Fermilab Strong Authentication Project

M. Kaletka, M. Crawford

Fermi National Accelerator Laboratory, PO Box 500, Batavia, IL, USA

[⋆]

Abstract

Experience shows that a major source of computer security incidents is the compromise of re-usable passwords by clear text transmission over the network, or by weakly protected storage on disk on individual systems. The strong authentication project proposes to greatly reduce the risk of such compromise by implementing an authentication system based on the Kerberos v5 protocol developed at MIT. This protocol avoids transmission or storage of passwords. A secure *portal* with non-reusable passwords will provide access between those systems where only Kerberos access is permitted (the *strengthened realm*) and those systems where other forms of access are permitted (the *untrusted realm*). A phased implementation is proposed, beginning with the Run II systems now under development.

Keywords: kerberos, authentication, security

1 Goals

An analysis of the major computer security incidents at Fermilab over the past year shows that a common root cause of incidents is the compromise of passwords by transmission in clear text over the network. Passwords in clear text are susceptible to “sniffing” by any compromised system in the network path and can be re-used to gain unauthorized access to the destination system. This is a well known and common method for hackers to gain unauthorized access.

Further, with user access to a compromised system, hackers can fairly easily gain access to crack the local password file, leading to further compromise. This aggravates the response, since it can lead to requiring all the users of the compromised system to change their passwords.

The primary goal of this project is to implement a strong authentication system that eliminates (so far as practical) the transmission of clear text re-usable passwords over the network and their storage on local systems. Secondary, but important, goals include:

- Providing a single sign-on environment for users. A single authentication should allow users to gain access to many services on many systems;
- Integrating existing accounts, especially the Kerberos v4 accounts used for AFS;
- Centralizing account maintenance, in order to reduce the account maintenance burden for system administrators and allow laboratory-wide control of authentication;
- Consistent enforcement of password policies, such as length, quality and lifetime.

2 Requirements

The strong authentication system must provide acceptable levels of improvement in authentication and access control. It must be adaptable to new computer security threats and changes in system

[⋆] Work supported by the U.S. Department of Energy under contract No. DE-AC02-76CH03000.

security requirements and new styles of computing and computing. It must be robust and stable. It must be readily deployable to universities and laboratories, including those outside the United States.

The system must include the supported Unix variants, as well as Windows NT. Support for Macintosh and Windows 95/98 systems is desirable. Embedded systems or specialized on-line systems may not be capable of participating directly. These may be accommodated by alternate access or protections methods.

The system must accommodate access by users and systems from outside the realm where strong authentication is enforced. In particular, it must accommodate strong authentication of users when the installation of special hardware or software on the users' desktops is not possible.

The system should be capable of establishing trust relationships with other institutions where compatible strong authentication systems are in place. This will allow users to have a single identity at multiple institutions. This assumes the security policies at the other institution meet our criteria.

3 Technical Overview

3.1 Implementation Model

The model divides the environment into four realms. The *strengthened realm* consists of all systems (whether on- or off-site) that require strong authentication for access from the network. These systems *must* replace all traditional means of access that use weak authentication, such as telnet, rlogin, ftp, etc, with strengthened versions. Local access (i.e. via the console or locally attached display) with weak authentication is allowed, as are means of access over the network that do not otherwise expose passwords.

The *untrusted realm* consists of those systems that do not require strong authentication and permit weak authentication and traditional means of access. These systems may expose cleartext passwords on the network. Direct connections from the strengthened to untrusted realm are allowed; connections from the untrusted to strengthened realm are not.

The *portal* provides a secure gateway between the untrusted and strengthened realms. Users authenticate between systems in the untrusted realm and the portal realm through non-reusable passwords (e.g. S/Key one-time password lists or CryptoCard password-generating hardware tokens). Other than physical possession of the one-time passwords by the user, no special hardware or software is required on the untrusted system.

Sites which implement strong authentication, and which meet certain criteria, may be included as a *trusted realm*. Trusted realms provide levels of security and authentication equivalent to our own. They use local strong authentication and trust relations (cross-authentication) to allow access without further authentication. Trusted realms are optional but desired.

3.2 Kerberos Authentication Features

The strong authentication protocol for this project is Kerberos v5. Kerberos was developed at MIT in 1987 specifically for use over insecure networks and has matured into a stable product with widespread operating system and application support. Kerberos continues to see active development, with new releases occurring about each year. Kerberos v4 is already in use at Fermilab as part of AFS and both Kerberos v4 and v5 are widely used at other laboratories and universities.

Kerberos provides mutual authentication for users as well as services running on systems, collectively known as *principals*. Each principal has a symmetric key used to encrypt and decrypt short messages exchange with a *key distribution center* (*KDC*). For a user, this key is a hash of the user's password; for a service, it is a random bit string. Knowledge of a key (equivalent to the ability to correctly decrypt messages from the KDC) authenticates the identity of a principal. The KDC holds a copy of the key for all the principals in the strengthened realm.

Tickets are obtained from the KDC to authenticate a user to a service on a system, such as telnet or ftp. A ticket contains information encrypted with the key of the service principal. The user's client presents the ticket to the service, and the ability of both to correctly decrypt the relevant parts of the ticket establishes knowledge of the correct keys and therefore authentication. A particular ticket is the *ticket-granting ticket*, which authenticates a user to the ticket-granting service of the KDC, and allows a user to obtain tickets for other services.

Tickets can be *forwardable*, *renewable*, and/or *post-dated*. Forwardable tickets can be rewritten by the KDC for use on a system other than the one they were originally obtained for. Renewable tickets can have their lifetime extended, by action of the user, beyond the default lifetime, up to an established limit. Post-dated tickets may be validated after a specified time in the future.

3.3 Portal Features

Authenticated network access to systems within the strengthened realm must only be possible through Kerberos; non-Kerberos methods of access must be replaced. The *portal* being developed at Fermilab provides the application gateway between the Kerberos strengthened realm and the non-Kerberos untrusted realm. In order to prevent disclosure of passwords on the untrusted network, non-disclosing one-time passwords must be used to authenticate to the portal. The portal will then obtain the initial set of Kerberos tickets on the user's behalf, allowing the user to work on the strengthened system *without entering the Kerberos password on an unencrypted connection*.

To work interactively on strengthened systems from the untrusted realm, a user telnets to the portal and provides non-reusable authentication. The portal obtains Kerberos tickets on the user's behalf and the Kerberos version of telnet on the portal system allows access to strengthened systems. The user may run X applications on the strengthened system or open multiple telnet sessions via the portal, but each telnet session to the portal requires a separate authentication (use of a one-time password). Ftp file "pushes" from the strengthened to the untrusted realm are allowed directly and do not involve the portal. File "pulls" use a modified ftp server that incorporates a Kerberos ftp client, allowing for "pass-through" file transfers.

3.4 System Administrator Issues

Users will find it most convenient if their own systems are in the strengthened realm, and installation of Kerberos on individuals' desktops will be encouraged and made as easy as possible. Placing a system in the strengthened realm will be a straightforward procedure. UPS install will load the required software onto the system, disabling the non-Kerberos clients and servers and replacing them with their Kerberos equivalents. A scan for unauthorized non-Kerberos services will be conducted regularly (and automatically) for systems requesting tickets in the strengthened Kerberos realm. Systems not meeting the necessary criteria will not be allowed to obtain tickets. Exceptions will be made for services that do not disclose passwords (e.g. anonymous ftp).

Kerberos manages *authentication*, establishing the identity of a user. Kerberos does not manage *authorization*, what services a user is allowed to access. The local system administrator manages authorization. By default, Unix will map a Kerberos user principal (less the local realm name) to a matching user in the local password file (i.e. the Kerberos principal *noman@FNAL.GOV* matches the local user *noman*) for login authorization. No password is recorded, however, in the local password file. In addition, if multiple principals are granted access to the same local account, or if the principal's realm name is not the local realm (i.e. a login from a trusted realm), the individual principals can be listed in a *$HOME/.k5login* file, similar to a *.rhosts* file. This technique is useful for shared group accounts, particularly root accounts.

With a desktop in the strengthened realm configured to obtain initial tickets, users enter their Kerberos password once for the initial login to their desktop. As long as the limited lifetime of the initial ticket-granting ticket doesn't expire, the clients for services such as telnet and ftp obtain tickets automatically and transparently when accessing other strengthened systems. For very long sessions, the ticket-granting ticket can be renewed before expiration, up to the maximum renewable lifetime. These lifetimes are set long (13 hours lifetime and 7 days renewable lifetime) to support both long interactive sessions and batch jobs. Once the ticket-granting ticket expires, new connections cannot be opened, but existing connections are not terminated.

4 Implementation Phases

The initial implementation phase consisted of installing a prototype KDC with a small number of principals and performing basic functionality checks of the MIT distribution software on a small number of desktops. This phase will provided "proof of concept". Preliminary investigations were done of issues for user interface, operations and maintenance, software development and hardware requirements. Portal hardware and software requirements have been investigated, including any pre-existing software implementations that can be adapted for use here.

The next phase consisted of a small pilot project with "real" end users and applications. The CDF Run II Analysis Prototype and the Computing Division build cluster were chosen. Included are about forty users, forty desktops and servers, and most of the supported operating system flavors. Software distributions for these operating systems have been built and made available via UPS, and supported for the pilot project. This phase also included acquisition and installation of KDC and portal systems similar to those expected for final production.

The limited production phase will include the remaining systems, users and applications needed for the Run II experiments. By the end of this phase, approximately 1500 systems and 1000 users will be using the strengthened realm and portal. These will include the Run II farms, new and old analysis systems, mass storage and on- and off-site desktops. Based on the needs of Fermilab, other systems may be included in the limited production phase.

The final production phase assimilates the remaining areas of Fermilab, with necessary upgrades to the KDC and portal, additional training and documentation, and incorporation of Kerberos authentication into applications where desirable or necessary.

References

1 B. Tung, "Kerberos: A Network Authentication System", Addison-Wesley, Reading MA, 1999.

2 J. Kohl & C. Neuman, "RFC1510: The Kerberos Network Authentication Service V5", `ftp://ftp.isi.edu/in-notes/rfc1510.txt`, 1993.

3 K. Hornstein, "Kerberos FAQ, v1.11", `http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html`, 1999.

4 "Kerberos: The Network Authentication Protocol", `http://web.mit.edu/kerberos/www/`, 1999.