pointsec
A PROTECT DATA COMPANY

Pointsec – Enterprise Encryption and Access Control for Laptops and Workstations

Overview of PC Security

Since computer security has become increasingly important, almost all of the focus has been on securing large, multi-user machines. This made sense because mainframes and large servers are not only major repositories of data, they are also crucial to daily operations.

However, there is an equally serious and growing risk of compromise to the myriad of smaller, mostly single user, machines such as desktops, notebooks, and even pocket PCs and other PDAs. These machines frequently store the most current and valuable information of a given enterprise. Increasingly, such devices also store passwords, login scripts, and certificates used to access the enterprise network. The small size and portability of these devices means they are also much more vulnerable to theft or illicit access than large machines.

One additional often unrecognized problem is that the PC is the most available and vulnerable starting point for access to the network. Since all studies of computer crime reveal that insiders pose the largest threat, providing a means of securing PCs is an essential component of network security.

PC Security Measures

A variety of technologies have been employed to secure PCs and their contents, including physical controls (cables, locks on power supplies, anchored docking stations etc.) and electronic means such as data encryption, user authentication, audit logs and tracking utilities.

Physical access controls are becoming less relevant as users insist on portability. Consequently, there is an increasing emphasis on electronic protection. There are two general types of electronic PC security: encryption and boot protection/authentication.

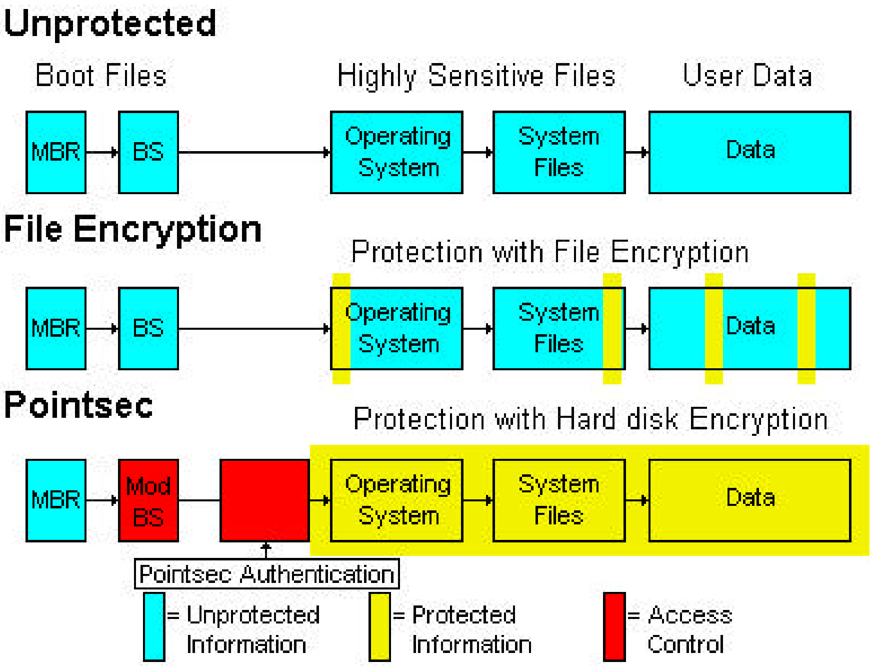
The first approach provides encryption tools that enable users to protect vital data. This approach, called file encryption, is usually easy to implement but is subject to user discretion regarding what to secure, and the willingness of users to consistently follow security procedures. Given this dependence on user compliance, organizations seeking to enforce a security policy often find file encryption insufficient.

The second approach is much more comprehensive. Here the goal is to prevent unauthorized access to the machine itself, and to provide further security by encrypting everything on the machine. Access control is accomplished through user authentication linked to boot protection; authorized access grants access to the encryption key, allowing encryption and decryption of data on the hard drive, which occurs automatically as needed. Yet that is an oversimplification – strong user authentication and boot protection are essential components of the complete system.

The importance of boot protection is often misunderstood or confused with the BIOS password schemes offered by the machine manufacturers. Authenticating users before the machine is booted prevents the operating system from being subverted by unauthorized persons using widely available password cracking tools. These utilities have proliferated on the Internet and can be used with devastating effect. Unfortunately, most BIOS level protection schemes are fatally weak and cannot be tightly linked with full disk encryption. Boot level access control has the further advantage of providing an effective deterrent to illicit network access via network-connected machines, especially if these machines are linked as part of a virtual private network.

While controlling access to the computer is important, this does not by itself protect the data stored on the disk. For example, a simple boot floppy disk could be used to bypass boot protection. Alternatively, removing the drive and placing it in another computer will make the file accessible to brute-force hacking attempts. Even in those rare cases where the drive itself is secured with a password, the data is not encrypted and is therefore vulnerable to several types of attacks. To secure this data, it must be encrypted. Once encrypted, the files will be inaccessible to any unauthorized person.

Full hard drive encryption offers several key advantages relative to file encryption. The most important is that full hard drive encryption is automatic and transparent to the user. Not only does this decrease user involvement and training requirements, but it creates the foundation for enforceable security. In addition, full hard drive encryption secures the system and temp files that often contain sensitive data but are missed by file encryption. Even removing the drive itself does not give access to any file or directory structure. Finally, hard drive encryption is performed sector by sector without creating temp or backup files: As a result, large files will decrypt without delay whereas file encryption is normally much slower. Full hard drive encryption also avoids such time consuming tasks as secure deletes of temp files or work files in clear text, and obviates the need to do a full delete on disks to be discarded.



Other considerations

The degree of security is only one of several issues that must be addressed to successfully implement a PC security system:

- Can the product be deployed and administered across the network without requiring individual installations?
- Can authorized persons always access their data in the event of a forgotten password by contacting a help desk?
- Does the organization retain control of the information residing on protected machines? Can the information be decrypted without user cooperation?
- Can the product be updated without having to remove and reinstall it?

Pointsec's Security Features and Benefits

Pointsec secures desktops and notebooks from unauthorized physical access, using both boot protection and volume encryption. *Pointsec* incorporates the following security functions:

- Strong user authentication
- Control of user access per partition
- Support for user identification using dynamic passwords
- Secure remote assistance for users who are traveling and have forgotten their passwords
- Central configuration and administration
- Keyboard lock and screen saver for Windows95/98
- Limited number of logon attempts with automatic locking
- Audit logging of events, i.e. successful and failed logon attempts

With *Pointsec*, all logical partitions/volumes are boot protected and encrypted. The careful integration of boot protection and automatic encryption provides a high degree of security with minimal impact on users. Boot protection prevents subversion of the operating system or the introduction of rogue programs while sector by sector encryption makes it impossible to copy individual files for brute force attacks. Full hard drive encryption secures the data even if the hard drive is removed and loaded into a controlled machine. This ensures security by allowing an organization to determine the security level instead of leaving it up to the user to see that the information is encrypted.

Pointsec employs hard disk encryption to guarantee that no users can access or manipulate information on an encrypted device, either from available files, erased files, or temporary files. *Pointsec* safeguards the operating system and the important system files (which often contain clues to passwords for Windows), shared devices, and the network.

Administration of *Pointsec*

Pointsec administration is designed to allow central control of policy and security settings, but decentralized deployment and day-to-day administration. System administrators are able to install and configure the system, delegate authorization throughout the network, modify the system for local conditions, and assign the properties and authorization of individual users by using profiles. *Pointsec* allows simple, but powerful, multi-point inspection of system information, group information, and individual user information.

Administration Rights and Permissions

Pointsec uses a hierarchical system for administration. This allows for simplified administration by using the inheritance of permissions from higher to lower levels. There are three levels in *Pointsec*:

- System Administrators
- Administrators
- Users

The recommended use of these levels is as follows:

The System Administrator

This is the highest authorization level in the administration of *Pointsec* and can perform the following tasks in the system:

- Create and administer profiles
- Configure system settings
- Add and remove administrators and users
- Configure settings for administrators and users
- Give remote assistance to users who are locked out or have forgotten their passwords

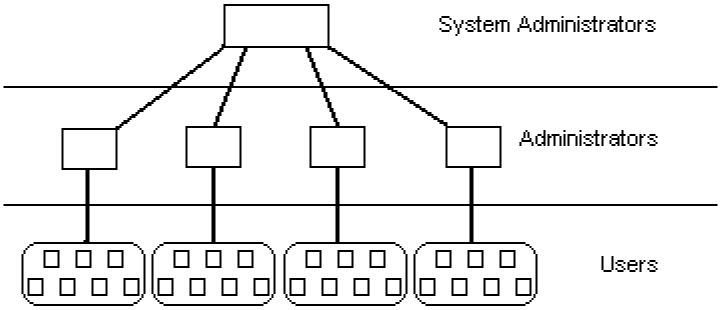
Administrators

Accounts at this level have limited authority in the administration of *Pointsec* according to what has been defined in the system settings. The Administrator can add, remove, and change settings for specific users. Administrators are not allowed to work with users who have higher administration privileges, nor can they raise their own authorization level. Administrators are normally given the authorization to provide remote assistance and to modify profiles.

Users

Accounts at this level have limited authorization to the *Pointsec* program based upon what has been defined in the system settings. Each user is assigned an account with a unique user identity and password that authorizes access to the entire hard disk or only specific partition(s) on the hard disk. This is especially useful for organizations with many users on the same computer as they can be given different partitions in which to store their data.

Using privileges these levels can be defined to meet the specific requirements of your organization.



System administrators are able to install and configure the system, delegate authorization throughout the network, modify the system for local conditions, and assign the properties and authorization of individual users by using profiles.

Each profile contains three sets of configuration settings:

- System information
- Group information
- User information

System Information

Contains information on paths to the central server concerning storage of key files, update profiles, program updates (patches), and partitions to be protected during the installation, type of security (encryption/boot protection), and encryption algorithms. The system information also contains definitions of the privileges of System Administrators, Administrators, and Users.

Group Information

Defines the system settings for local groups and their authorization, including the user's authorization to receive remote assistance and security settings such as keyboard lock. A group can be defined so that all users created in that group will inherit the group's settings.

User Information

Contains settings for individual users and their authorization, including the user's authorization for different partitions, remote assistance, and security settings such as time-out settings for the screen saver and unlocking the keyboard lock.