HOB GmbH & Co. KG
Schwadermühlstr. 3
90556 Cadolzburg
Germany

Tel: +49 09103 / 715-0
Fax: +49 09103 / 715-271
E-Mail:
support@hobsoft.com
Internet: www.hobsoft.com

WhitePaper

HOBCOM and HOBLink J-Term

Single Sign-On with Kerberos and RACF PassTicket to 3270 Applications on a Mainframe

February 2009

Technology
Future
Communication

Today's IT professionals use a multitude of different systems every day. To access Windows terminal servers, to get their e-mail, or to work with web-based applications, users almost always have to enter different logon credentials each and every time. From the user's point of view, this is a less-than-satisfying situation, which not only reduces productivity, but also exposes weaknesses in the system's security. A person who has to use ten or more different passwords on a frequent basis might very well tend to write these down on post-its and stick them, for example, to the PC monitor. Also, the passwords chosen would likely be simple, easy to remember ones. In such an event, it is very difficult for the IT manager to ensure adherence to strict, minimum standards. The resulting increase in administrative effort brings with it un-necessarily increased costs.

The typical IT system environment has grown historically and is therefore very heterogeneous. In the computer center there is a Mainframe standing next to the Windows Terminal Server, a VT server still receives passwords in clear text and the Web application transmits data SSL-encrypted. This diversity of data formats and the lack of interoperability between the communicating components are reasons for the above-described heterogeneous authentication scenario. Another problem with this is that in most client-server environments, only the user, but not the server or service, has to present proof of identity. This presents a great risk in the event of, for example, Web applications that use falsified "Phishing" addresses in order to discover user passwords.

This confronts IT managers with a difficult task: on the one hand, to increase user ergonomics by deploying single sign-on systems, and, on the other hand, to increase data traffic security by using uniform cryptographic standards. "Single Sign-On" means, literally, the user needs to prove his or her identity only once, usually when logging on to the system by entering a password or via certificates (SmartCards, Tokens), and need not individually log on to access each application and service for which he or she is authorized. The subsequent access to these is automatically authenticated by the "Single Sign-On" system.

The advantages of such a system are evident:

- Resistance to requirements for longer and more secure passwords can be lowered, as users will only have to enter these once.

- The Single Sign-On mechanism provides a uniform standard for authentication, which is an important contribution to increased security.

- Productivity is raised through time-savings in the logging on process.

- Each user has only one user account. From the point of view of IT management, this is a security gain as all changes are now centrally made. When this account is deleted, e.g., in the event an employee leaves the firm, all access authorization is terminated at once.

But isn't it a disadvantage, that if a user's login information, his "identity," is either lost or stolen, then all applications and services to which this user has access are compromised, i.e., open to attack? Even without Single Sign-On, most users have the same password for their various applications and services, so the potential damage in such an event is hardly higher. A good company security policy requires the regular changing of passwords and also has a mechanism to quickly block the Single Sign-On account in the event of password loss or identity theft.

A promising approach to realizing these goals is found in Kerberos, which was developed at the Massachusetts Institute of Technology (MIT) over 20 years ago. Kerberos unifies the idea of a uniform cryptographic standard (e.g., AES) for data transfer with a standardized authentication mechanism, and not only for authentication for the system, but also for services. Microsoft has seen the potential of this protocol as a real Single Sign-On system, without any transmission of the passwords or saving of them on the terminal devices. Since MS Windows 2000 was released, Kerberos has been a component of the MS Active Directory Server and other Microsoft products.

HOB GmbH & Co. KG has added Kerberos functionality to their range of products in order to provide both IT administrators and users with products that enable them to make the move to more security and convenience. Especially the IBM Mainframe, in many firms still an important part of the IT structure, together with its 3270 applications, is, in a Kerberos environment, no longer relegated to the fringes but becomes a fully integrated member.

Different than other Single Sign-On solutions which, e.g., save passwords locally and when so desired, enter them automatically, Kerberos works with so-called tickets to permit access. The two basic kinds of ticket are the TGT (Ticket Granting Ticket), which is issued at the time of the first authentication on Kerberos, and the Service Tickets for access to services and applications.

As the protocols for requesting tickets and the ticket structure are standardized, tickets can also be requested and exchanged platform independently. This interoperability in heterogeneous networks (e.g., Windows / Unix) is an important advantage on the way to a uniform administration of all structures. Kerberos encounters yet another decisive assumption: Terminals, but also services, are to be viewed as potentially insecure and have to identify themselves against a trusted instance, the Key Distribution Center (KDC), as well as against each other (mutual authentication). Thus the user can be certain that he is entering his data into the proper Web portal and not to a faked Web site. Prerequisite to a user's requesting tickets from a Kerberos Key Distribution Center is that this KDC "knows" this user. To do this, the KDC works together with a directory service, for example, in MS Windows, this is the ActiveDirectory. The Ticket Granting Ticket (TGT) that, in place of the passwords or a certificate-based PKI, is saved for further use, enables the use of applications and services in the user's context for a specific validity period, e.g., 8 hours or until the user logs off. The Service Ticket, which is requested via the TGT for an application, has for each individual user their access authorizations and thus supports a close integration of the applications.

The deployment of Kerberos requires, depending on the complexity of the network structures, comprehensive planning and configuration. Various system environments have to be integrated. The administrative challenges begin with the assignment of differentiated authorizations in all areas and reach all the way to a cross-application user management. Software developers also have work to do: they must explicitly adapt each application to support the Kerberos protocol (Kerberization). But all these efforts result in a system with a markedly higher security standard and user-comfort.

Unfortunately, the IBM Mainframe offers no Kerberos support for popular 3270 applications such as CICS, IMS TSO and others. This means the user is forced to enter user name and password into the host mask after starting a 3270 terminal emulation. To overcome this problem, HOB has a solution: The host software HOBCOM and the 3270 terminal emulation HOBLink J-Term offer a comfortable method of integrating these applications into the Kerberos infrastructure. HOBLink J-Term is a highly performant Web-to-Host solution with a large range of functions. In addition to 3270, it supports 5250, VT525, HP700, 97801, and 9750 connections, as well as RDP access to Windows Terminal Servers. The HOB Enterprise Access component provides centralized user administration and configuration. A platform-independent Java application, HOBLink J-Term can run under Windows, Mac OS X, Linux and other operating systems.

When deployed in a Kerberos infrastructure, HOBCOM functions as a central authentication server, for example, to CICS or other applications. HOBCOM saves the authentication data (name/password or RACF PassTickets) for various applications and transfers these in the background to the applications. Via this workaround, the logon to the host applications is carried out as Single Sign-On without any further user input.

The user starts his 3270 emulation HOBLink J-Term as usual on his Windows system. HOBLink J-Term then forwards the Service Ticket to the host application HOBCOM. The encrypted Service Ticket contains all required information, such as user names (principal) or service. A host application, e.g., CICS, that is started over HOBCOM then immediately receives in the opening login mask the correct user name and password. This is done over the function “screen mask,” which enables one also to create complex procedures. If RACF is to be used, logging in via an RACF PassTicket can be done very easily. A connection of the Kerberos infrastructure with RACF definitions can be made.

Using Screen Mask, various screen content, or pieces of it, can be queried and, in correspondence with the image, specific entries triggered. Thereby, not only the characters in the screen display are inspected, the attributes are as well. Inside of one Screen Mask entry the content of several screens can be described consecutively, so that one can automate processes over several screen masks. The possibility of linking several comparison operations, or to program complex operations, ensures no false entries will be made.

Thus users working on a Mainframe can have the ease of operation and high security that a Kerberos infrastructure provides.

JL February 2009