2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Attack Trends in Present Computer Networks

Robert Koch, Björn Stelte, Mario Golling
Faculty of Computer Science
Universität der Bundeswehr München
D-85577 Neubiberg, Germany
{robert.koch, bjoern.stelte and mario.golling}@unibw.de

Abstract: An integral component of security mechanisms in company and governmental networks are Intrusion Detection Systems (IDS), which have been under intensive research for over 30 years. Unfortunately, even with these high-level security measures, the number of security incidents remains on a very high level or even rises. Therefore, for identifying the corresponding weaknesses, an in-depth knowledge of the various kinds of threats and state of the art attacks is necessary. While plenty of research about weaknesses and threats is available for special categories like wireless networks or sensor networks, research with respect to general networks, such as traditional wired networks, is widely neglected. However, the most important real-world harassment affects these networks.

In this paper we present important attack vectors based on evaluations presented in the latest technical reports, such as McAfee, M86, Symantec and corresponding academic work. For example, insider attacks and attacks on the application layer are hardly detectable by current systems, presenting challenges for intrusion detection.

To analyse the shortcomings of current IDSs, corresponding taxonomies are presented and their usability with respect to the new attack vectors is discussed. Based on this, an enhanced taxonomy is presented which addresses the current shortcomings.

Using the new taxonomy, the weaknesses of current systems are discussed, explaining the high number of serious security incidents. This knowledge can be used to design a more efficient, next-generation IDS.

Keywords: *attack trends, intrusion detection, taxonomy, next generation IDS*

1. INTRODUCTION

Current solutions for securing networks are mainly packet filters (PF), application layer gateways (ALG) and IDS. PF and ALG are used to control traffic that enters a network and leaves a network based on packet information. They filter malicious network traffic according to predefined rule sets. Known shortcomings of PF and ALG are generally [1,2]:

- They cannot protect against attacks that bypass them, such as tunnelled traffic.
- They do not protect against threats caused by internal attackers.
- They hardly protect against the transfer of malicious code.

To overcome some of these shortcomings IDSs are used in combination with PFs and ALGs. IDSs are primarily for learning, detecting and reporting attacks as they happen in real time. Basically, two types of IDS are available: signature-based (misuse) and statistical-based (anomaly) detection. Signature-based IDSs use pattern matching to detect signature traces in network traffic. A detection of attacks is only possible for known attack signatures. Signature-based IDSs are considered to have a low false positive, but unfortunately a relatively high true negative, detection rate. In contrast, anomaly-based IDSs are able to detect new kinds of attacks but at the price of higher false positive rates. State-of-the-art IDSs are based on traditional taxonomies which hardly reflect recent attack vectors. Based on recent reports, such as [3-7], we have identified important threats for security solutions of traditional networks.

In Section 2 we will present these threats, which are application layer attacks, zero-day exploits, social engineering, targeted attacks, dissemination routes, data leakage and insider attacks, encryption, IPv6 attacks and attacks on and with the use of cloud computing. A taxonomy for intrusion detection is presented in Section 3 and the shortcomings of current systems are discussed. Finally, the paper is concluded in Section 4.

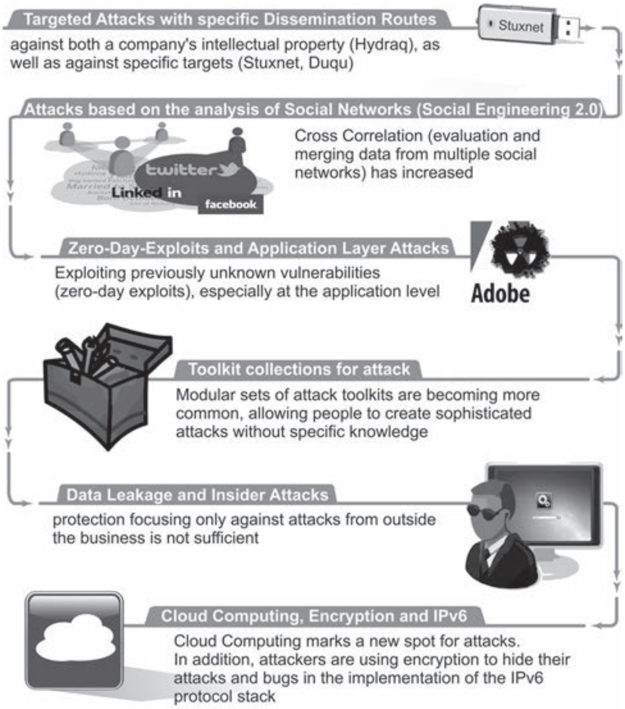
2. ATTACK AND TECHNICAL TRENDS

Nowadays, economic crime affects many large companies [8]. 61 percent of these companies reported that they have become the victims of economic crimes in the past two years. On average, these companies report eight cases a year. In addition to high financial losses, substantial non-pecuniary damage is reported: loss of reputation, damage to business and loss of morale.

Symantec recorded more vulnerabilities in 2010 than in any previous year since starting their internet security thread report[6]. While many attacks are directed at large enterprises and governmental organisations, they can also target small and medium businesses and individuals. Similarly, senior executives are not the only employees being targeted. In most cases, a successful compromise requires only victimising a user with just limited access to network or administrative resources. A single negligent user or unpatched computer is sufficient to give attackers a beachhead into an organisation from which to mount additional attacks on the enterprise from within, often using the credentials of the compromised user [34].

Based on annual security reports from Panda [4], McAfee [9], M86 Security [10] and Symantec [5-7], we have identified the following attack trends, summarised in Figure 1 and discussed in the next paragraphs: application layer attacks, zero-day exploits, social engineering, targeted attacks, dissemination routes, data leakage and insider attacks, encryption, IPv6 attacks, and attacks on and with the use of cloud computing.

FIGURE 1. TODAY’S ATTACK TRENDS



Targeted Attacks with specific Dissemination Routes

against both a company's intellectual property (Hydraq), as well as against specific targets (Stuxnet, Duqu)

Attacks based on the analysis of Social Networks (Social Engineering 2.0)

Cross Correlation (evaluation and merging data from multiple social networks) has increased

Zero-Day-Exploits and Application Layer Attacks

Exploiting previously unknown vulnerabilities (zero-day exploits), especially at the application level

Toolkit collections for attack

Modular sets of attack toolkits are becoming more common, allowing people to create sophisticated attacks without specific knowledge

Data Leakage and Insider Attacks

protection focusing only against attacks from outside the business is not sufficient

Cloud Computing, Encryption and IPv6

Cloud Computing marks a new spot for attacks. In addition, attackers are using encryption to hide their attacks and bugs in the implementation of the IPv6 protocol stack

A. Application Layer Attacks

Each communication layer has its own security challenges. In particular, the application layer with its variety of supported protocols offers many vulnerabilities and access points for attackers and in return makes it very difficult to fend off attacks. Furthermore, attacks on this layer are especially attractive to attackers, since this layer offers direct access to information without for example the need for a cumbersome extraction of the payload from the package.

Botnets are one of the most important security harassments today. Numerous systems like personal computers are misused and remote-controlled by the installation of local agents. Because of their placement within the network (which is typically secured against access from outside), Bots are able to communicate to an external server taking commands and executing attacks. Botnets are hard to detect for traditional IDSs, but even more complex because of encrypted communication methods and distributed control systems of modern botnets. Another important fact is that more than 70% of the current attacks are conducted on the application layer. Therefore, they have to be evaluated using the packet payload. On the other side, encryption technologies like TLS are more and more widespread, hampering the application of payload inspection methods (deep packet inspection, DPI).

Due to increasingly complex application software, like browsers with their numerous Add-Ons, extensive vulnerabilities are available and used intensely by attackers.

Some of the relevant application layer attacks are [7]:

- Scripting vulnerabilities
- Cookie poisoning
- Hidden field manipulation
- Parameter tampering
- Cross-site scripting
- SQL injection

In addition, traditional attack techniques like buffer overflows are also used to execute attacks on the application layer. Even techniques like address space layout randomization (ASLR), which makes sure that system functions are located at randomly chosen addresses (instead of being located at the same memory address anytime), or sandboxing can be overcome by sophisticated attacks like JIT-spraying. According to security reports published by Symantec, since a few years ago the proportion of application layer attacks is over 70% in comparison with the total amount of all attacks, and still increasing, therefore displacing traditional operating system and network layer-oriented attacks [6,7,11].

B. Zero-Day Exploits

A Zero-Day exploit occurs when a flaw is discovered in software and a programme exploiting the vulnerability is available before or on the day the vendor gets to know about the flaw.

So-called "file format vulnerabilities" remain the first choice for Zero-Day exploits. In this regard, most attacks relate to Adobe PDF, Flash Player and Microsoft Office Suite (PowerPoint, Excel and Word) and the corresponding third party add-ons (which make the patching process more complicated and thus increases the options for potential attackers). The time vendors need for developing patches against Zero-Day vulnerabilities is often too long, for instance because they want to stick to so-called Patch-Days instead of releasing updates individually. Often vendors are unable to fix vulnerabilities quickly due to a lack of security-by-design. In software engineering, this means that the software has to be designed from the ground up to be secure.

All in all, Zero-Day vulnerabilities remain one of the major threats and, therefore, require additional security measures.

C. Social Engineering

Social engineering was used intensely in the 1980s, for example by well-known hackers like Kevin Mitnick. Social engineering describes a non-technical kind of intrusion that relies heavily on human interaction and often includes fooling other people to dig normal security measures. Social engineering is a key component for today's and upcoming attacks, utilising the weakest link of the chain, the user. In distinction to other technical measures, here, attackers may seem unassuming and respectable (possibly a new employee or repairman and sometimes even with some credentials to prove the faked identity).

One of the most known attacks in the field of social engineering is called the phishing attack.

It uses emails or malicious websites to gather personal information by claiming to be a trusted organisation.

Other techniques, such as scareware, rogueware, and ransomware-attacks, are also known. Scareware includes several types of scam software with malicious payloads, or limited or no benefit, often sold to consumers by unethical business practices. The approach uses social engineering to cause shock, fear or the perception of a threat, usually to unsuspecting users. Rogueware is a form of computer malware that causes users to pay money for the faked or simulated removal of malware. Ransomware is computer malware that holds a computer system, or the data contained therein, as a hostage to its users with a demand for ransom for the restoration.

Awareness of the risks and available safeguards is the first line of defence for security of information systems and networks. Some problems which need to be addressed in the field of social engineering are [12]:

- People do not understand the technology
- People are caught off guard
- People trust known people (co-workers)
- People trust the system
- People are in a hurry
- People get careless

D. Targeted Attacks

The times of large-scale virus attacks have mostly passed. Some of the biggest threats to the security of corporate networks nowadays are targeted attacks. Here, in contrast to other attacks, the design is specifically tailored to individuals or organisations. Thus, on the one hand the probability that the victim actually opens the e-mail is increased and, on the other hand, existing protective measures are easier to be bypassed. Therefore, the attacker starts with identifying potential victims by making use of public available data like the website of a company or the data available in social networks like Facebook or Twitter. Many people are careless when dealing with sensitive data, especially in the context of social networks. Due to the personal data found in the network an individualised email concerning a current topic and containing a malicious payload is generated and sent to the victim. If the victim opens the payload, than the computer can be used and controlled by the attacker.

Since 2005, an increase in targeted attacks on federal agencies and industrial espionage can be observed [8]. Public attention was especially gained in 2007, when numerous computers in federal ministries and the German Chancellery were infected with spy-ware as a result of a targeted attack. Recently, some methods have emerged that allow an even more sophisticated profiling, enabling an attacker to start more advanced targeted attacks or to improve the efficiency of spam campaigns. Here, the profiles of the different social networks are evaluated by special procedures and automatically linked between each other to enrich the information (cross-correlation). It has been demonstrated that – based on a list of about 10.4 million e-mails – the automatic user profiling of more than 1.2 million user profiles, including the linking between different social networks, is possible.

Other important examples of targeted attacks are the Hydraq Trojan (also known as Aurora) which affected Google and several other large companies in 2009, or the attack on RSA in 2011, which was compromised by attackers using this Trojan [13]. In Aurora, a Zero-Day vulnerability which affected three versions of Internet Explorer and various Windows operating systems was used. The attackers sent targeted emails to people of high-ranking management who had privileged access rights to various applications [4]. Afterwards, the malicious code was used to access and steal information from Gmail accounts. The attack on RSA and the consecutive attacks on Lockheed Martin and other US defence contractors are some of the latest and most sophisticated examples of a targeted attack. First, the network of RSA was attacked by the use of social networks and a vulnerability in Adobe Flash [14]. In the next step, data about employees of the company was collected and used to send personalised phishing emails. The emails contained a malicious spreadsheet which exploited a Zero-Day vulnerability in Adobe Flash and enabled remote access to the attackers. By that, information about 40 million two-factor authentication accounts of SecureID was stolen. After that, malware and phishing attacks were used to link tokens to end-users [3]. Based on this association, the consecutive attacks on Lockheed Martin and other companies were carried out by compromising the SecurID accounts.

E. Dissemination Routes

The dissemination routes of malicious software are not restricted to networks like the Internet or services like email. Just like at the beginning of the development of malicious software in the mid-80s, data storage media is an important method of distribution. The formerly used floppy disks have been replaced by cheap memory sticks with high capacity. Because of the use of the autorun-functionality, an infection can be automated easily. For example, promotional gifts like USB-sticks given away at trade shows are popular instruments [34]. By connecting the stick to a computer, a Trojan – previously placed on the stick – installs itself onto the system [34]. Therefore, malicious code is injected directly into the target system or inside a network, bypassing the security systems.

With the help of this offline-propagation method, formerly secure systems and networks like Supervisory Control And Data Acquisition Systems (SCADA) can also be compromised, as demonstrated by the well-known example of Stuxnet [34].

In addition, the attack tool’s automation level and their sophistication continue to improve. No technical in-depth knowledge is needed to create new, unknown and malicious software any longer [15]. The first attack kit named Virus Creation Lab in 1992 provided basic functionality, but state-of-the-art kits like Mpack and Nukesploit or Command-and-Control toolkits such as Spy Eye or Zeus are highly professional [16]. These toolkits are sold for several thousand Dollars with different service levels. Due to their professionalisation and commercialisation, these easy-to-use attack kits can produce serious damage.

F. Data Leakage and Insider Attacks

The term data leakage prevention (DLP) refers to the protection against a suspected, but not measurable and sometimes not even detectable, sharing of information to unwanted recipients [17]. In contrast to insider threats, data leakage includes accidental or unintentional data loss in addition to malicious theft [18]. Numerous scandals about data loss and data theft have gained public interest in the recent past [19, 20]. While governments and militaries were in the spotlight of attacks during the cold war, today, the industry is the most important target for espionage. For example, a study of the consultancy PricewaterhouseCoopers and the University Halle-Wittenberg specified that the economic loss for each individual business company in Germany was on an average about 5.57 million Euros in 2009. Sixty-one percent of all large-scale enterprises had been hit by business crime in the past two years [8].

Regarding the protection against industrial espionage and information flows out of the company, many businesses focus only on protection against attacks from outside. In times of rising fears of losing one's job, permanently growing workloads and often a lack of appreciation of performance, many employees are increasingly willing to enrich themselves at the expense of the company they are working for. Loyalty to the employer is no longer always natural. A loss of wages is thus more often compensated by a small additional income. The particular endangerment by the insider is based on the authorised access and their knowledge about the security mechanisms. The numbers of insider threats compared with all incidents of data loss differ keenly from 17% up to 80% [21, 22]. When investigated in a study conducted of German companies about types of employees who were specifically responsible for the espionage, first and foremost, the clerks (who usually have many access rights including access to sensitive documents and information) with 31.4% were identified, followed by skilled workers with 22.9% and 17.1% within the management. Together these three areas caused about two thirds of the entire data leakage of the company.

Countermeasures to avoid data leakage are quite complex. For example, all files that are read by or written to all USB devices must be logged so that each change to sensitive data is traceable. Furthermore, with the use of a unique serial number, a USB stick can be assigned to only one specific user. As the stick is encrypted, reading the data on the stick is only possible for colleagues of the department or superiors.

G. Encryption

Cryptography was invented to protect communication; this is the reason why militaries in the world and scientists have developed it. Even the protection of stored data can be seen as a form of communication [23], here with the addition that each key must exist as long as the encrypted data exists. The storage of these keys is thus as important as the storage of the data. Therefore, encryption is not reducing the number of secrets that must be stored safely; it is only making their size smaller. In the past, keys have been stored in the human brain and by that in a way that is not connected to a network (and thus kept safe in principle), but this approach does not work for the Internet today. Often, keys are needed for the communication between systems in an automated fashion; shared secrets must be stored, etc. So, keys can no longer be saved in the brains of people. They must be stored on the same computer that hosts the data or at least on a network-wide available system – and that is a lot riskier.

Beside the challenges regarding the security of the keys itself, the usage of encryption rises generally. Not only are more and more services and servers offering encrypted access to their customers, the attackers are also making increasing use of cryptography to hide and to secure their activities. For example, the latest botnets use encrypted communication channels to hide their presence from IDSs or next generation firewalls.

The trend towards the use of encryption will also be enforced with the broader application of IPv6. This will have a significant impact on the applicability of security devices and mechanisms and the detectability of attacks.

H. IPv6

At the moment, due to missing IPv6 security features in routers, firewalls and other critical network infrastructures and the lack of IPv6 testing and experience, many Internet providers tend to slowly migrate from IPv4 to IPv6, or at least they deploy IPv6 parallel to IPv4. A recent study showed a percentage of IPv6 traffic of just 0.03% compared with 0.002% from the previous year [24]. Nevertheless, the amount of IPv4-to-IPv6 tunnels will increase and it is still not clear whether all of these tunnels are implemented correctly. Some have the view that attacks that make use of IPv4-to-IPv6 tunnels to conceal the attack are already known.

IPSec is a mandatory component of IPv6 and is implemented using the authentication header and the Encapsulating Security Payload extension header [25]. In February 2011, the last address block of IPv4 was assigned [26]. The lack of IPv4 addresses on the one side and the increasing number of new devices on the Internet on the other side, for example mobile devices like smartphones, will speed-up the utilisation of IPv6 in the near future and, therefore, also the even wider distribution of encryption as mentioned above.

I. Cloud Computing

Many people and organisations are nowadays using cloud services to take advantage of convenience and attractive pricing (e.g., pay-as-you-go financing).

Nevertheless, there are valid security concerns including lack of control of data, downtime due to an outage and lack of visibility as already outlined in [33]. Despite excellent security practices employed by many cloud providers, the fact remains that these services are likely to be prime targets. During 2011, as mentioned in [10], Sony’s PlayStation network was hacked, leading to a shutdown in the service that affected about 77 million users. LastPass, a web-based password management company, also had its system breached, resulting in the necessity for all users to change master passwords [33]. Cloud service providers are huge targets. Since the data is concentrated, and the systems are standardised, a successful breach could yield a lot of valuable data for an attacker. For these reasons, it is predicted that more high-profile attacks on cloud service providers are to come in 2012 [10].

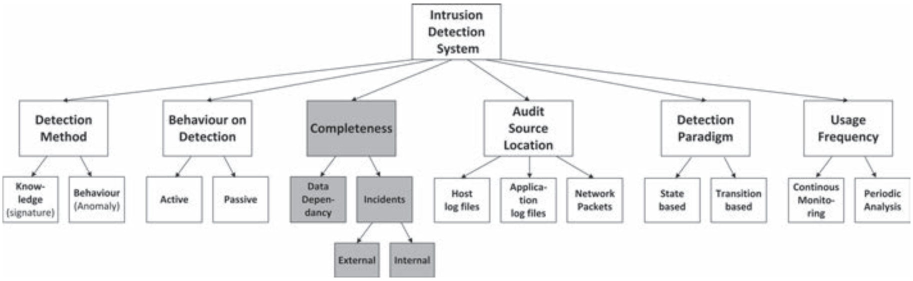
In addition it has been demonstrated, for instance in [35], that attackers can make use of cloud services for purposes like breaking encryption using tools, like the so called ‘Cloud Cracking Suite’.

3. TAXONOMY

To understand the origin of the security incidents respectively the shortcomings in the detection process, current IDSs, can be evaluated by a taxonomy. A classification or taxonomy is a hierarchical structure of a field of knowledge into groups. The classification has to be made in a manner that several properties are satisfied (e.g., [27, 28]): mutual exclusiveness, completeness, traceability, convenience, clarity and acceptance. The divisions are used, for example, to investigate new systems ordered by weaknesses.

No generally accepted taxonomy is available for the allocation of IDSs, therefore, various classifications of very different levels of detail can be found in the literature. The taxonomy published by Debar et al. [29] is widely used: The most common characteristic is the detection method, behaviour- (anomaly) or knowledge- (signature) based. The behaviour of detection can be active or passive while the audit source location can be the host or application log files or network packets. While the detection paradigm can be state- or transition-based, the frequency of usage can be continuous monitoring or a periodic analysis. With respect to present attacks and technical trends, this division is not sufficient for the analysis and evaluation of today's IDSs. Especially, the aspect of the completeness of the evaluation must be taken into consideration for modern systems because of the increasing amount of traffic which is encrypted and is, therefore, not analysable by most IDSs. Because of this, we enhanced the current taxonomies with the category "completeness" and the corresponding sub-levels "data dependency" and "incidents" (see Figure 2). While the first one describes the dependency of an IDS to have access to the communication data, especially the payload of the network packets, the latter one considers the detectability of attack sources, both external and insiders.

FIGURE 2. CLASSIFICATION OF IDS BASED ON THE TAXONOMY OF DEBAR AND EXTENDED WITH THE CATEGORY COMPLETENESS



Also, the categories like social engineering, targeted attacks or insider attacks are not represented. Even though this is not the original goal of the (technical) IDS taxonomies, these are the most important attacks today, thus having an high influence on the assessment of IDSs. Numerous other taxonomies exist, e.g. the comprehensive classification by Sabahi and Movaghar [30], which includes aspects like the environment, or the taxonomies of Sundaram [31] and Bolzoni [32] which are specialised on a fine subdivision of the detection behaviour respectively, a specialised taxonomy for anomaly-based systems. Anyway, none of the existing taxonomies are able to reflect the current attack trends and, therefore, cannot give a meaningful evaluation of the performance of today's IDSs.

Regarding the attack and technical trends identified, the following requirements must be fulfilled by a modern IDS:

- A complete analysis of the network traffic must be provided, independent from the data layer and from protective measures like payload encryption.

- Several characteristics of modern attacks exploit human weaknesses, e.g. when using social engineering methods or targeted attacks. Also bots, which are installed on systems of e.g. a company network (therefore, already inside the trusted network) or activities by insiders can be difficult to detect. These are properties which can be hardly detectable on a technical layer. Therefore, the capabilities of an IDS must comprise detection methods for attacks from the outside as well as irregularities of any kind from the inside, which typically will only possible by sophisticated anomaly-based techniques.

The shortcomings of current taxonomies and the abstract enhancement with the category "completeness" emphasise the central challenge of today's intrusion detection: the sophisticated and advanced attack techniques make use of all levels of abstraction – from technical aspects to human weaknesses. Therefore, some important attack vectors are hardly detectable with purely technical procedures. Behaviour-based detection systems are mandatory to overcome the current shortcomings, but also with these techniques, the completeness of the detection with respect to the possible attacks remains a crucial factor which has to be evaluated for every IDS in depth.

4. REMARKS

As already reported in [33], the Internet has revolutionised our social and business habits today. It has evolved from a network of computers and information into a network of people. The future Internet will consist of dynamically scalable and virtualised resources, which will be provided by providers as a service over the Internet. Aside from the obvious socio-economic aspects, also the technical side will change considerably. Due to the fact that the number of "services over the Internet" will increase tremendously and get more and more important as new business models, the providers of the future Internet will need to cope with new problems.

They will not only have to solve scalability and availability problems, but more importantly new security issues will arise and so new kind of attacks on the future Internet will be feasible. Key challenges in such a highly complex environment where data and services are also located somewhere in "clouds" are security, privacy and trust. The term "services over the Internet" implies that not only the data of the end users has to be encrypted, but also the whole network communication from end user to service providers. This claim for encryption is not only to justify the end user acceptance of services. Legally, regulations like BASEL II and most EU and national data privacy laws mandate that firms are to encrypt information transferred over the network when using services provided in the future Internet [33].

The emergence of new technologies and services, as well as trillions of devices and petabytes of data to be processed and transferred, mean that we have to deal with new threats and vulnerabilities, in addition to handling the remaining old ones. One must cope with attacks on the networks, but well-established IDSs and Internet early warning systems (IEWS) will not defend anymore, because of the encrypted packet payload [33]. The provider has no chance to decrypt the packet payload since the decryption key is not available and de- and encryption of millions of packets is too resource devouring.

Since neither the Internet, nor the future Internet consist only of national networks and national providers, the described problem needs to be addressed on a multinational level. Services are already offered nowadays to the end users without the information where the services or parts of the services are located (e.g. cloud computing). Nor is the end user interested in the service location but only in the availability and the safeguarding of the service. National and international providers need expert knowledge in how to secure provided services to end users and how to detect and prevent next-generation networks attacks.

5. CONCLUSION

Even if firewalls and state-of-the-art IDSs are in place in today's company networks, the number of incidents remains on a high level and new incidents are reported on a day-to-day basis. Several aspects have been identified which are responsible for the bad performance of current security systems: more and more attacks are targeted attacks and specifically designed and social engineering is used to bring the victim to execute the malicious operation. By the use of, for example, memory sticks, secured and isolated systems and networks can also be attacked. Application layer attacks, an increasing number of Zero-Days and the insider threat are further tendencies. The specific characteristics of these trends cannot be reflected by current taxonomies, therefore, hampering the development of new security systems and devices. The human being remains the weakest link of the chain, enabling sophisticated attacks where the legal user is manipulated to execute the disguised attack by himself with his authorised access and without realising the subjacent attack. To overcome these shortcomings, new concepts for the support and comprehension of users into the security processes are necessary.

REFERENCES:

[1] S. Jin, Y. Wang, X. Cui, and X. Yun, "A Review of Classification Methods for Network Vulnerability," In *Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics*. IEEE, October 2009, pp. 1171–1175.

[2] V. M. Igure and R. D. Williams, "Taxonomies of Attacks and Vulnerabilities in Computer Systems," In *IEEE Communication Surveys, ser. IEEE Communication Surveys and Tutorials*, IEEE, 2008, vol. 10, pp. 6–19.

[3] Reuters, *Hackers breached us defense contractors*, [Online]. Available: http://www.terminalx.org/2011/05/hackers-breached-us-defense-contractors.html#axzz1QCJWtZJz, May 2011.

[4] Pandasecurity, *Annual report PandaLabs 2010*, Tech. Rep., 2010. [Online]. Available: http://www.pandasecurity.com.

[5] M. Fossi et al., *Symantec Global Internet Security Threat Report*, Symantec Corporation, Tech. Rep. XV, April 2010.

[6] M. Fossi et al., *Symantec internet security report trends for 2010*, Symantec Corporation,350 Ellis Street, Mountain View, CA 94043 USA, Tech. Rep., April 2011.

[7] M. Fossi et al., *Symantec internet security report trends for 2011*" Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043 USA, Tech. Rep., April 2012.

[8] K.-D. e. a. Bussmann, *Wirtschaftskriminalität 2009*, Pricewaterhouse-Coopers, Martin-Luther-Universität Halle-Wittenberg, Tech. Rep., September 2009.

[9] M. Labs, *McAfee threat predictions 2012*, McAfee Corporation, 2821 Mission College Boulevard, Santa Clara, CA 95054 USA, Tech. Rep., Jan 2012.

[10] M86 Security, M86 *Security Labs: Thread predictions 2012*, 8845 Irvine Center Drive, Irvine, CA 92618 USA, Tech. Rep., Jan 2012.

[11] M. Fossi, *Symantec internet security report trends for 2009*, Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043 USA, Tech. Rep., April 2010.

[12] ENISA, *A Users' Guide: How to Raise Information Security Awareness*, European Network and Information Security Agency, Tech. Rep., 2006.

[13] EMC, *Open Letter to RSA SecurID Customers*, [Online] Available: http://www.rsa.com/node.aspx?id=3891.

[14] M. Kobie, *Rsa blames flash flaw and social media for attack*, [Online] Available: http://www.pcpro.co.uk/news/security/366532/rsa-blames-flash-flaw-and-social-media-for-attack.

[15] J. McHugh, A. Christie, and J. Allen, *"Defending yourself: The role of intrusion detection systems"*, in *Software*, IEEE, 2000, vol. 17, no. 5.

[16] M. Fossi, *Symantec Report on Attack Kits and Malicious Websites*, Symantec Corporation, Tech. Rep., 2010.

[17] P. Papadimitriou and H. Garcia-Molina, "Data leakage detection," in *Knowledge and Data Engineering, IEEE Transactions on*, vol. 23, no. 1, pp. 51 –63, Jan. 2011.

[18] M. McCormick, "Data Theft: A Prototypical Insider Threat," in *Advances in Information Security*, vol. 39, no. 1, pp. 53–68, April 2008, ISBN-10:0-387-77321-5.

[19] M. Simons, *Ministry of Defence in new data loss scandal*, [Online] Available: http://www.cio.co.uk/news/3225/ministry-of-defence-in-new-data-loss-scandal, October 2008.

[20] Backup-Technology, *Data loss incident affects NASA*, [Online] Available: http://www.backup-technology.com/5451/data-loss-incident-affects-nasa/, December 2010.

[21] KPMG, *e-Crime-Studie 2010*, [Online]. Available: http://www.kpmg.de/Themen/21481.htm, 2010.

[22] W. e. a. Baker, *2011 Data Breach Investigations Report*, Verizon Business, Tech. Rep., [Online] Available: http://www.verizonbusiness.com, 2010.

[23] B. Schneier, *Secrets and lies: digital security in a networked world*, John Wiley, 2000.

[24] C. Labovitz, *Six Months, Six Providers and IPv6*, [Online] Available: http://asert.arbornetworks.com/2011/04/six-months-six-providers-and-ipv6/, 2011.

[25] D. Kaushik, *Ipsec & ipv6 - securing the nextgen internet*, [Online] Available: http://ipv6.com/articles/security/IPsec.htm, 2008.

[26] M. Ermert, *Ipv4-adressen: Abschiedsgrüße, Mahnungen und Pappschilder*, [Online] Available: http://www.heise.de/netze/meldung/IPv4-Adressen-Abschiedsgruesse-Mahnungen-und-Pappschilder-1183204.html, 2011.

[27] J.D. Howard and T.A. Longstaff, *A Common Language for Computer Security Incidents*, Technical report, Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550, 1998.

[28] S. Jin, Y. Wang, X. Cui, and X. Yun, "A Review of Classification Methods for Network Vulnerability," in *Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics*, pages 1171–1175. IEEE, Oktober 2009.

[29] H. Debar, M. Dacier, and A. Wespi, *"A Revised Taxonomy for Intrusion-Detection Systems"*, Technical report, IBM Research, Zurich Research Laboratory, 8803 Rüschlikon, Switzerland, 1999.

[30] F. Sabahi and A. Movaghar, "Intrusion Detection: A Survey," in *Systems and Networks Communications*, 2008. ICSNC '08. 3rd International Conference on, pages 23–26. IEEE Computer Society, Oktober 2008. DOI 10.1109/ICSNC.2008.44.

[31] A. Sundaram, *An introduction to intrusion detection*, Crossroads, 2(4):3–7, April 1996. DOI: http://doi.acm.org/10.1145/332159.332161.

[32] D. Bolzoni. *Revisiting Anomaly-based Network Intrusion Detection Systems*. PhD thesis, University of Twente, 2009. DOI: 10.3990/1.9789036528535.

[33] M. Golling and B. Stelte, "Requirements for a future EWS-Cyber Defence in the internet of the future," In *3rd International Conference on Cyber Conflict (ICCC)*, IEEE, 7-10 June 2011, pp. 135–150.

[34] R. Koch, "Towards next-generation Intrusion Detection," In *3rd International Conference on Cyber Conflict (ICCC)*, IEEE, 7-10 June 2011, pp. 151-168.

[35] T. Roth, *Breaking encryption in the cloud: GPU accelerated supercomputing for everyone*, Black Hat DC 2011, [Online], Available: http://blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html.