OpenFortress*
digital signatures

Cryptografische Bijsluiter voor LockTop™ producten

Dit is de Cryptografische Bijsluiter voor de LockTop productlijn. Het is bedoeld als hulp bij de beoordeling van de veiligheidsklasse van deze producten.
Veiligheid breekt steevast op de zwakste schakel. Daarom pint deze bijsluiter invariante eigenschappen vast waarvan het hele product doortrokken is, en waar afwijkingen zijn worden die beschreven. Dit is kwaliteitsmanagement voor security-systemen.

Risicoanalyse

Naar goed cryptografisch gebruik moeten geheimen 128 bits lang zijn, en gebruikt worden met algoritmen die die lengte ten volle benutten. Alledaagse passwords komen lang niet op deze lengte, en de technologie van de LockTop verwerkt ook maar 32 bits aan entropie (of 'verrassende bits') op het token-beschermende password. In dit geval levert 32 bits geen probleem omdat het token zichzelf vergrendelt na vijf mislukte pogingen. Vijf zulke pogingen om een 32-bit geheim te kraken bieden een kraker een kans van 5 uit 2^{32}, dus één kans op 858 miljoen.
Bovendien is het token-password onderdeel van een twee-factor veiligheidsschema: Om het token-password te kraken moet het token in fysiek bezit zijn. De eigenaar van een token moet een token dus altijd bij zich dragen, bijvoorbeeld aan de sleutelbos.

128 bit Security

LockTop oplossingen zijn doortrokken van een veiligheidsniveau van tenminste 128 bits, met twee welbekende uitzonderingen. 128 bit veiligheid betekent dat cryptografen aannemen dat gemiddeld de helft van 2^{128} pogingen nodig zijn om een systeem door gissen te kraken.
De eerste uitzondering is het token-password dat regelmatig door de token-eigenaar wordt ingetikt. Dit is al uitgelegd in bovenstaande risicoanalyse.
De tweede uitzondering is dat data-encryptie doorgaans een backupmogelijkheid biedt. Onder Linux is dat zelfwerkzaamheid (waarvoor PGP gemakkelijk 128 bit veiligheid kan bieden). Voor Windows is de backup gebaseerd op certificaten en lange symmetrische sleutels, die de 128 bit veiligheid in stand houden. Voor Mac OS X tikt de gebruiker een password in voor de persoonlijke kluis. Mac OS X gebruikers wordt aangeraden daarvoor een tool te gebruiken die 128 bit passwords genereert.

Symmetrische Crypto

LockTop is gebaseerd op symmetrische crypto. Dat betekent dat inloggende tokens van dezelfde geheime codes uit moeten gaan als de plek waarop ingelogd wordt.
Voor data-encryptie is het gebruikelijk dat een vaststaand geheim gebruikt wordt, zelfs als dat onder een asymmetrisch sleutelpaar ligt opgeslagen. We gebruiken dezelfde aanpak voor encryptie met de LockTop producten.
Voor desktop login gebruikt de LockTop elke keer een ander 'password'. Een al dan niet gecodeerde toegangscode opslaan op het token zou bijzonder onveilig zijn! Zodra een token ingelogd is wordt het password voor de volgende keer herleid en opgeslagen onder eenrichtingscodering. Het operating systeem moet deze informatie beschermen tegen overschrijven.

Tokenkwaliteit

Het LockTop token is ontworpen voor lokaal gebruik op het systeem waarop het token inlogt. De behuizing is ontworpen om kraakpogingen zichtbaar te maken, niet om ze volledige uit te sluiten. Zolang de behuizing niet gekraakt is zijn de vervatte geheimen goed beveiligd. Deze geheimen kunnen alleen worden gebruikt in geheim-maskerende berekeningen, en alleen als het token-password is ingegeven.