# Security :: Secure Authentication - Under the Hood

There are two discrete parts to the process that enables a user to access different network services - **authentication** and **authorization**.

## Authentication

Authentication is the process of determining that users are who they say they are. One of the more popular and secure systems of authentication is Kerberos.

Created at MIT, Kerberos issues “virtual tickets” to users and systems to enable secure authentication without sending passwords to every system a user wants to access, so passwords are kept on the Kerberos server, instead of being distributed across the network. Users are only prompted to enter a password the first time they attempt to access a "Kerberized" system. At that time, a Kerberos ticket is issued, which establishes authorization. From that point on, only the ticket is passed to other cooperating systems, not the password. This means that users do not have to keep entering their HSU User Name [1] and Password every time they need to access a different system. This process is known as **Single Sign-on** and also enables users to access multiple applications, such as those provided with Google Apps [2], simply by entering their HSU User Name and Password.

## Authorization

The second function needed to enable users to access any service is to determine whether the **authenticated user** is permitted to access specific network resources. This component is referred to as **authorization**.

While Kerberos is the system of choice for authentication, the **Lightweight Directory Access Protocol (LDAP)** is the system of choice for authorization. LDAP allows systems and applications to reference database and directory information that can be used for authorization; it can also be used to provide contact information for use by email clients and web-based directories. As Kerberos can also interoperate with Active Directory (see below), this pairing is particularly useful for security and access control policy enforcement.

Because of the complexity and incompatibility of the various systems and applications that might need authentication and access control, an infrastructure has to be developed to allow these disparate systems to function as a part of the HSU campus infrastructure. The middleware infrastructure consists of numerous synchronized systems built in a high-availability environment to minimize, if not eliminate, outages and down-time. These systems consist of, but are not limited to, Kerberos, LDAP, and Windows Active Directory.

## Desktop Authentication and Active Directory

Kerberos and LDAP can be used in many contexts, such as web sites, to provide authentication and authorization. Some operating systems can be configured to directly use LDAP and/or Kerberos for desktop authentication, but most require a much richer set of information to allow users to fully access a workstation's capabilities. Additionally, every operating system needs to access information unique to that operating system. By separating desktop authentication from the other aspects of campus

authentication, the risk of large scale outages is diminished. While Mac OS X clients and other Unix/Linux operating systems can use LDAP, the quirks of each system make integration complex. Active Directory supports these operating systems "out of the box" and allows for the use of desktop management tools built into the Windows operating system.

## Related Topics

Passwords & Digital Identities [3], Security [4]

**Source URL:** http://www2.humboldt.edu/its/security-secureauthentication

**Links:**
[1] http://www2.humboldt.edu/its/glossary/5#term99
[2] http://www2.humboldt.edu/its/glossary/5#term40
[3] http://www2.humboldt.edu/its/category/quicklinks/passwords-digital-identities
[4] http://www2.humboldt.edu/its/category/quicklinks/security