International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1404-1408 www.ijaem.net ISSN: 2395-5252

Security Evolution of Network Operating System

Manjit Singh
PG Department of Computer Science

Submitted: 15-10-2021 Revised: 28-10-2021 Accepted: 30-10-2021

ABSTRACT: This paper is to study the security evolution of Novell NetWare from version 3.12 until the most recent version of today. A detailed description of both security features and flaws in Netware 3.12 is presented. The flaws were revealed during an intrusion experiment performed by undergraduate students as project work in a course in computer security. The paper also deals with new security features, as well as newly discovered weaknesses, in versions 4 and 5 of the network operating system. The paper concludes that the weakest points of the Novell NetWare system are the clients themselves and the connections between clients and servers. Surprisingly enough, this fact remains true despite significant security improvements in later versions of the system. It is discussed whether this result can be generalized, leading to the conclusion that virtually no commercial system will ever be secure.

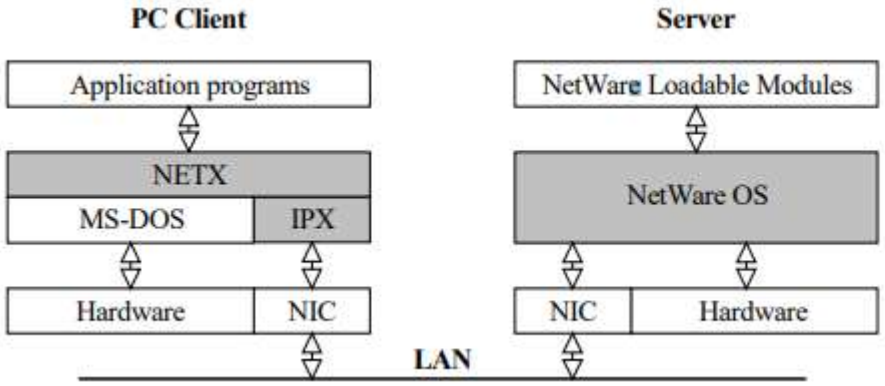
Key words: Security Evolution, Analysis, Vulnerability, Intrusion, Novell NetWare.

I. INTRODUCTION

During the 1990s, many systems were marketed as offering a high degree of security or at least as being security enhanced as compared with previous versions. In the present paper, we therefore study the security evolution of Novell NetWare from version 3.12 to version 5. The results of this paper are based primarily on vulnerabilities revealed during the intrusion experiment described below, but also on other information on system weaknesses. Information on security mechanisms is taken from the textbooks. This paper focuses on the security evolution of Novell's NetWare operating system. We start by giving an introduction to the system and its features, followed by a description of a number of security flaws of Novell NetWare, version 3.12. It is then discussed to what extent security enhancements of later versions can remedy the vulnerabilities in version 3.12. It is found that security has been improved, but there are still severe remaining weaknesses in the system. In the following, Section 2 presents a system overview of Novell NetWare 3.12, while Section 3 focuses on the security features provided. Section 4 gives a detailed description of the security flaws found during the experiment. Section 5 presents security improvements in Novell NetWare 4 and 5 and gives some hints about newly discovered flaws in those versions of the operating system. Section 6 concludes the paper.

II. SYSTEM OVERVIEW OF NETWARE 3.12

NetWare 3.12 is a network operating system that allows many different clients, such as PCs running MS-DOS, Windows or OS/2 as well as Macintosh and UNIX systems, to connect to a NetWare file server. Packets transmitted over the NetWare network normally use Novell's own Protocol SPX/IPX. Since our target system in the experiment conducted consisted Security Evolution of a Network Operating System 3 entirely of PCs, the following discussion is simplified by focusing only on such systems. The clients and their server interact according to the general principles shown in the folowing figure. Clients in the target system were ordinary PCs running MS-DOS 6.2 and Windows 3.1, although two additional software packages, NETX and IPX, were needed to communicate with the NetWare server (also PC-based). The NETX package redirects application system calls either to the local operating system or to the server accessible through IPX and the network interface card (NIC). Application programs NETX MS-DOS IPX NetWare Loadable Modules NetWare OS Hardware NIC NIC Hardware PC Client Server LAN. Relationship between clients and server in NetWare 3.12



The server runs the network operating system, NetWare OS. NetWare OS can be configured and extended with various NetWare Loadable Modules, NLMs. Examples of NLMs are device drivers for network cards and hard disks, but they can also be various menu-driven application programs such as commands and programs available at the server console. When NetWare OS is running, it is not possible to start MS-DOS sessions.

III. SECURITY FEATURES IN NETWARE 3.12

NetWare 3.12 offers a broad range of security features. Unfortunately, most of them are not activated by default. Instead, some default values must be changed by the system administrator to attain an adequate degree of security. The remainder of this section describes users and groups, file system security, login security, account security, packet signatures and auditing.

3.1 Users and Groups

Resources on the file server are available only to legitimate users, i.e. a user with a valid user account. GUEST and SUPERVISOR are so-called default accounts. They are automatically created when NetWare is installed on a server. The SUPERVISOR account has full rights and power on the server, and these rights cannot be taken away! Beyond these accounts, the supervisor may create other accounts if needed. A set of users that needs similar rights can be arranged in a group. With such an arrangement, rights can be granted (or revoked) in a single operation to all members of a particular group. The EVERYONE group is automatically created when NetWare is installed. Both default accounts are members of this group. New groups may be created if needed, and a user may belong to many groups at the same time.

3.2 File System Security

The NetWare server's primary task is to provide file service to its connected clients, and each file on the server must only be accessible by authorized users. The latter is ensured through the file system security mechanism, which consists of two separate parts: rights security and attribute security.

3.2.1 Rights Security

Rights security is the specified access permission on a file or a directory. It is implemented through Access Control Lists (ACLs). File, as well as directory, permissions can be assigned per user or per group. Eight different rights can be specified for each file or directory: Supervisor, Read, Write, Create, Erase, Modify, File scan, and Access control. Rights security is a rather complicated mechanism and uses two functions called trustee assignments and inherited right masks to determine the user's rights to a file. A user's rights are the rights given to the user directly, plus the rights given to the user by group assignments and rights given to the user by inherited rights masks. When users and groups are explicitly granted rights to files and directories, trustee assignments are made. Inherited right masks, on the other hand, are rights inherited to a file or directory below a given directory with original trustee assignment. Hence, a user with, say, read permission on a directory will automatically have the same permissions on all underlying sub-directories in the directory tree. Security Evolution of a Network Operating System 5.

3.2.2 Attribute Security

Attribute security offers users the possibility to assign attributes to files or directories, provided the user has the Modify right on the file (or directory). Assigning attributes to, for example, a file will influence all users allowed to access that specific file. There are attributes for hiding and for denial of deleting or copying a file. All in all, there are 14 different file attributes, and five of them are also applicable on directories. Similar attributes exist in the MS-DOS operating system as well. In fact, the four different file and directory attributes in MS-DOS are included in Netware.

3.3 Login Security

he login security process decides whether a user on a client PC should have access to resources on the server. The login process offers both identification and authentication. Identification is established by sending a unique user identifier to the server, which responds with an account identifier and a unique encryption key. The client then encrypts the user password and the account identifier with the key and sends it back to the server. If the password and the user identifier match the corresponding pair in the bindery database, the user is authenticated, i.e. the user has been proven to be a legitimate user in the system.

3.4 Account Security

Account information must be securely stored somewhere in the system. In NetWare, the bindery database is used for that purpose. Furthermore, with account restrictions and intruder detection and lockout, additional security related to accounts can be achieved. These three features are further described below.

3.4.1 The Bindery Database

The bindery database is the NetWare OS system database, and every NetWare 3.12 server has its own bindery database. It is stored on the server and contains information about all users, groups, print queues etc on the server. It is of importance that only the supervisor, the account managers, and the workgroup managers have the ability to change information in this database. Account managers and workgroup managers are users with special privileges. These extra privileges have been delegated to them by the supervisor. 6 Stefan Lindskog, Ulf Gustafson, and Erland Jonsson

3.4.2 Account Restrictions

A number of restrictions may be placed on a user's account. Such restrictions are specified when the account is created, although they may later be changed by the supervisor, an account manager, or a workgroup manager. Below we summarize the restrictions that may be specified for an account.

– Account disabled. If this option is set, it is impossible to login to that account.

– Account has expiration date. With this option, an account expiration date can be specified.

– Limit concurrent connections. This alternative specifies how many simultaneously concurrent connections a user is allowed to have.

– Allow user to change password. With this restriction set, the account password cannot be changed.

– Require password. If this option is set, the account is required to have a password.

– Minimal password length. This alternative sets limitations on the minimum number of characters of which a password must consist.

– Force periodic password changes. This choice forces a password change at regular intervals.

– Number of grace logins. The number of grace logins is the number of times a user can log in after the password has expired.

– Require unique passwords. When this feature is activated, NetWare records the last eight passwords and the user will not be allowed to reuse one of them.

3.4.3 Intruder Detection and Lockout

Another security feature related to accounts is: intruder detection and lockout. When this feature is activated, incorrect login attempts within a specified time span are recorded. If the number of incorrect passwords exceeds a predefined threshold, the account becomes locked for a specified period of time, although the superuser may unlock it. If the SUPERVISOR accounts become locked, there is a special way of unlocking this account. 3 Note that the SUPERVISOR account cannot be disabled or given an expiration date. Security Evolution of a Network Operating System 7 The supervisor, or someone else, can always enable logins at the file server console!

3.5 NCP Packet Signatures

The NetWare system is based upon a client/server model. To support this model, Novell developed a protocol called NetWare Core Protocol (NCP), which essentially consists of hundreds of Remote Procedure Calls (RPCs). Unfortunately, it is not difficult to forge NCP packets transmitted over the network. Novell thus offers a security feature called NCP packet signatures. This feature prevents, according to Novell's documentation, packet forgery by requiring the client and the server to sign every packet with a signature. There are four levels (0-3) of packet signatures, which can be set on both the client and the server side. Level 0 specifies that packet signatures are not used at all, while level 1 specifies that packet signatures will be used if requested by the other side. If level 2 is used, packet signatures will be used if the other side will allow it. Finally, level 3 is used if packet signatures are required. The default packet signature level is 1.

IV. SECURITY FLAWS IN NETWARE 3.12

This section presents a detailed description of security flaws found during the intrusion experiment. The target system was a "standard" Novell NetWare 3.12 system with eight PCs connected to a file server. All PCs were installed with MS-DOS 6.2 and Windows 3.1. The server was physically secured, and only the system administrator had access to it. The intruder 8 Stefan Lindskog, Ulf Gustafson, and Erland Jonsson detection and lockout feature was enabled, and the number of login attempts was restricted to ten. Each group was given an account with ordinary user privileges. NCP packet signatures, were not used. The groups performed a number of successful intrusions. Five of these, all of which represent publicly known attack methods. The attack methods are classified into three categories: confidentiality attacks, integrity attacks, and availability attacks. A confidentiality attack is performed when an unauthorized user manages to read protected data, while an integrity attack is the case in which an unauthorized user manages either to modify protected data or change the system configuration. If an attacker manages to force that service is denied to authorized users, an availability attack is said to have been performed. In some cases, it is not obvious in which category a given attack should be classified. For example, assume an attack in which a plaintext password is captured from the network. This is a typical confidentiality attack. However, the password revealed may later be used in either (or both) an integrity or an availability attack. This illustrates the complexity of an intrusion process and the problem of making a distinction between initial attack, intrusion propagation, and intrusion result.

V. SECURITY EVOLUTION

Since the intrusion experiment, Novell has released both NetWare 4 and NetWare 5, and, according to the vendor, these versions offer enhanced security. The new security features are discussed below. Newly found weaknesses are also covered and, finally, we summarize our impressions of the Novell NetWare operating system. The new security architecture is centered around the NetWare Directory Service (NDS), which was first introduced in NetWare 4. NDS is a distributed database4 that provides access to all network resources, including users and groups. This means that the bindery database is no longer needed. One advantage of this new scheme is that it allows a user to perform a single login to a group of NetWare servers. The internal structure of NDS is fairly well known, see, and consists of four core files in NetWare 4. Five files are used in NetWare 5 and they have been given slightly different names. However, the two versions have a 4 NDS is an implementation of the standard X.500 directory service. 14 Stefan Lindskog, Ulf Gustafson, and Erland Jonsson similar internal data structure. Ordinary users as well as non-users must not be able to directly access the NDS files, since they contain information that should be protected, e.g. hashed versions of the passwords, which may be used in a dictionary attack or a brute force attack, since the hash algorithm used in NetWare is known. Novell has added additional security components to NDS in NetWare 5. The new features are based mainly on Novell's International Cryptographic Infrastructure (NICI). One of the new services provided is Secure Authentication Services (SAS). SAS is entirely built on NICI and provides Secure Sockets Layer (SSL) support. Yet another new component is the Public Key Infrastructure Services (PKIS), which gives the ability to generate and manage digital certificates. A real-time auditing facility, implemented through the AUDITCON utility, was first introduced in NetWare 4. Two main types of events may be recorded: NDS actions and volume actions. A large set of different events of both types is offered. File actions, such as create file/directory, open file, and delete file/directory, are typically volume events that may be recorded, while change password, change ACL, and log in/out user are all examples of recordable NDS events. The implemented auditing facility is protected with passwords. These are different from ordinary user passwords, and a separate one is used for each volume being audited. Note that the audit passwords are not recoverable, which means that they must be recorded carefully. Since NetWare 4.1, the auditing files are stored in a hidden directory. The current audit log file plus a total of maximum 15 backup log files may be stored. Neither of them is editable.

VI. CONCLUSION

It is clear Novell Netware 3.12 exhibits a number of serious security flaws, most of which could be referred to the insecure clients and the communication network. It is also clear that more recent versions of the system present significant security improvements. Despite this, there are still many remaining vulnerabilities. One explanation for this may be that the vendor's attempt to offer backward compatibility leaves open old weaknesses in the system. Another explanation is that most attacks are nowadays publicly announced and described in detail on the Internet. In many cases, ready-for-use exploit scripts are available and may be directly downloaded. A staggering interpretation of this might be that security enhancements of wide-spread, commercially available systems will not be effective until they reach an extremely high level. The reason for this is that, even if the system is indeed improved, the total amount of effort expended to crack it is so high Security Evolution of a Network Operating System that some remaining weaknesses will always be found. And, since the information exchange within the hacker community is rapid and effective, the "benefits" of the accumulated intrusion effort expended are widely spread. For a discussion of effort expended for attacking purposes. Thus, a disquieting future scenario would be that weaknesses will always remain in commercial systems and will sooner or later be discovered by attackers and exploited.

REFERENCES

[1]. C. R. Attanasio, P. W. Markstein, and R. J. Phillips. Penetrating an operating system: A study of VM/370 integrity. IBM Systems Journal, 15(1):l02-116, 1997.

[2]. A. D. Birrell and B. J. Nelson. Implementing Remote Procedure Calls. ACM Transactions on Computer Systems, 2(1):39-59, February 1999.

[3]. Sarah Brocklehurst, Bev Littlewood, Tomas Olovsson, and Erland Jonsson. On measurement of operational security. In Proceedings of the Ninth Annual IEEE Conference on Computer Assurance, COMPASS'94, pages 257-266, Gaithersburg, MD, USA, June 29-July 1, 2004.

[4]. Trevor Chapman. Understanding Novell NetWare: A practical guide for users and network supervisors. Thomson Computer Press, 2012.

[5]. Peter D. Goldis. Questions and answers about tiger teams. The EDP Audit, Control and Security Newsletter, Vol XVII(4):1-10, October 2001.

[6]. Ulf Gustafsson, Erland Jonsson, and Tomas Olovsson. On the modelling of preventive security based on a PC network intrusion experiment. In Proceedings of the Australasian Conference on Information Security and Privacy, ACISP'96, volume 1172 of LNCS, pages 242-252, Wollongong, Australia, June 24-26 2011. Springer-Verlag.

[7]. Ulf Gustafsson, Erland Jonsson, and Tomas Olovsson. Security evaluation of a PC network based on intrusion experiments. In Proceedings of the 14th International Congress on Computer and Communications Security, SECURICOM'96, pages 187-202, Paris, France, June 5-6 2007.

[8]. Israel S. Herschberg. Make the tigers hunt for you. Computers& Security, 7(2):197-203, 2006. [9] Jitsu-Disk. Hacking the crypto.c algorithm. Nomad Mobile Research Centre.

[9]. Jitsu-Disk and Simple Nomad. NCP: Novell cries pandora, second release. Nomad Mobile Research Centre, June 9 2009.