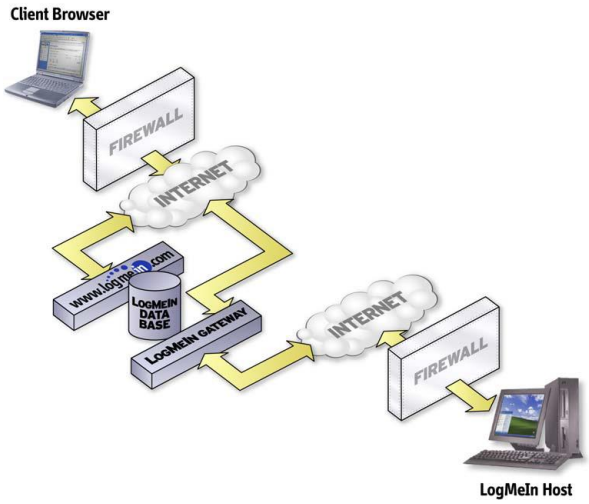
Logmein findings:

Security seems to be pretty rock-solid. Aside from being encrypted traffic all the way from the initiation of the connection between host and client and multiple SSL certificate exchanges, there are a wide variety of options that allow the user to increase security on the host machine, such IP restrictions, One-time passwords, and short-lived, single use passwords that are delivered to the user over email (page 7 of LogMeIn white paper).

General consensus of well-known and respected IT forums such as Experts Exchange seems to be that the biggest security threat to an LMI session is the user, rather than anything about the connection.

How the connection works:

There is more detail in the white paper starting on page 6, but this is a quick look at the way the connection works.



"The LogMeIn host in the illustration above maintains a constant SSL-secured connection with one of the LogMeIn gateway servers in our physically secure datacenter. This link is initiated by the host and the firewall treats it as an outgoing connection, not unlike secure web-browsing traffic.
The client browser establishes a connection to www.logmein.com and authenticates itself. The gateway then forwards the subsequent encrypted traffic between the client and the host. It is worth noting that the client will still need to authenticate itself to the host – the gateway mediates the traffic between the two entities, but it does not require that the host implicitly trust the client."

Possible security policy concerns:

Information Security manual section 402

“Direct connections to the data network are controlled and restricted to authorized personnel only by means of email credentials and a registration process for computers. All remote connections are limited to approved gateways only. All machines connected to the network are subject to the company Network Security Policy”

There is no way to set the host computer’s screen to blank when a connection is made to it by default. There is a toolbox that allows you to blank the host computer’s screen once a connection has been established, but until that has been done, if the monitor on the host computer is turned on, anybody looking at the monitor can see exactly what is going on.

According to the security information and diagrams contained in the white paper from LogMeIn, the LogMeIn Gateway strictly acts as a forwarding agent between the host and the client computer. There is no point at which any data is stored and then forwarded from one computer to the other. As long as we take LMI’s word for it, there should be no concern about data retention policies since there is no data being retained, and in fact I have not been able to locate a data retention policy.

LogMeIn installs a hidden administrator account on the host computer called LogMeInRemoteUser.

“If LogMeIn is installed on a computer that does not have a password secured Administrator account, it will ask you to create a computer Access Code. This code is actually linked to a hidden Administrator account called LogMeInRemoteUser to satisfy the above security criteria. Strength of password/access code could be an issue here and we would want to advise our users to choose a password carefully in order to avoid opening their machine up to potential brute/force or other password exploits.