



Leverage Active Directory with Kerberos to Eliminate HTTP Password

White Paper

PistolStar, Inc.
PO Box 1226
Amherst, NH 03031 USA

Phone: 603.547.1200
Fax: 603.546.2309
E-mail: salesteam@pistolstar.com
Website: www.pistolstar.com

© 2009 , PistolStar, Inc. All rights reserved.

Leverage Active Directory with Kerberos to Eliminate HTTP Password

Table of Contents

<i>Introduction</i>	1.0
Repeated Password Prompts: The Downside of Accessing Multiple Applications	1.1
Simplifying Authentication Without Using a Complicated Solution	1.2
<i>Kerberos Network Authentication Protocol</i>	2.0
What is Kerberos?	2.1
How Does Kerberos Work?	2.2
Benefits of Kerberos Authentication	2.3
<i>Using Kerberos in a Domino World</i>	3.0
Facilitating Single Sign-On to Domino Servers	3.1
The Solution: Single Sign-On to Domino Servers Using Kerberos	4.0
PistolStar's Password Power Plug-In for Domino SSO via Kerberos	4.1
<i>System Requirements</i>	4.1.1
<i>Deployment</i>	4.1.2
Benefits of PistolStar's Password Power Plug-In for Domino SSO Via Kerberos	4.2
Other Password Power Plug-Ins For Achieving SSO to Domino HTTP	4.3
<i>Summary</i>	5.0
<i>Appendix A – Resources</i>	6.0

1.0 Introduction

1.1 Repeated Password Prompts: The Downside of Accessing Multiple Applications

The beauty of having various business applications to execute critical tasks and communicate effectively is that they make the workday more efficient and productive. However, the ugly truth is that the efficiency and productivity gained through automation can be impacted because of security requirements, i.e. the need to authenticate every time an application is opened.

Employees in companies using IBM Lotus applications typically have numerous password prompts. Passwords are needed to access Microsoft Windows as well as Domino HTTP sessions such as Lotus Domino Web Access (“iNotes”), Sametime, Quickr (“QuickPlace”), and Domino Web applications.

As a result, the password management process for administrators becomes extremely complex. When end-users forget their passwords, administrators need to perform password resets in several places. There are also numerous sets of password quality rules that need to be reconciled. When an employee joins or leaves the organization, accounts need to be created and disabled in multiple places.

1.2 Simplifying & Securing Authentication Without Using a Complicated Solution

Frequently, companies implement an authentication solution that smoothes the process, however it is difficult to install and manage, or it compromises security rather than improving it. Companies need a strong and secure authentication method that is not only simple to execute, but allows end-users to authenticate from a browser and does not require a complicated client installation. One such method is the Kerberos network authentication protocol.

Kerberos is a sophisticated network authentication system that has been publicly available since introduced by the Massachusetts Institute of Technology (MIT) in 1989. Kerberos has become the preferred authentication mechanism in Microsoft Windows and Active Directory, making it also the most widely employed in the operating system market that Microsoft leads. Because of its openness, Kerberos can be utilized to create single sign-on network environments, allowing end-users to employ one set of credentials to access all resources, regardless of platform or operating system. Kerberos is also more secure than other authentication methods because it does not send plain text passwords over the network and instead uses encrypted tickets.

This paper will discuss the workings and benefits of Kerberos, focusing on its single sign-on capabilities, its multi-pronged security, and its ease of use. We will further look at how integrating Kerberos in an authentication solution for IBM Lotus Domino applications resolves the issue of dealing with multiple password prompts for those applications.

2.0 Kerberos Network Authentication Protocol

2.1 What is Kerberos?

Originally developed at and used by the Massachusetts Institute of Technology (MIT), Kerberos has become the foundation for authentication in Windows operating systems since Microsoft implemented it as the default authentication mechanism in Windows 2000.

According to “Kerberos: The Definitive Guide” by Jason Garman, Kerberos is “a secure, trusted third-party mutual authentication service that provides single sign-on.”¹ Kerberos is secure because it does not transmit plain-text passwords openly over the network or involve caching passwords on the end-user’s hard drive. Instead, it uses *tickets* incorporating secret key cryptography, which are sent to the designated server with the end-user’s encrypted credentials.

Kerberos is a trusted third-party service because it utilizes a centralized authentication server, such as Microsoft Active Directory, which all systems in the network inherently trust and through which all initial authentication requests are routed. “Mutual authentication” means that Kerberos not only ensures that the person using the login credentials is who they say they are, but that the server with which they are communicating is genuine. Because Kerberos enables single sign-on, once the end-user has authenticated to Kerberos when logging in to their workstation,

their credentials are transparently sent to the other network systems that they try to access.²

2.2 How Does Kerberos Work?

The centralized authentication server(s) that Kerberos utilizes are called the Key Distribution Center(s) or KDCs. Kerberos requires direct connectivity to a KDC, as it contains the database of usernames and passwords for both end-users and the Kerberos-enabled services. In Microsoft Windows, the KDC is any Microsoft Active Directory domain controller. The KDC is that trusted third-party through which all initial authentication requests are routed.

The end-user first authenticates to the KDC using an Active Directory domain account. If successful, they receive a Ticket Granting Ticket (TGT), which is cached by the local security subsystem of the end-user's workstation, typically for 8-24 hours. The TGT is used to prove the end-user's identity to the KDC when the end-user requests authentication to other services, such as Domino HTTP. The KDC validates the end-user's TGT, ensures the requested service exists within its directory, then encrypts the end-user's information and a session key in a *service ticket*.

The end-user's browser automatically transmits this ticket to the service, but they cannot actually decrypt the service ticket. Only the service and the KDC can decrypt the service ticket to get the end-user's information and the session key. The service trusts the credentials in the service ticket because it knows the ticket could only be created by the KDC and thus recognizes the end-user must have been authenticated by the KDC in order to receive the ticket. The service ticket has a limited lifetime and the receiving service can store used tickets, thus preventing replay attacks.

2.3 Benefits of Kerberos Authentication

Using encrypted tickets rather than sending passwords over the network makes Kerberos a highly secure means of authentication. In addition to safeguarding end-users' credentials, Kerberos enhances overall security and offers added convenience.

Mutually authenticating the end-user and the server allows Kerberos to prevent server attacks and malicious programs that try to impersonate the server to get the end-user's information. Also, Kerberos' ability to accurately identify end-users and servers allows programmers and administrators to provide authorization and auditing to further enhance the security of their networks.

Centralizing end-users' information in the KDC helps ease administrators' workloads, as they now only need to maintain a single username/password database. Security administrators benefit specifically because they now have only a small set of machines on which usernames and passwords are stored and can protect these machines accordingly.

Since Kerberos is deeply and seamlessly integrated with Microsoft Windows and Active Directory, it enables users on Windows 2000, XP and Vista to just logon to a Windows domain at the start of their workday. Therefore, when the end-user wants to access a server for which they use Kerberos authentication, their browser retrieves the service ticket from the KDC and sends it to the server automatically.

Kerberos is a server-side solution, therefore it does not require a client-side software installation and is less intrusive. For organizations that do not want to invest in a time-intensive and complicated installation, a Kerberos authentication system is an excellent option.

3.0 Using Kerberos in a Domino World

3.1 Facilitating Single Sign-On to Domino Servers

Organizations that are considered IBM Lotus shops typically have more than one Lotus Domino application and often have several, such as Lotus Domino Web Access ("iNotes"), Sametime, Quickr, and Domino Web applications. Having numerous Domino applications employed in an organization means administrators have to manage multiple user accounts and end-users encounter several separate password prompts. Consequently, both administrators and end-users experience loss of time and productivity. Administrators find the password management demands also place a drain on resources. Security effectiveness is diminished as end-users can have passwords that are of poor quality or strength. Also, with too many usernames and passwords to remember, end-users often either store or leave their information in unsafe places.

Because of its openness, Kerberos allows organizations to transparently establish single sign-on network environments. Administrators can completely remove the task of managing separate sets of passwords for each of the Domino servers in their organization, and end-users can enter their credentials one time and access all Domino servers and resources on the network.

Authentication to Domino through a browser is best achieved using Kerberos. It enables organizations to easily extend its single sign-on infrastructure to the Web for both internal intranet applications as well as external Internet applications. Using encrypted tickets to transmit end-users' credentials over networks ensures that end-users' information is protected, while establishing Domino as a Kerberos-enabled environment requiring sign-on only once per login session provides a richer end-user experience.

As mentioned previously, Kerberos is an excellent authentication option for organizations that seek only a server-side solution.

4.0 The Solution: Single Sign-On to Domino Servers Using Kerberos

4.1 PistolStar's Password Power Plug-In for Domino SSO via Kerberos

The Password Power Plug-In for Lotus Domino Single Sign-On (SSO) via Kerberos allows end-users connecting to Domino to achieve SSO to all Domino HTTP servers using the Kerberos authentication protocol to Microsoft Active Directory.

The end-user begins Domino single sign-on by launching a browser from their client desktop and requesting a resource from the designated Domino server. The Password Power Domino Server API (DSAPI) filter on the Domino server sends a response to the end-user's browser requesting Negotiated authentication (SPNEGO or Simple and Protected GSSAPI Negotiation Mechanism). For more information, go to: <http://en.wikipedia.org/wiki/SPNEGO>.

The browser then automatically requests a Kerberos service ticket for the Domino server from the Active Directory domain controller, which is acting as the KDC. The KDC responds with a service ticket after validating the end-user's credentials (done automatically if the user has logged in with an Active Directory domain account), looking up the server's account with the requested service name and encrypting the ticket using the service account's credentials. The service ticket replaces the use of proprietary tokens that is typically found in other Password Power products.

With the service ticket in its possession, the browser makes another request for the resource from the Domino server. The DSAPI filter parses out the service ticket and attempts to validate it. If successful, the end-user's Kerberos (Active Directory) name is extracted from the ticket. Another option for this step is to use the Kerberos name in full or in part to lookup the end-user's Person document in the Domino Directory to retrieve their full canonical Notes name.

The DSAPI filter then signals Domino that the end-user has been authenticated successfully, sending it the end-user's authenticated name. Domino thus provides the end-user with access to the requested resource, along with sending them either an LTPA session token (if Domino's Multiple Servers sessions are enabled) or assigning its own HTTP session, which is set in the end-user's browser. Single sign-on to Domino applications is then successfully achieved via Kerberos, and subsequent requests from the end-user are quickly authenticated using the session token instead of performing the full Kerberos authentication each time.

4.1.1 System Requirements

The Password Power Plug-In for Domino SSO via Kerberos supports Microsoft Windows XP and Vista client machines, Windows 2003 and 2008 Active Directory as KDC (MIT KDC not supported), and Lotus Domino R6/7/8/8.5 on Windows and AIX. Internet Explorer 5.0 or higher or Mozilla Firefox 1.5 or higher are required. End-users must log in using their Active Directory domain account. Machines on which Domino is running must be joined to the Active directory domain and Domino should run as a service.

4.1.2 Deployment

Installation of the Password Power Plug-In for Domino SSO via Kerberos is seamless and requires no changes to the Active Directory/LDAP schema. A server-side software installation (single DLL implemented as a DSAPI filter) is required on each Domino, Lotus Sametime and/or Lotus Quickr server for which browser single sign-on

functionality via Kerberos is desired. Notes.ini variables control how the Plug-In operates and any logging goes directly to the Domino server console/log.nsf. The HTTP task only needs to be restarted to put the changes into effect.

Additional client-side software (i.e. the Password Power Web SSO Plug-In) is not required as Internet Explorer and Mozilla Firefox have built-in support for Kerberos authentication to Web servers. However, some minor modifications to the browser settings may be necessary on the client machines to enable Kerberos/Negotiate (SPNEGO) authentication.

4.2 Benefits of PistolStar's Password Power Plug-In for Domino SSO Via Kerberos

The Password Power Plug-In for Domino SSO via Kerberos provides all the benefits of using the Kerberos authentication protocol described above and more:

- No plain-text passwords are sent over the network;
- End-user and server are mutually authenticated, preventing server attacks and malicious programs that try to impersonate the server to get the end-user's private information;
- Administrators remove the need to manage separate passwords for their Domino HTTP servers;
- Administrators only need to maintain a single username/password database;
- Security administrators now have only a small set of machines on which usernames and passwords are stored and can protect these machines accordingly;
- Kerberos is a server-side solution; client-side software is not required;
- The HTTP session token allows the end-user to avoid repeated or full Kerberos authentication while they are using the Domino HTTP cache, which dramatically increases the server's response time;
- Kerberos authentication enables end-users on Windows 2000, XP and Vista to just logon to a Windows domain at the start of their workday, as it provides further integration with Windows and Active Directory; and
- Overall password security is enhanced.

4.3 Other Password Power Plug-Ins For Achieving SSO to Domino HTTP

Kerberos authentication is one of three options PistolStar's Password Power offers for achieving SSO to Domino HTTP. The other options include proprietary SSO tokens (Domino SSO Plug-In) and via login to a portal such as Microsoft SharePoint (the Portal Plug-In).

The Password Power Domino Single Sign-On (SSO) Plug-In allows end-users connecting to Lotus Domino via a browser to authenticate with their network directory or LDAP password for access to all Domino Web applications as well as Microsoft Windows. The Domino SSO Plug-In also removes the need for administrators to manage separate passwords for Domino Web applications. Passwords for Microsoft Active Directory, Novell eDirectory, Sun ONE LDAP, Lotus Domino LDAP, IBM Tivoli Directory Server, and OpenLDAP can be used to achieve single sign-on access to all Domino HTTP sessions.

The Password Power Portal Plug-In allows end-users to login to an enterprise information portal such as Microsoft SharePoint or BEA WebLogic and access applications without repeated login prompts. Users achieve portal single sign-on using their Microsoft Active Directory credentials, which are used to create tokens that enable seamless access from the portal to applications and servers within, such as SAP NetWeaver, IBM WebSphere, and IBM Lotus Domino applications (Lotus Notes, Domino HTTP, Lotus Sametime and Lotus Quickr).

See PistolStar's Tech Briefs on these products for more information.

5.0 Summary

In order for employees in an organization to logon to a computer and gain access to the various applications they need to do their jobs, they need to identify, or *authenticate*, themselves. The most common method of authentication is through a password — a critical piece of information that confirms the person behind the keyboard is whom they claim to be.

With passwords, several issues emerge with respect to the users:

1. The challenge of remembering long, complex strings of letters and numbers that are frequently changing;
2. Password quality/use of easily guessed passwords; and
3. The increasing number of passwords that must be maintained as the number of applications, servers and machines grows.

Another, more important issue is that passwords could be sent over a network in clear (unencrypted) text, thus they would be readable if intercepted by others on the network, who can use the password to impersonate the password's legitimate owner.

Kerberos is a computer network authentication protocol that allows end-users in client-server environments to identify themselves more securely. Most notably, Kerberos allows end-users to reduce the number of passwords they possess and the number of logon attempts they need to make to just one. It also encrypts the end-users' identity so it is not openly sent over the network. Organizations find that Kerberos is a highly secure authentication method that delivers huge benefits for both end-users and administrators, and it contributes to improving their overall security.

Kerberos has become the most popular cross-platform, network-wide authentication system available, as it is now deeply integrated with Microsoft Windows and Active Directory. As a leading provider of password management products integrating Active Directory, PistolStar has developed a Kerberos-based solution using Active Directory as an option for customers who want a server-side product that enables them to execute single sign-on to gain access to all their Lotus Domino servers. The Password Power Plug-In for Domino SSO via Kerberos combines all the benefits of Kerberos authentication with the convenience and ease of use typically found in Password Power.

Therefore, given a choice of solutions for accomplishing Domino single sign-on and enhancing the security of their networks — one using proprietary SSO tokens, one enabling portal SSO, and one offering Kerberos authentication — IBM Lotus shops can now implement the perfect one for their organization and environment.

6.0 Appendix A

PistolStar Resources

[“Achieving Single Sign-On for Your Organization’s End-Users”](#) - PistolStar TechNote #255

[“Storage, Handling and Security of End-Users’ Passwords”](#) - PistolStar TechNote #256

[“Username Mapping with Authentication Redirection”](#) - PistolStar TechNote #257

[“The Rise of Portals in the Enterprise: Addressing the Resulting Password Challenges,”](#) PistolStar White Paper, October 2006.

[“Using Active Directory in the Domino World,”](#) PistolStar White Paper, October 2005.

[“The Realities of Single Sign-On,”](#) PistolStar White Paper, September 2005.

[“The Role of Password Management in Achieving Compliance,”](#) PistolStar White Paper, May 2005.

[“The Evolution of Password Authentication and Management: Simplifying It Without Having a Complicated Solution,”](#) PistolStar White Paper, January 2005.

[“Eliminating Notes ID File Password Management: A Ground-breaking Alternative,”](#) PistolStar White Paper, September 2004.

###

Annotations

¹ Garman, Jason. Kerberos: The Definitive Guide. First Edition. Sebastopol, CA: O'Reilly & Associates, Inc., 2003, pg. 6.

² Ibid.