HØGSKOLEN I AGDER
Agder University College

Threat to Information Security. The System Vulnerability and Denial of Service Attacks.

by

Kjetil Eiklid Braathen and Silje Salte

Masters Thesis in
Information and Communication Technology

Agder University College
Faculty of Engineering and Science

Grimstad, May 2004

Abstract

The use of the Internet has increased drastically the last few years. This trend has led to a constant increase in attacks toward computer systems and networks, and the methods for attacking are becoming more and more advanced. By this, we mean that new tools are developing in a way that makes it more difficult for people to protect themselves against, while the use of the tools is more user friendly than before, and the hackers do not need as much skills as they used to.

In order for security practitioners to know how to protect themselves against new attacks, it is important for them to know how the hackers work and think. Therefore, we have described the hacker environment, tried to map how many they are, how they find information, and how they share information.

Vulnerabilities and denial of service are considered to be the main parts of the report, with a model to each case. To get an overview over vulnerabilities and factors that influence vulnerabilities, a system dynamics model is discussed. The model shows variables like vulnerable hosts, patching, hackers with or without scripts, sophisticated and non-sophisticated hackers, attacks, and attack frequency. This is an overall description of a single vulnerability problem, but the problem with multiple vulnerabilities is also briefly discussed.

Some of the biggest threats when it comes to information security today are denial of service (DoS) attacks and distributed denial of service (DDoS) attacks. DoS and DDos attacks are possible to be the most potent and difficult to tackle, and they can do enormous damages. These types of attacks are described, and we use and discuss a model over a specific denial of service case. The case is about a turf war between the two German hackers “Mixter” and “Randomizer”, and the model includes variables that are specific to the case, and variables that are more general about hackers and the Internet world.

As we have been working with the master thesis, a big problem has been data collection. This has been a problem for us because it is hard to find data on information security. Some organizations choose not to publicize of different reasons, this can be that they are afraid of bad publicity. It takes a lot of time and effort to do this kind of data collection, and people who do it, collect for a narrow purpose. Systematically collected data is therefore not always available.

Preface

This thesis is our final report at the Master's degree program in Information and Communication Technologies at Agder University College. It represents 30 ECTS credits ("studiepoeng" in Norwegian), which is equivalent with a 1 full-time semester. The work has been carried out from January 2004 until May 2004.

We would like to thank our supervisor, Professor Jose J. Gonzalez, for all of his good advices and guidance in the writing of our report. Another thank you goes to Ph.D. student Johannes Wiik, who made the system dynamic models we were to discuss and find information to.

Grimstad, May 2003

Kjetil Eiklid Braathen and Silje Salte

Table of contents

List of figures

List of tables

Introduction

Attacks that exploit system vulnerabilities and denial of service attacks are some of the biggest threats when it comes to information security today. However, many of the contributing factors to computer security problems are non-technical in nature – that is, they are dependent upon human and organizational actions.

Vulnerabilities

When programmers write information technology products, there are always design, implementation and management errors. These are what we call flaws in the technology products. When these flaws can be exploited, we also call them vulnerabilities.

To avoid vulnerable systems being exploited, system managers have to patch their systems. A patch is code that is added to the original program, which eliminates the vulnerability.

The number of vulnerabilities reported to CERT/CC[1] is growing.

In addition to the above trend, more sophisticated attack tools are made. Such tools can be used to exploit the vulnerabilities in larger scale, at the same time requiring less technical knowledge from the attacker.

Denial of Service

Denial of service (DoS) is a type of attack that is designed to hang or crash a program, or bring down the entire system, by flooding it with useless traffic.

Distributed denial of service (DDoS) attacks is based on many of the same mechanisms as DoS attacks, but they are more complex and have the potential to do damage that is more widespread. The spurious traffic originates from multiple machines in the Internet, while it originates from a single machine in DoS attacks. DDoS attacks have therefore much bigger impact, and are more difficult to fight.

While Denial of Service (DoS) attacks have been around for many years, they are becoming increasingly menacing as the Internet extends further into the global communications fabric. Over the past several years, DoS attacks have been overshadowed by Distributed DoS (DDoS) attacks in which multiple systems can be used to launch an attack, significantly increasing the potential for widespread damage.

[1] CERT is an acronym for Computer Emergency Response Team, but CERT Coordination Center is currently operating with a much wide range of computer security activities than this name indicates. The center coordinates activities and research within the areas of vulnerability analysis, incident handling, survivable enterprise management, education, training and Survivable Network Technology. For more information available at: http://www.cert.org/meet_cert/meetcertcc.html#bkgd

In early 2000, most people became aware of the dangers of DDoS attacks when a series of them knocked popular Web sites like Yahoo, CNN, and Amazon off the air.

Attack tools are becoming increasingly sophisticated, and they are becoming more user friendly and widely available. This results in unsophisticated users using the available tools to identify and take advantage of a large number of vulnerable machines. To develop new and more powerful distributed attack tools, intruders are using currently available technology. There has been an increase in the development and use of distributed sniffers, scanners, and denial of service tools. Intruders are actively seeking systems with good network connectivity for compromise and installation of daemon programs.

Problem definition

Threat to Information Security. The System Vulnerability and Denial of Service Attacks.

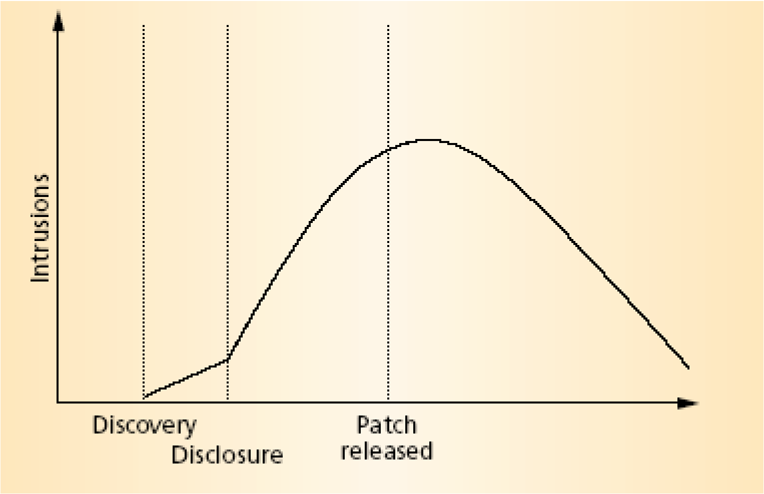
Attacks on information networks typically originate with the discovery of a system vulnerability' by advanced intruders. Crude exploit tools are developed and distributed, leading to the first attacks. Next, advanced automated scanning/exploit tools are used to roll out more numerous and more sophisticated attacks. On the 'victims' side, a process of developing defenses ensues (detection of the source of the vulnerability, development of a software patch, distribution and installation of the patch). Ultimately, the attack wave subsides. The whole process is referred to as a 'vulnerability exploit cycle' or 'vulnerability life cycle'.

Traditionally, the hacker community has performed most attacks on information networks. Although nasty enough, hacker attacks have mostly caused transient problems. However, the hacker threat might become an increasing nuisance as more advanced attack tools are developed and an exponentially growing number of poorly maintained units belonging to single individuals expand the number of vulnerable sites to unprecedented levels.

In our paper, we will present the following problems, and our job will be to find information on them, and discuss models on them.

The Single Vulnerability Problem

Briefly stated, the problem is to understand the determinants of the life cycle of a single vulnerability (Arbaugh, Fithen et al. 2000). For illustrating the issue, the problem can be simplified to understand a generic life cycle such as given in Figure 1.



- Figure 1: Intuitive life cycle of a system vulnerability. (Arbaugh, Fithen et al. 2000)

A successful model would throw light on aspects of the hacker community that are difficult to assess directly (i.e. the ability of the model to render actual reference behavior from several well-studied vulnerabilities would increase our faith in the model's assumption about how knowledge spreads in the hacker community, etc.)

Further, the model could be used to:

- Experiment with policies to prevent or at least reduce the impact of attacks.
- Help identify trends and explain the determinants of trends.
- Assess the extent to what current data can be used for numerical simulation analysis; suggest further empirical studies; suggest further modeling studies.

For us, the goal is to find data that makes us able to support the model or criticize it. We will give a thorough discussion of the model in this paper.

The Multiple Vulnerability Problem

Hackers roll out attacks on vulnerabilities so that exploitation of several vulnerabilities might overlap and interact. A successful model would throw light on aspects of the hacker community that are difficult to assess directly (i.e. recruitment to the hacker community, how the hackers pick various vulnerability types, the R&D pipeline in the hacker community, etc).

In this paper, we will not present a system dynamics model on this problem, but we will discuss the possible determinants and variables in such a model.

Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks

We wish to get a deeper understanding of the DoS and DDoS attack problem by finding information in different sources, and by discussing a causal loop diagram over a specific DDoS problem.

Our job will be to find out what denial of service attacks and distributed denial of service attacks are, how such attacks are pulled off by hackers, the impact that the attacks have, any types of trends of the use of DoS and DDoS, what type of tools that are used in such an action, and who writes and uses the tools.

The causal loop diagram of a DDoS case will be discussed thoroughly. The DDoS case is about the hackers "Mixter" and "Randomizer". They were both pioneers in denial of service attacks, and members of two different hacker clubs that competed with each other. The causal loop diagram will describe different aspects of the case, like the impact of word of mouth, bragging, possession of chatrooms, turf wars, etc.

Data Restrictions

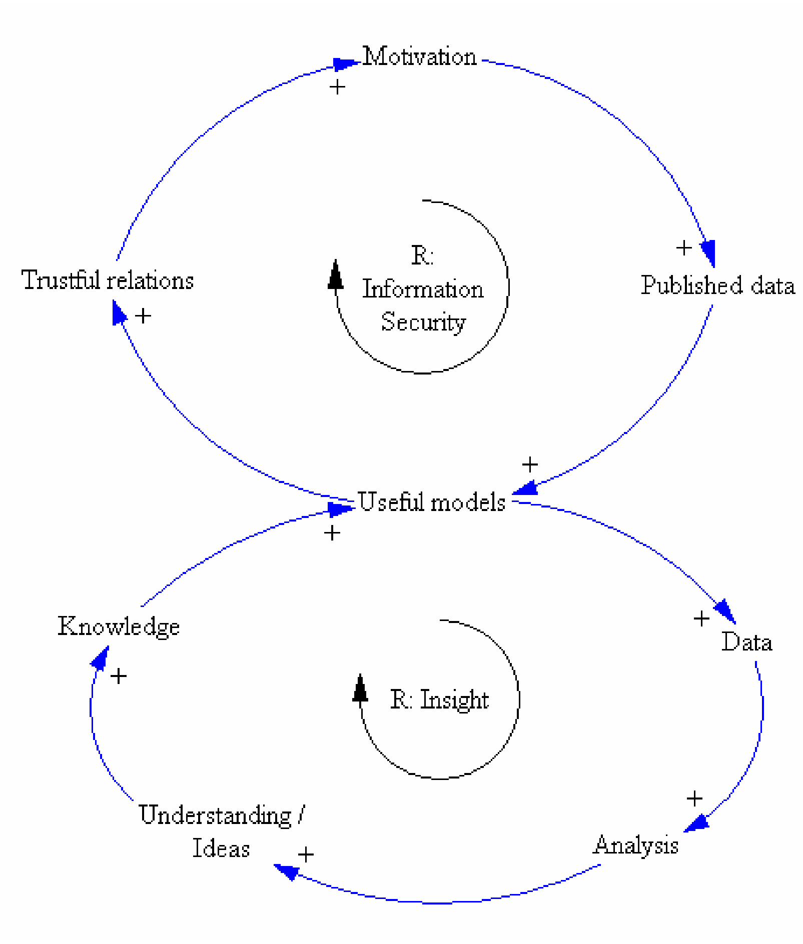
One of the main problems in our work, will be to find the information that we will be searching for. Generally, this is a difficulty in systematic modeling of attacks on information assets. Attacks on networked systems are increasingly frequent, and systematically collected data on these attacks is not generally available.

Not all data is shared. Organizations might choose to withhold data on their being attacked, because they are afraid of bad publicity, and thereby get a bad reputation. This is a general problem for researchers on this kind of data. Citibank is an example of this (Schneier 2000). It lost $12 million to a Russian hacker in 1995, and announced that the bank had been hacked into, and introduced new and more profound security measures. They did this to prevent such attacks from occurring in the future. But their action backfired; immediately after their announcement, millions of dollars were withdrawn by people who believed their funds were vulnerable. Citibank learned their lesson: "Do not publicize". Schneier disagrees. He says: *"We need to publicize attacks. We need to publicly understand why systems fail. We need to share information about security breaches: causes, vulnerabilities, effects, methodologies. Secrecy only aids the attackers."*.

Because of the fact that not all data is shared, the statistics that are made by CERT/CC over reported attacks, probably underrates the real number of attacks. There are many unknowns, and this makes it harder for us to know which data to trust the most in the different sources that will be searched.

The attackers, on the other hand, want people and networks to be as little prepared of attacks as possible. Therefore, they try to conceal as many aspects of their attacks as they can, because they want to preserve the utility of their methods so that the networks will not be prepared of any attacks. While attackers conceal what they are doing, the defenders are burnt out, have little motivation for doing large data collections, and it takes too much time for them. The purposes for why defenders gather data, are often very narrow (Wiik, Gonzalez et al. 2004).

We wish to use a causal loop diagram to illustrate the improvement of information security between data owners (i.e. organizations) and modelers (who use data provided by organizations to create models leading to insight), through the buildup of trustful relations. "*Causal loop diagrams (CLDs) are an important tool for representing the feedback structure of systems"* (Sterman 2000). A + sign means that when the variable at the tail of the arrow changes, the variable at the head always changes in the same direction. A - sign has the opposite meaning; if the tail variable changes then the head variable changes in the opposite direction.



- Figure 2: Improvement of data collection in information security.

The CLD in Figure 2 has two reinforcing feedback loops. The top part of the CLD shows information security, while the bottom part shows insight. More useful models makes more trustful relations, this makes the data owner more motivated, and will end up in more published data. With more published data, there will be even more useful models, and the new useful models will lead to more data, and when data is collected, you can analyze it. The analysis gives you a better understanding and more ideas, which again gives you more knowledge, the knowledge inspires the modelers to do more searches for new models (and he/she will have a bigger basis/foundation for doing new searches), and it all results in a reinforcing causal loop (the R in the figure shows that it is reinforcing).

The effect of the reinforcing loops goes both ways. The reinforcing loop "R: Insight" can in our case for example become a vicious circle and run backward if the searches for information among the useful models that CERT/CC does, are very limited (less data gives less to analyze, and this will lead to a poor understanding and less ideas, impaired knowledge, and have a less foundation for new searches, and this will again lead to poorer/less data). This means that the other reinforcing loop; "R: Information Security" has few trustful relations, less motivation for doing searches and documentation, the published data will become poorer, and the models will become less useful.

Work Description

In this project, we searched and analyzed open source information, like books, periodicals, reports, the Internet and other official media. We used the library database at Agder University College to search for papers and articles. Another useful information source was the CERT Coordination Center (www.cert.org). Through the project, we got frequent guidance from our supervisor Professor Jose J. Gonzalez, and Ph.D. student Johannes Wiik made the milestone models.

An important part of the work was to organize and determine our sources. The progression of the project emerged from constantly new searches, finding relevant information to the system dynamics modeling. The project also developed in proportion to the feedbacks we got from Professor Jose J. Gonzalez and Johannes Wiik. In example, they visited the group modeling workshop held at SEI, Pittsburgh (16-20 February 2004), which in fact turned out to be the substantial factor for us studying Denial of Service (DoS) attacks.

Clearly, it is important for us to document our references. Therefore, we have made a "mini library" of articles. It is actually a small box containing all the articles and references to books, which we have used in our paper. The references are also saved systematically by name of author electronically in EndNote-files.

Through the working period, we have made memos on our searches, which document the progression of the project. Those memos are appendixes to this paper.

Method

The purpose of the project is to find and analyze available information about computer security in books, periodicals, reports, web, etc. The method we used to find information was theoretical research.

In the master thesis, we are involved in the process of analyzing and mapping of data. The goal is to get an understanding, see connections, and show new aspects to the topic. We go deeper into software-based vulnerabilities and denial of Service (DoS) attacks.

The main process of the project has been to deliver memos on agreed subjects of security information, to our project supervisor Jose J. Gonzalez. Through the memos, we contribute to deliver background information to the system dynamics models, made by Ph.D student J. Wiik and Professor J. J. Gonzalez. In the research, and the process of gathering enough information to substantiate the models, we develop knowledge in the dynamics of the problem. Through this, we can discuss and validate the models in this paper.

The project will be an inductive approach / grounded theory. We start with recording our observations, where the purpose is to find patterns that can be made theories or general concepts out of. The information will be analyzed and classified. As researchers, we will try to be as open as possible when it comes to the data that is observed, and draw conclusions.

Grounded theory is "*an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data*." (Myers 1997)

Report Outline

The rest of our report will include the following:

Threats to information security will be described in the chapter “The Threats to Information Security”. CERT/CC’s statistics with trends over incidents and vulnerabilities will be presented and discussed here, and also incidents versus hosts. Further, it will include different types of attack methods and some basic attack tools, and also identification of hackers, the hacker environment and hacker wars.

“Modeling the threat to Information Security” has a brief description of system dynamics, which is a introduction to the next part; the model over the single vulnerability problem. The end of this chapter describes the multiple vulnerability problem very briefly.

Denial of service and distributed denial of service attacks are to be discussed in the next chapter; “Denial of Service (DoS) Attacks and Distributed Denial of Service (DDoS) Attacks”. First, it explains what the attacks do. Secondly, a specific DoS case is told. At last, a causal loop model over a DoS war is presented and discussed.

The discussion is written in sub-chapters after the presentations of the models.

The following two chapters contain conclusion, and some recommendations for future work are presented.

DDoS tools and attacks, explanation of words, and abbreviations are listed up in a chapter each after the references. and at the end of the report, the Appendixes are added.

The Threats to Information Security

In this chapter, we will show the reader vulnerability statistics, and give detailed information on hackers, attacking tools and the hacker environment.

CERT Coordination Center (CERT/CC)

Established in 1988, the CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. They have their own web site, www.cert.org, which is a very good site for finding reliable security information. As well as being a place for receiving and publish security information, they do presentations, training and education, research and analysis.

The next section concentrates on statistics from CERT/CC, and tries to show the evolution of the threat to information security, vulnerabilities.

Numbers and Trends – statistics

Below are numbers taken from the CERT/CC statistics page.

In this paper, we inherit the expressions defined by CERT/CC. We remind the reader of the definitions of two terms:

Incident - An activity that has security or survivability implications.

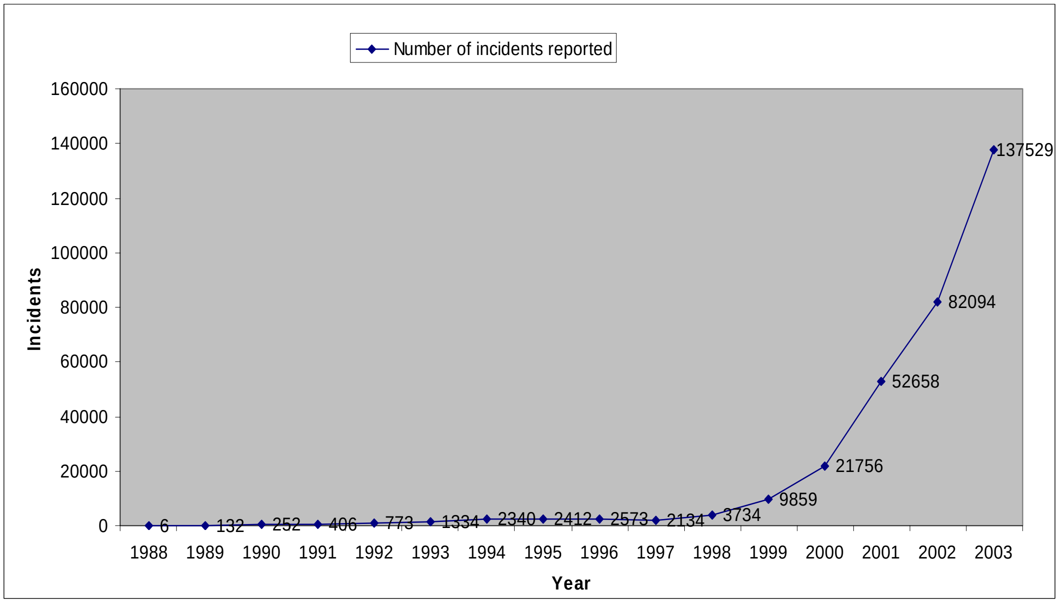
Vulnerability - A flaw or defect in a technology or its deployment that produces an exploitable weakness in a system, resulting in behavior that has security or survivability implications.

- Table 1: Number of incidents and vulnerabilities reported

Number of incidents reported:		Vulnerabilities reported:	
Year	Incidents	Year	Vulnerabilities
1988	6	1988	-
1989	132	1989	-
1990	252	1990	-
1991	406	1991	-
1992	773	1992	-
1993	1 334	1993	-
1994	2 340	1994	-
1995	2 412	1995	171
1996	2 573	1996	345
1997	2 134	1997	311
1998	3 734	1998	262
1999	9 859	1999	417
2000	21 756	2000	1 090
2001	52 658	2001	2 437
2002	82 094	2002	4 129
2003	137 529	2003	3 784

Note that an incident may involve one site or hundreds, or even thousands, of sites. In addition, some incidents may involve ongoing activity for long periods.

We have visualized the numbers of incidents and vulnerabilities from Table 1, in Figure 3 and Figure 4.



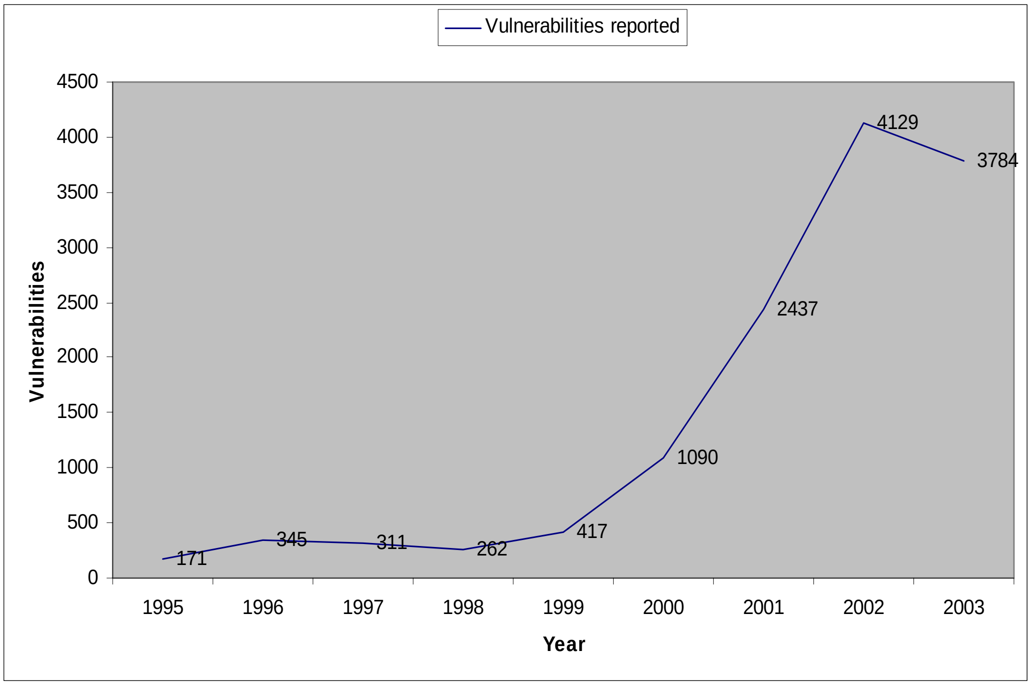
- Figure 3: Incidents reported 1988 – 2003

We see that the incidents reported, have approximately doubled each year, during the last six years. This is an enormous development in hacking activity.

In the recent years, the activity of reporting vulnerabilities and incidents to CERT/CC has grown. Therefore, older numbers would probably be higher, if the activity started earlier.

This would probably have less impact on the trend. However, we can assume that very few are aware of, or capable of reporting, and few people report anything at all. In addition, companies are afraid of reporting because of bad publicity. Therefore, these numbers are like spot tests of the actual numbers. In addition, our educated guess, seeing development of Internet and the security issue, is that it could be used as a good estimate of the trend.

There must be several reasons for the increase in incidents. In the following chapters, we will point out some of them. (Again, we emphasize that these numbers are only incidents reported to CERT/CC, and can therefore only be treated as an estimate of the trend.)



- Figure 4: Vulnerabilities reported 1995 – 2003.

When we look at Figure 4, we actually see that there is a decrease in reported vulnerabilities from 2003 until 2002, which is against the trend of preceding years. Why this is, may have several reasons.

Yet, there is no proper explanation of the decrease in vulnerabilities. CERT/CC does not say anything in their annual report 2003 (Unknown 2004) about this. Here we humbly discuss the problem.

One assumption could be that program developers are programming more carefully, using techniques or development tools, which do not lead to software vulnerabilities. This is not a likely assumption, because there has not been "a revolution" in programming techniques or development strategies. However, today, when it comes to security, there is often bad development practice in many organizations. In addition, such a change would probably take years. No publications searched[2] indicate this.

Another reason could be that "something" happened that decreases the companies' willingness to report vulnerabilities. E.g., there have been a number of leaks of vulnerability information from CERT/CC several days of advance of CERT/CC's intended release of information to the public (Edwards 2003). For this reason, there may be companies that do not trust CERT/CC as much as they used to, and do not report their vulnerabilities for this reason.

Each of the vulnerabilities represents a weakness in a product that can be exploited in some way to help an attacker achieve the objective of compromising a system. When we think of that, and the fact that there are millions of hosts on the Internet, we see that there are enormously many possibilities for a potential hacker to cause havoc.

Incidents versus Hosts – the Evolution

We know that the number of Internet hosts is increasing, and we know that the number of reported incidents also is increasing. But which of them are increasing the most? It would be interesting to show trends for the hacking activity.

Table 2 shows collected numbers from ISC Internet Domain Survey and CERT/CC. The first column shows the year, the second column shows the number of hosts (http://www.isc.org/index.pl?/ops/ds/) and the third column shows the number of incidents (http://www.cert.org/stats/cert_stats.html).

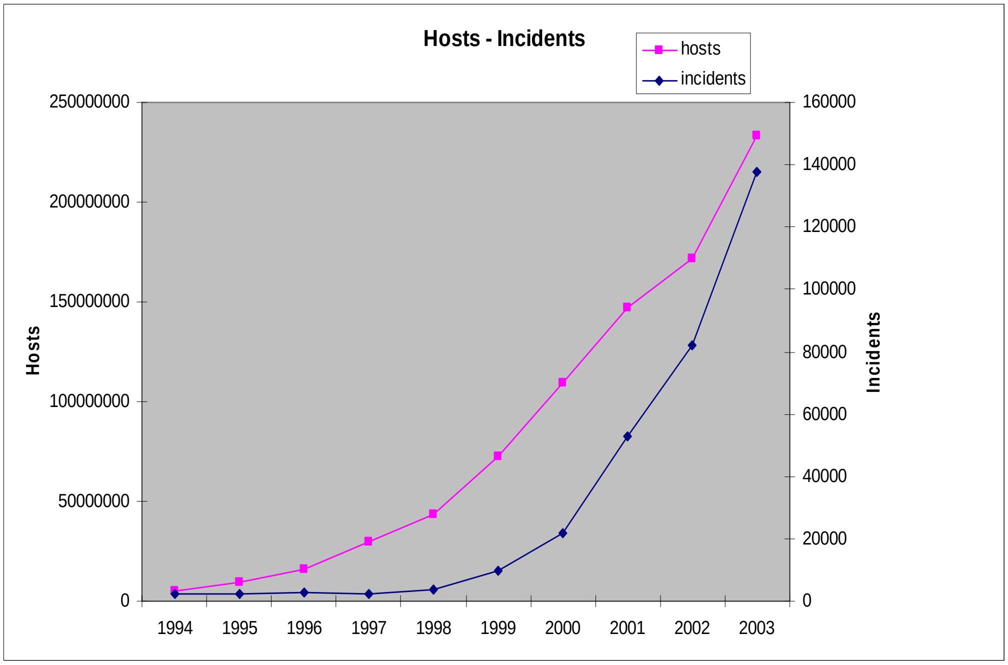
The next two columns show results from the equation

*incidents / hosts * factor = X*

- Table 2: Evolution of hosts and incidents

Year	Hosts	Incidents	Incidents/Hosts	Factor=100000 X=
1994	4 852 000	2 340	0,000482275	48,2275
1995	9 472 000	2 412	0,000254645	25,4645
1996	16 146 000	2 573	0,000159358	15,9358
1997	29 670 000	2 134	7,19E-05	7,1925
1998	43 230 000	3 734	8,64E-05	8,6375
1999	72 398 092	9 859	0,000136178	13,6178
2000	109 574 429	21 756	0,00019855	19,855
2001	147 344 723	52 658	0,00035738	35,738
2002	171 638 297	82 094	0,000478297	47,8297
2003	233 101 481	137 529	0,000589996	58,9996

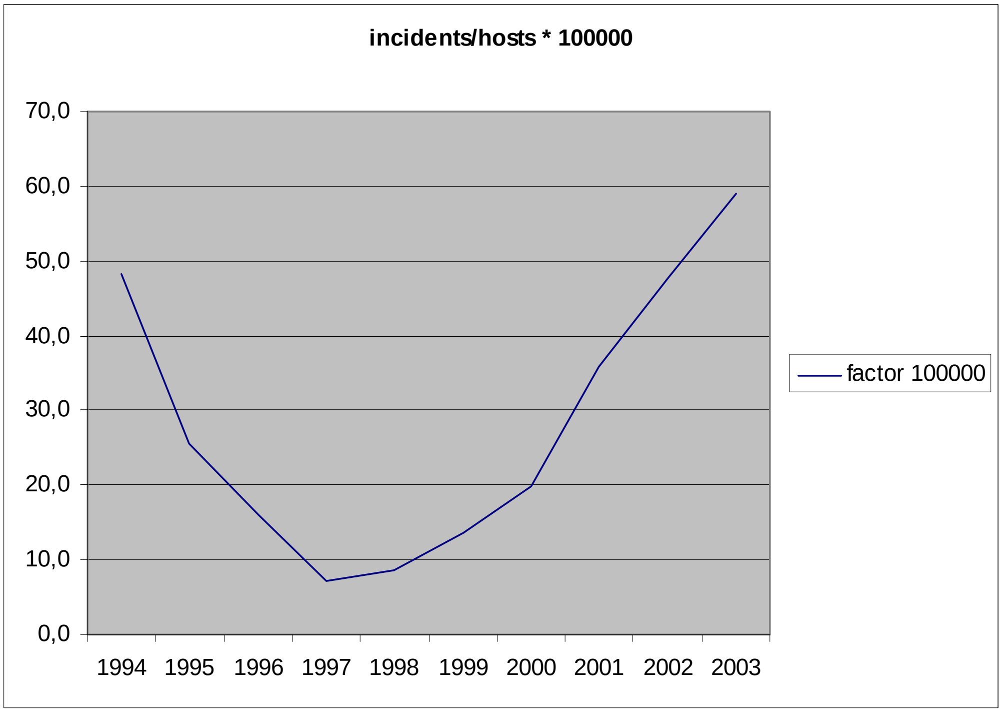
[2] Searches using "Google" (www.google.com)



- Figure 5: Hosts versus incidents 1994 – 2003.

From Figure 5, we see that both hosts and incidents have been increasing dramatically during the recent years. We also see that the growth in hosts started earlier than for incidents. This has of course natural reasons, because incidents cannot happen without hosts to attack, and with the growth of hosts, potential attackers and hacking activity will also increase. However, the interesting part would be to see how many incidents there are per host over several years. This way we can estimate if the "hacking activity" grows or sinks those years.

Figure 6 shows the relationship between incidents and hosts. You can clearly see that from 1994 until 1997 there was a decrease in activity per host. However, since 1997 the trend turned, and the activity per host has continuously been growing until 2003. It is most likely still growing today, because of the development of sophisticated attacking tools. The tools are made to harm a greater number of hosts, and to be used with less knowledge of hacking. We tell more about this in the chapter "Attacking methods".



- Figure 6: Relation between incidents and hosts.

Vulnerabilities

Protecting software in the face of attacks is a difficult task. Vulnerabilities (weaknesses that can be exploited to compromise the operation of the system) can creep into the system in a variety of areas.

Some of these vulnerabilities are difficult to correct because they are the result of architecture and design decisions that were made early in the product's development cycle. In these cases, the vulnerabilities can only be removed by changing the basic architecture of the product. These types of fundamental changes often have consequences that affect other aspects of the product's operation. These types of vulnerabilities are typically long-lived, and product users must find some other way to protect themselves from attacks that attempt to exploit the vulnerabilities (e.g. invest in anti-virus software in order to detect and remove viruses before they operate on the vulnerable system).

Other vulnerabilities are easier to correct since they are the result of low-level design decisions or implementation errors (bugs in the programs). Often the vendor can quickly correct these types of vulnerabilities, once discovered, and the corrections (oftentimes called "patches") can be made available to the customers.

However, even though the corrections may be available quickly, it is not always the case that they can be deployed quickly. System operators need to insure that the corrections do not have unintended side effects on their systems, and typically test the corrections before deployment. In addition, in the case of a widely used product, system operators must often update the software used in thousands of computers to deploy the correction. This is a labor intensive and time-consuming task in itself. Therefore, systems are attacked several months after vendors produce corrections to the vulnerabilities, in many cases. Deciding which vulnerabilities really matter, and effectively dealing with them, are key steps in an organization's risk management process. More about patching in the part “Problems with Patching” (pages 35-36).

Basic types of vulnerabilities

Here is a list of the general vulnerability types:

Default software installations - Performing a default software installation on computers with sensitive data is not good practice, especially when the chosen software is likely to be used by many people, such as on a public access computer or Web server. This often leads to backdoors for hackers that know the default services.

Ineffective use of authentication - Most organizations rely on authentication via passwords. Passwords can be a secure form of authentication when they are created properly. However, most people create poor passwords.

Patches not applied - Patches for known security problems are not applied.

Too many open ports and services running - Services listens for packets that arrive from other computers with matching port numbers. Too many ports open can give away a lot of information about the machine.

Not analyzing incoming traffic - Analyzing incoming packets allows you to weed out packets that do not match the security policy.

Backups not maintained and verified - If backups are not taken regularly, you will not be able to quickly recover from data loss. The backups should be verified.

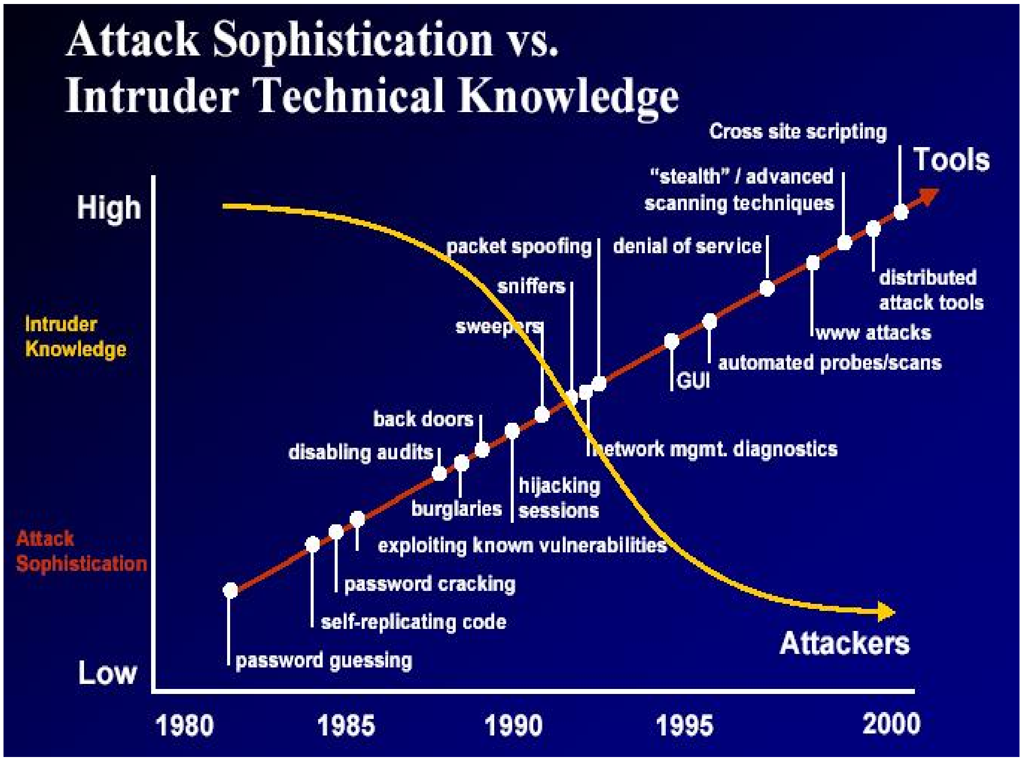
Lack of protection against malicious code - viruses, worms and Trojan horses (more on malicious code in “Attack methods”).

Attack Methods

There are many types of attacks. A general smart network attack usually happens like this: First, the intruder has to locate the system to attack. Then he gains user access or privileged access to that system, covers his tracks, and installs backdoors. Now he can attack other systems, take or alter information, or engage in unauthorized activity.

Most compromised systems are not patched, or they are configured wrong. Intruders use toolkits to try numerous exploits looking to capitalize on an exploit that has not been patched by system administrators.

Technology has changed, and so has the challenges of security professionals. It is important for them to keep informed because the attack methods used by hackers are many. Figure 7 below shows that the technical knowledge of the intruders has decreased. One reason for this is that the attack tools are published and made available through the Internet. While the attackers gets “dumber”, the attack sophistication increases. The attackers started by guessing passwords, and they are now using more advanced tools like XSS (cross site scripting) and distributed attack tools. The tools are much more user-friendly than they used to be, and the attackers’ average level of learning declines over time.



- Figure 7: Attack Sophistication vs. Intruder Technical Knowledge (Lipson 2000)

The Basic Attacks Tools

Probes and Scans

A probe is an attempt to gain access to a system or to discover information about the system. Probing can be compared to testing doorknobs to find an unlocked door for easy entry. Probes are sometimes followed by a more serious security event, but they are often the result of curiosity or confusion. A scan is a way of performing multiple probes using an automated tool. The most common kind of scan is a "port scan."

Account Compromise

Account compromise is the discovery of user accounts and their passwords on a system. It allows an unauthorized user to gain access to all resources for which that user account is authorized.

Packet Sniffer

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network. If the data captured by a packet sniffer is encrypted, it is unlikely that someone will be able to reveal any sensitive information. However, if the data is not encrypted, just about any information sent is vulnerable for being compromised.

Denial of Service

The goal of denial of service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial of service attack can come in many forms, but the underlying purpose to a denial of service attack is to bog down a system by giving it too much information to process quickly enough.

Malicious Code

Malicious code is a general term for programs that, when executed, can cause undesired results on a system. Users of the system are usually not aware of the program until they discover the damage. Malicious code includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self-replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but they usually require some action on the part of the user to spread to other programs or systems.

Spoofing

Spoofing is when attackers can forge their identity, appearing to be using a trusted computer, and therefore are able to gain unauthorized access to other computers.

Methods of Attacking

Hackers use several ways of attacking, and we wish to describe some of them:

Social engineering

Social engineering are techniques for persuading another person to do what you want. An example, which is a common hacker trick, is to telephone unsuspecting employees and pretend to be a network system administrator or security manager. To do these kind of scams, the hacker needs to gain knowledge about the company’s network to sound convincing, and thereby get passwords, account names, and other sensitive information from the employee. To gain this kind of knowledge, one can read newspapers, magazines, and annual reports.

The method is very effective, because it bypasses cryptography, computer security, network security, and everything else technological. It proves that the weakest link in any security system is the human.

The well-known hacker, Kevin Mitnick used this method. He testified before Congress in 2000, and said the following about social engineering: *"Companies can spend millions of dollars toward technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defenses or reveals the information they were seeking"* (Schneier 2000).

Other types of social engineering can be showing up at a computer room, or stealing credit card numbers.

Insider attacks

The insiders are malicious because they are already inside the system they want to attack. It is often a person that has a high level of access, and he/she can be considered to be trusted by the system he/she is attacking. Firewalls, intrusion detection systems, and most other computer security measures, try to deal with the external attacker, but are powerless against insiders.

Most security problems occur from within, and it's mostly hacking at the application level. Estimation is that former employees do 85% of all hacking against companies. *(Appendix D)*

Dumpster diving

Hackers frequently search dumpsters located outside of buildings for information sources such as operator logs, technical manuals, policies, standards, company phone books, credit card numbers, and dial-in telephone numbers. This is categorized as "dumpster diving". The information might help the hacker to gain access to the organization.

Hardware and Software tools

Phreaks use hardware devices to gain free phone access. They generate tones that allow them to navigate the various telephone switches.

A lot of software tools are available on the Internet or on bulletin board systems. This can be network sniffer software (to capture IDs and passwords), password cracker tools, or war dialers.

Reverse intent

CERT/CC advisories CIAC information bulletins are intended to notify people of security problems. Hackers and phreaks use this to their advantage, and the information is used to perform the opposite action of what it was intended to. When hackers find out about these announcements, they are quick to notify each other of it, and exploit the weaknesses.

Phishing

Phishing is when someone (phishers) are using spam to deceive consumers into disclosing credit card numbers, bank account details, Social Security numbers, passwords, and other sensitive information.

Phishers "fish" for personal information that can be used in identity theft, and thereby the name. They pass themselves off as Earthlink, eBay, or some other legitimate business, and tell the Internet user, via e-mail, that there is a problem with their ISP (Internet Service Provider) account, and provide them with directions to a Web site for clarification. By clicking on the link to this Web site, users get directed to a hoax Web site that probably is a perfect copy of for example Earthlink. At this page, users are fooled into providing personal information.

The phony e-mails and Web pages may claim that you have won a price, or they may encourage you to sign up for testing of a new product or service. Some of the Web pages may download computer viruses or Trojan horse programs to your computer automatically, and cause damage of your computer files, or the scammer might get your password. The scammer can be signing on to your ISP account, read your e-mail, send e-mail from you, etc., and all this because he/she got the hold of your screen name and password.

It is easy to get a phony Web site as well, because there are scripts for stealing Web sites. Reamweaver (http://reamweaver.com) is one of them. It works by downloading and extracting the file, uploading it to a Web site directory, and making sure that all the files have full permissions.

Users can do some precautions to protect themselves against phishing. They can do this by checking that their ISP is genuine, inspecting the accuracy of the Web address, and by being on lookout for a PKI (public key infrastructure) on a Web site. The PKI verifies the identity of the certified company (Selfridge 2004).

Identification of Hackers

Security practitioners need to understand hackers in order to protect their systems against unauthorized intrusion of their computer and communications systems. They need to know who they are, what motivates them to break into systems, and how they operate. What are the motives and modes of operation? How do hackers gather and share information? How do they break into systems?

The New Hacker's Dictionary has the following definition of a hacker: *"A person who enjoys learning the details of computer systems and how to stretch their capabilities – as* *opposed to most users of computers who prefer to learn only the minimum amount necessary"* (Norris 1995).

Who are the Hackers?

"Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker." (Raymond 2001)

The typical hacker profile in the early 1980's, was a highly intelligent, introverted teenager or young adult male who viewed hacking as a game. He was also from middle or upper class family. Hacking used to involve a elite group of individuals. The newer hacker stereotype is a socially awkward teenager (boy) with oversized glasses who never gets out. In reality, hackers can be very smart or of average intelligence, social or non-social, male or female, of all ages, and rich or poor.

Although most people consider hackers to be "bad people", many of them are not. Hackers can be divided into two groups: white-hat hackers and black-hat hackers. A cracker or hacker who breaks into a computer system or network with malicious intent, is a black-hat hacker. He/she takes advantage of the break-in, perhaps by stealing data or destroying files. In contrast, the white-hat hackers work with clients in order to help them secure their systems. These are "ethical" hackers. A samurai can be categorized as a white-hat, because this is a computer hacker who is hired legally to infiltrate corporate computer systems for legitimate reasons.

The hacker types mentioned above can again be divided into the following groups: "script kiddies", phreakers, competent programmers who modify existing tools and stars who build new tools.

Script kiddies and phreakers

The script kiddies are normally not technically sophisticated. They randomly seek out a specific weakness over the Internet in order to gain root access to a system, and do not really understand what he/she is exploiting. Someone else originally discovered the weakness. The script kiddies do not target specific information or a specific company, but use knowledge of a vulnerability to scan the Internet for a victim with that vulnerability.

Most hackers are script kiddies. They are estimated to be 90% of the total amount of hackers. This type of hackers is looking for an easy kill, and is looking for common exploits. The skills of these people are various. Some of them have no idea of what they are doing and what consequences it can lead to, while others are advance users who develop their own tools and leave behind sophisticated backdoors. Their methodologies are simple; they scan the Internet for a specific weakness, and when they find it, they exploit it. Most of the tools are automated, and they require little interaction.

Phreakers are people who crack the telephone network.

Competent programmers and stars

It is estimated that less than 10% of the hackers are competent programmers who modify existing tools, while the stars are real masters who build completely new tools. Less than 1% of the hackers fits into the star-category.

These real hackers look down upon the group of people who get a kick out of breaking into computers and phreaking the phone system, and call them crackers. They say that the crackers are usually the script kiddies, and the real hackers want nothing to do with them. They are considered lazy and not very bright. The hackers are the ones who build things, while crackers break them. To become a hacker, a person needs intelligence, practice, dedication, and hard work. The hackers have superior technical skills, are very persistent, and they often publish their exploits.

The Hacker Environment

The hacker culture does not have any leaders. It has culture heroes that have been around for a while and become well known. The community of expert programmers and networking wizards traces its history back to the first time-sharing minicomputers and the earliest ARPAnet experiments decades ago. Members of this shared culture were the ones who originated the term “hacker”.

Hackers share information through hacker clubs, publications, conventions, bulletin boards and newsgroups, Web sites, meetings, and through chatrooms. How large the environment is, is difficult to estimate, and different sources tell different things. Only one out of 10,000 or more people engage in hacking activity (Slawsky 2003). Another source (Graham 2001) says that about 100,000 hackers are skilled enough to bring down a major Internet portal for a few hours.

Most members of hacker clubs never physically meet, but they give a sense of companionship, and give the members help to work as a team toward common goals. By working as teams, they can achieve goals that can be out of reach for an individual hacker. Examples of hacker clubs are Legion of Doom (LOD), Chaos Computer Club, NuKE, and The Posse.

Some hacker clubs produce their own publications. Legion of Doom produces the hacker publication Phrack, and Chaos Computer Club produces Chaos Digest. The publications provide hackers with technical information, and they have a social function. Some publications are sent through postal mail, while others are received through electronic mail.

Many of the hacker conventions serve as venues for hackers to brag, swap stories, and exchange information. They tend not to be highly organized. Some hacker groups sponsor these conventions, like “the Chaos Congress” (sponsored by Chaos Computer Club) and “Hacking at the End of The Universe” (sponsored by Hack-Tic). DefCon is the largest underground hacking event in the world, held every summer in Las Vegas, USA. In 2001, more than 5,000 hackers were participants in the convention, and “Starla Pureheart” (a.k.a. Anna Marie Moore) was the first female hacker to win the ethical hacking contest that year. She is a good example of a hacker with sophistication, real skills, and ethics (Verton 2002) (Appendix E).

Internet newsgroups and bulletin board systems (BBS) are very similar, because they allow people a vast forum for communication. Hackers and hacker clubs primarily communicate through bulletin board systems, and the information found here is usually hot news. The difficult part can be to get access to a bulletin board, and as new members become more trusted, level of access to sensitive information increases.

Most of the hacking Web sites contain available hacking tools and free downloads of hacker programs. With these tools, instructions on how to perform attacks also follow. In addition, the number of hacking Web sites is increasing.

Chatrooms like IRC and ICQ are very popular for hackers to exchange information, and it is very common that the black-hats like to brag about their skills. An example of this, is the hacker "Mafiaboy". He is known for taking down Web sites like Yahoo, eBay, CNN, etc., in February 2000, and bragged over what he did on IRC. The chat log in the IRC hacker room *#!tnt* details a conversation between "Mafiaboy" (who has changed his nickname to anon (for anonymous))and other hackers (Appendix E) (Verton 2002):

T3: Mafiaboy, so who's next after dell
Anon: Microsoft will be gone for a few weeks
T3: oh man, that's evil
*T3: I need to get away from you before I get busted for being an accomplice or some sh***
Anon: I know what I'm doing
Anon: yahoo.com
*T3: So Mafiaboy, it was really you that hit all those ones in the news? buy.com, etrade, eBay, all that sh**?*
Anon: you just pin em so hard they can't even redirect
T3: they say you're costing them millions
Anon: surprised I didn't get raided yet, T3, they are fools

The communication on IRC is often very loose, and also the way that IRCers use and spell their language is very similar to their language used in an actual everyday conversation. Uncommon structure of sentences is also very common (Thorkildsen 2003).

It is not very common that hackers physically meet, but there are hacker clubs that have meetings for people that want to show up. 2600 (www.2600.org) have arranged meetings all over the world, and they all take place on the first Friday of the month. They meet in public areas like bars, at food courts at shopping centers, Internet cafés, or by a specific payphone. The meetings are free, and the target group is everyone interested in computers, telecommunications, security, and communications.

Table 3 illustrates some estimates of the hacker environment. The numbers vary greatly from one source to another, and is described closer with examples in *Appendix D.* Numbers of hackers vary from about one hundred serious hackers to hundreds of thousands. It is hard to estimate, because the sources may have different interpretations of what a hacker is, and the hackers use aliases to keep anonymous. Thereby, they can change their identity very quickly just by changing aliases. The table shows that there is an exponentially increase in number of Web sites, and also that the table is not complete because of the difficulty of finding data (numbers from 1999 and 2000 are lacking completely, and there are "holes" in the number of Web sites in 2001, and also in bulletin boards in 2002 and 2003. We did not find any numbers of publications, except from "dozens" in 1997).

- Table 3 Hacker Environment Information

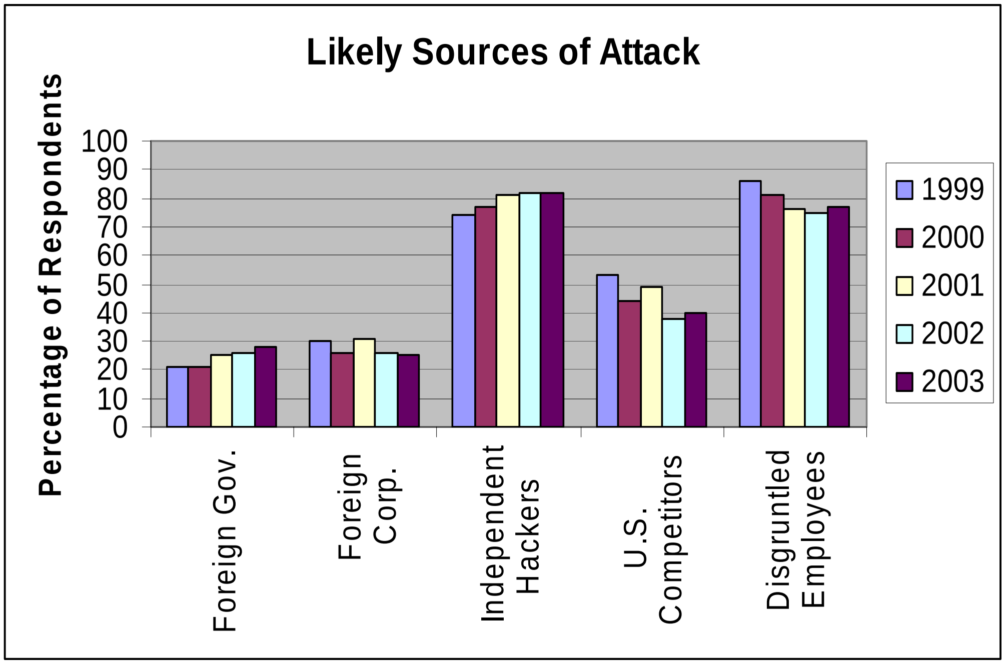
Hacker Information			
	Web sites	Publications	Bulletin Boards
April, 1997	1 900	Dozens	440
November, 1997	2 000		500
February, 1998	2 500		500
July, 2001			1 000
February, 2002	4 100		
February, 2003	6 000		

John Maxfield, a computer security consultant called a “hacker tracker”, estimated in 2001 that there were 50,000 hackers, and close to 1,000 bulletin boards. About 200 of the bulletin boards are “nasty”. This means they are posting credit card numbers, regional phone companies, banks, and have even authored tutorials on how to make bombs and explosives. Additionally, Maxfields estimates say that there were just 400 to 500 hackers in 1982, and every two years the numbers increase by a factor of 10 (Skidmore 2001).

Norris’s article from 1995 says that it was estimated to be about 1,300 underground bulletin boards only in the US. When this number is compared with table X, it shows that estimates are contrary to each other, and it is difficult to know which are most accurate. It is a good example in showing the problems with data collection, and we choose to believe in the numbers that seem reasonable compared to each other, and thereby disregard extreme numbers that do not seem to be correct. Still, we do not disregard the fact that we could have been wrong in some of our selection of sources, but we believe that the trends are realistic. In the conclusion of *Appendix D*, we have discussed this problem in connection with the number of hacker Web sites.

Hackers need three things to succeed; motive, opportunity, and means. The motive may be increased knowledge (intellectual challenge), a joy ride, or profit. Other motivations can be gang mentality, recognition, and theft of information, vandalism, blackmail, sabotage, or terrorism. *Appendix E* gives examples of this, as it contains information about different teenage hackers, and mentions some of their motives for hacking. The opportunity for people to hack systems has increased very much over the years, because computer systems can be found everywhere. The imagination and determination of a hacker is what limits the means of attack. *“Delete nothing, move nothing, change nothing, learn everything”* is a summary of the basic law of hacking (Norris 1995).

The motive of the hackers may affect which types of attacks they perform. Script kiddies might be hacking to gain knowledge and respect, while black-hats hack to find personal information and misappropriate information.



- Figure 8: Likely Sources of Attack. (CSI/FBI 2003 Computer Crime and Security Survey)

Figure 8 shows different likely sources of attacks. From 1999 to 2003, foreign governments and independent hackers have increased with 7 and 8 percentage points, respectively. These two groups can be considered growing threats. Foreign corporations, US competitors and disgruntled employees are more fluctuating, but they have all decreased from 1999 to 2003. Still, independent hackers and disgruntled employees are clearly the two most likely sources of attack.

Hacker Wars

Chris Belthoff, a senior analyst, said: *"These virus writers are fighting a war amongst themselves for attention and one-ups-manship, and we're all getting caught in the crossfire. The war definitely increases the chances that the variants will continue to come. But hopefully, it will help us pick up on clues as to who the virus writers are."* (Gaudin 2004)

More and more variants of worms are coming; the Bagle, Netsky, and MyDoom, and the viruses are devastating. The three viruses mentioned above, have infected more than 215 countries, and caused billions of dollars worth of damages.

Cyber wars are very efficient for the attacker from a risk/cost perspective, and the attacks can be just as damaging as physical attacks. It is also believed that the rivalry of the hackers leads to more attacks.

Why do hacker gangs fight each other? And how? We will try to answer these questions in the rest of this chapter.

IRC Wars and Bots

Hackers often use IRC channels (Internet Relay Chat). They use them to brag about their achievements and to chat with other hackers, but it is also used in cyber warfare in order to gain control of IRC chatrooms, and then keep control against attacks from rival gangs.

Several IRC servers offer hacker channels. The first person to start up a channel on an IRC server is automatically operator (OP). He has the power to kick off people, or invite people in, and he may also pass on the operator status to someone else.

"A hacker can get control of a chatroom by kicking off all the rival moderators. This is a way for hacker gangs to gain control of IRC chatrooms, and then keep control against attacks from rival gangs. Hackers are using a method called "the flood", which is a technique where a hacker sends a huge number of pings against the victim. There will be so much meaningless traffic that nothing else can get through." (Appendix G).

In the turf wars between hacker clubs, hackers run "bots" (automated programs). These bots are left behind in machines that the gangs hack into, where one kind of bot tries to stay logged onto the IRC chatroom, becomes moderator, and pass moderation privileges to other bots. Another kind of bot tries to use DoS on existing moderators from the defending gang in order to kick them off. As the defenders lose control, they become the attackers. The attackers can be using more DoS-bots, while the defenders are using more IRC-bots in order to maintain control.

IRC wars are still a small segment of the overall hacker community.

Hacktivism

Hacktivism is political hacking on the Internet. Patriotic hackers and religion extremist groups are common hacktivists, while peace activists who are against war is a new development of hackers. Hundreds of Web sites have been hacked by peace activists. This kind of hacking has been called the "new era of cyberwar". "Pr0metheus" is an example of a religious hacker (Verton 2002). He hates organized religion, especially Christianity, and replaced Christian Web sites with his own liturgy on the principle of Satanism. See also *Appendix E*.

Hacktivism began with a series of so-called network-direct actions against Web sites of the Mexican government in 1998. This became popular with the Israelis and Palestinians in the Middle-East crisis. Tactics like Web site defacement, worm and virus infections, DoS attacks, Web site sit-ins, and e-mail bombings have become popular in times of political crisis. Mig2 expected the damage on computer systems worldwide due to hacktivism to be $20 million in 2003.

The hacker turf wars seem to be battles for control of cyberspace, and the war is for power and seniority among authors of viruses or worms. Version J of the Bagle worm, had the following provocative statement in it: *"wanna start a war(?)"* (Koprowski 2004).

Cyber terrorists will probably use DoS and DDoS tools more and more, because they can be very destroying, and it is a "new" way to have a war between countries, as well as other groups. The point of cyber attacks is to terrorize, and it can impact an economy or jobs. But al-Qaida or some other Islamic extremist group are not solely to blame for these kinds of terrorist attacks, because some cyber crime comes from unethical businesses that seek to spy on, or sabotage, competitors.

Modeling the Threat to Information Security

In this chapter we will look at the paper "Modeling the Lifecycle of Software-based Vulnerabilities" by Johannes Wiik, Jose J. Gonzalez, Howard F. Lipson and Timothy J. Shimeall, and discuss the system dynamics model "software vulnerability lifecycle" within the paper.

System Dynamics

"System dynamics is a powerful method to gain useful insight into situations of dynamic complexity and policy resistance" (Sterman 2000). The method can be used in different contexts and different modeling processes – from large, data intensive models to very small models. System dynamics can be used to help solve high-stakes problems in real-time. It was developed by Jay Forrester to show how a model of the structure of a human activity system and the policies used to control it, could be used to deepen our understanding of the operation and behavior of that system.

An important tool for representing the feedback structure of systems, are causal loop diagrams (CLDs). The diagrams consist of variables connected by causal links shown by arrows denoting the causal influences among the variables. The links are either positive (+) or negative (-), and this shows how the dependent variable changes when the independent variable changes. When the link is positive, it means that if the cause increases, the effect increases above what it would otherwise have been. If the cause decreases, the effect decreases in below that it would otherwise have been. If the cause increases, and the effect decreases below what it would otherwise have been, and if the cause decreases, and the effect increases above what it would otherwise have been, the link is negative.

A loop identifier highlights the important loops, and indicates whether the loop is a positive (reinforcing) or negative (balancing) feedback. The identifier circulates in the same direction as the loop to which it corresponds.

For the modeling and simulation model below, the tool PowerSim® Studio Academic 2003 was used. There are specific diagramming notation for stocks and flows in system dynamics, where stocks are represented by rectangles, and inflows and outflows are represented by pipes (arrows) pointing into and out of the stock, respectively. Valves control the flows, while clouds represent the sources and sinks for the flows.

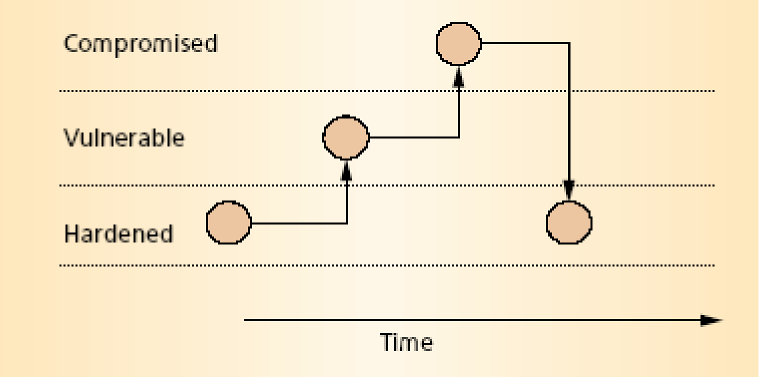
The Single Vulnerability Problem: "Modeling the Lifecycle of Software-based Vulnerabilities"

Introduction to the Model

"Many of the contributing factors to computer security problems are non-technical in nature – that is, they are dependent upon human and organizational actions and interactions in the political, social, legal, and economic realms. However, much of the research in computer security has had a predominantly technical focus. This paper represents a first attempt at using the concepts of system dynamics to model some of the human and organizational actions and interactions that impact the software vulnerability lifecycle. It represents the relationship over time between the discovery of security vulnerabilities (i.e., flaws) in software, and the occurrence of computer security incidents based on the exploitation of those vulnerabilities by attackers. Although our initial model relies on several simplifying assumptions, it points the way towards richer and more comprehensive models that can increase our capabilities and understanding in ways not possible through traditional computer security research approaches" (Wiik, Gonzalez et al. 2004).

Before we show the model, we would like to give a short description of the "host life cycle" and the "single vulnerability lifecycle" described by (Arbaugh, Fithen et al. 2000; Wiik, Gonzalez et al. 2004).

Computer systems oscillate between three different states, considering vulnerabilities. This is what is called the "host lifecycle". The three different states are hardened, vulnerable, and compromised. A host is hardened when all security relations are installed, typically installed with patches. The host enters a vulnerable state when at least one security related correction has not been installed. If the host is successfully exploited, it eventually enters the compromised state. The only state that is safe is the hardened state, and this is where system administrators want to keep their systems.



- Figure 9: Host life cycle. (Arbaugh, Fithen et al. 2000)

The "vulnerability life cycle" has several states. We refer to Figure 1. The states are:

Birth – the flaws creation (programmers make mistakes or have malicious intensions).

Discovery - someone discovers that the product has a flaw.
Disclosure - discoverer reveals details of the problem to a wider audience.
Correction - release of correction to the flaw, from vendor or developer.
Publicity - vulnerability known on a large scale, once the disclosure gets out of control.
Scripting - simplification of intrusion techniques, which exploit the vulnerability.
Death – when the number of systems the vulnerability can exploit shrinks to insignificance.

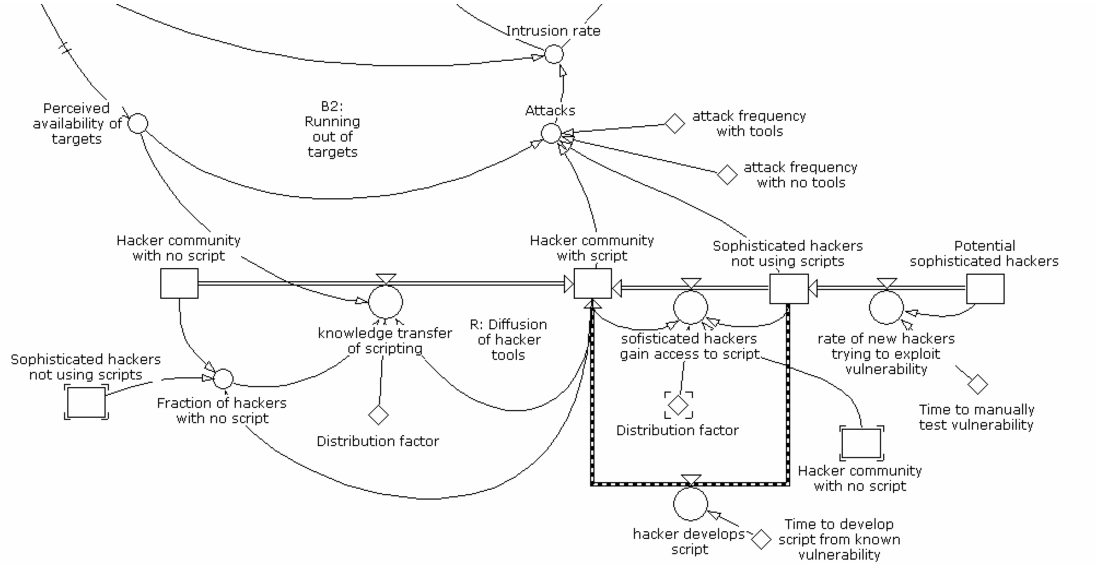
With this and the chapter “The Threat to Information Security” in mind, we present the SD model in the next section.

The Model

The model is divided into two parts, one attacking part, and one defending part.

The attack sector

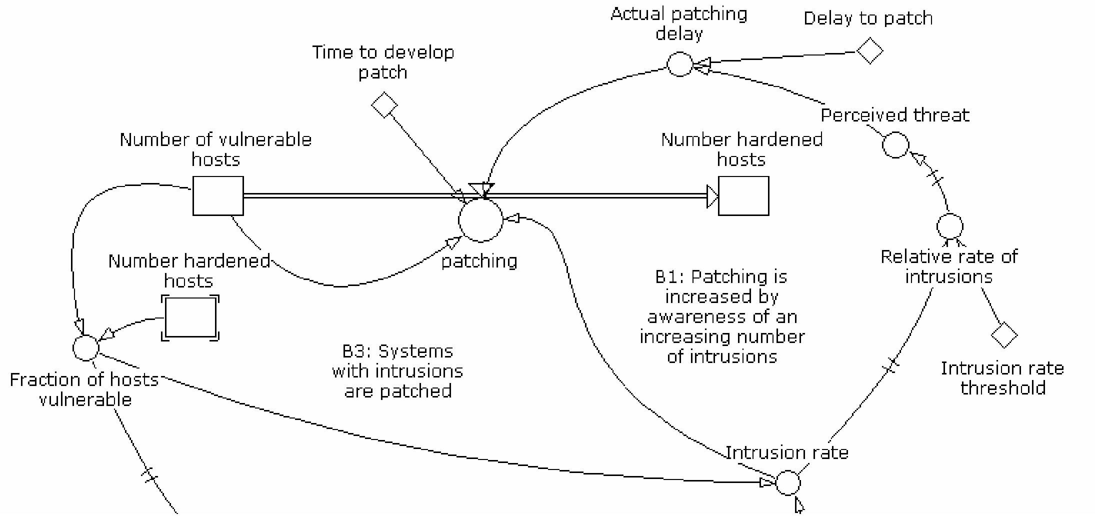
Advanced hackers are the only ones that have knowledge to attack in the beginning, so the first attacks, on a single vulnerability, typically come from advanced hackers. Such great skills are very rare. After gaining more knowledge of the vulnerability, scripts are developed by these advanced hackers, and through the hacker community, the scripts spread to hackers with less knowledge. Therefore, the scripts result in more potential hackers, and an increase in attack frequency for each hacker. See figure 10.


Intrusion rate
Perceived availability of targets
B2: Running out of targets
Attacks
attack frequency with tools
attack frequency with no tools
Hacker community with no script
Hacker community with script
Sophisticated hackers not using scripts
Potential sophisticated hackers
knowledge transfer of scripting
R: Diffusion of hacker tools
sofisticated hackers gain access to script
rate of new hackers trying to exploit vulnerability
Sophisticated hackers not using scripts
Fraction of hackers with no script
Distribution factor
Distribution factor
Time to manually test vulnerability
Hacker community with no script
hacker develops script
Time to develop script from known vulnerability

• Figure 10: The attack sector.

The defense sector

Figure 11 considers patching as the main defense mechanism. For a large number of hosts there is often a long delay to become patched, and for some hosts patching is never considered. However, the delay time decreases if the perceived threat is high. Publicity and awareness of increasing numbers of intrusions have the effect that administrators patch their systems quicker. This leads to more hardened hosts, which again affects the hackers that find fewer targets.


Actual patching delay
Delay to patch
Time to develop patch
Perceived threat
Number of vulnerable hosts
Number hardened hosts
Number hardened hosts
patching
B1: Patching is increased by awareness of an increasing number of intrusions
Relative rate of intrusions
Intrusion rate threshold
B3: Systems with intrusions are patched
Fraction of hosts vulnerable
Intrusion rate

• Figure 11: The defense sector

Problems with patching

Patch management is tough because there are too many patches and not enough time. Exploits to announced vulnerabilities are also materializing faster. Both clients and servers are attack targets, and the vulnerabilities are with Microsoft, Unix, and Linux.

The biggest mistake that companies make is leaving out the processes. People are looking for a tool that will save all their problems, but it is not just about the tool. To get less vulnerable, one needs diligent monitoring for new patches coupled with detailed evaluation, testing, deployment and validation that a team or individual manages.

Before a patch management process can be installed, the following pieces must be in place: network inventory, change management, configuration management, asset management, formalized record keeping, and an understanding of costs, prioritization guidelines, and maintenance and communications plans.

Companies have different procedures in patch management, and some are better than others. The time before patching varies a lot. We believe that Pitney Bowes is a good example of patch management: the client desktops are given a risk profile from 1 to 5, where 5 are the clients that must be the most secure. The desktops that are rated a 5 must therefore be patched in less than 24 hours. The worst security incidents have taken from 1,000 to 1,500 person-hours to correct, but the time is now down to 75 hours (Fontana 2003).

Agder University College is doing their patching about every two weeks on their Windows servers. Nevertheless, they keep an eye on what is happening, and if a new important patch is coming in, it will be installed as soon as the security experts are sure that it will not make any problems.

Model discussion

Critical and substantial variables and constants

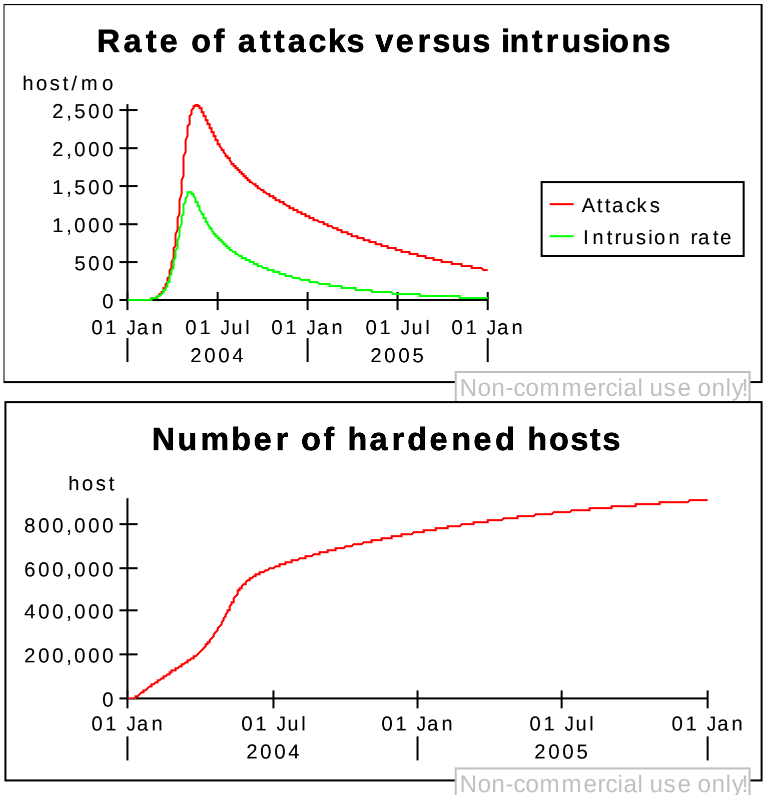
Let us look at the constant “Delay to patch” in the model. This constant affects the variable “Actual patching delay” together with “Perceived threat”. The definition of “Actual patching delay” is as follows: 'Delay to patch'*(1-'Perceived threat')

Initially “Delay to patch” is set to 12 months. This is probably a good estimate:

“*The most compelling conclusion from this research, however, is the surprisingly poor state in which administrators maintain systems. Many systems remain vulnerable to security flaws months or even years after corrections become available.”* (Arbaugh, Fithen et al. 2000)

The release of the patch can vary in relation to the vulnerability’s publicity, and vendor’s effort. However;

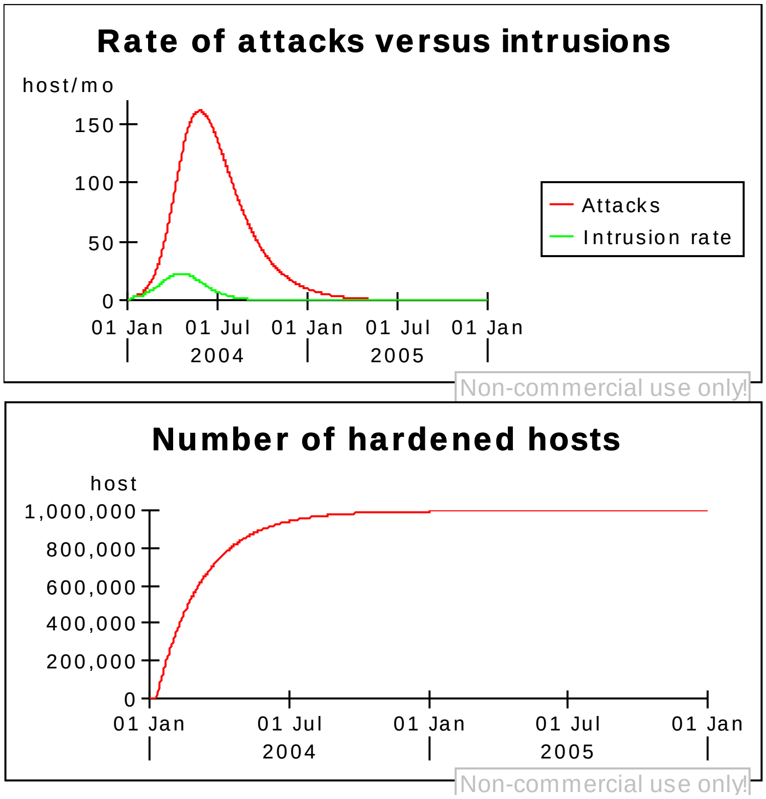
“- Nachi, Klez. Lovsan, SoBig, BugBear, Swen, Blaster and Yaha – represent only a sampling of the most prevalent worms and viruses that slithered into corporate networks this fall. But they all have one thing in common: Patches were readily available before most damage had been done.” (Fontana 2003)



- Figure 12: “Delay to patch” is 12 months

We look at the graphs in Figure 12 “Rate of attacks versus intrusions” and “Number of hardened hosts” with “Delay to patch” set to 12 months. The model shows that most attacks happen before the majority of hosts are hardened, and approximately 4 months after disclosure.

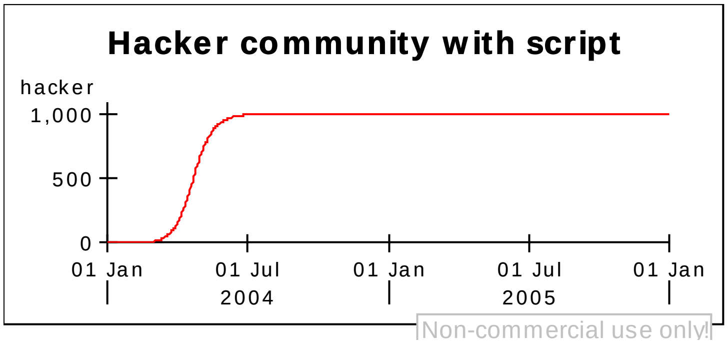
If we decrease the time “Delay to patch” to 2 months, as shown in Figure 13, we will see an enormous effect on the graphs. The result is that the majority of hosts are hardened before the attack wave comes, and the intrusion rate is therefore very small.



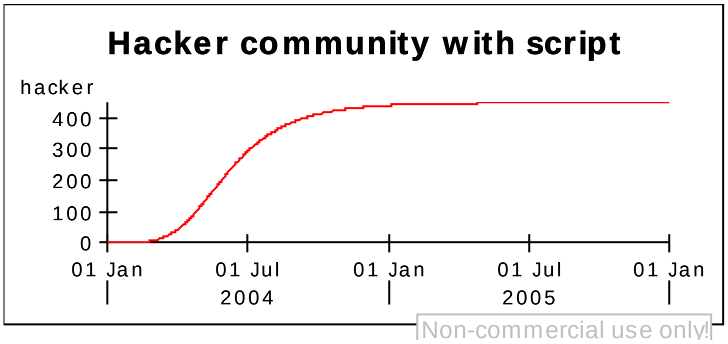
- Figure 13: “Delay to patch” is 2 months

Clearly, the patching process matters. The question is how organizations should manage their patching process (Fontana 2003).

If we look at the graph “Hacker community with script” in Figures 14 and 15, it also differs in result of hackers, considering the two states of “Delay to patch”. In both situations, there is an s-shaped curve, typical for the “word of mouth” effect. At the end of “simulation time”, the two graphs are flattening off at respectively 1,000 hackers and 400 hackers.



- Figure 14: “Delay to patch” is 12 months



- Figure 15: “Delay to patch” is 2 months

This means that fewer hackers will have the “script” when the “Delay to patch” is two months. Because the patch came earlier, the “Perceived availability of targets” decreases, and not that many hackers will therefore bother to gain the script. That does not mean that the availability of the script is poor.

What our searches show, is that the hacker community is growing *(Appendix C and D)*. There are more bulletin boards, publications and web sites than ever. Most of these media have direct links to attacking tools or “hacking information”. We believe that a publication of an attacking tool, would give a “jump in attacks” on that vulnerability, because of the “script kiddies”.

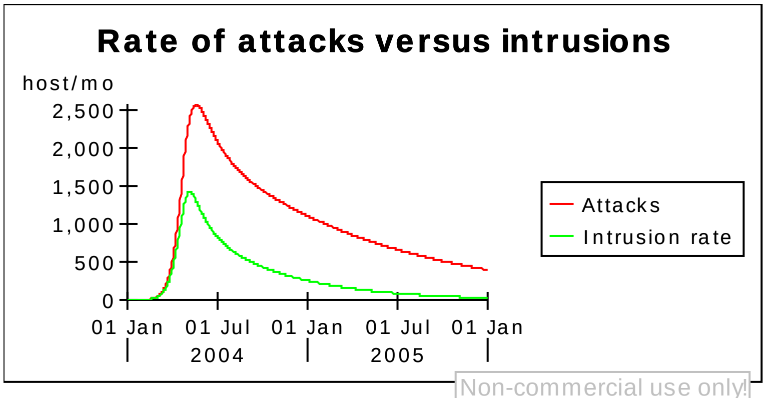
To show the devastating effect of the attack tool, we will examine the constants “attack frequency with tools”, and “attack frequency with no tools”.

Initially, the constant “attack frequency with tools” is set to 1 host/(wk/hacker), and “attack frequency with no tools” is set to 1 host/(mo/hacker). See Figure 15.

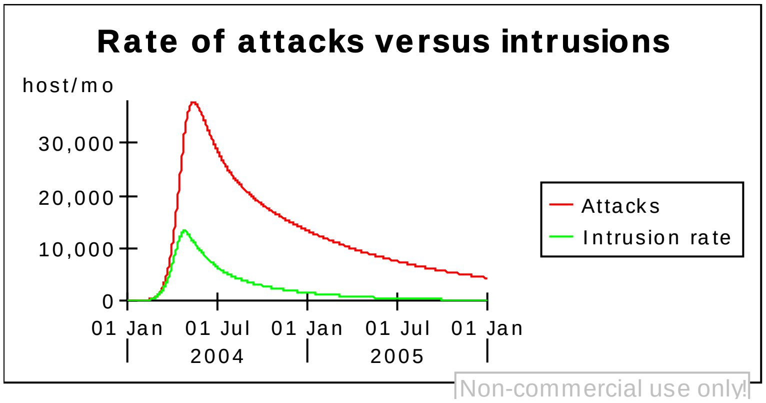
The “attack frequency with tools” is of course largest (four times the “attack frequency with no tools”), but rather moderate compared with what attack tools can accomplish.

”In the past, intruders found vulnerable computers by scanning each computer individually, in effect limiting the number of computers that could be compromised in a short period of time. Now intruders use worm technology to achieve exponential growth in the number of computers scanned and compromised. They can now reach tens of thousands of computers in minutes where it once took weeks or months.” (Pethia 2001).

Because of this, it would not be “wrong” to experiment larger numbers of frequency. In Figure 17, we set “attack frequency with tools” to 100 host/(mo/hacker), which still is moderate.



• Figure 16: "attack frequency with tools” is set to 1 host/(wk/hacker)



• Figure 17: “attack frequency with tools” is set to 100 host/(mo/hacker)

After 4 months, we see that attacks grow above 30,000 host/mo, compared to 2,500 when the "attack frequency with tools" was 1 host/(wk/hacker) (Figure 16), and that intrusion rate grow above 10,000 host/mo, compared to 1,500 host/mo.

This tells us that the effectiveness of an attacking tool can be tremendous.

Proposals to extend the model

The model assumes that after a while, a sophisticated hacker produces a script for this special vulnerability and that a larger scale of hackers starts to use the script. The definition of "script" is diffuse. If we use the term as defined in (Arbaugh, Fithen et al. 2000), it *"applies to any simplification of intrusion techniques that exploit the vulnerability, such as cracker "cookbooks" or detailed descriptions on how to exploit the vulnerability".*

This means that the script is not necessarily a sophisticated attack tool. This would lead to less activity on the vulnerability, because people would not have the skill enough, or they would not care to use the cookbooks, or descriptions to exploit the vulnerability.

The authors define the script as an attack tool: "*We did not include the process of further improved attack tools in this model but have kept it on an aggregated level with one type of automated tool that we call script*".

In reality, there are not developed attack tools for all vulnerabilities. We believe that only for "popular" vulnerabilities, it would be created sophisticated attack tools, leading to more interest from hackers with less knowledge, and therefore more attacks.

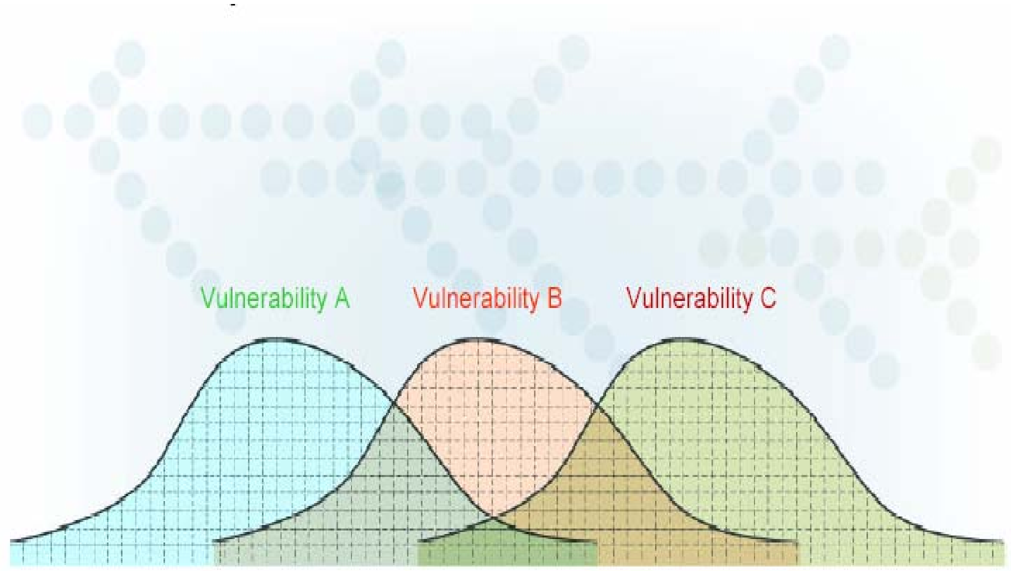
In addition, if there are not created sophisticated attack tools, there will not be as many attacks, according to the model. Since this model always assumes that there will be created a script for the vulnerability, perhaps it is suited for "popular" vulnerabilities.

Therefore, a more precise definition of "script", or split in definition, could extend the model. E.g., one could distinguish between vulnerability that has sophisticated tool(s) to exploit, and vulnerabilities that have not.

The Multiple Vulnerability Problem

Hacker tools often combine exploits of different vulnerabilities. The automation of an exploit creates a tremendous growth in exploits. Consequently, a single script can actually influence the life cycle of several vulnerabilities simultaneously.

Often, exploiting one vulnerability intensify the exploit of another vulnerability. This could be one reason for why the exploitation cycles of various vulnerabilities overlap, as shown in Figure 18.



• Figure 18: Multiple Vulnerabilities (© 1998-2003 by Carnegie Mellon University)

Another reason would be that within the hacker community there is competition of whom is the “cleverest”. Therefore, various vulnerabilities are used in the competitions between the hackers. Defenders will experience this as waves of attacks.

More and more worms are using multiple methods of propagation. They are attempting to exploit multiple vulnerabilities in widely used Internet services, which means that they can spread at a faster rate (Magee 2003).

A model describing multiple vulnerabilities would include many of the same variables as the single vulnerability model. However, it should also have some extra factors as well. This can e.g. be to have different vulnerabilities in different variables, and possibly with a patch for each of them since one can have many vulnerabilities and only some of them may get patched (but if a person gets aware of his/her vulnerabilities, he/she would probably patch everything, and not just install one or two patches).

The different vulnerabilities should also have different start-up periods in a model, since all of the vulnerabilities will not start at the same time.

The model could also include recruitment to the hacker community, how the hackers pick various vulnerability types, and the research and development pipeline in the hacker community.

Denial of Service (DoS) Attacks and Distributed Denial of Service (DDoS) Attacks

Denial of Service

The first publicized example of a denial of service attack against an Internet host, happened in September 1996, and the computers of Public Access Networks Corporation (Panix), a New York ISP. The method used was SYN flooding; a type of packet flooding attack described closer below.

Denial of service (DoS) is a type of attack that is designed to hang or crash a program, or bring down the entire system, by flooding it with useless traffic. The goal of exploits that shut down services is typically to knock out a server, router, or other system so that users can no longer access the process or service it supports. Attacks that exhaust system resources have the situation where the service may stay up, but users cannot reach it because the system's resources are overwhelmed, typically by bogus requests. This can be resources such as bandwidth, CPU cycles, and memory. However, the basic idea is the same for all DoS attacks: to flood the target with so much stuff that it shuts down.

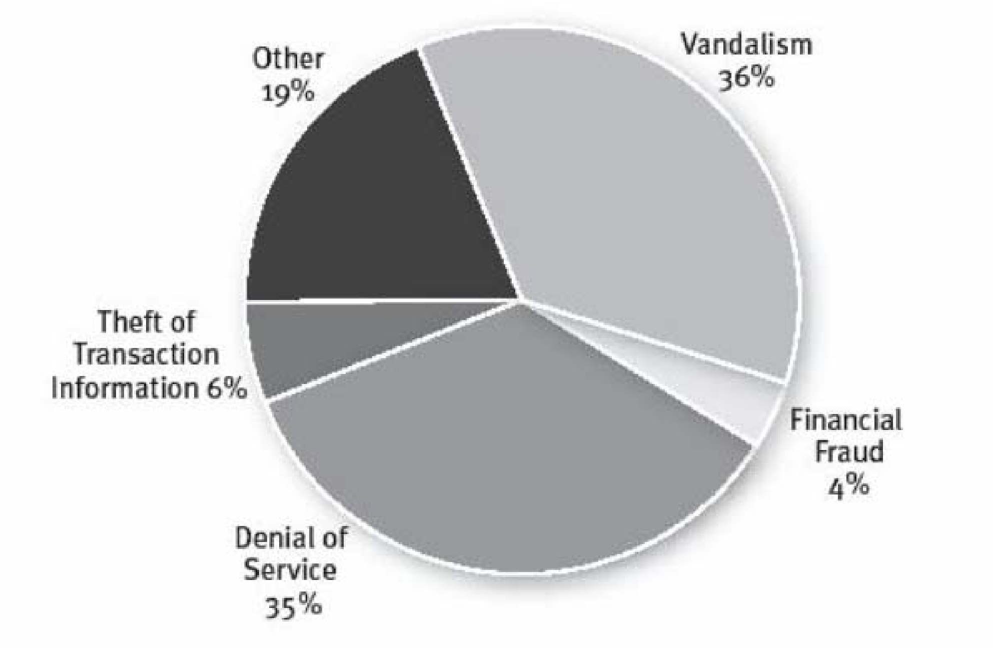
Packet flooding and logic attacks are two common methods for initiating a DoS attack:

- Packet flooding attacks; are aimed at overwhelming the target with spurious traffic and overloading it. The receiver gets exploded with multiple connection requests, but he fails to send the necessary acknowledgements in return. The result is half-open connections that tie up resources and prevent legitimate connections from being made. Consequently, any legitimate traffic, which becomes a fraction of the total traffic, is denied service. SYN flood attacks, Internet Control Message Protocol (ICMP) flood attacks, Smurf attacks, Trinoo, Tribe Flood Network (TFN), Shaft, Stacheldraht, Trinity, Targa3, and FloodNet are examples of attacks that involve packet flood exploits.
- Logic attack; the use of malformed packets are typically geared toward crashing a service. It exploits known software bugs on the target system in an effort to take it offline. The attacks exploit errors in TCP/IP stack by sending typically formatted packets. Buffer overflow is a common result of a logic attack. It occurs when too much data is written to a buffer, which can result in overwriting of data in adjacent buffers, alteration of data, file damage, and system crashes. Examples of malformed packet attacks are Ping of Death, TearDrop, NewTear, Bonk, Syndrop, Chargen, WinNuke, Land, and Joltz.

• Table 4: Denial of service attacks detected (by percent)

Year	DoS attacks
1998	31
1999	27
2000	36
2001	40
2002	42

The number of DoS attacks is increasing, from 31% in 1998 to 42% in 2002 (Table 4), and DoS attacks are a big part of Web site incidents, as seen in Figure 19.



• Figure 19: Web site incidents (CSI/FBI 2003 Computer Crime and Security Survey)

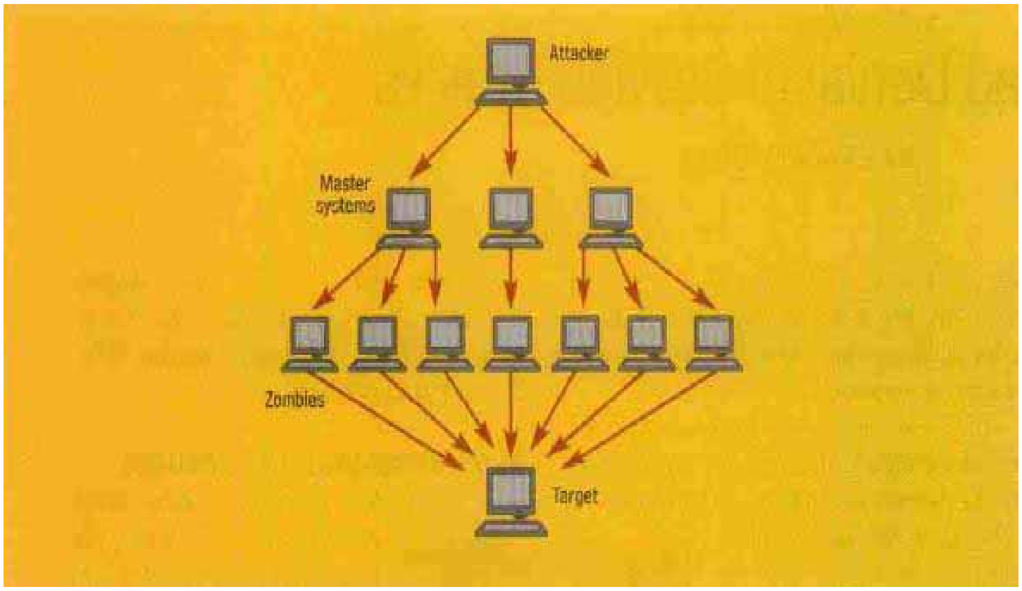
In 2002, denial of service attacks led to big financial losses. Theft of proprietary information was the attack type with the worst losses ($70,195,900), while DoS attacks came on a second place, with a loss of $65,643,300.

Distributed Denial of Service

A DDoS attack has the same impact on a target as a DoS attack. The difference between them, is that a DDoS attack originates from multiple machines on the Internet, while it originates from a single machine in a DoS attack. Distributed denial of service attacks are based on many of the same mechanisms as DoS attacks, but they are more complex and have the potential to do damage that is more widespread. Bruce Schneier compares DDoS attacks with a pizza delivery attack: Alice does not like Bob, so she calls a hundred pizza delivery parlors, and has a pizza delivered to Bob’s house at 11 p.m. from each one of them. The pizza parlors are all demanding their money at 11. They are the victims, and the attacker is nowhere to be seen (Schneier 2000).

The first widely publicized DDoS attack occurred in 2000, when the hacker “Mafiaboy” launched an assault using easily accessible tools from the Internet. Yahoo, CNN, Amazon, eBay and eTrade were among the victims of the fallout. The FBI estimated that it took about 50 machines to take down Yahoo. This does not mean that the tools used are sophisticated, or that the hacker is skilled.

To do DDoS attacks, the attacker first chooses the exploit and the attack type. He/she can download the software from the Internet, and compile the program. The attacker then enlists zombie systems to form an army of unwitting participants. To find these, the attacker scans the Internet for vulnerable IP addresses with a scanning tool (an RPC scanner program). Most machines will be immune to the scripts because of firewalls, but that still leaves hundreds of machines that is successfully hacked. After doing this, the attacker downloads a daemon (a program that executes command strings from the master system, onto the zombies). This gives the hacker complete control, and he/she should put a master control program on every 20th machine. When the command sequence is sent from the master system, the zombies will attempt to execute the attack, by for example bombarding the target with packets. See Figure 20.



- Figure 20: The DDoS Deluge (Clark 2003)

DDoS attacks will become more difficult to detect as they evolve, and they will be able to compromise more and more systems within shorter windows of time. There is also an increasing availability of more sophisticated automated tools for scanning and deployment, which means that the DDoS attack tools are becoming easier for less skilled attackers to launch.

Worms are not typically intended to be mechanisms for DoS or DDoS attacks, but they can result in serious denial of service conditions. When a worm is launched, it can spread to systems that were not deliberately selected as targets.

There are many types of DDoS attacks that can be launched, and the German hacker “Mixter” has written a couple of them: TFN (Tribe Flood Network), and its sequel, TFN2K. See more about DDoS tools in Table 5 (page 59-60).

Attacks rates of DoS/DDoS attacks are alarming: 500 packets per second can over-whelm a commercial server. And it takes 14,000 packet per second to disable a server with specialized firewall designs. In 2001, it was suggested that 4,000 DDoS attacks happen across the Internet each week, and the number is probably far higher now. A study estimated that 2.4 percent of all attacks could break through highly tuned/optimized firewalls (Sigmond and Kaura 2001).

There are three aspects to tackling DDoS: detection, identification of the source, and solution. The biggest challenge of reliable detection is separating normal traffic from spurious traffic, and several algorithms are used for detection. The identification of the source involves backward tracing the path of attack and identifying the key devices that are responsible for the spurious traffic, like routers and switches. The solution may involve filtering the traffic and/or the complete/partial shut down of a certain network path.

A DoS Case

The two German hackers, “Mixter” (a.k.a. Kemal A.) and “Randomizer”, had a turf war going on between their hacker clubs. They were both pioneers in the making of DoS tools. As mentioned in the previous part about DDoS, “Mixter” is the writer of the attack tool TFN and its sequel TFN2K. And “Randomizer” is the writer of Stacheldracht. These are all DDoS tools. TFN was the tool that “Mafiaboy” used to take down the major Web sites in February 2000.

“Mixter” and “Randomizer” were leaders of these two separate hacker clubs in Germany, and a war started up between their clubs around 1998 about the possession of IRC chatrooms (the part about “IRC Wars and Bots” describes how hackers work to gain control of IRC chatrooms (page 30)). They competed for bragging rights. “Mixter” got sentenced for computer sabotage, spying for data, and other attacks on businesses in 1998, and moved to Israel to live there for a few years.

In 2000, “Mixter” got sentenced to a 6-month youth prison sentence for computer sabotage, spying for data, and other attacks on businesses in 1998. The sentence got suspended to a two-year parole period.

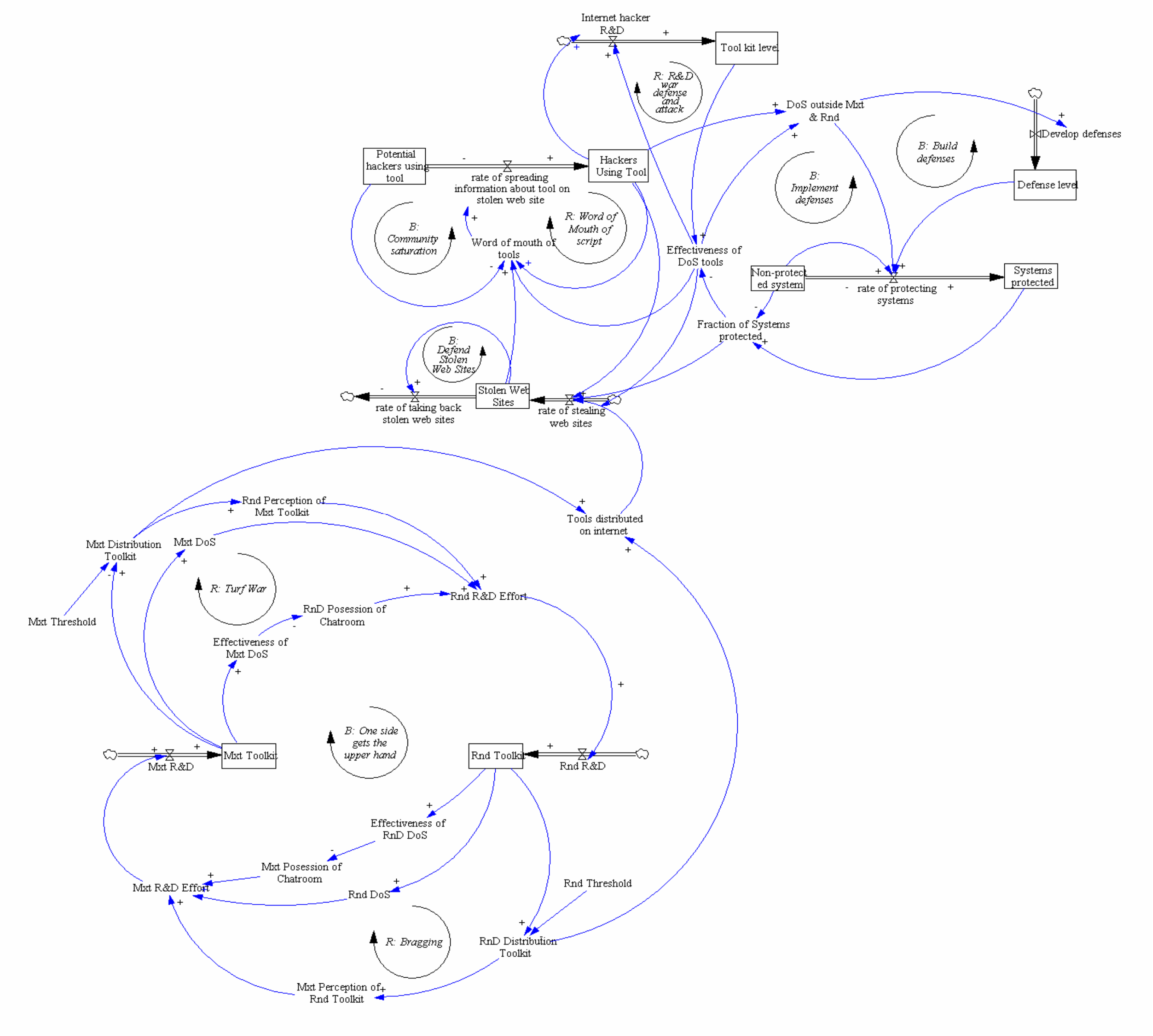
This particular case, along with some general information about the hacking and Internet environment, is modeled in a causal loop model in the following chapter.

Causal Loop Model

To describe the causal loop model in Figure 21, we divide the model into two parts, and describe the parts separately. As one can see from Figure 21, the top-part of the model is the general part about hackers, stealing of Web sites, the effect of word of mouth, and protection of systems, shown in Figure 23. The bottom part is more specific, Figure 22. It describes the case of “Mixter” and “Randomizer”[3]; their turf war, which side gets the upper hand, bragging, etc.,

More about system dynamics and causal loop diagrams in “System Dynamics” (page 32).

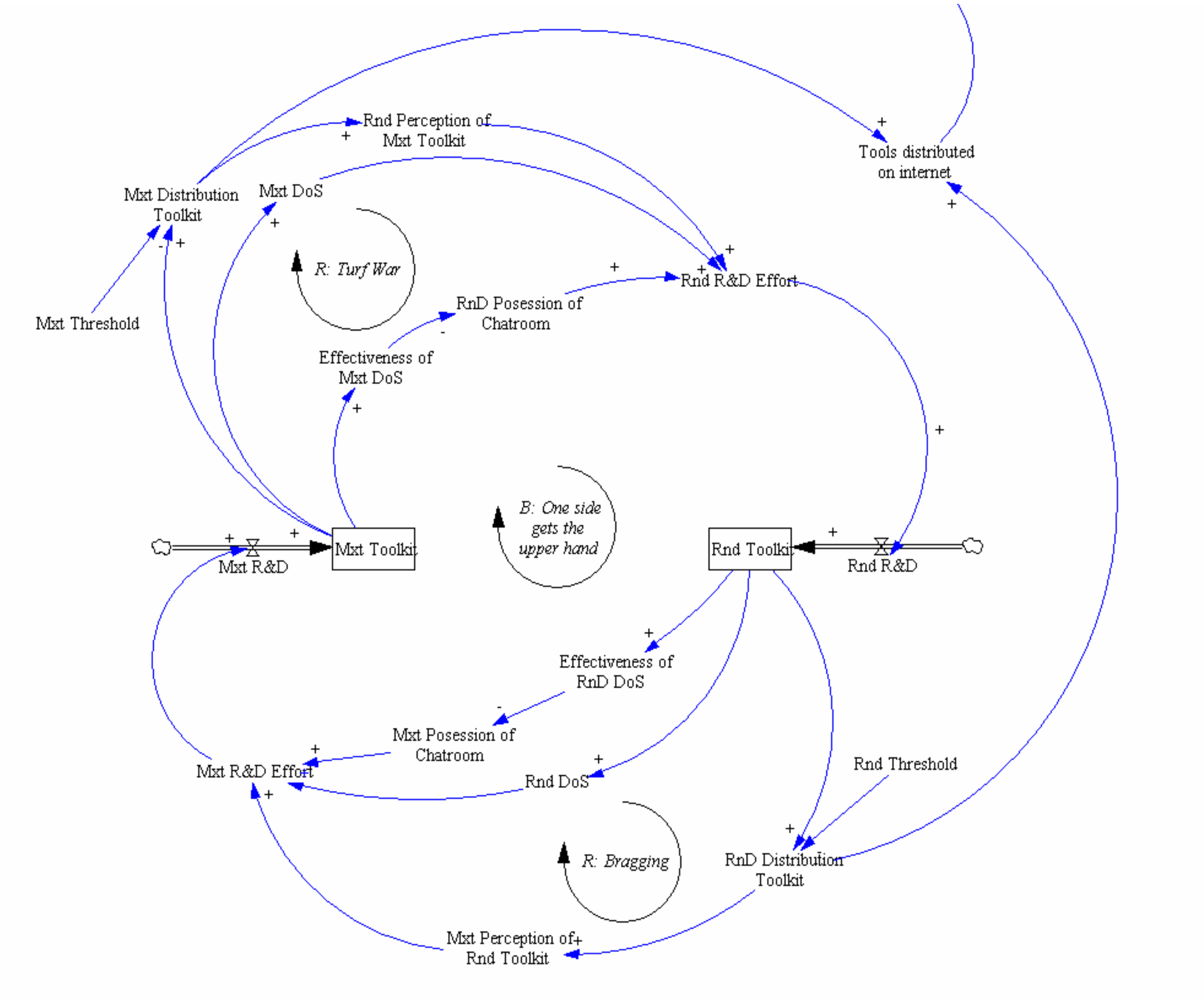
[3] Actually, it is the hacker groups led by ”Mixter” and ”Randomizer”.


Internet hacker R&D
Tool kit level
R: R&D war defense and attack
DoS outside Mxt & Rnd
Develop defenses
B: Build defenses
Defense level
Potential hackers using tool
rate of spreading information about tool on stolen web site
Hackers Using Tool
B: Implement defenses
B: Community saturation
R: Word of Mouth of script
Word of mouth of tools
Effectiveness of DoS tools
Non-protected system
rate of protecting systems
Systems protected
Fraction of Systems protected
B: Defend Stolen Web Sites
Stolen Web Sites
rate of taking back stolen web sites
rate of stealing web sites
Rnd Perception of Mxt Toolkit
Tools distributed on internet
Mxt Distribution Toolkit
Mxt DoS
R: Turf War
Rnd R&D Effort
RnD Posession of Chatroom
Mxt Threshold
Effectiveness of Mxt DoS
B: One side gets the upper hand
Mxt R&D
Mxt Toolkit
Rnd Toolkit
Rnd R&D
Effectiveness of RnD DoS
Mxt Posession of Chatroom
Mxt R&D Effort
Rnd DoS
Rnd Threshold
R: Bragging
RnD Distribution Toolkit
Mxt Perception of Rnd Toolkit

- Figure 21: DoS War

“Mixter” and “Randomizer”

Figure 22 can be divided into two equal parts, one side with the case of “Mixter”, and one side with “Randomizer”. When we describe this part of the CLD, the “Mixter”-side is exactly the same as “Randomizer”’s side, only with their names switched. One side can be looked upon as the reflection of the other (except from the names).



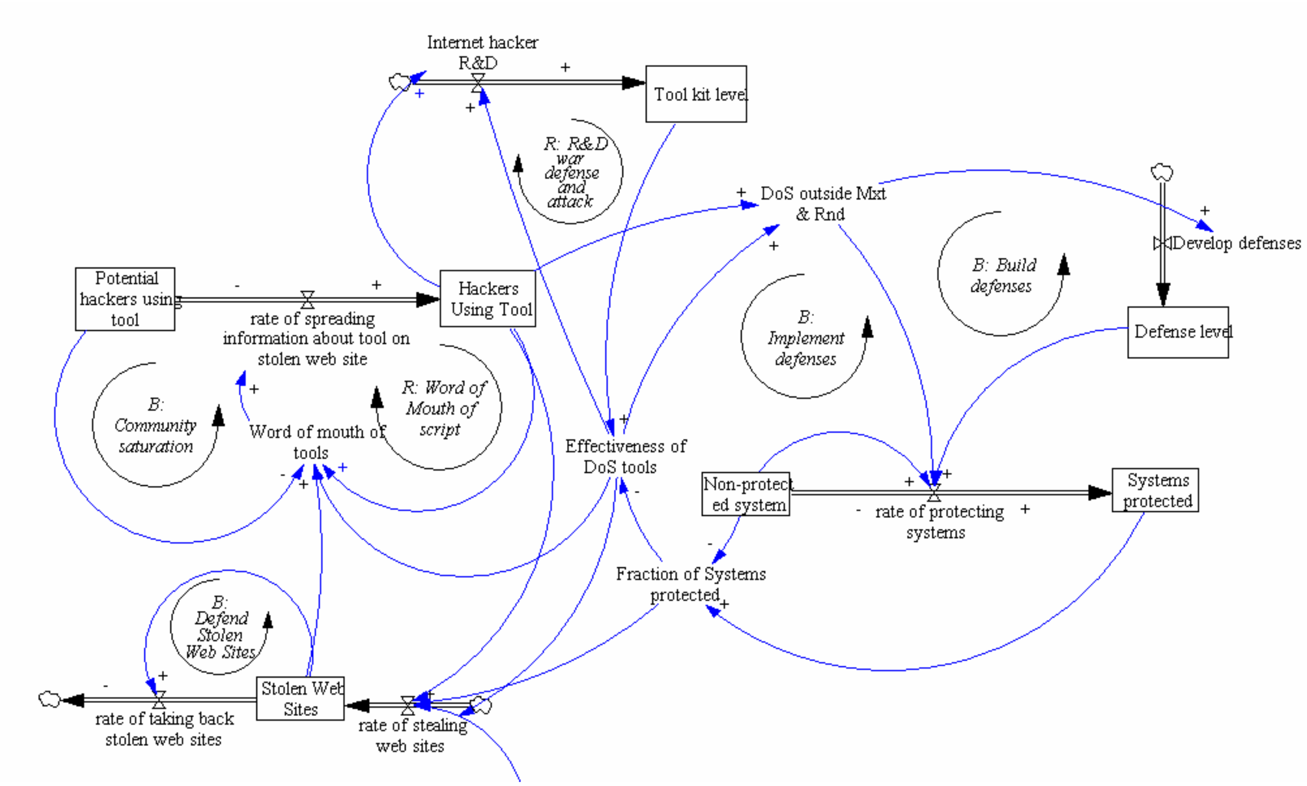
• Figure 22: The case of “Mixter” and “Randomizer”

Figure 22 has two flows; “Mixter”’s and “Randomizer”’s research and development (R&D). These flows are involved in all three causal loops in the model. The inner causal loop, “B: One side gets the upper hand”, includes the hackers’ research and development, their toolkits, the effectiveness of their DoS tools, one side’s possession of chatroom, and their effort in R&D. The loop is balancing because of the possession of chatrooms, which can change from side to side.

The “R: Turf war” – loop includes the hackers’ R&D, their toolkits, DoS, and effort in R&D. The tools get better and better as one side sees that the other side improves, and the loop is therefore reinforcing. The sides are competing to be better than the other, so an improvement in “Mixter”s DoS tool leads to an improvement in “Randomizer”s DoS tool, and vice versa.

Distribution of a toolkit, and the perception of the other's toolkit, make the "R: Bragging" – loop together with effort in R&D, R&D, and the toolkits. Hacker's bragging on IRC is described further in "The Hacker Environment" (page 27). The threshold affects the distribution, and the distribution affects the tools distributed on the Internet. This variable, "tools distributed on Internet", affects the other part of the model, Figure 23, which is to be described next.

Hackers and the Internet World


Internet hacker R&D
Tool kit level
R: R&D war defense and attack
DoS outside Mkt & Rnd
Develop defenses
B: Build defenses
Defense level
Potential hackers using tool
rate of spreading information about tool on stolen web site
Hackers Using Tool
B: Implement defenses
B: Community saturation
Word of mouth of tools
R: Word of Mouth of script
Effectiveness of DoS tools
Non-protected system
rate of protecting systems
Systems protected
Fraction of Systems protected
B: Defend Stolen Web Sites
Stolen Web Sites
rate of taking back stolen web sites
rate of stealing web sites

• Figure 23: Hackers and the Internet World

When tools distributed on the Internet increases (from Figure 22), the rate of stealing Web sites will also increase. This rate affects the number of stolen Web sites, which make a balancing loop called "Defend stolen Web sites" together with the rate of taking back Web sites.

Potential hackers and w.o.m. affects the rate of spreading information about tool on stolen Web sites, and these three factors make a balancing loop because of the community saturation. The rate of spreading information is also involved in the reinforcing loop "R: Word of Mouth of script", together with the w.o.m. and hackers using tool.

Effectiveness of DoS tools, Internet hacker R&D, and the tool kit level make a reinforcing causal loop over R&D war defense and attack.

The last two causal loops to be discussed here, are both balancing. “B: Implement defenses” includes the variables: DoS outside Mxt & Rnd, rate of protecting systems, systems protected, fraction of systems protected, and effectiveness of DoS tools. “B: Build defenses” includes the variables develop defenses and defense level as well as the variables used in the implementing of defences. The loops are both balancing because the effectiveness of DoS tools decreases as the fraction of systems protected increases.

Three factors, disregarding “Tools distributed on internet”, lead to an increase in the rate of stealing Web sites as they increase. These factors are fraction of systems protected, effectiveness of DoS tools, and hackers using tool.

Discussion

Discussion of CLD

Most of the variables in the CLD are more or less discussed in our report, directly or indirectly, and the model shows how they affect each other. A lot of the variables in Figure 20 in comparison to a hacker turf war, is supported in our sources. There are turf wars, usually for the possession over IRC chatrooms, and thereby for bragging rights on the IRC channels (about bragging and IRC on page 27). Because the bragging is related to IRC, we feel that the name of the “Bragging”-loop does not fit in the relation where it is now. The loop involves the distribution of toolkits, and one hackers perception of the other hackers tool, which has little to do with bragging. In our opinion, the loop should have another name, and bragging should be put somewhere in relation with the possession of chatrooms.

If the model was to be extended, two new variables could be included in the balancing loop “One side gets the upper hand” are “bots” – DoS-bots and IRC-bots. These factors can be used in relation with who gets the control of IRC chatrooms (page 30).

Other factors can affect the variables in Figure 22, that are not just related with “Mixter” and “Randomizer”. These factors can be other DoS tools, that other hackers than them have developed. For example, “Randomizer”’s effort in research and development will probably increase when other DoS tools than “Mixter”’s improves and gets distributed. This factor does not affect the turf war between them though, but it can improve R&D and the tools developed.

The other part of the model, Figure 23, is more general and not specific related with the “Mixter” and “Randomizer” case (as mentioned earlier). We feel that this part of the model is missing at least one thing: no factors in the model are affecting the variable “Non-protected system”. It is natural that “Systems protected” would affect the number of non-protected systems, because as the number of systems that get protected goes up, the number of non-protected systems will go down (if you ignore the introduction of new systems – which can be both protected and non-protected). A variable named “Systems in total” could be included in a possible extended model, because this variable would be the total of protected and non-protected systems.

One can also question who are “Potential hackers using tool”? Is it people using the Internet all over the world, people with some computer skills, or people that are already hackers? This is a diffuse variable, and can be interpreted different by different people. It can therefore be difficult to know what number would be put in here.

The stealing of Web sites is often described in relation with phishing (referring to the part about phishing page 24), and does not necessarily have anything to do with a denial of service war. Because of this, the part about stealing Web sites can after our opinion be considered misplaced and do not need to be included in this model at all. Tools distributed on the Internet could therefore e.g. as well be affecting the word of mouth of tools directly, and/or the Internet hacker research and development.

DoS Attacks and DDoS Attacks

As we were finding information about DoS and DDoS, we believed that some of the sources used DoS as a collective term of DoS and DDoS (only DoS was mentioned in statistics and not DDoS). When we look at Table 4, we see that the number of DoS attacks increased from 31% in 1998 to 42% in 2002. A reason for this can be the introduction of DDoS attacks. The table shows that the numbers went down to 27% in 1999, compared to 1998, but went up again to 36% in 2000.

2000 was the year of the big attacks on Web sites, and it was also the year when DoS attacks increased with 33% (from 27 to 36 percent). This makes a lot of sense, because it was at the same time as the introduction of DDoS tools. After DDoS got known, hackers knew the impact that these attacks could make, and the DDoS tools were further developed and used. The future use of DDoS tools will probably depend on the research and development of DDoS tools and other attack tools.

It was also estimated that 2.4 percent of all attacks could break through optimized firewalls. This number is from 2001, and a lot of things have changed since then. People are more aware of the problems of worms and other kinds of attacks than they used to, they are installing firewalls, anti-virus software, and are getting better at patching. But at the same time, the attack tools are getting more sophisticated. These two things are factors which affects a possible “new factor”; successful attacks. This could make a starting point in a new system dynamics model, or in an extension of the model already made (Figures 10 and 11).

A problem in our research was to find information about the “Mixter” and “Randomizer” case. We heard a story from professor Jose J. Gonzalez, that Timothy Shimeall from CERT/CC had told him (on the group modeling workshop February 16-20, 2004 at SEI/CERT, Pittsburgh), about a turf war between these two German hackers.

This story seemed impossible for us to find on the Internet or in books, except from small bits and pieces. At “Mixter”’s homepage, he describes himself as a white-hat hacker with no harmful intentions, which contradicts with what other people has said about him (Timothy Shimeall, among others). This can be a natural thing, because he wants to present himself in the best possible way.

We found no information about the turf war between the two clubs that they were members of, or that they were leaders of the clubs. Because of this, we question some of the things that Tim Shimeall has said, and wonder if some of the story is guessed upon on the basis of vague facts. For example, in his story he told that “Mixter” and “Randomizer” were leaders of each of their hacker clubs, while the first sentence of “The Hacker

Environment" (page 26) says the opposite: *"The hacker culture does not have any leaders"*. But because they are admired because of their skills and achievements in making of DoS tools, they are probably looked upon as heroes by other hackers. Shimeall also said that "Mixter" had to flee to Israel, while we found a source (Wegner 2000) where "Mixter" said in an interview that he was going to Israel to work, so he was not fleeing from the FBI.

Still, there is no doubt that the causal loop model over the case presents a very realistic situation. There are often turf wars between hacker clubs, and the wars often happen in order to possess IRC chatrooms. Our problem is that we can not verify the story about the hacker war.

Conclusion

Some of the results we have found were pretty much as expected. The number of hosts on the Internet is constantly increasing, and the number of attacks and vulnerabilities reported to CERT/CC has increased each year. The number of incidents reported was 6 in 1988, while it was 137,529 in 2003. Reported vulnerabilities has gone up from 171 in 1995 to 3,784 in 2003. The only deviation from this trend, is that reported vulnerabilities was higher in 2002 (4,129 vulnerabilities) than it was in 2003. This result came as a surprise to us.

We have also mapped some common vulnerabilities and attacks methods. There are often vulnerabilities because of default software installations, ineffective use of authentication, patches that are not applied, traffic that is not analyzed, backups that are not maintained and verified, and the lack of protection against malicious code. Malicious code, spoofing, denial of service, probes and scans, account compromise, and packet sniffing are some of the most common attack tools, while social engineering, insider attacks, dumpster diving, the use of hardware and software tools, reverse intent, and phishing are some of the most used methods of attacking.

An interesting trend is that while the attack tools are becoming more and more advanced, the technical knowledge of the hackers does not need to be as high as it used to. Earlier, the hackers were highly intelligent people who wrote the tools themselves, but nowadays the hackers are mostly script kiddies who use tools that they find on the Internet. Attack tools are easy to find, and they are easy to use. 90% of the hackers are probably script kiddies, less than 10% are competent programmers who modify existing tools, and less than 1% are stars who write new tools. Still, not all hackers are bad. They can be divided into two groups; white-hat (ethical) hackers and black-hat hackers (who take advantage of the break-in).

IRC wars between hacker groups are common to gain control of IRC chatrooms, and then keep control against attacks from rival gangs.

Hackers share and get information through hacker clubs, publications, conventions, bulletin boards and newsgroups, Web sites, meetings, and through chatrooms. And the numbers of hacker Web sites and bulletin boards are increasing. An estimate is that about 1 out of 10,000 people engage in hacking activity, while another source says that there are about 100,000 hackers. There are different motives for why people are hacking: increased knowledge, recognition, theft of information, vandalism, blackmail, sabotage and terrorism are some examples.

The single vulnerability model has led to the following findings: if we compare the variable delay to patch, when it is set to 12 and 2 months, the variance is vast. Both the attack rate and the intrusion rate go considerably down, and most of the hosts get hardened before the attack wave comes. Delay to patch also affects the hacker community, because fewer hackers will have script when the delay to patch is set to 2 months. In our simulation, when delay to patch is set to 12 and 2 months, the graphs are flattening out at 1,000 and 400 hackers with script, respectively. This proves how much patch management matters.

Another finding in the model was that the effect of the attacks and intrusion rate could be extremely effective as the attack frequency rose from 1 host/(mo/hacker) to 100 host/(mo/hacker). Attacks grew from 2,500 host/mo to above 30,000 host/mo, and the intrusion rate grew from 1,500 host/mo to 10,000 host/mo.

There was hardly any information to find about multiple vulnerabilities, so we found out that a lot of research remains to be done here.

Denial of service attacks and distributed denial of service attacks are becoming more and more dangerous, and some of these attacks have proved that they can do enormous damage to major Web sites. In 2002, the financial losses because of DoS attacks, were $65,643,300, and the number of attacks have increased from 31% in 1998 to 42% in 2002. It is also more difficult to protect oneself against the attacks than ever before.

Our conclusion when it comes to the case about “Mixter” and “Randomizer” is that we can not validate the story given from Timothy Shimeall, and our opinion is that if those two hacker clubs had a big turf war, it would probably have been publicized somewhere. Nevertheless, hacker wars (in general) are contributing factors for the development of hacker tools, because of the need to prove their skills, which is shown in Figure 21.

Recommendations

In this chapter, we wish to give some suggestions of further work.

- Model the problem with multiple vulnerabilities. The model could include recruitment to the hacker community, how the hackers pick various vulnerability types, the research and development pipeline in the hacker community, etc. Multiple vulnerabilities is a hard subject to find information about, and a lot of research work remains to be done.

- Discuss the problem of patching and the protection of systems as new attack tools are emerging.

- Find out what would happen if a billionaire fundamentalist were to fund an organized activity involving hundreds of brilliant computer scientists for the purpose of identifying dormant system vulnerabilities, develop advanced exploit tools, and roll out a series of devastating attacks toward some neuralgic point of the global information network (without advanced notice). A system dynamics model could illustrate this case.

- Research more about why people/organizations do not report their vulnerabilities, and if the trend is about to change since the numbers of reported vulnerabilities decreased from 2002 to 2003. Are organizations only afraid of bad publicity, or are there other reasons?

- Hacker wars is an interesting theme, but since our story was based on a story we could not find any evidence on, it could be an alternative to find and discuss a hacker war that is easy to find information about and to go into. This could be a hacker war between clubs or between countries, and one suggestion is to discuss both of these cases, and compare them.

References

Arbaugh, W. A., W. L. Fithen, et al. (2000). "Windows of Vulnerability: A Case Study Analysis." Computer **Vol 33**(Issue 12): pages 52-59.

Clark, E. (2003). "Lesson 182: Distributed Denial of Service Attacks." Network Magazine **Vol. 18**(Issue 9): 2 p.

Coyle, R. G. (1996). System Dynamics Modelling. A Practical Approach. London, Chapman & Hall.

Devi, C. (2003). "Hacktivism Rises in Era of Cyberwar." New Straits Times (Malaysia).

Edwards, M. J. (2003). CERT Bulletin Leaked Early--Again. Windows Network & .Net Magazine.

Ellison, R. J., D. A. Fisher, et al. (1999). Survivability: Protecting Your Critical Systems. **2004**.

Ellison, R. J. and A. P. Moore (2002). Trustworthy Refinement Through Intrusion-Aware Design (TRIAD), CMU/SEI. **2004**.

Fontana, J. (2003). "Patching: Process matters." NetworkWorld **Vol 20**(Issue 48): 2p.

Gaudin, S. (2004). Hacker War Keeps the Worms Coming. Datamation. **2004**.

Ghosh, A. K. (2000). Code-Driven Attacks: The Evolving Internet Threat, Cigital**:** 4p.

Graham, R. Opinion: On Magic, IRC wars, and DDoS. **2004**.

Graham, R. (2001). Hacking Lexicon. **2004**.

Koprowski, G. J. (2004). "The Web: Hacker Turf War Raging Online." UPI (United Press International) Technology News.

Krane, T. (2003). Hacker Danger For Power Supply?, The Associated Press. **2004**.

Lipson, H. F. (2000). Survivability – A new security paradigm for protecting highly distributed mission-critical system. **2004**.

Magee, J. (2003). What kinds of trends are you seeing in the development of new worms? Ask the expert. **2004**.

Meinel, C. (2002). MORE on Hacker Wars on Internet Relay Chat (IRC). The "MORE" series. **2004**.

Mixter Mixters homepage. **2004**.

Myers, M. D. (1997). Qualitative Research in Information Systems, MISQ Discovery (original publisher). **2004**.

Norris, E. (1995). "Protecting Against Hacker Attacks." Information Systems Security **Vol 4**(Issue 2): 9p.

OWASP (2003). "The Ten Most Critical Web Application Security Vulnerabilities." 27.

Pethia, R. D. (2001). Information Technology—Essential But Vulnerable: How Prepared Are We for Attacks?, Director, CERT® Centers, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213.

Pethia, R. D. (2002). Information Technology—Essential But Vulnerable: Internet Security Trends, Director, CERT® Centers, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213.

Raymond, E. S. (2001). How To Become A Hacker. **2004**.

Rudolph, J. W. and N. P. Repenning (2002). "Disaster Dynamics: Understanding the Role of Quantity in Organizational Collapse." Administrative Science Quarterly **Vol 47**: pages 1-30.

Scacchi, W. (2003). Cybercrime, Cyberterrorism, and Cyberwarfare. **2004**.

Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. New York, John Wiley & Sons, Inc.

Selfridge, C. (2004). "Use PKI to beat phishers." Computer Weekly.

Shankland, S. (2000). "Hacker discloses new Internet attack software."

Sigmond, S. and V. Kaura (2001). "DDoS Attacks: Precursor to Digital Terrorism." Siliconindia **Vol. 5**(Issue 11): 3 p.

Skidmore, D. (2001). "Grown-Up Laws Sought For Computer Criminals." Phrack World News **Vol. 1**(Issue 6).

Slawsky, R. (2003). "Know Your Enemy." New Orleans CityBusiness: 1p.

Spitzner, L. (2000). Know Your Enemy. **2004**.

Sterman, J. D. (2000). Business Dynamics : Systems Thinking and Modeling for a Complex World. Boston, Irwin/McGraw-Hill.

Tanner, J. (2003). "Network In-Security." America's Network: 6p.

Thorkildsen, S. E. (2003). Datakriminalitet, lovgivning og utviklingen av et hybrid anomali- og signaturbasert innbruddsdeteksjonssystem. Department of Informatics. Oslo, University of Oslo**:** 117 p.

Unknown 2600 Meetings. **2004**.

Unknown E-mail Viruses, Hoaxes, & Hyperlink Safety, VIN (Veterinary Information Network). **2004**.

Unknown Known DDoS Tools. **2004**.

Unknown Reamweaver. **2004**.

Unknown Webopedia. **2004**.

Unknown Whatis? **2004**.

Unknown (1999). Results of the Distributed-Systems Intruder Tools Workshop. Distributed-Systems Intruder Tools Workshop, Pittsburgh, Pennsylvania (November 2-4, 1999), CERT Coordination Center.

Unknown (2000). German Creator of Site Crashing Program Gets Heavier Sentence. **2004**.

Unknown (2003). 2003 CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

Unknown (2003). CERT/CC Overview Incident and Vulnerability Trends. Pittsburgh, CERT® Coordination Center. **2004**.

Unknown (2003). "Number of Hacking Web Sites Grow 45%." Worldwide Videotex Update **Vol. 22**(Issue 2).

Unknown (2003). The Ten Most Critical Web Application Security Vulnerabilities, OWASP (The Open Web Application Security Project)**:** 27p.

Unknown (2004). CERT® Coordination Center 2003 Annual Report.

Unknown (2004). EarthLink fights data-stealing Web sites, CNN.com. **2004**.

Unknown (2004). Preliminary System Dynamics Maps of the Insider & Outsider Cyber-threat Problems Vr. 1.0. Pittsburgh. **2004**.

Unknown, C. C. C. (2002). Overview of Attack Trends, CERT® Coordination Center.

Unknown, C. C. C. (2003). CERT/CC Statistics 1988-2003. **2004**.

Vaughan-Nichols, S. J. (2004). Understanding and Preventing DDoS Attacks. Datamation.

Vaughan-Nichols, S. J. (2004). Understanding and Preventing DDoS Attacks. Datamation. **2004**.

Verdeschi, J. M. (2003). MasterCard Site Data Protection Program. **2004**.

Verton, D. (2002). The Hacker Diaries: Confessions of Teenage Hackers, Osborne/McGraw-Hill.

Verton, D. (2003). Blaster worm linked to severity of blackout. ComputerWorld.

Wegner, J. (2000). Interview: Mixter Mischt das Netz Auf, Focus Magazin. **2004**.

Wiik, J., J. J. Gonzalez, et al. (2004). "Modeling the Lifecycle of Software-based Vulnerabilities." 19.

DDoS Tools and Attacks

- Table 5: Known DDoS Tools (http://www.riverheadnetworks.com/re/known_ddos_tools.html)

Name of Tool	Flooding Capabilities	Short Description
Trinoo	UDP	Only initiates UDP attacks to random ports. Communication between master and slave is via unencrypted TCP and UDP. No IP spoofing. Uses UDP ports 27444 and 31335.
TFN	UDP, ICMP Echo, TCP SYN, Smurf	Uses IP spoofing. Uses ICMP Echo reply packets to communicate between zombie and master.
Stacheldracht v4	UDP, ICMP, TCP SYN, Smurf	Uses encryption for communications (but not for ICMP heartbeat packets that zombie sends to master) and has an auto-update feature (via rcp). Has ability to test (via ICMP Echo) if it can use spoofed IP addresses.
Stacheldracht v2.666	UDP, ICMP, TCP SYN, Smurf, TCP ACK, TCP NUL	Uses encryption for communications (but not for ICMP heartbeat packets that zombie sends to master) and has an auto-update feature (via rcp). Has ability to test (via ICMP Echo) if it can use spoofed IP addresses.
TFN 2K (Tribal Flood Network)	UDP, ICMP Echo, TCP SYN, Smurf	Same as TFN - but the slave is silent so difficult to spot. No return info from slave. Zombie to master communication is encrypted.
FAPI	UDP, TCP SYN, TCP ACK, ICMP	Can spoof IP addresses
Carko (Stacheldraht v1.666 + antigl + yps)	UDP, ICMP, TCP SYN, Smurf, TCP ACK, TCP NUL	Uses the backdoor hole of snmpXdmid and uses UDP port 530.
Freak88	ICMP	NT specific zombie. No spoofing capabilities. Sends ICMP 1500 octet packets marked as fragments.
Shaft	UDP, ICMP, TCP SYN	Uses UDP ports 18753 and 20433. Has optional IP spoofing capabilities (needs root). Can set ICMP/UDP packet size.
Mstream	TCP ACK	Usually uses TCP port 12754 but can use any port. Master connects via telnet to zombie. Communication between zombie and controller is not encrypted. The target gets hit by ACK packets and sends TCP RST to non-existent IP addresses. Routers will return ICMP unreachable causing more bandwidth starvation.
Blitznet	TCP SYN	Can spoof IPs and do IP flooding
Ramen	Multicast	Ramen is a worm that propagates by using a newly compromised system to scan Class B (/16) wide address spaces, searching for port 21 (FTP)

		and looking for new vulnerable hosts. SYN scanning performed by Ramen can disrupt network traffic when scanning the multicast network range.
Targa	ANY	Works by sending malformed IP packets known to slow down or hang up many TCP/IP network stacks.
Spank	Multicast	Will only work on a multicast enabled network. Similar to Mstream.
Stick	Any	Stick uses the straightforward technique of firing numerous attacks at random, from random source IP addresses to purposely trigger IDS events. Stick is a DoS tool against IDS systems.
Trank		
Omega	TCP ACK, UDP, ICMP, IGMP	Can spoof IPs and has a chat option between attackers
NAPHTA	TCP	Naptha attacks exploit weaknesses in the way some TCP stacks and applications handle large numbers of connections in states other than "SYN RECVD," including "ESTABLISHED" and "FIN WAIT-1."
Trinity (also called MyServer and Plague)	UDP, TCP Fragment, TCP SYN, TCP RST, TCP RandomFlag,TCP ACK, Establish, NULL	Listens to TCP port 33270. When idle it connects to Undernet IRC server on port 6667.
IRC bots	ICMP, UDP	Zombie systems controlled via a central IRC channel. Sub7 Trojan used to maintain control over the zombie.
HTTPSmurf	TCP HTTP	Using public IIS servers as unsuspecting zombies, it sends a string of data to multiple web servers and they reflect the data to the target.
Code Red	TCP HTTP	Using a known IIS bug to infect Web servers, this Trojan DDoS will only attack whitehouse.org but it will utilize 225,000 infected IIS systems. It exploits a vulnerability in the Indexing Service on systems running Microsoft IIS.
Power worm	TCP HTTP	Utilizing an IIS hole in regards to Unicode support, this worm uses IRC as a back channel to control an army of zombies.
Cisco	ICMP	Use a Cisco router as a zombie for an ICMP based ping attack.
Nimda	TCP HTTP	Worm utilzing yet another MS IIS hole.
SQL — Voyager Alpha	TCP HTTP	SQL with no password (default). The hacker takes over the system and uses it as part of IRC botnet to DDOS victims.

Explanation of terms

Activity	A group of events that occur on the Internet and relate to one another in any of several ways.
Antivirus program	A tool that searches a hard disk for viruses and removes any that are found.
Authentication	The process of identifying an individual or data.
Backup	To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails.
Black-hat hacker	A black-hat hacker is a hacker or cracker who breaks into a computer system or network with malicious intent. He/she takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose.
Buffer overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. It may occur through a programming error (bug), and it is an increasingly common type of security attack on data integrity.
Bug	Some sort of programming mistake.
Chat	Online chatting provides real-time anonymous communication. IRC and ICQ are popular in the hacking community.
CIAC (Computer Incident Advisory Capability)	CIAC has been providing the US Department of Energy with incident response, reporting, and tracking, along with other computer security support since 1989.
CLD (Causal Loop Diagram)	A tool for representing the feedback structure of systems.
Cookies	Small bits of data that a web site can place on your system, and requests your browser to send them back to the web site the next time you visit.
Cracker	This is a malicious hacker who decrypts passwords or breaks software copy protection schemes.
Cryptography (crypto)	The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *codebreaking*, although modern cryptography techniques are virtually unbreakable. Cryptography is needed to protect banking transactions, personal information, and to protect our infrastructure from infowar attacks.

Daemon	A daemon usually provides some kind of service (e.g., e-mail, printing, telnet, FTP, and web access). It is a program running in the background (in UNIX).
DDoS (Distributed Denial of Service)	An attack that pits many machines against a single victim.
DefCon	The worlds largest underground hacking event.
Defect (flaw)	A technology product feature that can be used to produce undesirable behavior.
DoS (Denial of Service)	An exploit whose purpose is to deny somebody the use of the service to crash or hang a program or the entire system.
Event	Fundamental unit of information that describes the aspects of network or host behavior.
Firewall	A device that isolates a network from the Internet. Firewalls are installed between internal (private) networks and the (public) Internet. All the traffic to and from the internal network goes through the firewall, which acts as a “gate” with virtual guards that examine the traffic.
Flood	A class of hacker attack where the victim is flooded with traffic.
Hacker	Someone who is able to manipulate the inner workings of computers, information, and technology.
Hacktivism	Hacktivism means “hacker activism”, or breaking into Web sites as part of a cause.
ICQ (“I Seek You”)	An instant messenger service.
Incident	An activity with security or survivability implications.
Intrusion	Describing the act of compromising a system.
IRC (Internet Relay Chat)	The most popular chat program in the hacker community.
ISC (Internet Domain Survey)	The Domain Survey attempts to discover every host on the Internet by doing a complete search of the Domain Name System.
ISP (Internet Service Provider)	Provides access to the Internet. The ISPs get together and form agreements among themselves as to how the Internet should operate.
Linux	A freely-distributable open source operating system that runs on a number of hardware platforms.
Malware	Malware is short for malicious software. It is software designed to damage or disrupt a system (such as a virus or Trojan horse).
Microsoft	The Microsoft Corporation is one of the largest and most influential companies in the personal computer industry. It was founded in 1975 by

	Paul Allen and Bill Gates.
Panix (Public Access Networks Corporation)	A New York ISP.
Patch	A fix to a program bug.
Phreaker	A person who is using a computer or other device to trick a phone system.
PKI (Public key infrastructure)	A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.
Probe	An attack that only gathers information from the target system.
RPC (Remote procedure call)	A type of protocol that allows a program on one computer to execute a program on a server computer. A system developer does not need to develop specific procedures for the server while using RPC. The client program sends a message to the server with appropriate arguments and the server returns a message containing the results of the program executed.
Samurai	A computer hacker who is hired legally to infiltrate corporate computer systems for legitimate reasons.
Scan	A way of performing multiple probes using an automated tools.
Script	A list of commands that can be executed without user interaction.
Script kiddie	A type of hacker with technical knowledge often less than the average computer user. He/she knows to do a little more than run pre-packaged scripts against computers hoping to break into them.
Sniffer	A wiretap that eavesdrops on computer networks.
Social engineering	A form of hacking that targets peoples minds rather than their computers. An example is to pretend to be from a company’s computer department and call up a user asking for their password (or call up the computer support department and tell them you've lost your password).
Spoof	The word generally means the act of forging your identity. More specifically, it means forging the sender’s IP address (IP-spoofing).
SYN flood	This is a type of DoS attack. A SYN (synchronize) packet notifies a server of a new connection. By spoofing large numbers of SYN requests, an attacker can fill up memory on the server, which will wait for more data (that will never arrive).
System dynamics	A method to gain useful insight into situations of dynamic complexity and policy resistance.
Trojan	A class of malware. Trojans are one of the leading causes of breaking into machines. They do not replicate themselves, but they can be just as destructive as a virus. One type of Trojan horse claims to get your

	computer rid of viruses, but instead introduces viruses on your computer.
Unix	A popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s.
Virus	A virus is a program (or a fragment of code) that replicates by attaching a copy of itself to other programs. For a virus to be activated, the software it infects must first be run.
Vulnerability	In this context, the word “vulnerability” describes a problem that allows a system to be attacked or broken into. The problem can be a bug or common misconfiguration.
Warez	Warez means pirated software (illegally copied software).
White-hat hackers	These are “ethical” hackers who work with clients in order to help them secure their systems.
Wiretap	A classical wiretap is when law enforcement eavesdrops on your phone line.
Worm	This is a program that propagates itself by attacking other machines and copying itself to them.
XSS (Cross site scripting)	XSS occurs when a web application gathers malicious data from a user.
Zombie	Computers that are “owned” by hackers for the purpose of directing them against other victims. In a DDoS attack, the zombies are used to flood the victim.

Abbreviations

Anon	Anonymous
ACK	Acknowledgement
AOL	America Online
ATM	Asynchronous Transfer Mode
BBS	Bulletin Board Systems
BIND	The Berkeley Internet Domain
Bot	Robot
CCC	Chaos Computer Club
CERT/CC	Computer Emergency Response Team Coordination Center
CIAC	Computer Incident Advisory Capability
CLD	Causal loop diagram
CPU	Central processing unit
CSI	Computer Security Institute
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
EIM	Employee Internet Management
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
ICMP	Internet Control Message Protocol
ICQ	“I Seek You”
ID	Identification
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IRC	Internet Relay Chat
IRT	Incident Response Team
ISC	Internet Domain Survey
ISP	Internet Service Provider
LOD	Legion of Doom
OP	Operator
Panix	Public Access Networks Corporation
Perl	Practical Extraction and Report Language
PKI	Public key infrastructure
R&D	Research and development
RPC	Remote Procedure Call
RST	Reset
SD	System Dynamics
SEI	Software Engineering Institute
SYN	Synchronize
TCP	Transmission Control Protocol
TCP NUL	No flags
TFN	Tribe Flood Network
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
w.o.m.	Word of mouth
XSS	Cross site scripting

Appendix

The appendixes are arranged in order of the date they are written. They are memos to our teaching supervisor, and meant as background information to the modeling discussion. The appendixes are listed as following:

Appendix A (KEB&SS)Searching for vulnerabilities040116.doc

Appendix B (KEB&SS)Hacker Information040122.doc

Appendix C (KEB&SS)Hacker Information040127.doc

Appendix D (KEB&SS)Hacker Information040204.doc

Appendix E (KEB&SS)TeenageHackers040225.doc

Appendix F (KEB&SS)Blaster and blackout040225.doc

Appendix G (KEB&SS)MixterAndRandomizer040308.doc

Appendix H (KEB&SS)DoSAndDDoS040315.doc

Appendix I (KEB&SS)DoSandDDoS040323.doc

Appendix A (KEB&SS)Searching for vulnerabilities040116.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

Searching for vulnerabilities

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: January 16, 2004

Re: Vulnerability types

Organization of this memo:

Introduction

The purpose is to understand and map the types of typical vulnerability threats. We will use this in further study. We have studied the links recommended in the e-mail you sent us, and we found relevant information to our topic. We have also searched the Internet, and we have looked through articles, reports and papers by CERT/CC staff.

Discussing papers, finding vulnerability types

Through this memo, we have divided the sections into the papers or texts we have found interesting.

Overview of Attack Trends, CERT® Coordination Center (Unknown 2002)

Abstract

The CERT Coordination Center has been observing intruder activity since 1988. Much has changed since then, from our technology to the makeup of the Internet user community, to attack techniques. In this paper, we give a brief overview of recent trends that affect the ability of organizations (and individuals) to use the Internet safely.

Methodology

In this paper the author lists up six trends in exploiting vulnerabilities. For each trend, the author gives an explanation. The six trends are automation, increasing sophistication of attack tools, faster discovery of vulnerabilities, increasing permeability of firewalls, increasingly asymmetric threat and increasing threat from infrastructure attacks. After this, the author concludes that the trends seen by CERT/CC indicate that organizations relying on the Internet face significant challenges to ensure that their networks operate safely and that their systems continue to provide critical services, even in the face of attack. In the appendix of the paper there is a list of sources for more information about the problems.

Results

We now know more about infrastructure attacks like “distributed denial of service” (DDoS), worms, attacks on the Internet Domain Name System (DNS) and The Berkeley Internet Domain (BIND), and attacks against or using routers.

Personal conclusions

This paper raises readers' awareness of current trends in attack techniques and tools. Our goal was to find types of vulnerabilities, and especially attack methods, which this paper gives us examples of. The links in the appendix will be interesting in the further study.

Secrets & Lies – chapter 18: Vulnerabilities and the Vulnerability Landscape (Schneier 2000)

Abstract

To successfully make use of the vulnerabilities that an attacker has found, he has to find a target, plan the attack, do the attack, and get away. It's not enough for a potential criminal to find a flaw in the encryption algorithm for the ATM network. He/she has to get access to the communications line, know enough about the protocols to create a bogus message letting him/her steal money, steal the money, and get away with it.

Methodology

First, Schneier looks at attack methodology which tells us five steps to a successful attack. Then he describes countermeasures, which are methods to reduce vulnerabilities. Next, he tells about the vulnerability landscape and breaks it down into four broad categories that are all described closer. Finally, Schneier explains how to rationally apply countermeasures.

Results

There are three parts to an effective set of countermeasures: protection (cryptography, firewalls and passwords), detection (intrusion detection systems) and reaction (a login system that lock users out after three failed login attempts).

One of the five steps to a successful attack: is to identify vulnerabilities. Schneier breaks down the vulnerability landscape into four broad categories: the physical world (locks, guards), the virtual world (firewalls, authentication, end-to-end data encryption), the trust model (who to trust within an organization), and the system's life cycle (when and where to conduct the attack).

Personal conclusions

We like the organization of the vulnerability landscape into categories, but would wish that there would be more concrete examples of vulnerabilities, and not just examples of the countermeasures. For example, the virtual security section is described very briefly, it tells that countermeasures that are needed are firewalls, strong authentication and end-to-end encryption, but it doesn't say anything about any concrete vulnerabilities.

The Ten Most Critical Web Application Security (OWASP 2003)

Abstract

The top 10 list was created to focus government and industry on the most serious of web application vulnerabilities. Organizations should understand and improve the security of their web applications and web services, and the consequence of an attack can be devastating.

Methodology

There is first a list over the top ten vulnerabilities. Then, the author goes thoroughly into each one of these with a description, environments that are affected, examples and references, how to determine if you are valuable, and how to protect yourself.

Results

The top vulnerabilities in web applications are: invalidated parameters, broken access control, broken account and session management, cross-site scripting (XSS) flaws, buffer overflows, command injection flaws, error handling problems, insecure use of cryptography, remote administration flaws, and web and application server misconfiguration. Other vulnerabilities that were considered for the list include unnecessary and malicious code, broken thread safety and concurrent programming, denial of service, unauthorized information gathering, accountability problems and weak logging, data corruption and broken caching, pooling and reuse.

Personal conclusions

It gives a good insight into some of the web application vulnerabilities because they are not only mentioned, but also described in depth. The conclusion also mentions other areas that were considered for the list, which we think is a good thing.

Network in-security (Tanner 2003)

Abstract

People are more aware of the importance of security than before. This is among others because of the many worms and vulnerabilities that have been announced in Microsoft products. The industry has a tendency to introduce new technology without delivering appropriate security for it. Many companies tend to cut costs regarding to security, and there are network managers that don’t install patches on their servers when software vulnerability is found. It’s often an issue that it’s not until people get hacked that they wished they had invested in it.

Methodology

The article first tells about hard security requirements. Then, we get to know about attitude changes toward security over time, and people are aware of the problem. Still, they shouldn’t blindly trust the security that they buy. The next section is about reactionary security, and among others says that the security industry is part of the problem. Cutting of costs of security is the next theme, and different types of threats are mentioned in this relation. The article continues by explaining that threats aren’t always external, and therefore tells about different types of internal threats. At the end, we are told that the human is the weakest link when it comes to security. People don’t understand it yet.

Results

The vulnerabilities mentioned in this article are both external and internal threats. There is theft, like hacking into bank accounts or copying sensitive data, identity theft (becoming a person), intellectual property (patents, DVDs, etc.), and brand theft (pretending to be a web site). There are also DoS, surveillance and viruses that are designed to infect a system and cause damage. Still, most security problems occur from within, and it is mostly hacking at the application level. The internal threats can be disgruntled company employees selling company secrets and opportunists running fraud operations to consumer-level users on a commercial private network. One can prevent internal attacks with audit trails, comprehensive internal security procedures and adequate user-level authentication and access to critical resources.

Vulnerabilities include operating systems as well as network elements such as firewalls, Ethernet switches, WAP gateways and dial-up modem banks. VPNs and voice mail are also risks. At the application level there are examples like Web browsers and Microsoft Outlook. Other problems are IRC and instant messaging, and Java and cookies. Server software is also at risk of attack, especially where remote control applications are used.

Personal conclusions

This is an article that describes security issues in a good way. It describes both external and internal threats to the security, even though these threats are not further deepened, they are just mentioned briefly.

Conclusion

We have found some types of vulnerabilities, but we are sure we will find more, when we continue our studies, and make searches for new keywords. In the follow-up we could do new searches, and/or gather more information on the links already discovered.

Summary

We have studied four different texts.

We now know more about infrastructure attacks like “distributed denial of service” (DDoS), worms, attacks on the Internet Domain Name System (DNS) and The Berkeley Internet Domain (BIND), and attacks against or using routers.

There are three parts to an effective set of countermeasures: protection (cryptography, firewalls and passwords), detection (intrusion detection systems) and reaction (a login system that lock users out after three failed login attempts).

The top vulnerabilities in web applications are: invalidated parameters, broken access control, broken account and session management, cross-site scripting (XSS) flaws, buffer overflows, command injection flaws, error handling problems, insecure use of cryptography, remote administration flaws, and web and application server misconfiguration.

Vulnerabilities include operating systems as well as network elements such as firewalls, Ethernet switches, WAP gateways and dial-up modem banks. VPNs and voice mail are also risks. At the application level there are examples like Web browsers and Microsoft Outlook. Other problems are IRC and instant messaging, and Java and cookies. Server software is also at risk of attack, especially where remote control applications are used.

Signature

Kjetil E Braathen, Silje Salte

References

Norris, Ed. 1995. Protecting Against Hacker Attacks. Information Systems Security 4 (2):9.

OWASP. 2003. The Ten Most Critical Web Application Security Vulnerabilities.27.

Schneier, Bruce. 2000. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, Inc.

Tanner, John. 2003. Network In-Security. America's Network:6.

Unknown, CERT® Coordination Center. 2002. Overview of Attack Trends: CERT® Coordination Center.

Sources searched

Cert Coordination Center (www.cert.org)

The Library, Agder University College (www.hia.no/hiabib) (EBSCO: “academic search elite”, ”business source premier”, ”regional business news”, and ”business source elite”)

Keywords

Here are the keywords used in EBSCO:

Vulnerabilities + Security
Vulnerability threats
Buffer overflow
Vulnerability
Security
Buffer overflow
Security
Vulnerability
Buffer overflow

This memo

The following link is found in an article on EBSCO (http://search.epnet.com/direct.asp?an=9036216&db=afh&site=ehost).

The link is much more fulfilling:
http://heanet.dl.sourceforge.net/sourceforge/owasp/OWASPWebApplicationSecurityTopTen-Version1.pdf

Appendix B (KEB&SS)Hacker Information040122.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

Hacker information

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: January 22, 2004

Re: Hacker information

Organization of this memo:

Introduction

The purpose of this memo is to answer the following questions: How does hacker information spread? How does hacker script spread? How does script develop? How large is the hacker environment, and how large are the segments? How big is the hacker activity? How do incidents affect hacking? How do incidents affect patching? Reference modes (time-series)? And how many vulnerabilities are reported per year?

Discussing papers, finding hacker information

Through this memo, we have divided the sections into the papers or texts we have found interesting.

Protecting Against Hacker Attacks (Norris 1995)

Abstract

This article presents a profile of hackers and hacker clubs, their methods of communication, and specific methods of information gathering and attack. Recommended procedures and controls for countering such hacker activities are provided.

Methodology

The article starts by telling what a hacker is; the profile of a hacker, hacker clubs, publications, conventions and bulletin boards and newsgroups. This is the section we choose to focus on. Then, it tells about different methods of attack; social engineering, dumpster diving, hardware and software tools, and reverse intent. At the end, it explains security monitoring and recommended course of action.

Results

Computer systems are to be found everywhere now, and the opportunity to hack these systems has increased. Hackers use used equipment which is inexpensive and adequate to the tasks. There is no exact number mentioned of how many people are involved in hacking, so estimated numbers vary greatly from hundred serious hackers to hundreds of thousands. The hacker activity is hard to monitor because of the use of aliases.

Hacker information spreads through hacker clubs, hacker publications, hacker conventions, and bulletin boards and newsgroups. Example of hacker clubs are Legion of Doom (LOD), Chaos Computer Club, NuKE, The Posse, and Outlaw Telecommandos. The clubs help members work as a team to achieve goals which might be out of reach for an individual hacker, even though most members never physically meet. The publications, such as Phrack, 40Hex and Chaos Digest, provide technical information, and provide a social function. They can be received over e-mail or regular mail. Conventions are held in Europe and the US so that people can brag, tell stories and exchange information. Examples of conventions are the Chaos Congress, Hacking at the End of The Universe and HoHoCon. Bulletin board systems are the primary way for hackers and hacker clubs to communicate, even though they can be difficult to get access to. It is estimated to be about 1,300 underground bulletin boards in the US. Information found here is mostly current and state-of-the-art.

Personal conclusions

It says a great deal about the spreading of hacker information, about the hacker environment and hacker activity. How large the environment is, and how many people are involved, seems impossible to find out. We would also wish to mention that this article is old, and lots of things have happened since then.

Survivability: Protecting Your Critical Systems (Ellison, Fisher et al. 1999)

Abstract

Society is growing increasingly dependent upon large-scale, highly distributed systems that operate in unbounded *network* environments. Unbounded networks, such as the Internet, have no central administrative control and no unified security policy. Furthermore, the number and nature of the nodes connected to such networks cannot be fully known. Despite the best efforts of security practitioners, no amount of hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack. The discipline of survivability can help ensure that such systems can deliver essential services and maintain essential properties such as integrity, confidentiality, and performance, despite the presence of intrusions. Unlike traditional security measures, which require central control and administration, survivability is intended to address unbounded network environments. This paper describes the survivability approach to helping assure that a system that must operate in an unbounded network is robust in the presence of attack and will survive attacks that result in successful intrusions. Included are discussions of survivability as an integrated engineering framework, the current state of survivability practice, the specification of survivability requirements, and strategies for achieving survivability.

Methodology

The authors start this paper by introducing the new network paradigm, organizational integration. This new paradigm represents a shift from bounded networks with central control to unbounded networks. Next, they define *survivability* (as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents). In addition, they explain the environments of unbounded networks, and characterize a survivable system. At last, they discuss strategies for achieving survivability.

Results

To maintain their capabilities to deliver essential services, survivable systems must exhibit the four key properties: resistance to attacks, recognition of attacks and the extent of damage, recovery of full and essential service after attack, adaptation and evolution to reduce effectiveness of future attacks. The traditional view of information systems security must be expanded to encompass the specification and design of survivability behavior that helps systems survive in spite of attacks. Only then can systems be created that are robust in the presence of attack and are able to survive attacks that cannot be completely repelled.

Personal conclusions

This is a rather old paper (1999), but still is relevant to system survivability thinking today. Questioning how much a system can tolerate from massive coordinated attacks, clearly the “four key properties” are applicable.

Code-Driven Attacks: The Evolving Internet Threat (Ghosh 2000)

Abstract

Over the last two years (2000) the intrusion threat to computer systems has changed radically. Instead of dealing with hackers, we are now faced with defending our systems against code-driven attacks. One of the key characteristics of this new threat is that malicious code can spread on an Internet scale in Internet time, rendering current intrusion detection approaches impotent.

Methodology

First, the paper describes the code-driven attack threat; the problem of code driven attacks and next generation code-driven attacks. Then it describes active-scripting-based attacks, which is an approach to addressing a specific class of the code-driven attack threat.

Results

The nature of the threat against computer systems is changing radically. The most significant emerging intrusion threat is code-driven attacks, and the most costly intrusions are being perpetrated per code, rather than individual hack-in attempts. For example, the Love Letter is estimated to have cost businesses $8 billion in lost productivity. Code that spreads itself over Internet connections, can quickly bring down very large segments of the Internet.

The code-driven threat is aimed against the Win32 platform because this platform is used both in homes and in offices. Scripting-based attacks are developed in popular scripting languages such as VB-Script, Jscript, VBA macros, Perl and Python, and go through applications like Web browsers, mailers, MS Office applications and the Windows scripting host.

Personal conclusions

The article discusses the development of hacker tools, and describes types of scripts and applications that it spreads through. It also mentions methods that can be used to prevent this.

CERT/CC Statistics 1988-2003 (Unknown 2003)

Below are statistics from CERT/CC web page.

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

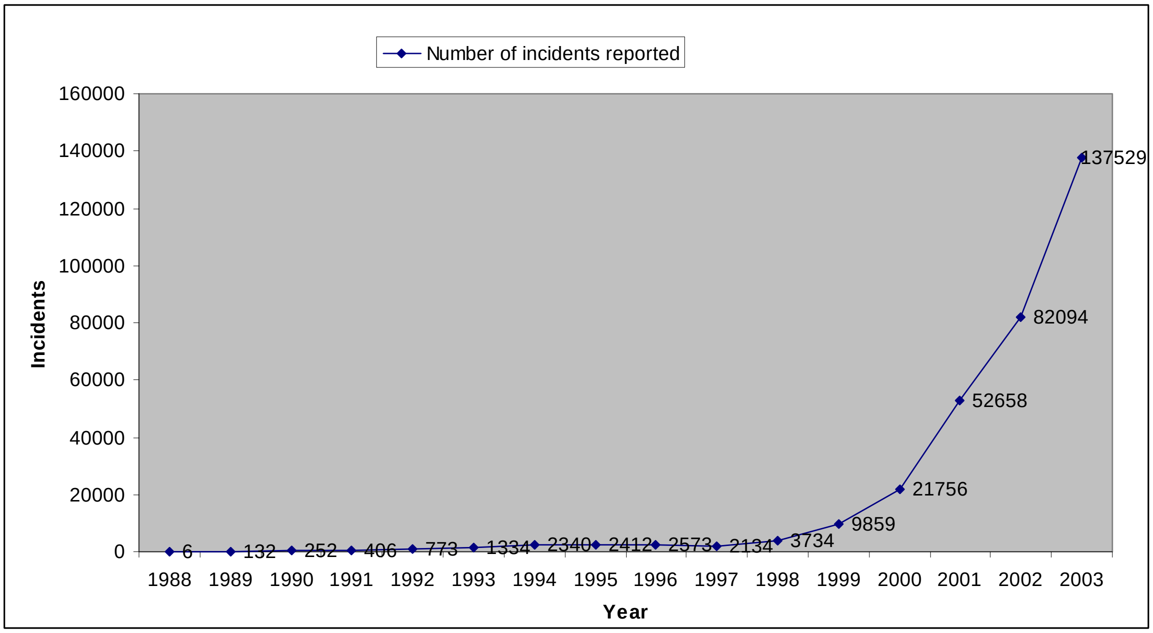
Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

Total incidents reported (1988-2003): **319,992**

Below we have visualized the statistics.



Vulnerabilities reported

1995-1999

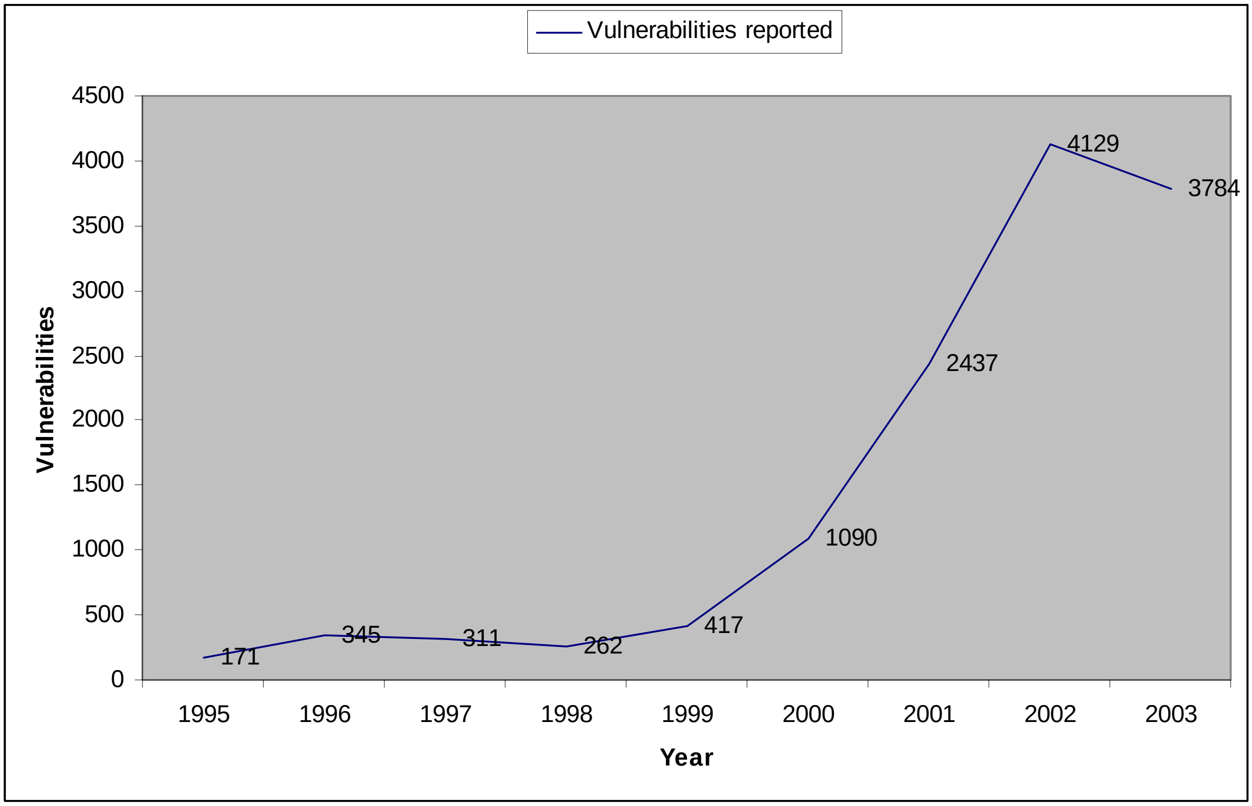
Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2003

Year	2000	2001	2002	2003
Vulnerabilities	1,090	2,437	4,129	3,784

Total vulnerabilities reported (1995-3Q 2003): **12,144**

Below we have visualized the statistics:



Personal conclusions

For now, we just observe these numbers. It is clear that the number of incidents are increasing drastically, and that reported vulnerabilities are also increasing each year except 2003.

Conclusions

We managed to find answers to some of the questions, but not all. We found questions like how incidents affect hacking and patching, to be hard to find answers to. Hacker information spreads through clubs, publications, conventions, bulletin boards and newsgroups, and we would therefore think that script is spread the same way. The hacker environment and the hacker activity is hard to estimate, and also depends upon how you define a hacker. There are no clear numbers. But it is clear that the number of incidents and the number of vulnerabilities is increasing each year.

Summary

Hacker information spreads through hacker clubs, hacker publications, hacker conventions, and bulletin boards and newsgroups (as mentioned in the conclusion). These help members work as a team to achieve goals which might be out of reach for an individual hacker, even though most members never physically meet. Bulletin board systems are the primary way for hackers and hacker clubs to communicate.

The traditional view of information systems security must be expanded to encompass the specification and design of survivability behavior that helps systems survive in spite of attacks. Questioning how much a system can tolerate from massive coordinated attacks, clearly the "four key properties" are applicable.

Code that spreads itself over Internet connections, can quickly bring down very large segments of the Internet. The code-driven threat is aimed against the Win32 platform because this platform is used both in homes and in offices.

Signature

Kjetil E Braathen, Silje Salte

References

Ellison, Robert J., David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, and Nancy R. Mead. Survivability: Protecting Your Critical Systems 1999 [cited. Available from http://www.cert.org/archive/html/protect-critical-systems.html.

Ghosh, Anup K. 2000. Code-Driven Attacks: The Evolving Internet Threat: Cigital.

Norris, Ed. 1995. Protecting Against Hacker Attacks. Information Systems Security 4 (2):9.

Unknown, CERT® Coordination Center. 2003. CERT/CC Statistics 1988-2003.

Sources searched

Cert Coordination Center (www.cert.org)

The Library, Agder University College (www.hia.no/hiabib) (EBSCO: "academic search elite", "business source premier", "regional business news", and "business source elite")

Keywords

Here are the keywords used in EBSCO:

"hacker information"
"hacker script"
"hacker" + "spread" + "information"
"hacker activity"
"hacker community"
"scripting" + "hacker"

This memo

http://www.cert.org/stats/cert_stats.html

Appendix C (KEB&SS)Hacker Information040127.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

Hacker information continued

To: Jose J Gonzalez
From: Kjetil E Braathen, Silje Salte
CC: Johannes Wiik
Date: January 27, 2004
Re: Hacker information continued

Organization of this memo:

Introduction

The purpose of the memo is to continue with finding hacker information with the use of more and better words, and to search for newer articles by looking at references and authors. We will also try to find answers to the following: Experiences and strategies of patching? How long time does it take before patching? How long time does it take a hacker to develop scripts? What do scripts do? Do scripts change, and are there different types of versions? How do the attacks happen? How many hackers are there, and how many hacker communities are there?

Discussing papers, finding hacker information

Through this memo, we have divided the sections into the papers or texts we have found interesting.

Know Your Enemy (Slawsky 2003)

Abstract

Companies learn to think like hackers to protect their computer systems. This means that they should keep up with the latest in hacker techniques by reading trade journals and participating in organizations such as the Information Systems Security Association. It can also be necessary to adopt an assumed identity and looking at web sites that are devoted to hacking and hacker activity.

Methodology

It is a very short and continuous article that is not divided into chapters or sections.

Results

There has been a development in what hackers do. They used to be a elite group of people who were interested in how computers works. Now, there are people that write hacking tools and release them so that anyone with a computer can get online, download the tools, and start to use them. These are known as “script kiddies”.

Any system can be broken in to by a determined hacker. But only one out of 10,000 or more people engage in hacking activity. A big concern is the increasing popularity of wireless networks.

Personal conclusions

The article is very new and up to date. We would still wish that it wasn't so brief, and described things more in depth.

Patching: Process matters (Fontana 2003)

Abstract

Patch management is tough. It's tough because there are too many patches and not enough time, and because exploits to announced vulnerabilities are materializing faster. Clients are becoming the attack targets as much as servers. "This typically isn't a task for one person. It has to involve the security group, the operations group and the developers, so what also makes patching tough is a lack of resources. (Felicia Nicastro)"

Methodology

The article is divided into a chapter about how to patch, an example of patching in action, and at last a chapter is about Pitney Bowes named "open season on clients". There are also a list over what to do, and what not to do when it comes to patching, and a list over the most popular patching tools.

Results

A big mistake for companies, is to leave out the processes such as monitoring for new patches coupled with detailed evaluation, testing, deployment and validation that a team or individual manages. The following pieces must be involved before a patch management process can be installed: network inventory, change management, configuration management, asset management, formalized record keeping, and an understanding of costs, prioritization guidelines, and maintenance and communications plans.

At Centura Bank, they notify a lead engineer after a new patch is identified. If the patch is for a critical flaw, notification is sent straight to the vice president of engineering who decides if the patch is needed and structures the process toward deployment, if necessary. The patch is then tested.

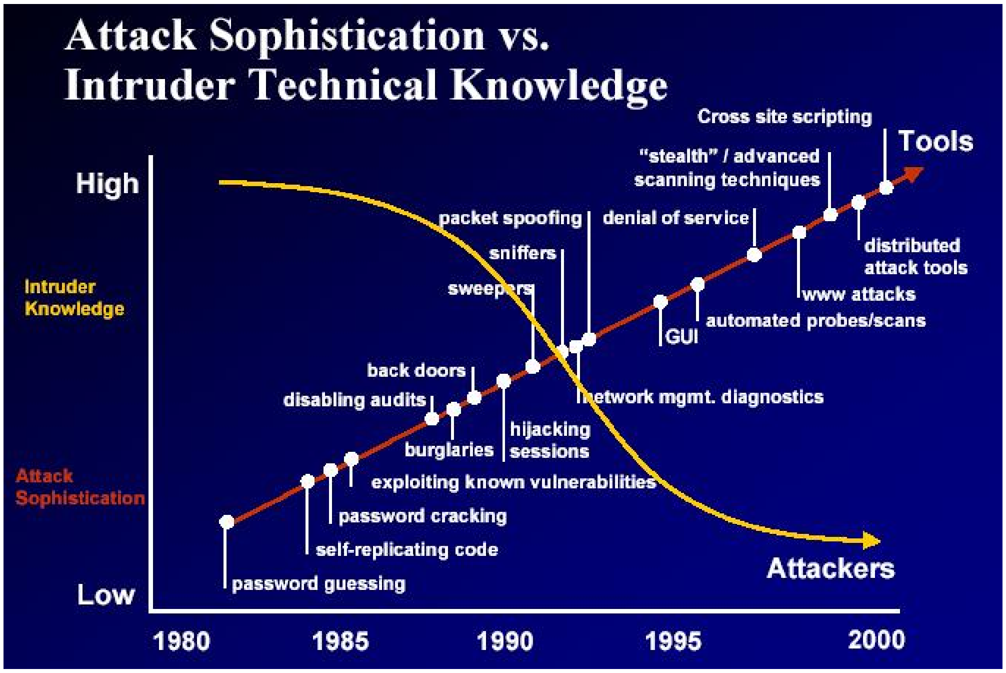
Pitney Bowes categorizes its network assets and their relevance to the company. Client desktops are given a risk profile from 1-5, so that desktops rated a 5 (clients that must be most secure) must be patched in less than 24 hours.

Personal conclusions

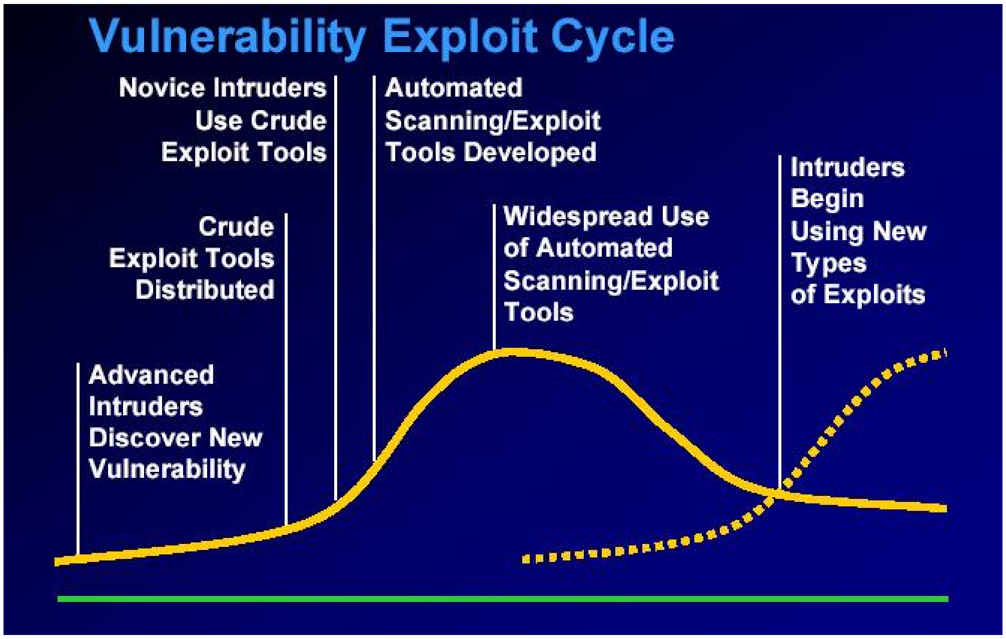
The article shows examples of how two different companies perform patching. It also has a short list over what to do, and what not to do, when it comes to patching.

Survivability – A New Security Paradigm for Protecting Highly Distributed Mission-Critical Systems (Lipson 2000)

We chose to use the following figure, Attack Sophistication vs. Intruder Technical Knowledge, because it shows that the intruders technical knowledge has been sinking dramatically while the sophistication of attacks are constantly increasing. In the 1980's, the attacks started out being password guessing, and developed to become more advanced, like using back doors, sniffing, packet spoofing, denial of service and cross site scripting.


Attack Sophistication vs.
Intruder Technical Knowledge

The next figure shows the vulnerability exploit cycle from when an intruder discovers new vulnerability, to the use of different types of exploit tools.


Vulnerability Exploit Cycle

Novice Intruders Use Crude Exploit Tools
Automated Scanning/Exploit Tools Developed
Crude Exploit Tools Distributed
Widespread Use of Automated Scanning/Exploit Tools
Intruders Begin Using New Types of Exploits
Advanced Intruders Discover New Vulnerability

MasterCard Site Data Protection Program (Verdeschi 2003)

Abstract

The protection program from MasterCard give insight into how the hackers work, and how to prevent this.

Methodology

It is a PowerPoint presentation that begins with some slides about the hacker; the profile, motivations, tools, and 7 phases for an attack. This is the part we concentrate on. It also shows some slides that show a couple of hacker web sites. At the end, there is mostly information about MasterCard SDP Security Standard and how to protect themselves.

Results

The typical hacker is characterized as bored and antisocial individuals or groups, where 90% are “script kids” that have little knowledge, but access to hacker tools. Less than 10% are competent programmers who modify existing tools, and only less than 1% build new tools. Some of the motivations that the hackers have are: intellectual challenge, joy riding, gang mentality, recognition, theft of information, vandalism, blackmail, sabotage and terrorism.

Some hacking tools were mentioned in numbers. There are 30 hacker publications, 440 hacker bulletin boards, and 400,000 web sites dedicated to “hacking tips”. Hackers.com, 2600.com and insecure.org are examples of hacker web sites.

We couldn’t find statistics over the mentioned numbers, so the following table is found in different articles

[1][2][3][4]

Hacker information			
	Web sites	Publications	Bulletin Boards
April, 1997	1 900	Dozens	440
November, 1997	2 000		500
February, 1998	2 500		500
July, 1999	30 000		
(Unknown date) 2003	400 000	30	440

We can see from this, that the development of hacker web sites has increased dramatically, while the number of publications and bulletin boards hasn’t changed much.

Before a hacker attacks, he must do following things: get information about the target’s network, find weaknesses / deploy tools, exploit weakness and gain entry, gain privileged access, hide tracks, utilize sniffers to monitor / steal information, and expand control from one to many hosts.

Personal conclusions

The presentation gave us some numbers that can give some insight of the hacker community. It also showed an estimate in percent of the different types of hackers. We don't know if the numbers are exact .

Information Technology—Essential But Vulnerable: Internet Security Trends (Pethia 2002)

Abstract

Mr. Chairman and Members of the Subcommittee:

My name is Rich Pethia. I am the director of the CERT® Centers. Thank you for the opportunity to testify on computer security issues that affect the government. Today I will discuss the vulnerability of information technology on the Internet, including information about recent security trends, and steps I believe we must take to better protect our critical systems from future attacks.

My perspective comes from the work we do at the CERT Centers, which are part of the Survivable Systems Initiative of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. We have 14 years of experience with computer and network security. The CERT Coordination Center (CERT/CC) was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, acting as a wake-up call for network security. In response, the CERT/CC was established at the SEI. The center was activated in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled well over 173,000 incidents and cataloged more than 8,000 computer vulnerabilities.

The CERT Analysis Center, established just two years ago, addresses the threat posed by rapidly evolving, technologically advanced forms of cyber attacks. Working with sponsors and associates, the CERT Analysis Center collects and analyzes information assurance data to develop detection and mitigation strategies that provide high-leverage solutions to information assurance problems, including countermeasures for new vulnerabilities and emerging threats. The ultimate goal of this work is to predict technologically sophisticated cyber attacks and develop defensive measures to protect against them before they are launched. The CERT Analysis Center builds upon the work of the CERT Coordination Center.

The CERT Centers are now recognized by both government and industry as a neutral, authoritative source of data and expertise on information assurance. In addition to handling reports of computer security breaches and vulnerabilities in network-related technology, we identify preventive security practices, conduct research, and provide training to system administrators, managers, and incident response teams. More details about our work are attached to the end of this testimony (see Survivable Systems Initiative).

Methodology

This congressional testimony explains which threat the society faces. There are several brief chapters, using "reported numbers" as instrument that easily clarify our challenges.

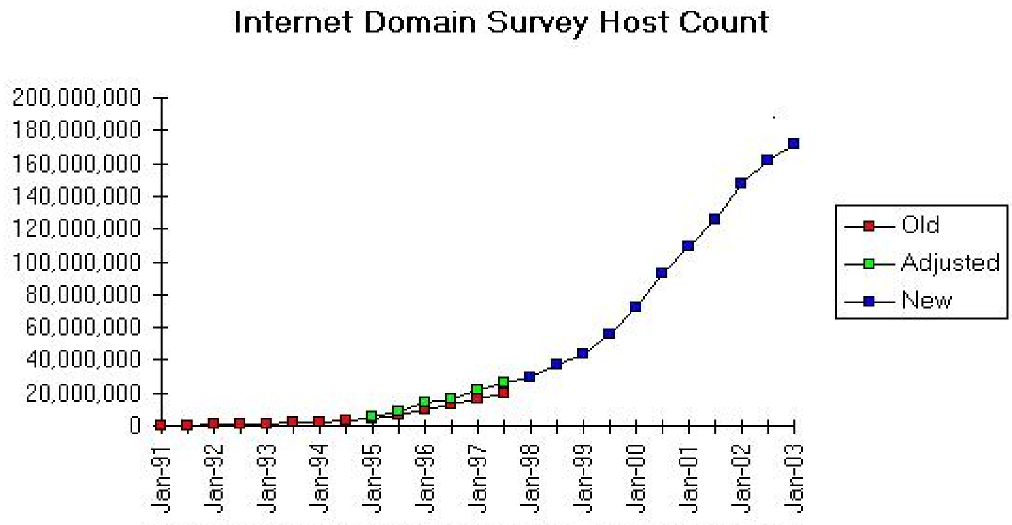
The author gives an overall description, and uses headings such as: The growing risk, the growing threat, Cyber space and physical space are one.

Results

Internet numbers:

The Internet Domain Survey (http://www.isc.org/ds/) reports that the Internet grew from 109 million computers in January 2001 to more than 147 million in January 2002.

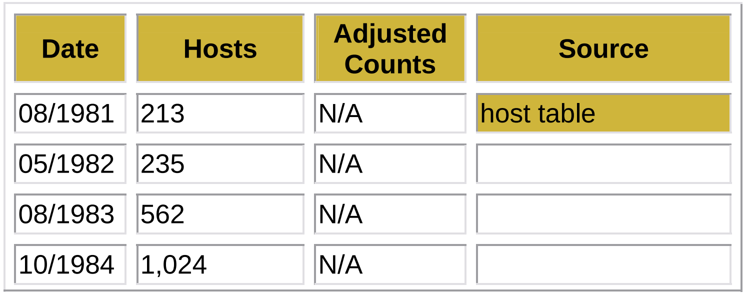
The following figure [5] shows how many hosts that have been connected to the Internet from the beginning of 1991, and until January 2003.



Source: Internet Systems Consortium, Inc. (www.isc.org)

We can also see the numbers shown in a table (http://www.isc.org/index.pl?/ops/ds/ (Host Count History)), from August 1981.

ISC Domain Survey:
Number of Internet Hosts



Date	Hosts	Adjusted Counts	Source
08/1981	213	N/A	host table
05/1982	235	N/A	
08/1983	562	N/A	
10/1984	1,024	N/A	

10/1985	1,961	N/A	
02/1986	2,308	N/A	
11/1986	5,089	N/A	
12/1987	28,174	N/A	old domain survey
07/1988	33,000	N/A	
10/1988	56,000	N/A	
01/1989	80,000	N/A	
07/1989	130,000	N/A	
10/1989	159,000	N/A	
10/1990	313,000	N/A	
01/1991	376,000	N/A	
07/1991	535,000	N/A	
10/1991	617,000	N/A	
01/1992	727,000	N/A	
04/1992	890,000	N/A	
07/1992	992,000	N/A	
10/1992	1,136,000	N/A	
01/1993	1,313,000	N/A	
04/1993	1,486,000	N/A	
07/1993	1,776,000	N/A	
10/1993	2,056,000	N/A	
01/1994	2,217,000	N/A	
07/1994	3,212,000	N/A	
10/1994	3,864,000	N/A	
01/1995	4,852,000	5,846,000	
07/1995	6,642,000	8,200,000	
01/1996	9,472,000	14,352,000	
07/1996	12,881,000	16,729,000	
01/1997	16,146,000	21,819,000	
07/1997	19,540,000	26,053,000	
01/1998	29,670,000	N/A	new domain survey
07/1998	36.739,000	N/A	
01/1999	43,230,000	N/A	

07/1999	56,218,000	N/A	
01/2000	72,398,092	N/A	
07/2000	93,047,785	N/A	
01/2001	109,574,429	N/A	
07/2001	125,888,197	N/A	
01/2002	147,344,723	N/A	
07/2002	162,128,493	N/A	
01/2003	171,638,297	N/A	

We can make significant progress to survivability by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems.

A particular relevant comment to our task is perhaps this: “A recent article in the Washington Post 1 reports that our growing dependence on computer-controlled and network-connected infrastructures—and the damage that could result from cyber attacks against those infrastructures—has not gone unnoticed by terrorist organizations. As the article reports: "…U.S. investigators have found evidence in the logs that mark a browser's path through the Internet that al Queda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transport, and communications grids." And "…al Queda prisoners have described intentions, in general terms, to use those tools."”.

Personal conclusions

This is a good article providing overall knowledge. It gives us some relevant numbers, and confirms that concentrated attack from terrorists is probable.

Conclusions

It was hard to find articles that had more than one or two answers to the questions we were to find out. And it was also hard to find out newer information from some of the former authors. The CERT/CC annual report 2003 will probably come in February, which perhaps will give us new information.

Summary

Any system can be broken in to by a determined hacker. But only one out of 10,000 or more people engage in hacking activity. A big concern is the increasing popularity of wireless networks.

A big mistake for companies, is to leave out the processes such as monitoring for new patches coupled with detailed evaluation, testing, deployment and validation that a team or individual manages

The typical hacker is characterized as bored and antisocial individuals or groups, where 90% are “script kids” that has little knowledge, but access to hacker tools. Less than 10% are competent programmers who modify existing tools, and only less than 1% builds new tools.

There are 30 hacker publications, 440 hacker bulletin boards, and 400,000 web sites dedicated to “hacking tips”. Hackers.com, 2600.com and insecure.org are examples of hacker web sites.

Signature

Kjetil E Braathen, Silje Salte

References

Fontana, John. 2003. Patching: Process matters. NetworkWorld 20 (48):2.

Lipson, Howard F. 2003. Survivability – A new security paradigm for protecting highly distributed mission-critical system 2000 [cited 17.11.2003 2003]. Available from http://www.cert.org/archive/pdf/surviv-paradigm.pdf.

Pethia, Richard D. 2002. Information Technology—Essential But Vulnerable: Internet Security Trends: Director, CERT® Centers, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213.

Slawsky, Richard. 2003. Know Your Enemy. New Orleans CityBusiness:1.

Verdeschi, John M. MasterCard Site Data Protection Program 2003 [cited. Available from http://www.electran.org/education_meetings/2003Annual/presentations/Verdeschi10.pdf.

Sources searched

Cert Coordination Center (www.cert.org)

The Library, Agder University College (www.hia.no/hiabib) (EBSCO: “academic search elite”, ”business source premier”, ”regional business news”, and ”business source elite”)

Keywords

Here are the keywords used in EBSCO:

Number of hackers
John Shors
Tim Jordan
Paul Taylor
Hacker attacks
Patching
Script version

Script attacks
Attach automation
Attach script
Hacker club
Script kiddies
Patching + Strategies
Computer underground
Hacker culture
Script development
Hacker bulletin boards
Hacker web sites

This memo

The following links are used for information that shows development over time.

[1] http://www.silkroad.com/papers/pdf/war_reprint1.pdf
[2] http://search.epnet.com/direct.asp?an=290091&db=bsh&loginpage=login.asp&site=ehost
[3] http://search.epnet.com/direct.asp?an=9712125076&db=bwh&loginpage=login.asp&site=ehost
[4] http://search.epnet.com/direct.asp?an=9705206527&db=bwh&loginpage=login.asp&site=ehost
[5] http://www.isc.org/index.pl?/ops/ds/

Appendix D (KEB&SS)Hacker Information040204.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

Hacker information continued 2

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: February 4, 2004

Re: Hacker information continued 2

Organization of this memo:

Introduction

This memo is written as a continuation on *(KEB&SS)Hacker Information040127*, because of doubt of the numbers in the table on page 5 in the article "MasterCard Site Data Protection Program" by Verdeschi. It seems to us that 400,000 hacker web sites is too much. Based on this, there was another article found from the same year, which this memo tells about.

Discussing papers, finding hacker information

Number of Hacking Web Sites Grow 45% (Unknown 2003)

Abstract

Hacking tools used by employees within organizations may be the biggest security threat to emerge this year (2003), leading to increased vulnerabilities, lost data, and wasted time and resources.

Methodology

It is a short article that reports from a leader of employee Internet management (EIM), Websense Inc., San Diego, California. At the end of the article, there is a section about Websense.

Results

The number of hacking web sites has increased with 45% the last 12 months. Total number of web sites is now approximately 6000 sites, with more than one million pages of content. The increase in hacking web sites may have much to do with political and economic issues, and the most hacked country in the world is the United States. 85% of all hacking against companies is committed by former employees. It is so, because the former employees have knowledge of the company's computer system.

Most of the hacking web sites contain archives of available hacking tools. These hacking tools can be denial of service attack software, sniffer and anti-sniffer software and password crackers. The sites also offer free downloads of hacker programs that enable employees to be self-taught, and step-by-step instructions for beginners on everything from how to gain unauthorized access to computer systems to instruction on how to perform attacks on routing protocols.

Personal conclusions

The article has some good facts about hacker web sites, and it is only a year old.

Conclusions

We have, as mentioned in the introduction, doubt about two of the references used in *KEB&SS)Hacker Information040127*. The sources here are found searching on www.google.com, while all the others are found on Agder University College's library database, EBSCO. In addition, is sounds more likely to us that the number of hacker web sites was 6,000 in 2003, than 400,000.

The article, *Number of Hacking Web Sites Grow 45%*, says that the number of web sites has increased with 45%, which means that the number in the beginning of 2002 must have been around 4,100 hacker web sites. We use this number, and create a new table compared to the one in last memo. We have also removed the two sources that seems doubtful to us. The new table is as following:

Hacker information

	Web sites	Publications	Bulletin Boards
April, 1997	1 900	Dozens	440
November, 1997	2 000		500
February, 1998	2 500		500
February, 2002	4 100		
February, 2003	6 000		

Signature

Kjetil E Braathen, Silje Salte

References

Unknown. 2003. Number of Hacking Web Sites Grow 45%. Worldwide Videotex Update Vol. 22 (Issue 2).

Sources searched

The Library, Agder University College (www.hia.no/hiabib) (EBSCO: “academic search elite”, ”business source premier”, ”regional business news”, and ”business source elite”)

Keywords

….

This memo

….

Appendix E (KEB&SS)TeenageHackers040225.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

Teenage Hackers

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: February 25, 2004

Re: Teenage Hackers

Organization of this memo:

Introduction

The purpose of this memo is to provide information about teenage hackers, who they are and why they do what they do. The Hacker Diaries tells the life stories of today's teenage computer hackers and profiles some of the most notorious hackers and hacking groups of recent years.

Discussing the book, finding information about teenage hackers

The Hacker Diaries: Confessions of Teenage Hackers (Verton 2002)

Abstract

Computer hacking and Web site defacement has become a national past time for America’s teenagers, and according to the stories you’ll read about in *The Hacker Diaries* – it is only the beginning.

- Who exactly are these kids and what motivates a hacker to strike?
- Why do average teenagers get involved in hacking in the first place?

This compelling and revealing book sets out to answer these questions – and some of the answers will surprise you. Through fascinating interviews with FBI agents, criminal psychologists, law—enforcement officials – as well as current and former hackers – you’ll get a glimpse inside the mind of today’s teenage hacker. Learn how they think, find out what it was like for them growing up, and understand the internal and external pressures that pushed them deeper and deeper into the hacker underground.

Methodology

The book is divided into chapters, where each chapter tells a story about a teenage hacker (sometimes two).

We wish to tell about some of these hackers to illustrate how a hacker can be like, why he/she was hacking, what he/she has done, etc.

Results

Genocide

Genocide grew up in Fairbanks, Alaska. Most of his high school hacking career was spent causing chaos on the school’s computer network. His cousin Tony had learned him lessons in social engineering (the art of collecting information from unsuspecting individuals by asking what seems to be harmless questions or by pretending to be somebody you’re not). His first hack consisted of logging in with his chemistry teacher’s name and password, and changed a grade so that he would get to graduate on time.

His mother started taking college courses, and Genocide began accompanying her to the college. He spent a lot of time surfing bulletin board systems (BBS), and also by reading and learning about various commands, operating systems and hardware design. When he became bored of that, he cracked a password file. He barely got away with it. Hacking was all about the taste of adrenaline, the challenge, and to push the limits.

Genocide began to make hacker friends after a while, and they kept their distance in the beginning. The members of the group shared similar view about hacking, and they were pissed off at the ignorance of the media and the general population when it came to understanding what a hacker was. The group became the Genocide2600 group (www.genocide2600.com (this is the new page, and not the original page)) and started to share their information with anyone willing to listen. A hacker could even visit the Genocide2600 site and learn how to defeat the FBI's lock-in trace capabilities, accept a free long-distance call by lowering the voltage on the phone, make a low-budget two-party phone line, etc.

The group started to attack pedophiles online. A program called AOHell was the tool that they used to hack into private AOL chat rooms in search of child pornographers and zap them with e-mail bombs that would crash their systems. Their Internet connection would be broken, he would reconnect, and the hackers hit him again.

Genocide2600 now claims to have more than 100 members from coast to coast.

Mafiaboy

Bill Swallow moved from a management position to the undercover team of agents who posed as teenage hackers online. He, and other undercover agents had to do hacks, or else they would have lost credibility. Hackers who knew they were jammed up, quickly became the FBI's trainers and consultants. They showed Swallow how to act in various IRC chat rooms and how to respond to questions and challenges from other hackers. The best source of intelligence about a hacker is another hacker.

The first of the big attacks by Mafiaboy (14 years old at the time) started on February 7, 2000. Yahoo! got hit. Yahoo! was dealing with a hacker who knew what he was doing and who took the time to learn about his target and plan the attack. It was a DDoS attack (DDoS = Distributed Denial of Service). The same night, Mafiaboy was on an IRC (Internet Relay Chat) channel bragging about his skilz (skills). The next day, Buy.com, eBay and Amazon.com got hit, and Mafiaboy was again on IRC that night and claimed responsible of the attacks once again. Somebody on the channel suggested CNN for a good next target, and within minutes CNN got hit. Dozens of computers had been hijacked and used in the attacks. The intruder had planted malicious software on these systems that had turned them into autonomous launching pads for denial-of-service attacks.

IRC is one of the most popular and most interactive services on the Internet. You need a Web browser and an IRC client to connect to an IRC server. The next step then is to get into one of the channels (an IRC server can have dozens, hundreds or thousands of chat channels open), and get yourself a nickname. Participants in the chat can exchange ideas on common interests, and even many businesses now hold scheduled chat sessions.

The chat log in the IRC hacker room #!tnt details a conversation between Mafiaboy (who has changed his nickname to anon (for anonymous) and other hackers:

T3: mafiaboy, so who's next after dell

Anon: Microsoft will be gone for a few weeks

T3: oh man, that's evil

*T3: I need to get away from you before I get busted for being an accomplice or some sh***

Anon: I know what I'm doing

Anon: yahoo.dom

*T3: So Mafiaboy, it was really you that hit all those ones in the news? buy.com, etrade, eBay, all that sh**?*

Anon: you just pin em so hard they can't even redirect

T3: they say you're costing them millions

Anon: surprised I didn't get raided yet, T3, they are fools

This is part of the chat log captured by several security experts in the private sector and other hackers, and sent it to the FBI.

Mafiaboy got caught by the FBI. When investigators picked apart his computers, they found no technical evidence linking him to the attacks. Without wiretap and data interception operation, they wouldn't a case. On September 12, 2000, Mafiaboy got a eight-month sentence in a juvenile detention center. He pleaded guilty to dozens of charges related to the February attacks.

The last time the FBI had dedicated nationwide resources and manpower to hunt down a single hacker was with Kevin Mitnick (America's most wanted hacker) in the late 1980's and early 1990's. The Mafiaboy investigation involved more than a hundred agents in two countries. Neither Mafiaboy nor Mitnick were very good hackers. Mitnick was far better at social engineering than he was at hacking. His success was a direct function of the phone numbers, account numbers, and passwords ha was able to fool unsuspecting people into giving him. For Mafiaboy, successful hacking was a matter of downloading software tools from the Internet, following directions, and hitting the Enter key on his keyboard.

Pr0metheus

Pr0metheus became a hacker when he was 14, and he is one of Satan's hackers. His organized hacking career started with a well-known group called PoizonBox. The group was responsible for more than 900 Web site defacements.

Pr0metheus got bored of PoizonBox, and became the leader of a new defacement group called Hacking For Satan. All he wants is to spread the word of Satanism. It's not about raising people's awareness of Internet security issues, or about the love of technology or the thrill of the hack. He hates organized religion, and especially Christianity.

One of the hacks that he did, included the search for hosts that contained the words *church* and *holycross* in their name, and seconds later the online system spits back a list of more than 2,000 servers. To narrow down the list, he wrote or modified several automated scripts using the Perl (Practical Extraction and Report Language) programming language. The next script he used, was to check for the servers ran on the Windows operating system. The last script that was run, checked for FrontPage systems that had open ports and access controls that enabled "everyone" to modify the site's content. One of his first targets was the Southgate Baptist Church in Springfield, Ohio, where Pr0metheus used the script to replace their Web site with his own liturgy on the principles of Satanism.

Starla Pureheart

Anna Marie Moore (with nickname Starla Pureheart) grew up in a computer-oriented family. She was exceptionally bright, and had successfully hacked her own Windows system. This was no big achievement for her, so by the time she was 13, she was well on her way to mastering the Linux operating system.

The characterization of hackers as socially awkward teenagers with oversized glasses and pocket protectors doesn't apply to Anna. She contradicts the image of the teenage hacker as dark, brooding, and antisocial misfit. In her case, hacking is the ruthless quest for knowledge and the study of technology.

When Anna was 15, she won the CyberEthical Survifor contest at the annual DefCon hacker conference in Las Vegas. DefCon (www.defcon.org) is the worlds largest underground hacking event in the world, and gathered more than 5,000 hackers.

Hacking still remains a passion to Anna. She was supported by her parents all along with her hacking and they have helped her to develop moral and ethical compass.

General results

The book illustrates that there is no stereotype hacker. They are of all ages, from all walks of life and from everywhere. What is very often common with hackers, is that they often spend their time in front of the computer until late at night (or early in the morning). At this time, some of them talk to other hackers through IRC-channels, searching through Bulletin Board Systems, etc. Hackers are motivated by intellectual curiosity.

There is a new trend within the hacker culture. Teenage hackers used to be interested in exploring and sharing information, but a growing number of them are interested in destroying and blocking information flow. Most of the hackers are script kiddies.

A core belief in the hacker community, is that when hackers discover new vulnerabilities, they force companies to take action to plug the security holes in their software that might otherwise go unfixed. Technology is more fragile than people like to believe.

Personal conclusions

This is a very entertaining book, and it comes up with a lot of facts about the hacker culture. The book describes, as mentioned before, each of the hackers, why they did it, some of the things they have done, etc. When you read this book, you get another more "friendly" impression of hackers. Several of the hackers in the book try to explain the real meaning of being a "hacker". They mean that a "real hacker" is what we know as a "white hat" hacker, a person with good intentions. They mean that there is pride being a hacker, and that most of the hackers do not have malicious intentions. But, anyway, when it comes to criminality, they are balancing on a thin line, and most of the hackers do cross it.

Signature

Kjetil E Braathen, Silje Salte

References

Verton, Dan. 2002. The Hacker Diaries: Confessions of Teenage Hackers: Osborne/McGraw-Hill.

Sources searched

Keywords

This memo

http://www.mirc.com/irc.html (information about IRC - Internet Relay Chat)

Appendix F (KEB&SS)Blaster and blackout040225.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

Blaster and blackout

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: February 25, 2004

Re: Blaster and blackout

Organization of this memo:

Introduction

The issue here will be to find out whether or not the MS Blaster worm was linked to the major blackout in parts of US and Canada on August 14, 2003.

Discussing papers, finding hacker information

Through this memo, we have divided the sections into the papers or texts we have found interesting.

Hacker Danger For Power Supply? (Krane 2003)

Abstract

Since the blackout August 14, 2003, utilities have accelerated plans to automate the electric grid, replacing aging monitoring systems with digital switches and other high-tech gear. But those very improvements are making the electricity supply vulnerable to a different kind of peril: computer viruses and hackers who could black out substations, cities or entire states.

Methodology

The article focuses on danger of hacking for power supply, and the Blaster worm and the Slammer worm are mentioned in this connection. It also tells about the renewal of the electric grid requires a vulnerable connection to a computer network. There are system weaknesses, and there are bad practices for patching.

Results

The grid has a growing number of vulnerabilities, and security experts have warned about it, especially after U.S. National Security Agency hackers proved that they could break into the grid control networks in 1998. Computer viruses are a new worry.

The MS Blaster worm flummoxed an estimated half-million computers around the world in August 2003 might have made worse utilities’ problems during the blackout. It might have brought down – or perhaps blocked communications – on computers used to monitor the grid. The worm didn’t cause what happened, but it could have exacerbated what happened.

Personal conclusions

The article says very clearly that the Blaster worm didn’t cause the blackout. It may have worsened the situation, though.

Blaster worm linked to severity of blackout (Verton 2003)

Abstract

WASHINGTON -- The W32.Blaster worm may have contributed to the cascading effect of the Aug. 14 blackout, government and industry experts revealed this week. On the day of the blackout, Blaster degraded the performance of several communications lines linking key data centers used by utility companies to manage the power grid, the sources confirmed.

Methodology

In this article, the author (Dan Verton) accumulates comments from different persons, having different backgrounds, on the W32.Blaster worm issue. He doesn't take side, but simply quote several opinions.

Results

There are both people thinking that the worm did have influence on industry systems, and not.

Personal conclusions

We get the feeling that the worm did affect several industry systems and the blackout, but there is not enough information on this to make conclusions. We probably don't get the "whole story", simply because this is "classified information".

Conclusions

Before there is more evidence, there is difficult to conclude that the MS Blaster worm was linked to the major blackout in parts of US and Canada on August 14, 2003. The two articles in this memo fulfill this.

Signature

Kjetil E Braathen, Silje Salte

References

Krane, Tim. Hacker Danger For Power Supply? The Associated Press, September 11 2003 [cited. Available from http://www.cbsnews.com/stories/2003/09/11/tech/main572770.shtml.

Verton, Dan. Blaster worm linked to severity of blackout 2003 [cited. Available from http://www.computerworld.com/printthis/2003/0,4814,84510,00.html.

Sources searched

CERT Coordination Center (www.cert.org)

The Library, Agder University College (www.hia.no/hiabib) (EBSCO: "academic search elite", "business source premier", "regional business news", and "business source elite")

www.google.com

Appendix G (KEB&SS)MixterAndRandomizer040308.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

Mixter and Randomizer

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: March 8, 2004

Re: Mixter and Randomizer

Organization of this memo:

SOURCES SEARCHED

KEYWORDS
THIS MEMO

Introduction

The purpose of this memo is to find information about the two German hackers Mixter and Randomizer. They were both pioneers in denial of service attacks, and members of two different hacker clubs that competed with each other. It all started in 1995, and we will try to find the whole story.

Discussing papers, finding hacker information

Through this memo, we have divided the sections into the papers or texts we have found interesting.

Opinion: On Magic, IRC wars, and DDoS (Graham)

Abstract

The thing about hacking is that it is a lot like the magic tricks you see in Las Vegas. The key to magic is not coming up with difficult tricks, but obfuscation them with distractions. On the other hand, hacker attacks are only frightening and attention-grabbing because people don't know the boring details. Users scare easily, and most users are afraid of their machines because they can't seem to master all the complexities. In reality, there are only a few ways hackers break into PCs, and only a few steps users need to be aware of to defend themselves.

Methodology

The article is divided into an introduction, a part about mundane Internet principles, a section about wars between hacker clubs, a section about DDoS, one part that says that effect doesn't equal sophistication, and a summary. At last, resources and news articles used are mentioned.

Results

The system that the Internet is based upon, is based on trusting its users, and is therefore defenseless against "internal" attacks. There are about 20 hackers in the world that are skilled enough to bring down the Internet in a similar manner that Robert T. Morris took down the net with a "worm" 10 years ago. But on the other hand, there are about 100,000 hackers that are skilled enough to bring down a major Internet portal for a few hours.

The method of how the attacks on Yahoo and the other big Web sites happened: the hacker breaks into about 50 machines that are attached to a high-speed Internet connection, and runs a program on each of these machines. The program causes the machines to send network traffic as fast as they can against the victim.

Hacker gangs are breaking into machines and are using them for attacks against Internet Relay Chat (IRC) chatrooms. A hacker can get control of a chatroom by kicking off all the rival moderators. This is a way for hacker gangs to gain control of IRC chatrooms, and then keep control against attacks from rival gangs. Hackers are using a method called "the flood", which is a technique where a hacker sends a huge number of pings against the victim. There will be so much meaningless traffic that nothing else can get through.

The FBI estimated that it took about 50 machines to take down Yahoo. It does not mean that a sophisticated tool and a skilled hacker is used just because the attacks are impressive. To do this kind of an attack, DDoS, all you need to do is to download the software from the Internet, use a scanner program against millions of IP addresses, and the machines that are not secured against scripts will get hacked. The scripts will give you full control of the machines through a remote command window. When you log into one of these machines, you start installing bots like Trin00 (Trinoo), TFN (Tribe Flood Network), or Stacheldraht. "Bot" is short for "robot", and it is an automated program. For example, one kind of bot tries to stay logged onto the IRC chatroom, become moderator, and pass moderation privileges to other bots.

Personal conclusions

The article is very general, and the discussion about how hacker gangs compete gives an insight into how they fight. This does not mean that this is the way that the hacker gangs of Mixter and Randomizer competed against each other.

Hacker discloses new Internet attack software (Shankland 2000)

Abstract

A programmer familiar with attack software has disclosed three new attack programs of the type believed to have taken down major Internet sites last week, complicating the jobs of security experts trying to fight the malicious programs.

Methodology

It is a short, continuous article that is not divided into sections. There is also a link to a page that describes how a denial of service attack works, and a link to a page that contains different other links to articles about Mixter, Mafiaboy, the big attacks against Yahoo, eBay, etc., about denial of service attacks, etc,.

Results

Packet Storm is a site that publishes malicious software so security professionals can scrutinize it. Mixter, at Packet Storm, is the author of the attack tool TFN (Tribe Flood Network) and its sequel, TFN2K. These are both distributed denial of service tools (DDoS). Other examples of DDoS tools are: Blitznet written by "phreeon", Trinoo written by "phifli" and Stacheldracht written by "Randomizer".

There are online detection tools that are used to find computers infected with DDoS attack software, f.e., MyCIO. Of more than 10,000 who have used it to scan their systems, the MyCIO software has found five cases of Stracheldraht, one of TFN and one of Trinoo.

Personal conclusions

It is explained who has written what DDoS tool, and a little about what they do and how to detect them. But the article is very short, and we would wish that it told us much more about Mixter and Randomizer and the story behind.

Website of Mixter: .mixter security (http://Mixter.void.ru/index.html)

Abstract

Here's a short summary of the less boring technical things I've done so far. I consider this my personal home page and feel like writing my boring history on this page. If you fall asleep, you've been warned. :P Far from all of this is professional security work, some of it was done for fun and education. I started out in C with maintaining and contributing a bit to the development of eggdrop, the all-purpose IRC bot. My old Tcl script for eggdrop is entity, which is still available, now for 1.6 eggdrop bots. :) It's designed specially for large distributed eggdrop networks and has very efficient channel- and basic intrusion protection. Some people use and like it for its ease of use. This was my first experiences with programming distributed networks, sort of.

Structure of the website

This website is divided into three main pages, .home, .about and .mail. From the .home location, you can download scripts and tools made by Mixter and other hackers, or view papers written by Mixter. You can also read other articles and DDOS related material from here. There is also a page with security links. In the .about section, which we find interesting, Mixter has written his project history, a personal profile, and facts about the DDOS incident. The .mail link links you to your e-mail client.

Results

Randomizer is just mentioned on this website (as the writer of “Stacheldracht”, and a TESO member). This is Mixter’s own personal profile, written in 2002:

Nickname: Mixter
Real Name: Isn't exactly a secret, but I prefer to keep my privacy. Ask me.
Current age: 23
Contact: mixter@hacktivismo.com
Citizenship: German
Residence: Germany, at the moment
Politics: Libertarian
Areas of Interest:
Maintaining friendships around the world.
Hacktivismo, and technical projects using the Internet in new ways.
Distributed applications and decentralized peer-to-peer.
Philosophy. Mostly, recognizing and challenging established authority.
Amateur biochemistry and bioinformatics. I'm also into Life Extension.
Practical security, vulnerabilities. I don't have time for it right now.
Forcing myself to learn things like openssl or all of ANSI C++.
Music: Classical, Psytrance. I also composed some ambient tracks.
Employment: Recently started as a senior developer at a Germany-based security/crypto company.
Current Projects: Hacktivismo and Six/Four. Right now, I don't feel like getting involved in any new projects.

Maintained Projects: Mostly, nsat and libmix. I have some private projects.

Personal conclusions

Good website with good links, well written. Would it be an idea to e-mail Mixter and ask him about the hacking clubs and Randomizer?

Conclusions

It seemed impossible to us to find the whole story that started in 1995. Randomizer is barely mentioned in some of the articles, and we have not found any information about the two hacker clubs that competed. A lot of time has been used to search for information this time, and little exact information has come out of it (compared to what we wished). The results that we found were mainly written right after the attacks in February 2000. An idea would perhaps be to write an e-mail to Mixter, and ask him about the hacking clubs.

Summary

Randomizer is just mentioned as the writer of “Stacheldracht”, and a TESO member, and a boy who “shrouds his identity in secrecy”. Mixter participates in larger projects, and seems to shear knowledge in a wider way.

Signature

Kjetil E Braathen, Silje Salte

References

Graham, Robert. Opinion: On Magic, IRC wars, and DDoS [cited. Available from http://www.robertgraham.com/op-ed/magic-ddos.html.

Shankland, Stephen. 2000. Hacker discloses new Internet attack software.

Sources searched

Cert Coordination Center (www.cert.org)

The Library, Agder University College (www.hia.no/hiabib) (EBSCO: “academic search elite”, ”business source premier”, ”regional business news”, and ”business source elite”)

www.google.com

Keywords

The keywords used are:

- denial of service + pioneers
- denial of service + pioneers + German
- denial of service + pioneers + German + hackerwar
- denial of service + pioneer + German
- dos pioneers + hacker
- German hacker clubs

- hacker clubs + Mixter
- hacker clubs + war between
- hacker war + pioneer dos
- hacker war + pioneer + dos + German
- packet storm + German + hacker + clubs + war
- packet storm + Mixter + randomizer
- packet storm + cyberwar
- packet storm + cyberwar + German
- turf war + Mixter
- Mixter + 1995 + hacker
- Mixter + 1995 + hacker + TFN
- Mixter + 1995 + hacker + TFN + packet storm
- Mixter + hackerwar
- Mixter + packet storm + German
- Mixter + packet storm + German hacker
- Mixter + packet storm + German hacker + attack
- Mixter + packet storm + German + war
- Mixter + packet storm + Germany
- Mixter + packet storm + Germany + turf war
- Mixter + packet storm + war
- Mixter + packet storm + randomizer
- randomizer + leader + hacker club
- hacker + randomizer
- hacker + randomizer + hacker club
- randomizer + stacheldracht
- cyberwar + Germany
- cyberwar + Germany + Mixter

This memo

http://Mixter.void.ru/index.html

http://news.com.com/2100-1001-236731.html?legacy=cnet

http://zdnet.com.com/2100-11-518461.html?legacy=zdnn

http://news.com.com/2100-1001-236904.html?legacy=cnet

http://progsystem.free.fr/hackingnews.htm

http://news.com.com/2100-1023-236876.html?legacy=cnet

http://news.com.com/2100-1023-236848.html?legacy=cnet

http://teso.scene.at/

http://www.hacktivismo.com/

Appendix H (KEB&SS)DoSAndDDoS040315.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

DoS and DDoS

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: March 15, 2004

Re: DoS and DDoS

Organization of this memo:

Introduction

In this memo, we will try to find more information about denial of service attacks, and distributed denial of service attacks. We will also try once again to find more information about the story behind the hacking war between the clubs of Mixter and Randomizer, which we found hard to do in *(KEB&SS)MixterAndRandomizer040308*.

Discussing papers, finding hacker information

Through this memo, we have divided the sections into the papers or texts we have found interesting.

Lesson 182: Distributed Denial of Service Attacks (Clark 2003)

Abstract

Focuses on distributed denial of service (DoS) attacks, a computer virus. Goal of the virus; Common methods for initiating a DoS attack; Initiation process of the distributed DoS attack.

While Denial of Service (DoS) attacks have been around for many years, they are becoming increasingly menacing as the Internet extends further into the global communications fabric. Over the past several years, such exploits have been overshadowed by Distributed DoS (DDoS) attacks in which multiple systems can be used to launch an attack, significantly increasing the potential for widespread damage.

Methodology

The article describes the DoS method at first, and divides it into the two common methods for initiating a DoS attack; packet flooding and the use of malformed packets. After this is described, the article tells about DDoS in detail. At the end, there is a section about some incidents that happened in 2003 (until September, when the article was written), and which tools were used.

Results

Denial of service attacks are divided into two primary groups:

- Packet flooding attacks, which are aimed at overwhelming the system resources. The receiver gets exploded with multiple connection requests, but he fails to send the necessary acknowledgements in return. The result is half-open connections that tie up resources and prevent legitimate connections from being made. Two types of packet flooding attacks are Internet Control Message Protocol (ICMP) flood attacks, and Smurf attacks. Trinoo, Tribe Flood Network (TFN), Shaft, Stacheldraht, Trinity, Targa3, and FloodNet are other examples of attacks that involve packet flood exploits.

- The use of malformed packets are typically geared toward crashing a service. The attacks exploit errors in TCP/IP stack by sending atypically formatted packets. Buffer overflow is a common result of a malformed packet attack. It occurs when too much data is written to a buffer, which can result in overwriting of data in adjacent buffers, alteration of data, file damage, and system crashes. Examples of malformed packet attacks are Ping of Death, TearDrop, NewTear, Bonk, Syndrop, Chargen, WinNuke, Land, and Joltz.

Distributed denial of service attacks are based on many of the same mechanisms as DoS attacks, but they are more complex and have the potential to do more widespread damage. In an attack like this, the attacker first chooses the exploit and the attack type, and then enlists zombie systems to form an army of unwitting participants. To find these, the attacker scans the Internet for vulnerable IP addresses with a scanning tool. After he/she has done this, he/she downloads a daemon (a program that executes command strings form the master system, onto the zombies). When the command sequence is sent from the master system, the zombies will attempt to execute the attack, by for example bombarding the target with packets.

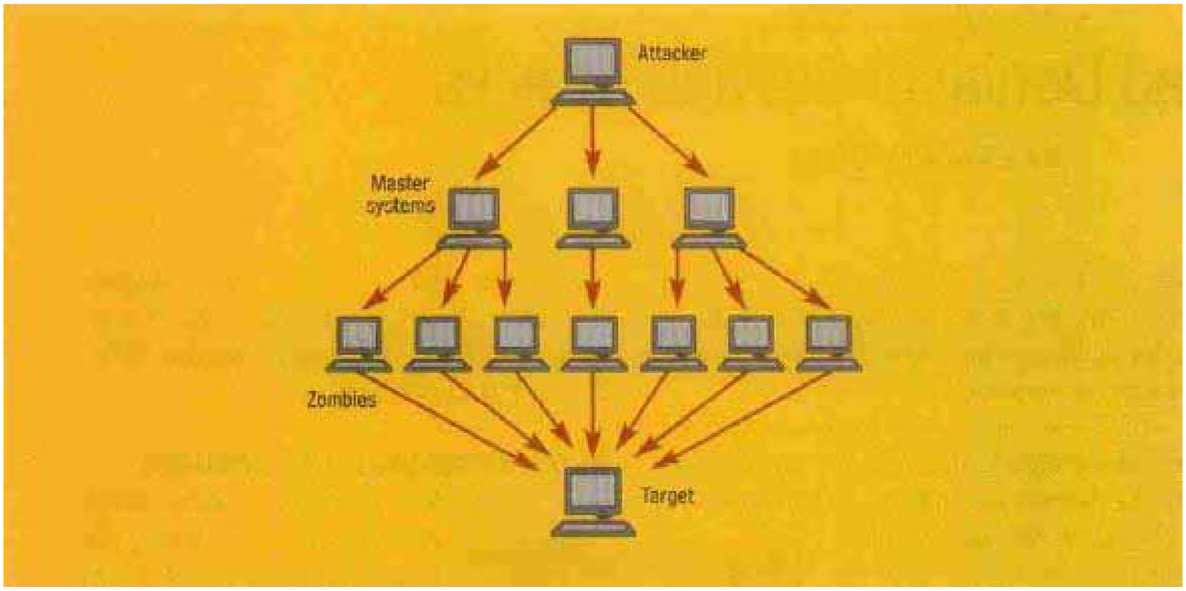


Figure 1: The DDoS Deluge

DDoS attacks will become more difficult to detect as they evolve, and they will be able to compromise more and more systems within shorter windows of time. There is also an increasing availability of more sophisticated automated tools for scanning and deployment, which means that the DDoS attack tools are becoming easier for less skilled attackers to launch.

Worms are not typically intended to be mechanisms for DoS or DDoS attacks, but they can result in serious denial of service conditions. When a worm is launched, it can spread to systems that were not deliberately selected as targets.

Personal conclusions

Both DoS and DDoS attacks are described in an understandable way, and the article is pretty easy to read. It explains how the types of attacks work, and also gives examples of them.

German Creator of Site Crashing Program Gets Heavier Sentence (Unknown 2000)

Results

The 21-year-old hacker, “Mixter”, got sentenced to a 6-month youth prison sentence for among other things "computer sabotage", "spying for data", and also other attacks on businesses in 1998. The sentence got suspended to a two-year parole period.

Conclusions

We found a good article about DoS and DDoS attacks, and just a small site that mentioned a few things about Mixter. We still did not manage to get the whole story, which seems impossible to find on the Internet.

Signature

Kjetil E Braathen, Silje Salte

References

Clark, Elizabeth. 2003. Lesson 182: Distributed Denial of Service Attacks. Network Magazine Vol. 18 (Issue 9):2 p.

Unknown. German Creator of Site Crashing Program Gets Heavier Sentence 2000 [cited. Available from http://www.internetnews.com/bus-news/article.php/6_332571.

Sources searched

Cert Coordination Center (www.cert.org)
The Library, Agder University College (www.hia.no/hiabib) (EBSCO: “academic search elite”, "business source premier", "regional business news", and "business source elite")
www.google.com
www.yahoo.com

Keywords

Keywords used in the search:

- Story of hacking
- DoS
- DDoS
- Denial of service
- Distributed denial of service
- Germany + hackerwar
- Mixter + Randomizer
- Mixter + TFN + war
- Mixter + TFN + hacker clubs
- Randomizer + Stacheldraht
- Story behind DoS
- Story behind DDoS
- Mixter + Israel
- Mixter + sentenced

Appendix I (KEB&SS)DoSandDDoS040323.doc

Kjetil Eiklid Braathen, Silje Salte
Agder University College
Faculty of Technology and Science
Institute of ICT
Groosveien 36
N-4876 Grimstad
Norway

HiA

DoS and DDoS

To: Jose J Gonzalez

From: Kjetil E Braathen, Silje Salte

CC: Johannes Wiik

Date: March 23, 2004

Re: DoS and DDoS

Organization of this memo:

Introduction

This memo is written to find more information about DoS and DDoS attacks, and also to examine the two links http://www.cert.org/reports/dsit_workshop.pdf and http://www.robertgraham.com/op-ed/magic-ddos.html. The original purpose of the links, given to us by Tim Shimeall, was to find more information about the Mixter and Randomizer case.

Discussing papers, finding hacker information

Through this memo, we have divided the sections into the papers or texts we have found interesting.

DDoS Attacks: Precursor to Digital Terrorism (Sigmond and Kaura 2001)

Abstract

It's well established that hackers can cause havoc, knocking down important Web sites, like Amazon.com, and causing major financial loss. But, in this networked world, just how large could the threat be? A new breed of cyber threats is emerging. As the Internet becomes an integral part of the economic fabric, concerns about its safety and reliability continue to mount. Ironically, some of the most powerful features of the Internet, namely interconnectivity, distributed computing, and the ability to transmit information instantaneously, are the very factors that could bring down this digital lifeline and everything that it feeds. Perhaps the most potent and difficult to tackle hacker attacks are distributed denial of service (DDoS) attacks.

Methodology

The article starts with a little introduction, then explains the development from DoS to DDoS. After this, the authors take a look at how big the impact is, a small part about FAA (Federal Aviation Administration), about how DDoS belongs to the next generation, how to tackle DDoS, and that it is an emerging business opportunity. At the end, there are numbers of estimated costs of different DDoS attacks.

Results

There have been warnings from security experts that say that future attacks will not come from "script kiddies" and casual hackers, but they will come from highly-trained cyber-terrorists and the cyber-armies of enemy states.

The purpose of a DoS attack is to render the target system completely useless. There are two strategies to do this:

- flood attack; flooding the target with spurious traffic and overloading it. Examples are ICMP attack, SYN attack, AmurF attack and Fraggle attack.
- logic attack; exploits known software bugs on the target system in an effort to take it offline. Examples are Ping of Death, Teardrop, Land and Chargen.

A DDoS attack differs from a DoS attack, in that the spurious traffic originates from multiple machines in the Internet, while it originates from a single machine in DoS attacks. DDoS attacks have therefore much bigger impact, and are more difficult to fight.

In 1999, 27 percent of the respondents to CSI/FBI annual surveys indicated experiencing DDoS/DoS attacks. The numbers went up to 36 percent in 2000. It is suggested that 4,000 DDoS attacks happen across the Internet each week (2001). It is also estimated that 2.4 percent of all attacks could break through highly tuned/optimized firewalls.

Cyber wars are very efficient for the attacker from a risk/cost perspective, and the attacks can be just as damaging as physical attacks.

Hackers are busy creating smarter versions of the hacker tools. This can be new types of DoS attacks, which cause degradation of service, and do not result in denial of service. Degradation of service is when the victim's servers are not completely overwhelmed, but are stunned with a barrage of significant network activity. The use of "pulsating zombies" is another version of the attack. This is when the pulsating zombies are never active for sufficiently long durations, while normal zombies are always on. Another way to explain this, is to say that short bursts of attack traffic are directed at an intended target. Zombies are computers that are controlled remotely by crackers. Another type of attack involves "reflectors" (all Web servers, DNS servers, and routers are reflectors). Here, the zombies (a couple of hundred) send packages to reflectors (hundreds of thousands) after spoofing the victim's source address. The reflectors interpret the packets as coming from the victim and end up sending reply packages to the victim.

Detection, identification of the source, and solution are three aspects to tackling DDoS. These kind of attacks can result in billions of dollars in lost business within hours.

Personal conclusions

DoS and DDoS are very briefly described, with examples, and thereby not explained thoroughly. We question the contention that future attacks will come from highly trained cyber-terrorists, because the tools that hackers use are becoming more and more user-friendly. But cyber-terrorists will probably use these kinds of tools more and more as well, because they can be very destroying, and it is a "new" way to have a war between countries.

Understanding and Preventing DDoS Attacks (Vaughan-Nichols 2004)

Abstract

It was in early 2000 that most people became aware of the dangers of distributed denial of service (DDoS) attacks when a series of them knocked such popular Web sites as

Yahoo, CNN, and Amazon off the air. More recently, a pair of DDoS attacks nailed The SCO Group's Web site, which many people thought had to be a hoax, since surely any company today could stop a simple DDoS SYN attack. Wrong.

Methodology

The author starts saying in this article that DoS and DDoS attacks are continuously launched against the Internet. Then the author describes some attacks and attack types. At the end, he suggests how to deflect them.

Results

There are many types of DDoS attacks. Often, when we are talking about DDoS attacks, we mean attacks on the TCP/IP protocol. There are three types of such attacks: the ones that target holes in a particular TCP/IP stack; those that target native TCP/IP weaknesses; and the boring, but effective, brute force attacks. For added trouble, brute force also works well with the first two methods.

What you should do to deflect attacks: all the usual security basics can help you (antivirus client, firewall, patching). This will not stop all DDoS attacks, but it will stop some of them. Keep yourself current on the latest DDoS developments. A good site for this is the University of Washington hosted Distributed Denial of Service (DDoS) Attacks/tools site (http://staff.washington.edu/dittrich/misc/ddos/). This site has a good archive of articles and other DDoS material.

Personal conclusions

This article is informational on the DDoS subject. We will examine the links.

Hacker War Keeps the Worms Coming (Gaudin 2004)

Abstract

The onslaught of worm variants has slowed slightly in the past few days, but at least one security analyst says the attack of three vicious viruses seems far from over.

Methodology

This is a short article with some facts and quotations, which lead to the main message: the rivalry of the hackers that instigate more attacks.

Results

“What appears to be fueling the virus writers' fire is that they are actually sniping at each other”.

"These virus writers are fighting a war amongst themselves for attention and one-upsmanship, and we're all getting caught in the crossfire."

The above quotations confirm the hacker war.

When the virus is written just to kill another virus from another “hacking club”, it confirms the rivalry.

Personal conclusions

This is a rather short article, which shows us the hacker fronts clearly, and maybe it shows us some of the hackers mind: that the goal is not always the intrusion or virus itself, but to state an example of power.

Results of the Distributed-Systems Intruder Tools Workshop (Unknown 1999)

Abstract

In a denial of service attack using distributed technology, the attacked system observes simultaneous attacks from all the nodes at once – flooding the network normally used to communicate and trace the attacks and preventing any legitimate traffic from traversing the network.

Methodology

The paper is the outcome of the work done at a Distributed-Systems Intruder Tools Workshop in Pittsburgh, Pennsylvania (November 2-4, 1999). It starts with a summary, followed by an introduction, recent activity involving distributed attack systems, some audience-specific information (specific information for groups in the Internet community: managers, system administrators, Internet service providers (ISPs), and incident response team (IRTs)). We choose not to discuss the last part in this memo, but focus on the relevant things for our use.

Results

The intruder community is loosely organized when it comes to development of attack tools. There are parallels to draw with open system development, because there are many developers and a large, reusable code base. Tools that are used, are becoming increasingly sophisticated, and they are also becoming more user friendly and widely available. This results in unsophisticated users using the available tools to identify and take advantage of a large number of vulnerable machines.

To develop new and more powerful distributed attack tools, intruders are using currently available technology. There has been an increase in the development and use of distributed sniffers, scanners, and denial of service tools.

Intruders are actively seeking systems with good network connectivity for compromise and installation of daemon programs.

Personal conclusions

The paper is from December 1999, and has therefore no recent information about Distributed-Systems Intruder Tools. There was good information about DDoS (we chose not to write all of it here so that we would not repeat ourselves).

2003 CSI/FBI Computer Crime and Security Survey (Unknown 2003)

In this part, we look at statistics over denial of service attacks.

Table 1: Denial of service attacks detected (by percent)

Year	DoS attacks
1998	31
1999	27
2000	36
2001	40
2002	42

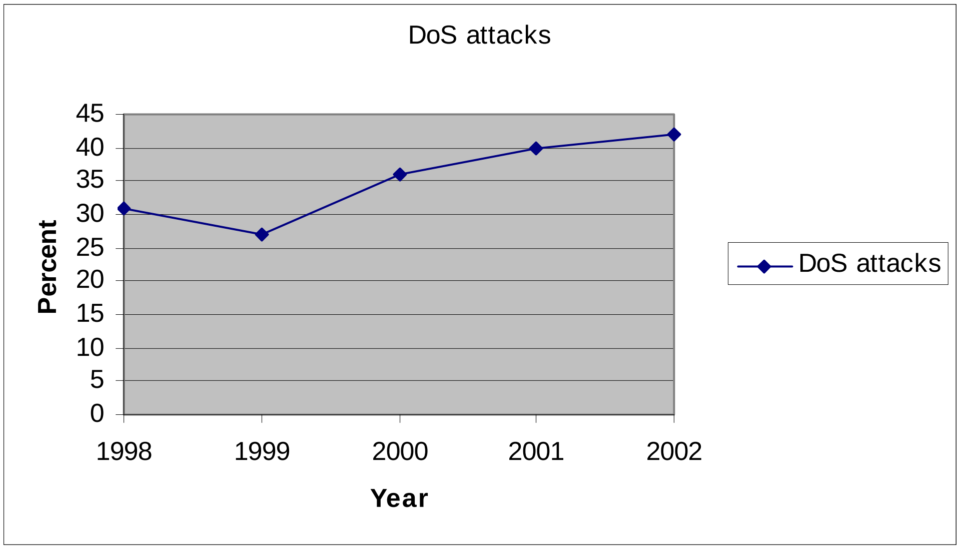


Figure 1: Denial of service attacks

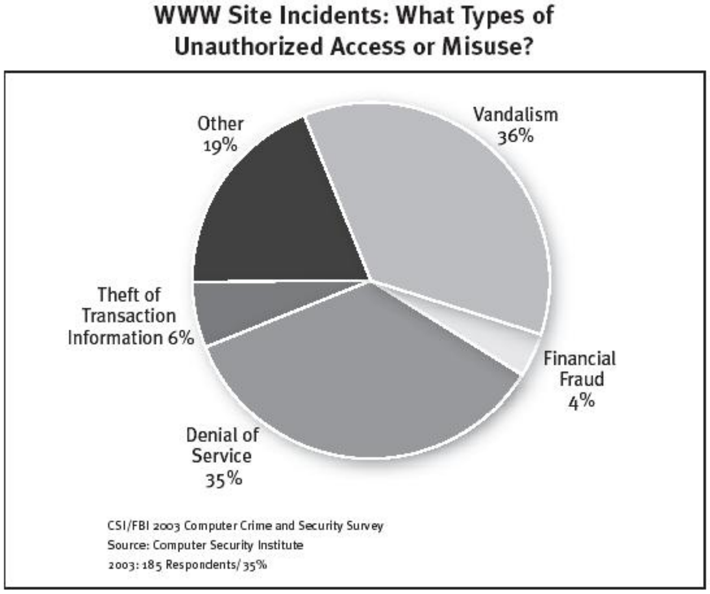


Figure 2: Web site incidents

The figures shows that the number of DoS attacks are increasing (except from 1999 when it decreased), and that these kind of attacks are a big part of Web site incidents. But the portion of DoS attacks detected went down in year 2000.

Summary

A DDoS attack differs from a DoS attack, in that the spurious traffic originates from multiple machines in the Internet, while it originates from a single machine in DoS attacks. DDoS attacks have therefore much bigger impact, and are more difficult to fight.

Cyber wars are very efficient for the attacker from a risk/cost perspective, and the attacks can be just as damaging as physical attacks.

Cyber-terrorists will probably use these kinds of tools more and more, because they can be very destroying, and it is a “new” way to have a war between countries, as well as other groups.

There are many types of DDoS attacks that can be launched. Often, when we are talking about DDoS attacks, we mean attacks on the TCP/IP protocol.

The rivalry of the hackers leads to more attacks.

The intruder community is loosely organized when it comes to development of attack tools. There are parallels to draw with open system development, because there are many developers and a large, reusable code base.

Conclusions

The two links mentioned in the introduction were misleading in the way that the Distributed intruder tools report (http://www.cert.org/reports/dsit_workshop.pdf) had no information at all about Mixter and Randomizer. The paper was written before the February 2000 attacks against the big Web sites (Yahoo etc.,). The other article (http://www.robertgraham.com/op-ed/magic-ddos.html) was one of the sources used for the memo *(KEB&SS)MixterAndRandomizer040308*. We read this one more time, and our conclusion is like last time; no direct information about the Mixter and Randomizer case.

A good site for information on DDoS, is the University of Washington hosted Distributed Denial of Service (DDoS) Attacks/tools site (http://staff.washington.edu/dittrich/misc/ddos/). This site has a good archive of articles and other DDoS material. We believe that this site could lead to more useful information, but we have not yet examined the site.

Signature

Kjetil E Braathen, Silje Salte

References

Gaudin, S. (2004). Hacker War Keeps the Worms Coming. Datamation.

Sigmond, S. and V. Kaura (2001). "DDoS Attacks: Precursor to Digital Terrorism." Siliconindia Vol. 5(11): 3 p.

Unknown (1999). Results of the Distributed-Systems Intruder Tools Workshop. Distributed-Systems Intruder Tools Workshop, Pittsburgh, Pennsylvania (November 2-4, 1999), CERT Coordination Center.

Unknown (2003). 2003 CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

Vaughan-Nichols, S. J. (2004). Understanding and Preventing DDoS Attacks. Datamation.

Sources searched

Cert Coordination Center (www.cert.org)
The Library, Agder University College (www.hia.no/hiabib) (EBSCO: “academic search elite”, ”business source premier”, ”regional business news”, and ”business source elite”)

www.google.com
www.yahoo.com

This memo

http://staff.washington.edu/dittrich/misc/ddos/

http://www.robertgraham.com/op-ed/magic-ddos.html

http://www.wired.com/news/technology/0,1282,43697,00.html