Network Security: Important Issues

H.S. Venter and J.H.P. Eloff
Department of Computer Science, Rand Afrikaans University

In current times, sending confidential data over the Internet is becoming more commonplace every day. Some people and organizations, e.g. commercial banks, are completely dependent on electronic transmission of confidential data. Computer networks are the transport medium for these electronic data transmissions. Hackers mostly target networks as their primary point of infiltration, whether it is internal or external from a private network. What should one know about the security of networks these days? How should security be implemented to safeguard a network? How should security be managed? This article will address the above questions and will give an idea of where we stand with network security in current times.

Introduction

A paradigm shift has taken place in the commercial sectors of most first-world countries during the past decade. With the advent of the Internet, most organizations are rethinking their business strategies to exploit the biggest single quantum leap in technology for many years. In the race to find new competitive advantages, some important issues are, however, slipping through the proverbial cracks. One such issue is Internet security. Internet security, however, directly relates to the subject of network security.

The aim of this article is to elaborate on network security, whilst giving an idea of what the important issues of network security are in this new millennium. In addition, the article will evolve around the following important issues.

- *Network security awareness*. It is a very important issue to be aware of network security. Organizations that are connected to the Internet must provide employees with the necessary training and information so that the employees can understand the need for network security.
- *Network security policy*. A network security policy acts as a mechanism that not only is a legal document that stipulates the do's and don'ts concerning the network security in an organization, but also promotes the network security awareness issue. A network security policy differs from a general information security policy in the sense that a network security policy contains more technical support detail than a general information security policy so that anyone throughout the organization would be able to apply the network security policy in a practical fashion.
- *Insider threats*. So many times organizations implement robust network security measures to safeguard their networks from threats outside of their organizational domains, but they completely neglect to implement measures to minimize network security violations from within their own organizational domains. Individuals within the organizational domain often cause the greatest network security violations.
- *Hackers are out there!* Hackers do not always need to use highly sophisticated tools to hack into a network domain. Hackers often use their skills simply by exploiting weak spots or backdoors in network security applications to gain access to resources in an organization's network.
- *Network security administrators*. Managing the security of a network can often be a very comprehensive and complex task, especially in large organizations. In the latter case, a general system administrator may not be able to cope with normal administrative tasks and manage the security of the organization's network as well. Appointing a dedicated network security administrator will not only ease the job of the general system administrator, but he will also be able to focus directly on the network security in the organization with competent network security management as a result.
- *Network security health checking*. Network security can be compared to a person that suffers from a chronic illness. In the same way that such a patient has to regularly undertake medical check-ups at a medical doctor to determine if his/her current health status is still in a satisfactory condition, the network security must undergo regular software 'check-ups' to determine if the current 'health state' of the network security is still in a satisfactory condition. Such network security health checking procedures are carried out with security-monitoring tools that can be used to determine if the 'health condition' of the network security could possibly be 'infected' by the infiltration of hackers and malicious software. Some network security software exists that even acts like an antidote by preventing software infiltrations or even acts like a serum by 'curing' the network security if an infiltration has been detected. Examples of such tools are discussed later in this article.
- *Implementation of the network information security services*. These services form the building blocks of a competent network security implementation. When performing secure transactions over a network, these services can be seen as a protocol for applying security to the transaction.

The remainder of this article will be devoted to a discussion around some of the important issues mentioned above. Network security services will be elaborated on and one particular service will be discussed in more detail. A discussion will then follow on hackers and the tools they

use as well as the tools used against them. The article will conclude with a graphical representation of how various network-security tool categories can be mapped onto the network information security services.

Network Security Services

In order to effectively audit and assess the network security needs of an organization, some systematic way of defining the security requirements is needed. In addition, the approaches to be followed in order to satisfy these requirements must be identified. One such approach is to consider the network security *services*.

The concept 'network security' does not only cover the safeguarding of electronic data in transit. It also involves the safeguarding of *any* information or data transmitted over a network [GOOT 98]. For any organization, the network security objective is achieved with the incorporation of the following services [ITCO 97]:

- Identification and authentication (Access control): Ensuring that the origin of information can be correctly identified over a network, with the necessary assurance that the identity is not false.
- Authorization: Making information available over a network only to those who have a right to access it.
- Confidentiality: Making sure that information sent across a network can only be accessed/opened by those for whom the information is intended.
- Integrity: Ensuring that information be protected against unauthorized modification whilst in transit.
- Availability: Ensuring that information be made available and accessible over a network if and when required.
- Non-repudiation: Ensuring that neither the sender nor the receiver of the information is able to deny the transmission over the network.

What, then, is a service? A *service* enhances the security of networks and information systems. A detailed discussion on these services can be found in [VSEL 00]. There is, however, still another revolutionary service that originates as a result of modern networks and state-of-the-art network security referred to as 'network security health checking'.

- Health checking: Ensuring that security-enabling technologies, such as firewalls and security software, are frequently checked for their competence by means of network-monitoring and security-auditing and assessment tools. These tools use certain *health-checking* techniques that probe the network or try to penetrate the network's current security-enabling technologies and services by compromising the network security in an ethical manner in a bid to identify weak spots in the network's security structure. If such weak spots could be identified by means of *health checking*, it is reported to the responsible people and/or processes in order to 'patch' or correct the security weak spot.

Health checking relates closely to *ethical hacking*. The difference between ethical hacking and health checking, however, is that ethical hacking is a *manual* process supported by tools that is carried out by an *ethical hacker*, which is a person that is normally hired to audit and assess the state of security in an organization [HARI 99]. Ethical hacking, thus, is a subset of health checking. Health checking does not only include the tasks of an ethical hacker, but it also includes *automatic* processes to audit and assess network security at appropriate time intervals. Therefore it is important to realize that health checking has become an integral part of network security management and is a part of the day-to-day operational network activities. It is for this reason that health checking is identified as a service, particularly in the field of network security.

These are the services identified to audit and assess network security. Now that the security services have been identified, how and where do they fit into the network security framework? Hackers can attack these services, but how do they go about it doing so? What tools can be used as countermeasures to minimize the onslaughts of hackers? The answers to these questions will be answered in the next two sections.

Hacking

Hackers do not always have privy to exceptional digital tools in order to break into important systems. They often target the workforce in the hope to find gullible employees. Untrained employees do not realize that they could become targets for hackers just because of the data to which they have access. Some of the ways in which these hackers go about hacking are as follows:

- They look for weaknesses in security policies.
- They look for signs of slack physical security, for example, switching network cables in a hub that has not been physically locked by a network administrator.
- They launch advanced network-analysis tools (for example, SATAN (Security Analysis Tool for Analysing Networks) [SATA 95]) on the network in an attempt to intercept the passwords that would enable them to gain access to private sections of networks.

Training employees against the onslaughts of hackers often takes up too much time and effort. An organization could have the most extensive and well-defined network security policy, but if it is not followed or implemented, it means nothing! Network security policies can often be huge documents — very few employees actually read them. There is no guarantee that all employees in an organization read and practice their network security policy. One approach that proved to be a relatively successful solution the past few years around this problem, is the use of anti-hacking tools. These tools provide many ways that network administrators can use to prevent hackers from gaining unauthorized access to an organization's network and resources. Examples of such tools are briefly discussed in the following section.

Hacking and Anti-Hacking Tools

Hackers use various kinds of tools to infiltrate organizations' networks and data. The realm of such tools involves the exploitation of weak spots and 'backdoors' in network-security systems. In addition, the realm of such tools has become two-fold. Hackers use such tools to infiltrate a network in an unethical manner while network security administrators use such tools ethically to try and hack into their own networks to identify weak spots in the network security structure. In some cases, however, some of the tools tend to be used more specifically by either the hackers or the network security administrators.

Hacking and anti-hacking tools can be categorized into network monitoring, sniffing, network analysis, scanning, anti-scanning and password cracking applications. Examples of such applications for each category will be discussed later in this section. The various categories of these hacking and anti-hacking tools are placed into perspective in Figure 1. There are many such applications available on the Internet. A number of these applications and software tools are discussed in [VENT 98]. Another comprehensive reference of such tools can be found on the Internet at [USSR 00].

Figure 1 illustrates two concepts. It divides hacking and anti-hacking tools into various categories as already mentioned. Each of these categories will be discussed in the following paragraphs. Figure 1 also gives an indication on the usage of the various categories of tools by hackers, users and network security administrators.

The next few sections will elaborate on specific hacking and anti-hacking tools found in the five tool categories listed in Figure 1. The reason why these specific tools were chosen as examples arises from the fact that most of these tools are widely available on the Internet either on a free trial basis for a certain period or as public domain software. The number of such tools that can be found on the Internet is, in fact, plentiful. Another reason why these specific tools are discussed was encouraged by their popularity under most network security administrators.

Monitoring and intrusion detection tools

Network *monitoring* can also be referred to as network *intrusion detection*. To monitor a network means to use certain tools to watch and capture the status of the network. Intrusion detection, in the same sense, means to monitor the network to find out when some irregularities in the network behaviour are occurring. Network monitoring tools are often combined with network scanning. Examples of network monitoring/intrusion detection tools are:

- RealSecure Internet Security Scanner (ISS) [REAL 00]: ISS is an automated, real-time intrusion detection and response system which unobtrusively analyzes activity in two-fold, namely across networks and computer systems. When monitoring networks, ISS monitors traffic on the LAN that ISS resides on as well as the traffic designated for the computer that ISS resides on. In addition, it provides the earliest possible warning of unauthorized activity here and can often terminate the attack before damage is done. When monitoring computer systems, ISS provides a complementary view of unauthorized activity by monitoring data that resides on the computer. In this way ISS can tell you whether an intrusion was successful and can provide some indication of intruder activity on the specific computer. ISS is also a scanner tool (refer to network scanner tools).
- NTManage [USSR 00]: NTManage is a Microsoft Windows NT management tool that can, amongst other NT management tasks, monitor TCP/IP-based services for hacker activity.

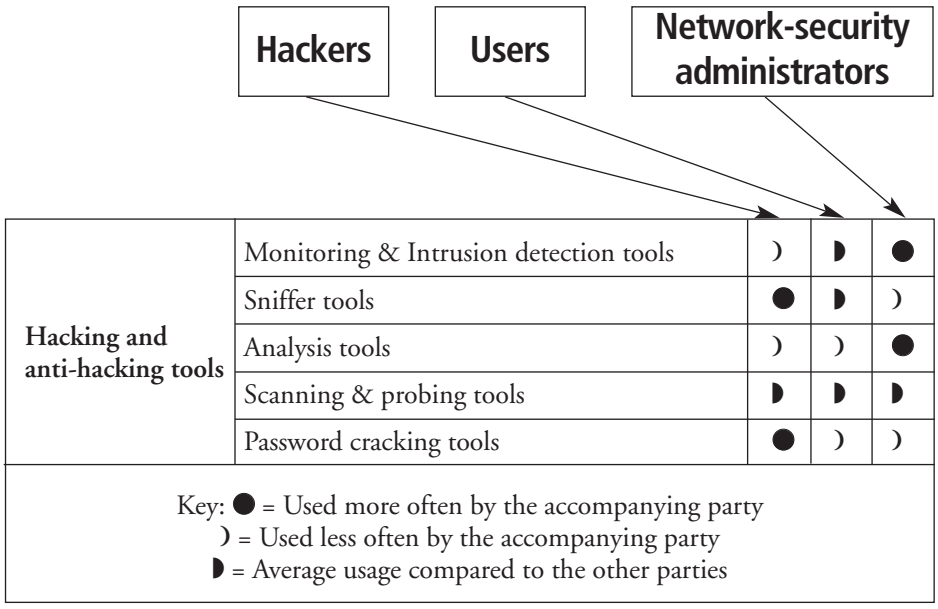

Figure 1: Specifying categories for network security tools and their usage frequency.

Sniffer tools

Network sniffing tools are used to intercept network traffic (TCP/IP packets) to retrieve either the content (for example a password) of a TCP/IP packet or information about the TCP/IP packet that may benefit a hacker. Examples are:

- Sniffer Pro (Windows NT/98/95-based) [SNIF 99].
- Fergie (DOS-based) [USSR 00].
- Gobbler (DOS-based) [USSR 00].
- NetXray (Windows NT-based) [USSR 00].

Analysis tools

Network *analysis* tools are used to perform network security assessment and auditing tasks. In doing so, they enable

the network security administrator to identify weak spots, 'back doors' and other network security vulnerabilities. Examples of such tools are:

- Kane Security Analyst (Windows NT-based) [USSR 00]: Some of the most common tasks that the Kane Security Analyst performs are to assess password strength on a Windows NT machine. In addition, it gives and assesses account policy information about every Windows NT machine on the network. It also has a very good reporting facility.
- SAFEsuite [USSR 00]: SAFEsuite is a network assessment tool that helps to close the security gap between security policy and security practice by providing the necessary visibility into network security vulnerabilities.

Scanning and probing tools

Network scanning tools can also be referred to as network probing tools. Network scanning tools scan the network and computers connected to the network for known vulnerabilities. Anti-scanner tools can also be referred to as intrusion detection tools. Anti-scanner tools prevent normal scanners from scanning the system where the anti-scanner tool is running. Some anti-scanner tools often have the ability to not only block a scanner tool, but to also disable ('crash') the scanner tool on the remote system where the scanner tool is running. Here are examples of scanner tools:

- RealSecure Internet Security Scanner (ISS) (Windows NT-based) [REAL 00].
- System Administrator Tool for Analyzing Networks (SATAN) (Unix/Linux/Solaris-based) [USSR 00].

Following are examples of anti-scanner tools:

- COPS (Unix/Linux/Solaris-based) [USSR 00].
- Tripwire (Unix/Linux/Solaris-based) [USSR 00].

COPS and Tripwire are actually intrusion detection tools, but these two tools are excellent at detecting when some unauthorized scanning tool is trying to scan your machine.

Password cracking tools

Password cracking tools are used in attempt to reveal (crack) passwords that reside in various locations on a computer. Some password cracking tools can even attempt to steal passwords from authorization attempts across the network. The latter tools are used for hacking purposes only. Most password-cracking tools can be configured to only guess for certain types of passwords, for example, the tool can be configured to guess passwords that only contain numbers. Following are examples of password cracking tools:

- L0pht Crack [LOPH 00].
- Crack [USSR 00].
- cracklib [USSR 00].
- OPIE [USSR 00].
- Passwd+ [USSR 00].

In the next section, a mapping of the above mentioned tool categories onto the network security services is drawn up in terms of how the tool categories 'attack' or 'protect' the network security services.

Mapping of Tools onto the Services

It is important to grasp the relationship between network security tools and network security services in order to understand why network security has become an issue that can no longer be overlooked. In short, this relationship is best explained by mapping the network security tools onto the network security services. The network security tools, as divided into various categories in the previous section, are mapped and compared to each network security service by indicating the intensity of how these network security tools (from a hacker's viewpoint) attack or (from a network security administrator's viewpoint) support the network security services. Figures 2 and 3

Tools *attacking* services from a *hacking* point of view…						
Various categories for network-security tools \ **Network-security Services**	Identification & Authentication	Authorisation	Confidentiality	Integrity	Availability	Health checking
Monitoring & Intrusion detection tools					●	
Sniffer tools	●		●	●		
Analysis tools		●	●		●	●
Scanning & probing tools	●	●	●		●	
Password cracking tools	●	●	●	●		

Figure 2: Mapping of various network security categories onto the network security services from a hacker's viewpoint.

Tools *supporting* services from an *anti-hacking* point of view…						
Generic categories for network-security tools \ **Network-security Services**	Identification & Authentication	Authorisation	Confidentiality	Integrity	Availability	Health checking
Monitoring & Intrusion detection tools	●	●	●	●	●	●
Sniffer tools	●	●	●	●	●	●
Analysis tools		●	●	●	●	●
Scanning & probing tools	●	●	●		●	●
Password cracking tools	●	●	●	●		●

Figure 3: Mapping of various network security categories onto the network security services from a network security administrator's viewpoint.

are the mapped representations of these viewpoints respectively.

Figures 2 and 3 are general mappings of the network security tool categories onto the network security services and, thus, stress the fact of how important it is to start considering network security in a very serious light.

Except from the awareness factor that it stresses, what does it really tell us? The mapping onto the first five services really is but an opinion from the author. Other network security administrators may have different opinions on some of the mappings given in Figures 2 and 3. It is the mapping of the tools onto the *health checking* service, however, that is of significant value. When comparing the two columns of the health checking service from the hacking and the anti-hacking viewpoints respectively, it is clear that hackers really do not use these tools to perform network security health-checking exercises as their main goal. Look at the *Monitoring & intrusion detection tools* line in Figure 2. This line denotes that hackers very seldom use monitoring and intrusion detection tools to aid them in their hacking process. The only time such tools may be used in this case is for an attack on availability by using, for example, Internet Security Scanner (ISS) to scan (in an unauthorized manner) whether a targeted machine is online and available for attack.

Network security administrators (anti-hackers), on the other hand, use such tools primarily to perform network security health-checking exercises and that should be the main message when looking at the health-checking columns of Figures 2 and 3. It is also clear from these two figures that the specific tools discussed in this article are used more frequently by network security administrators rather than hackers. These tools are, thus, primarily designed for network security administrators to perform health-checking on their networks.

Be that as it may, researchers spend days, nights and years in the race to find better security solutions. One of the major shortcomings in network security and one of the latest research topics is that of Real-time Risk Analysis [LABU 98] [VENT 99]. A good starting-point in learning more about network security is to study existing network security applications and tools such as those mentioned in this article.

Conclusion

This article has been dedicated to a baseline discussion on the current issues in network security. All across the globe, people are sure to be discussing these very issues right now. One can also be sure that most of them agree on this: that although current network security is already being maintained at a high standard, it is still far from ideal.

Network security is an issue that must be addressed by each and every organization that endeavours securely to conduct business using computer networks and the Internet. In terms of computer networks and the Internet, network security, therefore, is tantamount to the legal officer; the 'UN' of computer networks. Without it, there will be utter chaos, rendering the Internet untenable. This would, of course, culminate in the collapse of the entire business world, as we know it, because the Internet has already become such an integral part thereof.

Be that as it may, the discussion on network security is always going to stay a current issue. It is time for *everyone* to start to consider network security as a serious issue. You *can* help. Start considering network security as a serious issue — don't ignore it, because hackers will always be there! By doing so, our world of interconnected networks could be a much safer place in cyberspace.

References

[GOOT 98] Government Office of Technology; 16 May 1998; *State of West Virginia Information Security Policy*; What is Information Security?; http://www.state.wv.us/itc/std_cvr/policies/introduction.htm.

[HARI 99] Harilal, K., 11 November 1999; "Ethical Hacking — Computer Security Audits with Impact"; i-SEC Africa '99 Conference, Johannesburg, South Africa.

[ITCO 97] Information Technology Committee, October 1997. "What is Information Security", *Managing Security of Information*; ISBN 1-887-46431-X; International Federation of Accountants; pp. 12-13.

[LABU 98] Labuschagne, L. and Eloff, J.H.P., 1998. "The Use of RtRA to Enable Dynamic Activation of Countermeasures"; *Computers & Security*, Vol. 17 No. 4, 1998, pp. 347-357.

[LOPH 00] Lopht Heavy Industries; January 2000; http://www.lopht.com.

[REAL 00] RealSecure; January 2000; http://www.realsecure.com.

[SATA 95] Farmer, D. and Venema, W., 1995. "Info about SATAN", *Security Analysis Tool for Analyzing Networks*; http://www.cs.purdue.edu/coast/satan.html.

[SNIF 99] Network Associates, 1999; Sniffer Pro; http://www.nai.com.

[USSR 00] Underground Security Systems Research, January 2000. "Library"; http://ussrback.com/files.html.

[VENT 98] Venter, H.S. and Eloff, J.H.P., 1998. "Data Packet Intercepting on the Internet: How and Why? A Closer Look at Existing Data Packet-Intercepting Tools"; *Computers & Security*, Vol. 17 No. 8, 1998, pp. 683-692.

[VENT 99] Venter, H.S., Eloff J.H.P. and Labuschagne, L., 1999; "Real-time Risk Analysis on the Internet: A Prototype"; *Published Papers and Papers*; http://adam.rau.ac.za/~je/RtRA99.zip.

[VSEL 00] Von Solms, S.H. and Eloff, J.H.P., 2000. "The 5 Pillars of Information Security"; *Information Security*, Springer & Verlag, 2000, pp. 15-30.