OpenFortress*
digital signatures

Cryptographic Rationale for LockTop™ products

This is the Cryptographic Rationale for the LockTop product line. It is intended to guide evaluation of the security level of these products.
Security solutions break at the weakest point. For this reason, this rationale states invariant properties that apply throughout the product, and any diversions of this are documented. This is essential quality management for security systems.

Risk Analysis

Good cryptographic practice dictates the use of 128 bit secrets plus the use of algorithms that exploit these bits to the fullest. Normal daily passwords do not meet this criterium, and the LockTop technology processes only 32 bits of entropy (or 'surprising bits') on the token-protecting password. In the case of token passwords this is not problematic because the tokens lock after five failed logins. Five attempts on a 32-bit secret give a cracker a chance of 5 in 2^{32}, so one out of 858 million.
In addition, the token password is part of a two-factor security scheme: To take a stab at breaking the token password, the token must be in physically possession. For this reason, the token owner must always carry the token with them, for example on their key chain.

128 bit Security

The LockTop solutions provide a security level of at least 128 bits throughout the system, with two well-known exceptions. 128 bit security means that cryptographers expect it to take on average half of 2^{128} attempts to crack a system by mere guessing.
The first exception is the token-protecting password that is regularly entered by its owner. This is explained in the risk analysis above.
The second exception is that data encryption mechanisms usually have a backup mechanism. For Linux, this is self-arranged (but PGP can provide a 128 bit strong solution). For Windows, the backup mechanism is based on certificates and long symmetric keys, which meets the 128 bit strength. For Mac OS X, the user supplies a password for their personal vault. Users of the LockTop for Mac OS X are urged to use a tool to generate a 128 bit code and use that as a backup password.

Symmetric Crypto

LockTop is based on symmetric crypto. This means that tokens that login must work from the same secret as the computer accepting the login.
For data encryption, it is common that a fixed secret is used, even if that would be encrypted under an asymmetric key pair. We use the same approach for encryption with the LockTop product series.
For desktop login, the LockTop uses a different 'password' for every session. Storing fixed login credentials on the token would be highly insecure, even if it used encryption! As soon as a token logs in properly, the next-time password is derived and stored in an irreversibly encrypted form. The operating system must protect this form from being replaced.

Token Quality

The LockTop tokens are designed for local use on the system to which it logs in. Their casing is designed to be tamper-evident, not tamper-proof. While not tampered with, the secrets contained on them are safely stored, and cannot be retrieved. These secrets can only be used in secret-masking calculations, and only after the token password has been entered.