Multiple Buffer Overflows in Kerberos Authenticated Services

Kaiser Ali Bhat

Abstract—The buffer overflows occurs when data exceeds the array bounds, causing the variable and state information to change. Since the process does not check these additional changes and thus acts incorrectly thereby places the system in an un-secure state. This paper analyses the impact and existence of such vulnerabilities in Kerberos 5 developed by MIT. This paper dictates various measures to address these problems as proposed by MIT.

Index Terms— Kerberos, vulnerability, Buffer Overflow, KDC, TGS, TGT, Patches

1 Introduction: Buffer overflow is one of the most common vulnerabilities that are used to compromise the security of the system [3]. A Buffer overflow occurs when a program does not check the size of user input for a buffer array then areas near the array are overwritten by extra data and change the values of the array. If the overwritten area contains the return address of a function, the new value will be used as the address of the next instruction after the return. An attacker can inject his code into the memory and change the return address to point to the injected code can execute this code with attacked program's privileges. The attacker can also execute the malicious code by applying the same method to function pointers as well. Therefore, the program must never accept any input that exceeds the buffer size .range checking, bounds checking and hardware segmentation may be used to prevent the buffer overflows [4].

2 Description: Kerberos is a network authentication protocol. It works on a centralized authentication server which authenticates users to servers and vice-versa. It works on the principle of symmetric encryption and shares keys with the authentication server. Kerberos maintains a database of the private keys of the clients and servers. Kerberos uses these keys to authenticate one network node to another node. Kerberos also generates temporary session keys to be shared between two communicating nodes and the communication is the encrypted with the session keys. The process of authentication takes place in the following order: [7]

(1) The user logs on the client machine; the machine encrypts the password to create client key.

(2) The client machine sends clear request to Kerberos ticket granting server (TGS).

(3)Kerberos TGS responds with a message encrypted with client key, consisting of:

(a) Client /TGS session key. This key is used for future communications between the client and TGS.

(b) TGS ID, timestamp and ticket valid time.

(c)Ticket granting ticket (TGT), which contains the client ID, client address, timestamp, ticket valid time and client/TGS session keys which are encrypted in the TGS's private keys

(4) Client requests services from TGS sending: server ID, TGT and authenticator containing client ID, client address, and timestamp all encrypted in client/TGT session key

(5) TGS responds with a message encrypted client/TGS session key containing:

a) Server ID and timestamp

(b) The client and server session key

(c) The server's ticket containing client ID, client address, server ID, timestamp, ticket valid time, client/ server session key which are encrypted with server's private key

(6) Client authenticates to server by sending server ticket and authenticator containing client ID, client address and timestamp, ticket valid time, encrypted with client/server session key

(7) Server provides the requested service to the client [14].

3 Buffer overflows in Kerberos

Kerberos is an authentication process to secure communication between clients and servers on a network. In this process, the key distribution center (KDC) issues tickets and clients must issue these tickets to communicate with each server they are trying to access on the network. Kerberos uses DCS encryption for a secure connection between client and server. Kerberos run on Unix servers and workstations. It is used to develop a secure connection between different machines for administrative purposes. Buffer overflow vulnerability exists in different implementations of Kerberos 4 and Kerberos 5. When exploiting buffer overflow vulnerability, a remote or local user can make way to force commands into the memory that executes at highest access level, thereby the malicious user gains root access to a machine. This exploitation can lead to dereferencing of a pointer and crash and thus creating a denial of service (DoS) attack. This problem may occur to misconfigured Kerberos distribution centers(KDC).the vulnerability occurs in the TGS-REQ exchange in the Kerberos protocol which limits the denial of services (DoS) to authenticated users. The vulnerability exists in Kerberos library function that is used to convert principal names to user account names. The library function fails to properly parse the requests with long principal names and an attacker can create a specifically crafted request with a long principal name to overflow the buffer. The vulnerability exists in *krb5-aname-to-localname ()* library function. If the system is configured with explicit mapping, the attacker is required to access the services with the principal name listed in the mapping list. However, if the service is configured with the rules-based mapping, the attacker is required to create an arbitrary principal name in the Kerberos realm or remote realm that can be accessed by the cross-realm authentication.

4 Impact: The four distinct vulnerabilities in various versions and implementations of the Kerberos 5 software have been reported. The purpose is to exploit these vulnerabilities to gain root privileges.

- **Buffer overflow in krd-rd-req()library function**

This kind of vulnerability is present in version 4 of Kerberos and the compatibility code version 5 which can be exploited in services using Kerberos 4 or 5 when they perform version 4 authentications. This vulnerability can also be exploited locally via the v4crp setuid program of Kerberos 5.This vulnerability can be exploited by remote users to gain root privileges on systems running services linked against the vulnerability library. There is a buffer overrun vulnerability with the “Kerberized Berkley remote shell daemon (krshd)” for at least the i386-Linux platforms[6].The true vulnerability is with krd-rd-req () function that uses krshd.This issue becomes severe when we consider using Kerberos 4 authentication ,the krshd and the krd-rd-req() function becomes active on the realm’s Key Distribution Center(KDC) server. Once the attacker breaks the KDC within a realm, the entire network gets compromised, as the attacker now controls the server which generates all the tickets and also maintains the security keys.

- **Buffer overflow in krb425-conv-principal()library function**

MIT Kerberos 5 is vulnerable to buffer overflows in the krb425-conv-principal () library function which is actually part of the Kerberos 4 compatibility code. When used in conjunction with krd-rd-req() library function, a remote attacker could exploit this buffer overflow vulnerability to gain privileges to the system [9].

- **Buffer overflow in krshd**

This vulnerability is only present in Kerberos version 5 and it is not related to previous vulnerabilities. Remote users may able to execute arbitrary code as root on systems running a vulnerable version of krshd.There is an unrelated buffer overrun in the krshd that is distributed with the MIT Kerberos 5 distributions and it has not been established whether such an exploit exists for this buffer overrun and whether this overrun is actually exploitable or not.

- **Buffer overflow in ksu**

This vulnerability is also present in Kerberos version 5 and is not related to previous vulnerabilities. This vulnerability is corrected in krb-1.1.1 and krb-1.0.7-beta1**.** Local users can gain root to privileges by exploiting the buffer overflow in ksu[8]

5 Vulnerable distribution and programs:

The Source distributions containing vulnerable code include:

- MIT Kerberos 5 releases krb5-1.0.x, krb5-1.1, krb5-1.1.1
- MIT Kerberos 4 patch 10 and earlier releases
- Kerb Net (Cygnus implementation of Kerberos 5)
- Cygnus network security(CNS—Cygnus implementation of Kerberos 4)
- Daemons or services that may call krd-rd-req() function are vulnerable to remote exploitation include:
  krshd
  klogind(if accepting Kerberos 4 authentication)
  telnetd(if accepting Kerberos 4 authentication)
  rkinitd
  kpopd
  ftpd(if accepting Kerberos 4 authentication)[8 9]

Certain Daemons that are called from inetd may be safe from exploitation if their command line invocation is modified to exclude the use of Kerberos version 4 for authentication. This approach may work for krshd(*), klogind, telnetd. The (*) krshd program is still vulnerable to remote attacks even if Kerberos 4 authentication is disabled because of unrelated buffer overrun. So, it is recommended to disable the krshd program completely until a patched version is installed [8].

The v4rcp program should have its setuid permissions removed so that it cannot be possible to perform a local exploit against it.

The krb5 ksu program should have its setuid permissions removed if it was not compiled from krb5-1.1.1 or krb5-1.0.7 beta 1.By replacing the ksu binary with one compiled from krb5-1.1.1 or krb5-1.0.7 beta-1 has to be safe provided that it is not compiled from shared libraries[8].

For MIT Kerberos 5 release, it may be not feasible to disable Kerberos 4 authentication in the ftpd program [8].

6 Solutions:

The remedy is to apply patches from the vendors. If kerberos5 distribution is running and it can rebuild the binaries from source code, then apply patches advised by MIT to correct these issues. For running the Kerberos 4, patch the source code based on the version 5 as recommended by MIT. Only the patches of krd-rd-req() need to be applied to version 4 to remove the issues described in the advisory[8]. The following patches are very critical:

appl/bsd/krshd.c

lib/krb4/r dreg.c

lib/krb5/krb/conv_princ.c

Recompile the libraries and the vulnerable programs (krshd and ksu) and also recompile the programs that have been statically linked to the vulnerable libraries. The KDC software has to be recompiled for Kerberos version 4[8].

Administration has option to disable the functionality of any configurations of explicit or rules-based mapping. The administration has to observe closely the authentication logs for requests containing long principal names [8].

By applying the recommendations of MIT, Kerberos version 4 authentications in some daemons could be disabled at run time by just supplying command line options to these programs when started by inetd. This approach may work for the daemons such as krshd, klogind, telnetd[8].

The vulnerabilities can also be addressed by upgraded version Kerberos 5 version 1.2

7 Conclusions

Kerberos is an authenticated security system developed by MIT for computer networks based on symmetric cryptography that foil intimidations such as spying and impersonations. Kerberos has seen several modifications and transitions from Kerberos version 4 to Kerberos version 5. The major threats posed to Kerberos are buffer overflow vulnerabilities. Such vulnerabilities in Kerberos 5 can be overcome by either using patches as recommended by MIT or by various vendors. We can also disable the functionality of configuration of explicit or rules-based mapping. The vulnerabilities are supposed to remove by the implementation of the upgraded version of Kerberos 5 version1.2 as proposed by MIT [8].

References:

[1] M.Bishop, D.Howard, S.Engle, S.Whalen “A Taxonomy of Buffer Overflow characteristics**”**

[2] “A Survey of Kerberos V and Public key Kerberos Security”

[3] “Buffer Overflow Vulnerabilities, Exploits and Attacks”

[4] Cruz-cunha, M.Manuela“Hand book of Research on Digital Crime, Cyberspace Security-2014”

[5] “A Learning Tool for Kerberos Authentication Architecture”Williams.comp.ncat.edu

[6] G.Dual, N.Gautam, D.Sharma, A.Arora“Replay Attack Prevention in Kerberos Authentication Protocol”IJNC Vol.5, No.2, March 2013

[7] K. Bashir, M. Khalid Khan “Modification in Kerberos Assisted Authentication in Mobile Ad-Hoc Networks to Prevent Ticket Replay Attacks”

[8]CERT Advisory CA -2000-06 Multiple Buffer Overflows in Kerberos Authenticated Services, May-June 2000

[9] “MIT Kerberos Multiple Buffer Overflow vulnerabilities”. Cisco Security Advisories and Alerts, Published June-October 2004

[10] mit krb:Multiple Buffer Overflows in krb5-aname-to-localname—GLSA 200406-21

[11]J. Holcomb “Kerberos Network Authentication Security Protocol Recent Security Vulnerabilities” February 16, 2001, SANS Institute 2000--2002

[12] CERT [5] “CA—2000-06 Multiple Buffer Overflows in Kerberos Authenticated Services.”

[13] Tzi-cker, Chiueh Fu-Hau “RAD: A Compile-Term Solution to Buffer Overflow Attacks**”** Computer Sciences Department, State University of New York at Stony Brook.

[14] Xiaohong Yuan, Yaseen Qadah, Jinsheng Xu, Huiming Yu, R. Archer. “An Animated Learning Tool for Kerberos Authentication Architecture”

[15] Aruna. S “Security in Web Services-Issues and Challenges “International Journal of Engineering Research &Technology (IJERT) Vol.5 Issue 09, September 2016

[16] M.Bishop, D.Howard, S.Engle, S.Whalen “Taxonomy of Buffer Overflow Preconditions”

[17] A. Cencini, K.Y0u, and T.Chan “Software Vulnerabilities: Full Responsible and Non-Disclosure” December 7, 2005.

[18] “Troubleshooting Kerberos Errors” Microsoft Corporation .Published March 2004