ANL/ECT/CP--85500

Conf-9505223--1

Kerberos Authentication - The Security Answer for Unsecured Networks

Douglas E. Engert
deengert@anl.gov
Argonne National Laboratory
Electronics and Computing Technologies Division

ABSTRACT

Traditional authentication schemes do not properly address the problems encountered with today's unsecured networks. Kerberos, developed by MIT, on the other hand is designed to operate in an open unsecured network, yet provide good authentication and security including encrypted session traffic. Basic Kerberos principles as well as experiences of the ESnet Authentication Pilot Project with Cross Realm. Authentication between four National Laboratories will also be described.

KERBEROS BASICS

Kerberos is a system to provide mutual authentication between clients and servers over an unsecured network. Traditionally, a server would authenticate a client by requiring a password from the client; the client would not authenticate the server. This password would normally be in clear text. With Kerberos, no passwords are sent across the network, and the server is assured that it is communicating with the legitimate client, and the client is assured it is communicating with the legitimate server. The client is usually a person, while the server is usually a daemon process on a machine.

The mutual authentication is accomplished by having a third party that both the server and the client trust. This is usually referred to as the Key Distribution Center (KDC),

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Argonne National Laboratory
Electronics and Computing Technologies Division
Operated by The University of Chicago for the U.S. Department of Energy
under Contract W-31-109-Eng-38

and is sometimes referred to as Kerberos. The KDC can issue a ticket to the client which is usable only at the server. The client then presents this ticket to the server. The server may then present back to the client additional information to prove it is the legitimate server.

Much care is taken to encrypt the transmission of the tickets between the KDC and clients, and the clients and servers. Note that the server and KDC do not directly communicate, but the server can verify that the ticket was generated by the KDC for use by the specific client, and that the ticket has not been tampered with. Kerberos normally uses DES encryption. DES is an encryption standard which uses the same key for both encryption and decryption. Each client and server has its own key which are registered with the KDC. The key is the common secret which is shared by the client and KDC, and by the server and KDC which allows the mutual authentication to work. These keys are used to encrypt the tickets. Additional keys, called session keys, are also used which are generated by the KDC and included with the tickets for use by the client and server to provide for encrypted session traffic, among other things.

Clients and servers are referred to by the KDC as principals. A principal consists of three parts: name, instance and realm. This is written as name.instance@realm or name/instance@realm. The realm consists of all the clients and servers which are served by a KDC. In our case at Argonne, it is ANL.GOV.. There is one KDC, and its backups, which servers the entire Laboratory. For a user, the instance is normally null, so a user would have a principal of the form user@realm. For servers, there are normally multiple instances of these, with one on each machine. The telnet and Berkeley "r" commands such as rlogin use the name of rcmd or host, and the instance is the hostname of the machine. For example I, as a user, would have a principal name of dengert@ANL.GOV, and if I wanted to logon to a machine called stafford.ctd.anl.gov, the servers principal name would be rcmd.stafford@ANL.GOV or host/stafford.ctd.anl.gov@ANL.GOV. The ANL.GOV KDC would have both of these principals in its database.

WHY USE KERBEROS

Kerberos was designed to operate in an unsecured network environment, the same type of environment most of us operate in today. It was designed to allow the user to authenticate once to a network authentication service, and thus avoid having to authenticate to every server. This single network login actually makes it simpler for the user. The effects of a sniffer attack would be greatly reduced if Kerberos authentication was widely used, since when properly used, passwords are never sent over the network in clear text.

KERBEROS IS NOT ALWAYS KERBEROS

Just as there are many "UNIX" like operating systems, each with its own peculiarities, there are many "Kerberos" like products available, some of which can interoperate together.

There are two versions of Kerberos currently available, Kerberos Version 4 which is very stable and has been available for a few years but has some problems, and Version 5 which is still under development which has many improvements. Kerberos is not limited to UNIX operating systems. Kerberos Version 4 is available for VAX/VMS from TGV Inc. and clients are available for the Mac and PC with Windows for both versions. All of these interoperate with the UNIX versions.

There are some major improvements in Version 5 over Version 4, including the change to the definition of a server principal to include the fully qualified hostname. In the previous section the references to two versions of the server's principal names were listed for both Version 4 and Version 5. Ticket forwarding is supported, as well as better cross realm authentication.

Many people are working on Kerberos, and there are a number of sources of information. These include the Kerberos mailing list kerberos@mit.edu, and the usenet newsgroup: comp.protocols.kerberos. A Frequently Asked Questions FAQ is maintained, and a copy may be obtained via anonymous FTP from, among other places, rtfm.mit.edu:/pub/usnet/news.answers/kerberos-faq/user.

The source code for both Kerberos Version 4 and Version 5 is available from MIT via anonymous FTP from athena-dist.mit.edu. This is development quality code. There is a cleaned-up version of Kerberos Version 4 available from Cygnus Support at ftp.cygnus.com. Cygnus Support also sells Kerberos products and software consulting. OpenVision Technologies Inc. and CyberSAFE Corporation also sell Kerberos for many platforms. See the FAQ for address of these suppliers.

The Andrew File System (AFS) from Transarc Corp., uses Kerberos Version 4 for its security and it can interoperate with the MIT Kerberos Version 4. This is what we are doing at Argonne. The KDC function is provided by the AFS Kaserver, and the clients and servers such as rlogin and rlogind are compiled from the MIT source.

The Open Software Foundation's OSF/DCE use Kerberos Version 5 for its authentication. At the present time, the MIT versions of Kerberos do not interoperate with the OSF/DCE version. We would like to see this in the future, as it has great promises. OSF/DCE is available from most of the major computer vendors, including DEC, HP, IBM, SUN, and is available for PC/Windows from Gradient Technologies. One of the major deficiencies currently in OSF/DCE is the lack of Kerberoized versions of the fundamental distributed computing components: Telnet, FTP, and other traditional communications packages.

There are many other interoperability issues which are not covered here.

NATIONAL BUT NOT INTERNATIONAL

Kerberos can use a number of encryption methods, including DES which are considered munitions and are not exportable from this country without government approval. There are a number of systems which use Kerberos for authentication only, which have received the proper clearances. There is also a version of Kerberos called "Bones" that has all references to encryption stripped out of the source code which is exportable. One then only needs to add the encryption back in. At the same time, the DES algorithm is published, and books which contain it are exportable. There are versions of the DES libraries available on foreign servers.

This situation has kept many of the major software vendors from implementing Kerberos in their products. Many of them, considering their international markets, don't want to have to add Kerberos to their products if they can not offer it to all their customers. The cost of the paper work for having two versions is just too great.

We are starting to see this situation come back to haunt us with security within the U.S. One of the projects within ESnet wants to use Kerberos Version 5 as its prime authentication method, but also has many international collaborators. They are currently looking at what their options are for these people. It may turn out that the security of the whole system is much weaker, since the international collaborators will have to use some inferior authentication method and can not encrypt their communications.

ESNET CROSS REALM AUTHENTICATION

In mid-1993, the DOE Office of Energy Research funded four ESnet sites, Argonne National Laboratory (ANL), Lawrence Livermore National Laboratory (LLNL), the National Energy Research Supercomputer Center (NERSC) and Pacific Northwest Laboratory (PNL) to begin implementing and evaluating authenticated ESnet services using the advanced Kerberos Version 5. Cross realm authentication was first demonstrated in March 1994 using the Kerberos Version 5 Beta 3 with local modifications. Since then Kerberos Version 5, Beta 4, Releases 0, 1 and 2 have been used for the testing.

The findings of this project are available in:

> Johnson, G. R., C. L. Athey, D. E. Engert, J. P. Moore, and J. E. Ramus. 1995. "Final Report and Recommendations of the ESnet Authentication Pilot Project". PNL-10382, Pacific Northwest Laboratory, Richland, Washington 99352.

This may be obtained over Internet via anonymous FTP at: ftp.es.net:pub/esnet-doc/auth-and-security/auth-pilot-report.ps, or via the World wide web at http://www.es.net/pub/esnet-doc/auth-and-security/auth-pilot-report.ps.

A particular important modification called "Configurable Authentication Paths" was developed by the project. Without this modification, the names of realms wishing to participate in cross realm authentication were defined to be of a hierarchical nature. This hierarchy was used to define the authentication path, i.e., the list of intermediate realms which participate in the authentication process. With the modification, this dependence of the authentication path on the realm name is removed. This allows for rational choice of realm names, and gives groups of organizations the flexibility to define the authentication paths to be used, thus making cross realm authentication practical.

Cross realm authentication allows for the use of a universal user identification "user@realm". This user identification can be used for authorization in the .k5login file, and in AFS access control lists. The use of Kerberos Version 5 to obtain AFS tokens based on forwarded credentials across realms was developed.

Cross realm authentication also introduces some new problems in the areas of key management, auditing, logging and compromised passwords.

The key management problems arise from having to keep two keys in sync in two realms, each maintained by its own system administrator. They must work together to change the key at the same time, while not disclosing what the key is to other parties. Since these keys protect the whole realm, care must be used to exchange them.

Each realm does its own logging and auditing. When cross realm authentication is used, the local realm only logs the initial forwarded ticket request. How this forwarded ticket is used, is not reported back to the local realm. This makes it difficult to track hacker activity, since the logs of the separate realms must be combined manually.

If a password is compromised, the local realm's administrator can take steps to invalidate the users entry so no new tickets can be issued; but remote realms are not notified of the situation, and may continue to use a ticket from the local realm which should be invalidated.

Cross realm authentication between multiple organizations introduces new administrative problems based on varying requirements for security by the different organizations. Cross realm authentication can actually weaken security at some sites. Traditionally when an outside user needed access to a site, he would be assigned a userid and password for the site, and would have to abide by any of the site's security regulations which might include the use of smart cards, and/or firewall access points. With cross realm authentication, the user's authentication is determined by the user's realm which may not meet the requirements of the other organization. Before cross realm authentication is used, the organizations need to agree on these issues.

The Kerberos Version 5, Beta 4, Release 2, which was the latest release from MIT as of the writing of the project report, had some missing components many of which have now been addressed in Release 3. Ongoing testing still needs to be done to ensure that all of our concerns are addressed.

CONCLUSION

The project members have concluded that, with certain conditions, Kerberos Version 5 is a suitable technology to enable ESnet researchers to freely share resources and information without compromising the integrity of their systems and data. With proper coordination among other sites, this could be extended to cover other DOE activities as well. At the present time, only Kerberos Version 5 has the robustness to do cross realm authentication. Since it is still under development, any use of it will require good programming expertise at each site.