IT-Security Upgrade with Advanced Intrusion Detection Systems: A Cost/Benefit Analysis

DIPLOMARBEIT

zur Erlangung des Grades eines Diplom-Ökonomen
der Fakultät Wirtschaftswissenschaften der
Universität Hannover

vorgelegt von

Götz Johanning

[redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner
Hannover, den 30.06.2005

Index

1 Introduction

1.1 Problem and Motivation

In the IT milieu, an alteration from an isolated working environment to workplaces connected to the Internet has taken place within the last ten years. This involved a migration from centrally maintained mainframes to user administered desktop PCs. These changes challenge IT-security and pose possible threats to the IT environment. The use of object-oriented techniques which permit a prompt and unpretentious execution of transmitted programs or documents on many target devices provokes a new opportunity for the distribution of malicious software [THO04, 02:19]. As a result of the installation and operation of object-oriented techniques, computers and computer networks become more vulnerable to attack attempts and usually offer little protection against arising unwanted activities [THO04 14:40].

In principle, classic security procedures are prophylactic by limiting access. Access can be refused to unknown users or computers, but offers only little or no protection against manipulated computer addresses or forceful intrusions by guessing passwords. Limiting access only offers protection against known safety problems. The result of a study [OPM02] according to which an enterprise network is intruded every eight seconds indicates the severity of the situation.

Traditional safety technologies as, for example, firewalls[1] and intrusion detection systems (cf. Chapter 2) are used in order to protect endangered systems and networks against attackers as much as possible. However, these technologies have a decisive disadvantage: they are comparatively static and can only be adapted to altering threats with a time delay. Consequently, an attacker is always one step ahead of a defender. Attempts to reduce or even to eliminate the lead of an attacker with the help of traditional security technologies have not been possible to this day.

---

[1] Network firewalls are devices or systems that control the flow of network traffic between networks employing differing security postures. In most modern applications, firewalls and fire wall environments are discussed in the context of Internet connectivity and the TCP/IP protocol suite [JWA02, p. 3].

Honeypots (cf. Chapter 3) have emerged with the aim to minimize an attacker's advantage and to gain more information on the motives, procedures and tools of attackers. Nevertheless, this technology also has weaknesses. Honeypots are sophisticated tools which bear a risk to the IT environment if used inadequately. If they are compromised they can used as starting points for further attacks (cf. Chapter 3.5). Time still elapses between an attack on a honeypot and the evaluation of the attack by the defender. However, the results of the evaluation can be used to protect productive systems and networks against similar attacks in the future since honeypots can be used to learn from attackers.

1.2 Objective and Approach

The objective of this paper is the presentation of specific advanced intrusion protection systems, so-called honeypots, as well as a cost-benefit analysis from an organization's point of view.

- The first chapter gives an introduction to the thesis and depicts the problem and the motivation of this thesis. Existing attackers are categorized and the threats that arise from them will be explained. The chapter also takes a closer look at the reasons and methods of attacks as well as an outlook on future trends of attacks.

- In the second chapter, classic intrusion detection systems are introduced. It covers the tasks of intrusion detection systems and its components. Possible architectures are illustrated and the reaction possibilities are explicated. Finally, shortcomings and an outlook of intrusion detection systems are given.

- Chapter three initially defines honeypots and describes their historic development. Subsequently it explains how honeypots are used and which tasks they have. An overview of possible areas to deploy a honeypot in an existing network is also outlined. The chapter continues with the description of attack and deception strategies and a classification of honeypots followed by an extensive overview of honeypot types. The chapter ends by summarizing the main differences between intrusion detection systems and honeypots and by illustrating the strengths and weaknesses of honeypots.

- Available open source [2] and commercial honeypot products are introduced in chapter four. The chapter exemplifies honeypots by describing selected honeypot products.

- Chapter five describes the cost and benefits of honeypots and evaluates security investments. Several financial models are presented. The chapter will take a closer look at the cost of acquiring and maintaining a honeypot and presents an exemplary calculation of incident cost according to the honeypot project's forensic challenge.

- The concluding chapter six of the thesis gives an outlook on the possible future of honeypots.

This thesis is methodically based on a study of available literature, interviews with security professionals as well as experiments with open source and commercial honeypots.

1.3 Types of Attackers and Threats in General

1.3.1 Classification of Attackers

An attacker is generally understood as somebody who tries to illicitly access data which are on a computer system. Security mechanisms are often bypassed or suspended by him to accomplish his ambition. The access attempt of the unauthorized can either be carried out internally, that is directly on the same computer, or carried out externally via a network [ESK02, pp. 10-11].

---

[2] Open source software uses software source code that is open, unrestricted and available by downloading it from the Internet. The 'open' in open source software is intended in the philosophical sense of 'open or free speech' rather than as a free (i.e. no cost) product [KMO03, p.1].

Attackers have different qualifications; therefore, different magnitudes of threat arise for the attacked. Some only have basic skills and use available scripts[3] and software packages without profound knowledge; others have far-reaching knowledge which can extend over different platforms and languages. The following classification differentiates between these different abilities and shows the possible threats accordingly.

Script kiddies (low level attackers) only have basic knowledge. They use available tools and do not completely understand how their attacks work. They usually scan a section of a network and look for systems with certain weaknesses that can exploit and intrude by using their tools. Since many systems are insufficiently protected in networks, script kiddies can compromise a large number of systems despite their primitive methods in a short period of time.

So-called moderately skilled attackers are able to customize programs and scripts. They understand the functionalies of the different weak spots and know how to use available tools with high accuracy. Provided with this knowledge and the different tools available, they are able to inflict considerable damage on a target. However, they do not have the abilities to find new weak spots and to develop tools for the purpose of compromisation.

The so-called high-level attackers are the most skilled attackers. They are very experienced in a large number of platforms and languages. Unlike script kiddies, high-level attackers do not like to be in the limelight. They work in secrecy and always try to cover their tracks. Some high-level attackers also research the field of IT-security with the aim of finding weak spots in applications, operating systems and other programs. Therefore, some organizations permit them to intrude their systems to be able to compromise them effectively. This unique type of attackers is the so-called Tiger Team. That is the name of attackers who are assigned by IT-security operators to check systems for their weak spots [TRG05]. The results of the intrusion are partly kept secret to prevent public distribution and discovery of

[3] A script is nothing more than a plain-text file created using Notepad or some other text editor, and saved with a particular file extension (for example: .VBS if you are using the VBScript scripting language). A script file describes the steps required to complete a task [MTN03, p.1].

the weak spot. However, there are also high-level attackers who reveal the results of their investigations and consequently contribute to the improvement of the security of vulnerable systems [ESK02, pp. 9-10].

Since attackers are always considered to be fraught with risk, they are referred to as blackhats. Whitehats are the counterpart to blackhats. They are responsible for the safety of systems and try to defend themselves with all means against the attacks of blackhats. Both terms are derived from the dress code of old black and white western movies in which villains predominantly wear black hats and the representatives of law and order wear white hats [ESK02, p. 11].

1.3.2 Motives for Attacks

There is a variety of motives for attempting an attack and attacking such as, money, power, ego, destructiveness ideology an entrance into a specific social group (cf. Interview II, 11). These motives have been confirmed as a result of the use of honeypots [LSP03a, pp. 27-29].

Some blackhats misuse compromised systems as type of currency. They sell attacked accounts of stolen credit cards. Other motives which will not be explained in further detail can simply be bragging, downloading and storing illegal or copyright protected data as well as its distribution. Artificial justifications like the fight against political systems or rage against certain organizations are not the case (cf. Interview II, 11).

Possible motives for blackhats such as power or money was seen recently. MasterCard International reported that over 13.9 million credit card accounts were compromised. The attacker also gained access to names, account numbers, expiration dates and security codes of 40 million credit cards. Attackers use the the data to purchase stolen goods, secure cash advances or sell them in bulk at underground sites on the Internet [EDA05, p. B13].

Blackhats attempt to conceal their identity during and after an attack. For this reason they do not attack directly from their own system. Blackhats cover their tracks by interposing as many compromised systems as possible as a bouncer [4]. To keep the pursuers' efforts as high as possible, these interposed systems are often in different countries, in other time zones and at different Internet service providers as well as in countries with different juridical systems.

1.3.3 Methods and Tactics

Attacks can be divided into the categories passive and active attack. The ultimate passive attack is an assault which is not noticed by the attacked. Examples of passive attacks are wiretapping, intercepting data packets and passwords or installing Trojan horses [5] which collect data on the system and transmit them to the blackhat. The attacked can protect themselves for example by encoding their data as well as their communication and therefore making it more difficult for the blackhat to attain information from the data [RUC03].

Unlike the passive attack, the active attack is involved with a direct, noticeable effect on the attacked. The best known active attack is the Distributed Denial of Service (DDoS) attack which deactivates the network connection using a very high number of enduring enquiries to a computer system. During a distributed denial of service, a blackhat must get dozens to hundreds of systems under its control to be able to execute a successful attack on a target system. The blackhat is successful if legitimate users are not able to access the system. The more systems are involved in the DDoS attack, the more effective will the attacks be and the bigger are the effects on the target system. The attacked must protect themselves against active attacks by authentication methods, digital signatures [6] and further security procedures [MGE03].

---

[4] A bouncer is a program that listens on a port and requires the authentication of the user to offer him an access [ARO04, p.2].

[5] Unlike a virus a Trojan Horse does not attach itself to another file but contains all of the executable code in itself. Some are destructive in nature and do damage to your systems. Other will monitor your computer activities and report back to the creator [ABE05, p.1].

[6] This Standard specifies algorithms appropriate for applications requiring a digital, rather than written, signature. A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified [WDA00 p.3].

Blackhats usually use similar tactics to intrude a system as could be ascertained by the use of honeypots and honeynets in the Honeynet Project [LSP02a, pp. 126-130]. Although not all tactics are used by every blackhat, a common pattern could be identified and classified in 5 phases:

- In the first phase (reconnaissance), the blackhat tries to find out as much as possible about his target. This phase is comparable with the planning phase of a bank robbery. The bank robber enters the bank to closely inspect the safety precautions as well as their set-up. Skilled blackhats also examine their target closely before they start their attack, i.e. before they send data packets to the target. Possible analysis methods are the so-called social engineering which is a non-technical way of intruding into systems or networks. People are encouraged to violate safety guidelines and to disclose certain information [KMI03, pp. 4-29]. Further methods of scrutiny are searching through directories on the Internet as well as through other sources of information.

- A script kiddy usually skips this first phase and starts the attack immediately with phase two (scanning). The experienced blackhat is already provided with information on his target in the second phase. A bank robber would have obtained some information about the bank before and therefore would now begin to look for the weak spots in the system. Script kiddies scan entire subnetworks[7] for weak spots, while the experienced blackhats concentrate on a certain target which they

[7] Subnetworks are reusable network objects, which are invoked from a calling network. Subnetworks provide for hierarchical models in which subnetwork instances are independent, encapsulated objects, called with a set of parameters [JOR99, p. 197].

specifically check for weaknesses. Possible procedures are port scanning[8] or war dialing[9], for example.

- Once the blackhat has completed scanning the target network and generated a list on the weaknesses of the systems, he will try to obtain access to the system in the third phase (gaining access). In contrast to script kiddies who use available scripts, more skilled blackhats attempt more complex attacks.

- Although there are some blackhats who have a great interest in appearances effective for advertising purposes, most blackhats try to cover their tracks as far as possible in the fourth phase (covering tracks and hiding). This secrecy also serves to maintain the discovered access to the system as long as possible.

- Finally, in the fifth and last phase (maintaining access), the blackhat puts emphasis on maintaining access to the system he has obtained in the third phase and upholding the existing access rights. For this purpose, blackhats apply software like Trojan horses, backdoors [10] and rootkits[11] which are intended to keep the access to the system as undetected as possible.

---

[8] Port scanning allows someone to probe a given network to determine information about the hosts available on a given network, the ports open on each hosts, and even information about the operating system and particular services running on each host [ALE05 p.2].

[9] This is an old hacking technique where a hacker breaks into a network by calling phone numbers in the hopes of hitting an unsecured modem the target has accidentally left active or forgotten. Automated programs enable hackers to dial thousands of numbers in a matter of moments. The technique almost always works and is one of the tests ethical hackers run that usually turns up an intrusion alert [BCO03, p.2].

[10] A backdoor is a hidden software or hardware mechanism, usually created for testing and troubleshooting [ABO05, p. 12].

[11] Rootkit is a combination from two words, “root” and “kit”. “Root” was taken from “root” a name of UNIX administrator, which is the highest-access level in UNIX environments while “kit” can be referred to as tools. From this word we can interpret rootkit as tools or collection of tools that enable attacker to keep the root power on the compromised system in order to keep the power over the compromised server [SMA01, p. 1].

In addition to maintaining access and upholding access rights, the intruded and compromised system is usually updated with software updates to reject the access attempts of following blackhats [ESK02, pp. 145-476].

To develop tools for attacking systems, comprehension of programming languages and operating systems as well as experience in the development of applications is required. Yet only few blackhats have these abilities [LSP02a, p. 130]. The use of the tools developed by high level attackers (partially also developed by whitehats) as well as their customization is easier than their development. Consequently powerful tools exist that can be easily used by script kiddies may cause immense damage to a target system.

1.3.4 Trends of Attacks

The methods and tactics of blackhats change over time. These innovations represent a new and altered dangerous situation. Spitzner [LSP02a, p. 134-137] estimates great changes in highly developed Rootkits, scanning and encoding techniques and in worms[12].

The blackhats' scanning techniques are becoming more and more aggressive. The blackhats used to take their time to find out the weaknesses of systems before an attack was started. Meanwhile blackhats do not search for specific systems with possible weak spots any more. Instead the reaction of a system is simply tested independent by, regardless as to whether a certain weak spot is available on a system or not. Furthermore, blackhats increasingly use encoding to unrecognizably communicate with a compromised system undercover. Because of this, the use of sniffers [13] becomes ineffective for the analysis and improvement of knowledge on malware[14]. Blackhats do not only use the available encoding tools ,

[12] A computer worm is a program that self-propagates across a network exploiting security or policy flaws in widely-used services [NWE03, p.1].

[13] A sniffer is a program that looks at every frame sent on a wire and can record the actual data (the frame), or can look for specific kinds of frames (could look for only frames holding TCP segments, or could look for only those TCP segments that are part of an HTTP conversation, etc) [DHO03].

[14] Malware is a program that has malicious intent. Examples of such programs include viruses, trojans, and worms [MCH05, p.1].

instead they develop their own. This complicates the analysis and the evaluation of the procedure of blackhats, also when using honeypots (cf. Interview I, 2). However, the encoded communication of a blackhat can stand out from the normal data traffic in certain surroundings and thus can also draw unwanted attention of the system administrators.

Other trends concern the further development of rootkits. Traditional rootkits replace typical data, cover the tracks of a blackhat and create back doors for continuous access to the system. Further developed rootkits modify the kernel[15] of an operating system, for example that of Linux. Consequently the output of a compromised system cannot be trusted any longer, and it becomes more and more difficult to trace a blackhat.

Worms, which not only automatically affect systems but also reproduce themselves with an increasing efficiency on different platforms, are finally the most alarming. This vast exposure requires an increasingly shorter reaction time. The effective protection of systems and networks become more and more demanding.

[15] The kernel is the central software component of all Linux systems. Its capabilities very much dictate the capabilities of the entire system. If the kernel you use fails to support one of your target's hardware components, for instance, this component will be useless as long as this specific kernel runs on your target [KYA03, p. 156].

6 Conclusion

During the course of this paper it became obvious that honeypots are clearly different from other security technologies. Firewalls and intrusion detection systems are usually only able to recognize and rudimentarily comprehend a new kind of attack after it has been executed. In contrast, a honeypot is able to analyze an attack, to comprehend, to evaluate as well as to recognize the motive, the procedure and the background of the blackhat. In addition, a honeypot decreases the elapsed time between an attack and the evaluation.

This paper puts emphasis on the differentiation between honeypots with high and low interaction due to the different cost and specifications, especially when conducting a cost-benefit analysis of honeypots. It was shown that low interaction honeypots are suitable for companies that would like to supervise the network status and to assure the correct functionality of their services. They primarily observe suspicious connections in the network and do not distinguish between blackhats that scan systems for vulnerabilities, malware that attempts to spread in the network, poor network configurations or users looking for exposed resources. To assure an efficient infrastructure, these threats must be held off from the systems.

High interaction honeypots unlike low interaction honeypots address a different target group since these research honeypots are primarily used to learn from blackhats. They are interesting for companies that produce antivirus software to be able to learn from blackhats. Research honeypots can be used by non-profit organizations to discover or identify malware. The cost that arises from the implementation can be neglected compared to the benefits. However, most organizations must compare the benefit of a honeypot with the maintenance cost to be able to achieve an optimum security for themselves. IT specialized non-profit organizations on the other hand will tend to strive for absolute security, regardless of its cost.

When performing a cost-benefit analysis it is most important to consider the fact that the regular cost which are difficult to calculate in advance are the most crucial.

These costs cannot be reduced without negative effects on the systems. The costs depend on the number of occurrences and can greatly vary for that reason. High interaction honeypots are mainly actual computer systems which increase the risk for the complete infrastructure. A permanent and conscientious supervision of the honeypots is therefore of decisive importance.

Good, open source low-interaction honeypot solutions exist which can be configured easily exist as explained in Chapter 4. It is shown that there are open source programs designed in such a way that a system administrator, even with little computer knowledge, can extract a large amount of information from the reports, which are made by these programs. Therefore, one can get an idea of the condition of the network within minutes. Low interaction honeypots are a first-class solution for companies dealing with honeypots for the first time.

The technology of honeypots is still new and not fully developed. They still take too much time to deliver results, total cost is expensive and they are not yet fully reliable. Even though the technology of honeypots is relatively new, blackhats have already developed tools to defeat honeypots. Applications like Honeypot Hunter can recognize whether open proxies [48] are a honeypot or not [SSH05]. Moreover, blackhats are investing their time to publicize any honeypot that they discover.

Another problem of the honeypot technology is the lack of acceptance. Many of the security specialists the author interviewed during the CeBIT in 2005 (the largest international computer fair world-wide) about the newest technology were able to explain the technology of honeypots. Only some of them actually used the technology. Other specialists believe that honeypots are not fit for the future [CNE05]. One could conclude from this that the technology is still too complicated, has too many flaws, needs to much time and therefore is not accepted by the majority of specialists. Some IT specialists argue that honeypots are just as important as any other IT-security application. Most agree that the key to an

[48] A proxy is a software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination [AMA05].

economic optimum of security is only achieved if all security applications work together as one unit. In addition, time consumption with regards to the analysis of the results of honeypots, must decrease in the future. Having mentioned that honeypots are still a relatively new technology, the future of honeypots depends on their development and therefore is not clear.