When you compare their security attributes, you'll find that SSH and SSL have very strong similarities. They both offer data-in-motion encryption, server authentication, client authentication, and data integrity mechanisms.

1. SSL (superseded by the more modern [Transport Layer Security](http://en.wikipedia.org/wiki/Secure_Sockets_Layer)) is a general protocol that can be implemented on top of other transport-layer protocols such as HTTP and FTP. As such, you can use it to transfer files or view web pages securely, and there are many other applications. The best-known application for SSL is encrypting a form submission so you can send your credit card details to a retailer without fear of an eavesdropper on your network viewing your credit card number. SSL communication is not necessarily authenticated (you can encrypt your communication with a website without giving any username/password).
2. SSH is more specifically for remote login and has almost completely replaced Telnet for command-line access to remote computers. Other applications for SSH include file transfer using SCP and secure port forwarding (to provide private access to systems behind a firewall). SSH communication is generally authenticated (either with a username/password or a public/private key pair).

SSH

SSH means “Secure Shell”. It has a built-in username/password authentication system to establish a connection. It uses Port 22 to perform the negotiation or authentication process for connection. Authentication of the remote system is done by the use of public-key cryptography and if necessary, it allows the remote computer to authenticate users.

More often than not, SSH uses SSL under the hood, so they are both as secure as each other. One advantage of SSH is that using key-pair authentication is actually quite easy to do, and built right into the protocol.

SSL

SSL means “Secure Sockets Layer”. Many protocols — like HTTP, SMTP, FTP, and SSH ‘“ were adjusted to include the support of SSL. The port that it typically uses to make a connection to a secure server is 443.

Read more: [Difference Between SSH and SSL | Difference Betweenhttp://www.differencebetween.net/technology/difference-between-ssh-and-ssl/#ixzz4WUBuGi1q](http://www.differencebetween.net/technology/difference-between-ssh-and-ssl/#ixzz4WUBuGi1q)

* SSL is meant as a layer above or in an existing protocol : it provides cryptographic functions
* SSH is mainly used to connect from/to remote servers
* SSL does not require an authentication => you may browse anonymously in HTTPS sessions without giving user certificate.
* SSH requires client authentication
* If you want SSL to authenticate your users, it will work thanks to certificates exchange (can be a Public Key Infrastructure aka PKI).
* SSH can do certificates exchange but allows more way to authenticate users.

**SSL – Secure Socket Layer**

SSL is used to encrypt the communication between browser and server. SSL (HTTPS) is also called as security over HTTP.

In SSL, the communication can be authenticated via public-key/private-key pair.

**SSH – Secure Shell**

SSH is used to encrypt the communication between two computers connected over the internet.

Network Administrators are using SSH for remote login and remote control access between two computers. SSH uses port 22 for communication security.

In SSH, the communication can be authenticated either via **Public-Key/Private-Key** pair or via User-Id/Password pair.

