severity numerical evaluation" used by Paulauskas and Garsva to allow automated data processing. In contrast to the classification by Paulauskas, 17 classes are used at all; four of the original classes have been redefined and three classes have been added. In addition, the enumerations of some classes has been reordered: based on the idea that the most significant threat is allotted to the lowest number, some values are changed as noted below. Based on specific properties of the endangerments of a network or system, individual threats are not always identical. For example, examine two systems, a database storing secret construction plans and a control system of a power plant. While in the first case, a violation of the confidentiality of the secret data is the most important threat for the attack objective, prohibiting the system availability is the major endangerment in the second one (denying the control may result in the destruction of the power plant). Therefore, the concrete allocation of the threat levels to the items can be customized for specific systems or networks; on the other hand, such modifications may hamper or distort data exchange and automated data processing. This issue can be addressed by assigning an overall threat level to each classification as in the case of the Common Vulnerability Scoring System (CVSS): There, the scores ranging from 0 to 10 are built based on expert assessment. Utilizing such a score, a complete classification of an attack could be a vector $A = \{objective; detectability; \ldots; density; score\}$, for example $A = \{1.1; 2.3; \ldots; 17.2; 4\}$. By that, the endangerment given by the particular classes can be adjusted by an expert rating while keeping the principles of numerical evaluation.

In addition to changes within the items of some classes (ordering as well as concrete selection / composition), also two-dimensional evaluations have been introduced to respect the possibly attack vectors. For example, wrt. "type of the object location", the system type (e.g., local system or LAN) as well as the used medium (e.g., wired or wireless network) have to be considered.

In the following, the classes of our taxonomy are described in more detail.

Attack Objective: Seen from a strategic position, there are three elementary objectives for an attacker, namely violating confidentiality of information (e.g., stealing data), breaching integrity of information (e.g., modification of data) and prohibiting system availability. As already mentioned, the threat emerging from these objectives can differ wrt. the particular system or network, which can be addressed by the score value.

Attack Detectability: The most dangerous are specially crafted attacks, e.g., with malicious code developed specifically for one target. Because of their special design and the optimization for the target, security mechanisms like (next generation) firewalls, IDPSs and antivirus programs are ineffective. A combination of multiple, sophisticated attack vectors can also be hard to detect while "attack families" (e.g., based on the creation of malicious code by attack toolkits) may be detected by using heuristics in the detection engine (experience shows that powerful attack kits are able to generate code hardly detectable even by heuristics). Known attacks are, of course, most convenient to detect. E.g., signature-based techniques can be used to search for specific attack patterns.

ISO/OSI Layer: In contrast to all seven OSI layers used by Paulauskas, we make use of only three categories. Typically, attacks on the application layer are most dangerous (e.g., when executed over encrypted connections, most IDPSs are not able to investigate the traffic) while attacks on the network layer are comparatively easier to detect. Frequently, attacks on the physical layers are limited nowadays wrt. possible objectives. Looking at possible manipulations of COTS products, dangerous attacks may be possible on the physical layer, too. Therefore, the ranking of the categories may be subject to change depending on the considered network or system as already discussed before.

Target Type: If it is enough to hack an auxiliary device (e.g., a switch) instead of the actual target system, the attack may be even harder to detect. This is reflected in setting the auxiliary targets higher than the end devices.

Location of Attack Subject is an example for a two-dimensional matrix of the corresponding item list: the initial position of an attacker wrt. the system under consideration depends on (i) the physical position of the attacker and (ii) the initial access level (credentials) of the attacker for the system. The corresponding threat matrix expresses the degree of exposure of the respective combinations.

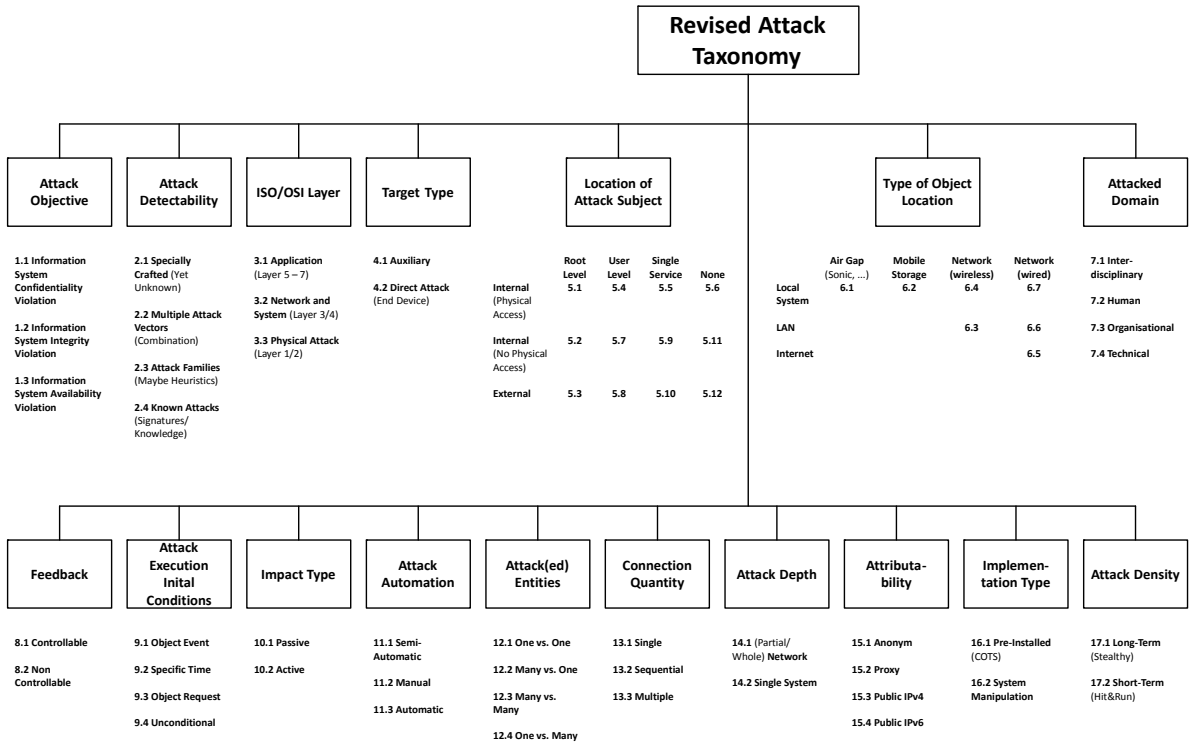

Figure 3. Revised attack taxonomy

Concerning the **Type of Object Location**, the target can be connected to a reachable network (wired or wireless) or isolated. In the latter case, the system may be reached by mobile storage devices or by even more sophisticated techniques to bridge the air gap (have a look at the recent discussion of using covert acoustical channels, e.g., see (Hanspach & Goetz, 2013)). Therefore, capabilities to bridge the air gap are treated as more dangerous than limited propagation possibilities.

The **Attacked Domain** can have a major influence on the severity of an attack. On the technical level, detection possibilities are given by the installation of security systems or the risk of noticeable system malfunctions during an attack (e.g., triggered by a faulty exploit). On the contrary, shortcomings on the organisational level can be even harder to detect. For example, insufficient measures for the safe disposal of confidential documents can result in divulging important information. Regarding the human source, effective and unremarkable social engineering can be done. Lastly, a combination of a careful information search in the different domains can be used to achieve an objective without attracting attention at all.

Feedback relates to the *controllability* of an attack by the originator. E.g., if a trojan horse can be updated and extended with new modules by the attacker after it has been installed in the target system, the possibilities to hide and resist are much higher.

Attack Execution Initial Conditions: Enabling an attack only if a specific event happens represents a serious danger. In that case, it can stay hidden most time, limiting the detection possibilities. This is also possible by activating a malware only after a special period or at a special point in time; anyway, the target may not be in the desired state for the attack our may not have the wanted information, lowering the possibilities of successfully executing the attack. An activation by request enables the possibility to stay hidden, but also opens up the possibility that the attack will not be activated if the attacker can't reach the system.

Impact Type: An attack can be active or passive, e.g., using exploits to penetrate a system or only sniffing on the wire. Of course, passive techniques are typically much harder to detect, therefore they are rated more dangerous than active ones.

Attack Automation: A semi-automated attack can be very dangerous, combining efficiency and the possibility to react and interact. Manual attacks can be controlled in depth, but typically are much slower while automated attacks could be error-prone (e.g., locking the system while executing an exploit).

With an increasing number of **Attack(ed) Entities**, normally also the chances for a detection of the attack rise.

Connection Quantity: Attacks can be executed over a single connection, a series of single connections over time (sequential) or by the use of parallel connections. Again, with an increasing number of connections, also the detection possibilities are rising.

Attack Depth: By affecting a network (fully or partially), an attack can resist and penetrate an environment more dangerously, than by influencing only a single system.

Attributability: The attribution of attacks is challenging (e.g., see (Koch, Golling & Rodosek, 2013; Mandiant, 2013)). When anonymizing networks like TOR are used, identifying the source of an attack is most difficult. Proxies are also challenging, although tracking is more likely possible. Public IP addresses are easier to identify, where (in theory) IPv6 addresses are better attributable than IPv4 addresses: while NAT is used extensively to mask numerous private IP addresses in IPv4, IPv6 provides the possibility to allocate a unique address for each device and system.

Implementation Type: Attacks can be executed onto up and running systems, e.g., by the execution of exploits - which is the typical case. On the other hand, malicious manipulations could have been done in advance, e.g., backdoors installed in COTS products. Pre-installed manipulations can be much more dangerous, because the (maybe detectable) installation process is not required any longer and also behaviour-based security systems can learn the initial bad behaviour of a new system as a benign one.

Attack Density: An attack can be executed in short-term horizon, trying to execute and complete as fast as possible even with an increasing risk of detection. On the other hand, stealth (paranoid) techniques can be used to stay as hidden as possible, expanding the attack over a long period of time.

6. Conclusion and Further Work

Smart Attacks can only be countered by a new and smart defence. Because current taxonomies were not able to represent and analyse the special characteristics of Smart Attacks, we proposed a new taxonomy for dealing with a new generation of Smart Attacks. By using the taxonomy, current shortcomings of Intrusion Detection and Prevention Systems can be identified. To close the current gaps, a combination and integration of different new

security mechanisms into the intrusion detection process has to be done. Here, our approach focuses on three elements: since especially the security report of Mandiant has illustrated that "90 percent of all computer attacks of China are located in one tower building in Shanghai", we propose the use of advanced geolocation for a geobased intrusion detection (e.g. inspecting new connections - originating from a location very close to where a recent attack was launched - in more detail). Based on that, we will illustrate our geolocation-aware Intrusion Detection Model. Furthermore, we will present our concepts on supervising COTS products (soft- as well as hardware), as both are lately used also in security environments, too, and pre-installed manipulations are hardly detectable at the moment. Finally, we will also show our concepts for similarity-based, multi-domain correlation to address behaviour-based intrusion detection without the need of a learning phase or any knowledge about neither the system respectively network to protect, nor the kind of attacks.

Acknowledgements

This work was partly funded by Flamingo, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

References

Almgren, M., Lundin, E., & Jonsson, B. E. (2003). *Consolidation and evaluation of ids taxonomies*. In proceedings of the eighth nordic workshop on secure it systems (nordsec 2003).

Alvarez, G., & Petrović, S. (2003). *A new taxonomy of web attacks suitable for efficient encoding*. *Computers & Security, 22*(5), 435-449. http://dx.doi.org/10.1016/S0167-4048(03)00512-1

Committee on National Security Systems. (2010). *National Information Assurance (IA) Glossary - CNSS Instruction No. 4009*. Retrieved from https://www.cnss.gov/Assets/pdf/cnssi 4009.pdf

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32. stuxnet dossier*. White paper, Symantec Corp., Security Response.

Fettke, P., & Loos, P. (2003). Classification of Reference Models: A Methodology and its Application. *Information systems and e-business management, 1*, 35-53. http://dx.doi.org/10.1007/BF02683509

Goodin, D. (2012). *Crypto breakthrough shows Flame was designed by world-class scientists*. Retrieved from http://arstechnica.com/security/2012/06/flame-crypto-breakthrough/

GReAT. (2013). *Gauss: Nation-state cyber-surveillance meets banking Trojan* (Kaspersky Lab Expert). Retrieved from http://www.securelist.com/en/blog/208193767/

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security, 24*(1), 31-43. http://dx.doi.org/10.1016/j.cose.2004.06.011

Hanspach, M., & Goetz, M. (2013). On covert acoustical mesh networks in air. *Journal of Communications, 8*(11). http://dx.doi.org/10.12720/jcm.8.11.758-767

Howard, J. D. (1997). *An analysis of security incidents on the internet 1989-1995* (Tech. Rep.). DTIC Document.

Howard, J. D., & Longstaff, T. A. (1998). *A common language for computer security incidents*. Sandia Report: SAND98-8667, Sandia National Laboratories. Retrieved from http://www.cert.org/research/taxonomy_988667.pdf

Igure, V., & Williams, R. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *Communications Surveys & Tutorials, IEEE, 10*(1), 6-19. http://dx.doi.org/10.1109/COMST.2008.4483667

Koch, R., Golling, M., & Rodosek, G. D. (2013). *Geolocation and Verification of IP-Addresses with Specific Focus on IPv6*. In 5th international symposium on cyberspace safety and security (css 2013) (pp. 1-20). Springer. http://dx.doi.org/10.1007/978-3-319-03584-0_12

Krypt3ia. (2012). *Apt: What it is and what it's not*. Retrieved from http://krypt3ia.wordpress.com/2012/02/10/apt-what-it-is-and-what-its-not/

Kumar, S. (1995). *Classiffication and detection of computer intrusions*. doctoral dissertation, Purdue University.

Lindqvist, U., & Jonsson, E. (1997). *How to systematically classify computer security intrusions*. In Security and privacy, 1997. proceedings., 1997 ieee symposium on (pp. 154-163). http://dx.doi.org/10.1109/SECPRI.1997.601330

Lough, D. L. (2001). *A taxonomy of computer attacks with applications to wireless networks*. doctoral dissertation.

Mandiant. (2013). *APT1 - Exposing One of China's Cyber Espionage Units*. Retrieved from http://intelreport.mandiant.com/Mandiant APT1 Report.pdf

Mirkovic, J., & Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53. http://dx.doi.org/10.1145/997150.997156

Nakashima, E. (2013). *U.S. said to be target of massive cyber-espionage campaign*. Washington Post. Retrieved from http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba story.html

Paulauskas, N., & Garsva, E. (2006). Computer system attack classification. *Electronics and Electrical Engineering*, *2*(66), 84-87.

Ponemon Institute. (2013, February). *Efficacy of emerging network security technologies*. Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-jnpr-network-security-report.pdf

Schneier, B. (2011). *Lockheed martin hack linked to rsa's securid breach'. Schneier on Security*. Retrieved May 30, 2011, from http://www.schneier.com/blog/archives/2011/05/ lockheed_martin .html

Symantec Corporation. (2011). *Industrial Espionage: Targeted Attacks and Advanced Persistent Threats (APTs)*. Retrieved from http://www.symantec.com/threatreport/topic.jsp?aid=industrialespionage&id=malicious code trends

Syverson, P. (1994). A taxonomy of replay attacks [cryptographic protocols]. *Computer Security Foundations Workshop VII,* 1994. CSFW 7. Proceedings (pp. 187-191).