GateKeeper Security Specifications

GateKeeper is a hardware based two-factor authentication and access control system for computers. Using the GateKeeper, a user can automatically lock their computer by walking away from it. To log on, the user will need to carry the GateKeeper token with them, AND enter a PIN at the lock screen. This system therefore allows the security administrator to enforce very long and complicated passwords for computer access, while maintaining the ease of access and workflow for the user.

User Information and Local Storage:

GateKeeper software requires the user to register their token (key) using their Windows credentials. These credentials are encrypted using AES-256 encryption using the AesCryptoServiceProvider class that is part of Windows SDK and is FIPS compliant. AES is specified in (FIPS 197) and approved in (SP 800-131A Rev. 1) for key lengths of 128, 192, and 256 bits. The same standard is used for encrypting web credentials for the user. These encrypted credentials are stored in a local database that is accessible only by administrators. This database is periodically synchronized with the server such that new users, credentials, and tokens may be added at any time from either the client or the server. The encryption key is unique for each computer and is stored in the registry.

Wireless Data:

GateKeeper uses Bluetooth 4 wireless standard for communications between the token (user carries this) and the USB Lock (plugged into the computer). The Bluetooth 4 standard allows the system to run on very low power and thereby increasing battery life to over 6 months. *The Bluetooth 4 communication protocol comes with AES 128 bit encryption that is part of the FIPS 140-2 encryption standard*.

The beauty of GateKeeper is that NO private information is transmitted over the air. Usernames and passwords are encrypted and stored on the GateKeeper server on the customer's network and protected by the customer's firewalls, and are **NEVER transmitted over the air**. At no time in the operation of GateKeeper is any private user transmitted between the GateKeeper Keyfob and the computer. During normal operation of the GateKeeper, the only data that gets transmitted over the air is signal strength, battery life and accelerometer response.

GateKeeper Token Authentication:

GateKeeper uses Bluetooth 4 wireless standard for communications between the token (user carries this) and the USB dongle (plugged into the computer). The Bluetooth 4 standard allows the system to run on very low power and therefore increases battery life to over 6 months.

The beauty of GateKeeper is that NO private information is transmitted over the air. Usernames and passwords are encrypted and stored on the GateKeeper server on the customer's network and protected by the customer's firewalls and are NEVER transmitted over the air. At no time in the operation of GateKeeper is any private info transmitted between the GateKeeper token and the computer. During normal operation of the GateKeeper, the only data that gets transmitted over the air is signal strength, battery life, and accelerometer response.

A read-only device firmware prevents cryptographic key readback if an attacker gains physical access to the token. The tokens only accept over-the-air firmware update when the firmware is signed by Untethered Labs – making it impossible to insert malicious firmware into a token.

In order to prevent duplication of GateKeeper tokens, a randomly generated SECRET KEY can be written to each token during the registration process. This SECRET KEY is then used to generate one-time-passcodes on the token which are advertised as part of the Bluetooth advertisement packets and scanned by the client software. These one-time-passcodes change every few seconds, and therefore prevent other Bluetooth devices from imitating a GateKeeper token.

Server Application:

The GateKeeper Hub server application is deployed on an onsite server and communicates with the client applications on networked computers over an SSL-encrypted channel. The Hub application stores user, computer, audit, and other data on a SQL database on the customer's network. All private information such as user credentials are encrypted with military-grade AES-256 encryption while stored in the database. The GateKeeper Hub server application is deployed on an onsite server and communicates with the client applications on networked computers over an SSL-encrypted channel. The Hub application stores user, computer, audit, and other data on a database on the customer's network. All private information such as user credentials are encrypted with military-grade AES-256 encryption while stored in the database.

Client-Server Communication:

By default, the client and server applications communicate using HTTPS by installing a self-signed certificate on the Hub. However, if the customer has a SSL certificate, that can be added to the server.