
Using PKI for PC Security

Executive Summary

Public Key Infrastructure (PKI) is an important foundation for network and information security. In essence, PKI provides an enterprise infrastructure for managing the keys necessary to operate a variety of familiar security applications such as Virtual Private Networks and secure email. PC security products can also be integrated with PKI, although there are some unique architectural and performance issues to be considered. Properly viewed, PKI is a useful, but not the only, means of integrating existing PC security products with an enterprise security architecture.

PKI does not itself secure PCs. However, it can be used facilitate the administration of both types of PC security - file encryption or full disk encryption. Consequently the issue is not whether to use PKI, but rather to make a deliberate choice between file or disk encryption products.

Given the considerable expense required to implement PKI, it is not cost effective to implement PKI for the sole purpose of central administration of PC security. This integration should be deferred until the enterprise can spread the cost of PKI across several PKI-enabled security applications. Meanwhile, some advanced PC security products provide effective proprietary means of central administration.

PKI provides central key management for PC security products

Because PKI is proposed as a universal security architecture, it is often erroneously believed that all security problems are resolved with the introduction of PKI. While PKI certainly makes a major contribution by providing scalable, central key management for multiple security applications, there remains the considerable task of creating those applications. PC security products are attractive targets for PKI implementation precisely because it has always been difficult to assimilate PCs into the enterprise security architecture.

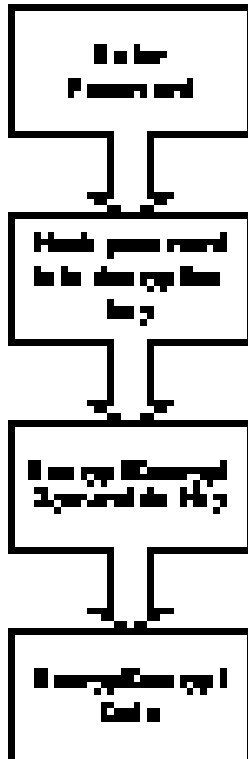
However, PKI is not the only way to centrally manage PC security. Some advanced products such as *Pointsec* have proprietary management tools that accomplish the same tasks. As the diagram below illustrates, PKI simply provides an alternative way to manage and secure the symmetric key that is actually used to encrypt or decrypt data. Symmetric keys are almost always used for bulk data encryption because they are an order of magnitude faster in operation than public-private key pairs. Since the symmetric key must be used to unlock the data, its own security is of paramount importance.

In a PKI system, the symmetric key is encrypted with the public key and decrypted by the corresponding private key when needed. For extra security, the private key can be stored in a secure device such as a smart card. While smart cards definitely enhance security, the difficulty in establishing card standards coupled with the cost and compatibility issues surrounding card readers and drivers have made this option impractical for most organizations at present. Consequently, the private key is often stored on the disk in company with the symmetric key that it decrypts.

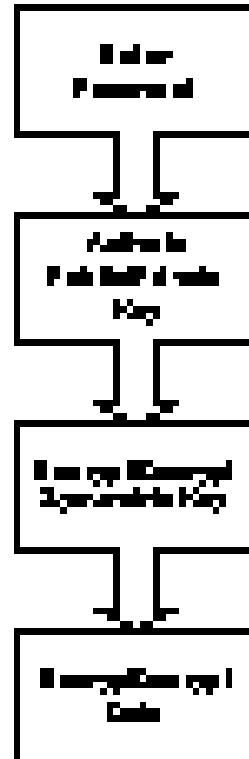
In a proprietary system, the symmetric key can be encrypted and decrypted using a one-way hash of a password known to the user. Provided the password is never stored on the PC, this is also effective security.

Both PKI and proprietary administration systems rely on a central authority to manage access to the symmetric key. Consequently, both systems lose control when the PC is not connected to the network. Even if user authorization has been revoked, the PC security software will not take appropriate action until communication with the central authority is re-established.

**Protecting the Symmetric Key
with encryption via one-way
hash of user password**



**Protecting the Symmetric Key
with encryption via PKI**



File and File Encryption products

Overview

File encryption products allow individuals in organizations to encrypt specific files on Windows based PCs. The files, once encrypted, are stored with and treated like any other file; thus users can copy, delete, or rename these files as security permissions permit. Except for those specifically encrypted files, access to the PC itself, the operating system, and system files remains uncontrolled.

Issues

- **High overhead degrades performance.** In contrast with disk encryption where PKI is only utilized once per user session, file encryption products must use PKI each time a file is opened or closed. Since the entire file must be decrypted before it is displayed, long files can require a substantial wait.
- **Inability to enforce security policy.** Since users cannot be forced to use a file encryption system, it is not feasible to have a uniform application of security policy within the organization. File encryption technology requires users to be cognizant of security policies and procedures and to use this knowledge to determine which data files should be secured. To maintain security, each user must act conscientiously to manually encrypt files or to store sensitive information in specific encrypted directories.
- **Incomplete security.** File encryption does not control access to the PC, the operating system, system files or temp files. It also leaves directories and file structures visible to attackers.

Full Hard Disk Encryption

Overview

Full hard disk encryption is attractive because it is automatic and transparent to the users. Every sector of the hard drive is encrypted at all times. Security is therefore not dependent on user knowledge and compliance with security standards. Full disk encryption is invariably linked to boot protection. Before the user can access the PC, he must authenticate himself to the security product. Requiring user authentication before the operating system can be started greatly improves overall security because it prevents the use of many widely available Windows cracking utilities that compromise passwords.

One clear advantage of full disk encryption is that PKI certificates, which contain the key pair, are fully encrypted with everything else on the hard drive. This process hides all directory structures making it virtually impossible to determine if a certificate is present or where it resides.

Issues

- **Boot level authentication cannot use PKI directly.** PKI certificates cannot be used without the PC operating system. However, this can be remedied by creating a linkage between the boot authentication and the process that starts the certificates. Essentially the authentication to the PC security system also triggers a check of the certificate once the operating system is available.