Pointsec 4.1

FIPS 140-1 Non-Proprietary Security Policy

Level 1 Validation

March 19, 2002

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for version 4.1 of Pointsec Mobile Technologies' hard drive encryption application. This security policy describes how Pointsec 4.1 meets the Level 1 security requirements of FIPS 140-1. This policy was prepared as part of FIPS 140-1 certification of Pointsec 4.1.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with operations and capabilities of Pointsec 4.1 in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Pointsec 4.1 application from the following sources:

- Overview information of Pointsec products and services can be found at: http://www.pointsec.com/solutions/solutions.asp

- For answers to technical or sales related questions, please refer to the contacts listed on the Pointsec website at www.pointsec.com.

1.3 Document Organization

The Security Policy document is one document in a complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This Security Policy and the other certification submission documentation was produced by Corsec Security, Inc. under contract to Pointsec Mobile Technologies. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is proprietary to Pointsec Mobile Technologies and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Pointsec.

2 Pointsec 4.1

2.1 Overview

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, an increasing emphasis is being made on electronic protection.

There are two general types of electronic PC security. The first approach is to provide 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 should be secured and the willingness of users to consistently follow the security procedures. Given this dependence on user compliance, organizations seeking an enforceable security program 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. This is accomplished through user authentication linked to boot protection, which in turn enables information to be automatically encrypted and decrypted. Because everything on the hard drive is encrypted, this technique is called full hard drive encryption. But that is an oversimplification – strong user authentication and boot protection are necessary components to this 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 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 encrypts 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.

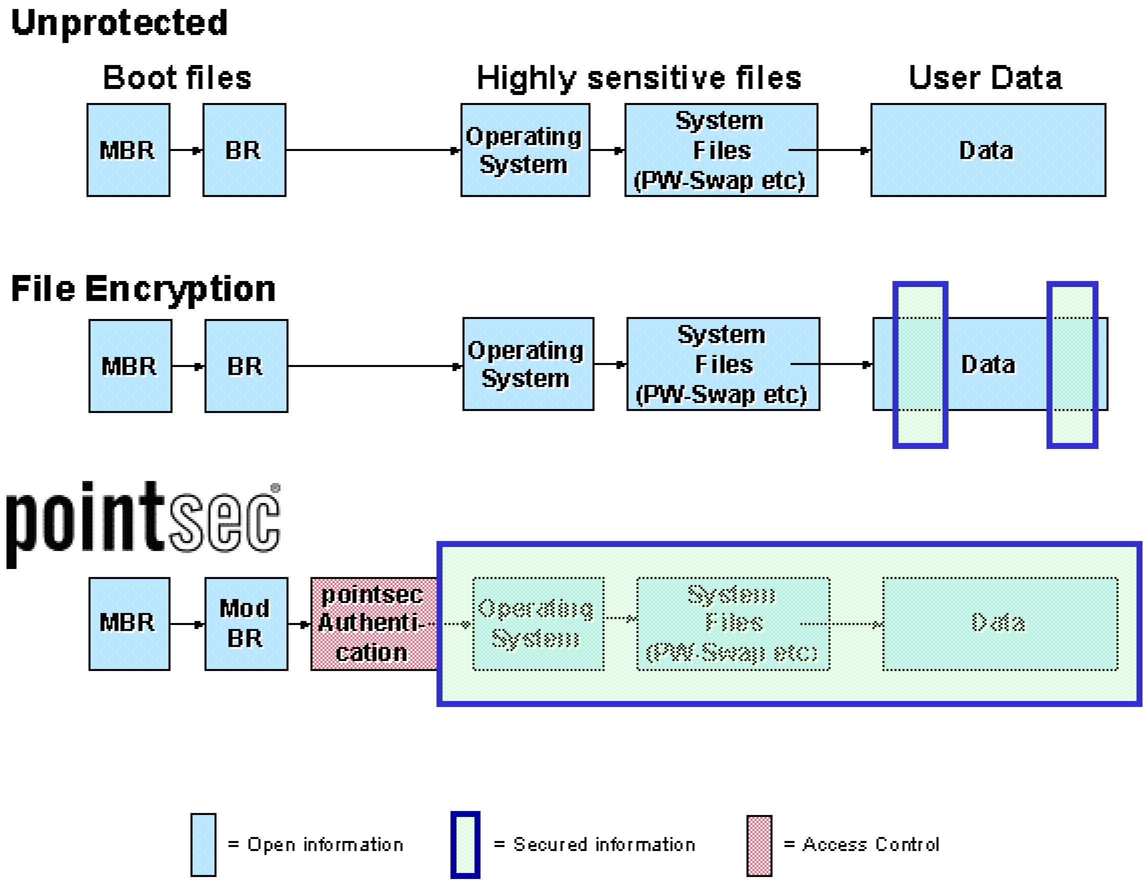

Figure 1 – Pointsec 4.1 Compared with Standard Encryption

Pointsec 4.1 secures desktops and notebooks from unauthorized physical access, using both boot protection and volume encryption. Pointsec 4.1 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 4.1, 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 encrypting sector by sector makes it impossible to copy individual files for brute force attacks. The 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 4.1 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 4.1 safeguards the operating system and the important system files (which often contain clues to passwords for Windows), shared devices, and the network.

Pointsec 4.1 was validated according to FIPS 140-1 standards using a general purpose Intel-compatible personal computer running Microsoft Windows 2000, Windows 95 and NT 4.0 SP6a (configured in single user mode) operating systems. The cryptographic module boundary is defined by the physical housing of a standard Intel-compatible commercial PC.

2.2 Module Interfaces

Pointsec 4.1 is classified as a multi-chip standalone module for FIPS 140-1 purposes. As such, the module includes a laptop running an operating system and interfacing with the computer, keyboard, mouse screen, floppy drive, CD-ROM drive, speaker, serial ports, parallel ports, and power plug.

Pointsec 4.1 provides a logical interface via an Application Programming Interface (API). The API interface provided by the module is mapped to the FIPS 140-1 logical interfaces: data input, data output, control input, and status output as described in the following table:

FIPS 140-1 Logical Interface	Module Mapping
Data Input Interface	input parameters to all functions that accept input from User entities
Data Output Interface	output parameters from all functions that return output and return values from functions
Control Input Interface	input parameters to all functions that accept input from Crypto Officer entities
Status Output Interface	information returned via exceptions and calls
Power Interface	does not provide a separate power or maintenance access interface beyond the power interface provided by the laptop computer itself

Table 1 – FIPS 140-1 Logical Interfaces

2.3 Roles And Services

Pointsec 4.1 performs identity-based authentication of its operators. Operators authenticate to the module using a username/password, username/smart card, or username/token+PIN. Based upon the attributes of the userid with which the authentication is associated, operator access to the module is granted as either a Crypto Officer or a user.

Pointsec 4.1 has three classes of operators. They are:

- System Administrators (Crypto Officer role)
- Application Administrators (Crypto Officer role)
- Users (User role)

The administrators and system administrators of the application assume the Crypto Officer role in order to configure and manage the application using Crypto Officer services, while the Users exercise only basic User services described below.

2.3.1 Crypto Officer Role

The rights and privileges associated with System Administrator and Application administrator are tantamount to the FIPS 140-1 Crypto Officer role. The following sections describe in detail the services available to the System Administrator and the Application Administrator, the two Crypto Officer roles supported by Pointsec 4.1.

2.3.1.1 The System Administrator

This is the highest authorization level in the administration of Pointsec 4.1. The System Administrator role is initially created at the time the module application is installed onto the general purpose PC. An operator authenticated as the system administrator has the following services available:

- Install the application
  - Specify type of protection (boot protection and encryption, encryption, etc.)
  - Identify which drives will be affected
- Create and administrate profiles
  - Generate new partition keys for added users
  - Specify role
  - Assign privileges
- Configure system settings
  - Unlock locked accounts
  - Backup or recover module partition keys
- Add and remove application administrators and users
  - The removal of a user will zeroize that user's partition key
- Verify the configuration of the application software and users
  - This provides the "show status" feature required by FIPS 140-1

2.3.1.2 Application Administrators

The Application Administrator role is initially created at the time the module application is installed onto the general purpose PC. Operators at this level have limited authority in the administration of Pointsec 4.1 according to what has been defined in the system settings by the System Administrator. The application administrator can add, remove, and change settings for specific users. Application administrators are not allowed to modify profiles of operators who have higher administration privileges, nor can they raise their own authorization level. Application administrators are normally given the authorization to provide remote assistance and to modify user profiles.

2.3.2 User Role

As mentioned above, the Pointsec application supports three operator levels. The user role in Pointsec 4.1 maps directly to the User role required by FIPS 140-1.

2.3.2.1 Users

Operators at this level have limited access to the Pointsec services based upon what has been defined in their user profile settings by the application administrator. Each user is assigned an account with a unique user identity and password. A user may be configured such that they are granted access to either 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. Only one operator may access the module at a time. Separation between users is accomplished through the use of separate userid/password combinations to access to the application and through uniquely-encrypted (wrapped) partition decryption keys (see section 2.8), which are associated with each userid that has been created by one of the Crypto Officer roles.

Users derive access to the module services to encrypt or decrypt portions of the hard drive or partition as they use the standard operating system commands to access files stored on the computer's hard drive. File sectors are decrypted when read from the hard drive and encrypted when written to the hard drive.

Pointsec 4.1 can be configured such that different users are granted access to the same protected portion of the hard drive (entire drive or a partition). At installation time, a Crypto Officer defines which portions of the disk are to be protected. The application creates a partition encryption key, K_P (see section 2.8) for each partition. For each userid subsequently created by a Crypto Officer and authorized for access to a particular partition, the associated K_P is encrypted and stored inside the module using a proprietary DES-based algorithm which uses the userid and password as part of its input to create a uniquely-encrypted copy of the K_P. User authentication is accomplished by the user's ability to successfully decrypt the encrypted K_P by supplying the module with their userid and the correct associated password. Providing an invalid password results in the incorrect decryption of the encrypted K_P and denial of access to the module.

2.4 Finite State Machine Model

Pointsec 4.1 is designed around a Finite State Machine (FSM) which is detailed in a Pointsec-proprietary document (*Pointsec 4.1 FIPS 140-1 Finite State Machine – Level 1 Validation*). Parties interested in reviewing this document should contact Pointsec thorough the sources listed in Section 1.2.

2.5 Physical Security

Pointsec 4.1 is a software module intended for use with Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT Server/WorkStation 4.0 SP6a (configured in single user mode), Microsoft Windows Millennium Edition, and Microsoft Windows 2000. The module was validated against FIPS 140-1 Level 1 requirements for physical security when running on a standard Intel-compatible personal computer running each of the Microsoft Windows operating systems listed above. This platform meets all FIPS 140-1 Level 1 requirements for physical security, providing a multi-chip standalone module with production grade equipment, industry-standard passivation, and a strong enclosure.

Although Pointsec 4.1 consists entirely of software, the FIPS 140-1 validated platform is a standard general purpose PC which has been tested for and meets applicable FCC EMI and EMC requirements for business use as defined in Subpart B of FCC Part 15.

2.6 Software Security

The application is written in C++ and C, with some assembly language for purposes of speed and low-level functionality not available in C/C++.

2.7 Operating System Security

Pointsec 4.1 is implemented as a single loadable module and is run (without modification) on Microsoft's Windows 95, 98, ME, NT (SP6a), and 2000 platforms. The module is a single user system and is a single dynamically linked library (DLL) that is always distributed as an executable to discourage unauthorized modification. Additionally, a cryptographic mechanism is used within the module to help ensure that the executable code has not been accidentally or inadvertently modified from its validated configuration.

2.8 Cryptographic Key Management

Each user has a uniquely-encrypted partition key (K_P) that is used to decrypt accessed portions of the hard drive after successful login. Each partition (or volume) is encrypted with a separate K_P; therefore, it is possible that one user may have more than one partition key. Each K_P is a different symmetric encryption key that is used to encrypt the operating system and all data files on a partition – everything except the Pointsec boot-strapping software on the master boot record. On a non-boot partition, the entire partition would be encrypted with K_P. Each partition has its own K_P, and thus for a system with two partitions, there would be a K_{P1} and a K_{P2}.

Each K_P is generated inside the module during install time by the installation program (thus, the module does not support key entry). The K_P is used during the install process to configure and initially encrypt the partition. The creation of the K_P uses the time & date on the machine, the windows up-time, and inter-keystroke timing as random seeds for the Blum Blum Shub algorithm. The output from this algorithm seeds an ANSI X9.17 PRNG to meet FIPS requirements.

The module does not support key distribution. For key archiving, the user database file can be copied to a remote directory for recovery purposes (the Crypto Officer configures this at installation). The file is encrypted with 3DES, and the partition keys in the user database file are encrypted with 3DES.Keys are exported in encrypted form for key archiving purposes only. All partition keys as well as the keys used to encrypt the user database (KD) and key recovery (KD) files are zeroized when the module is uninstalled or the hard drive is reformatted.

2.9 Cryptographic Algorithms

The Pointsec application implements the following algorithms: DES, 3DES, Blum Blum Shub, and ANSI X9.17. To generate the partition keys, the output of the Blum Blum Shub algorithm seeds an ANSI X9.17 PRNG. DES is used to one-way hash user passwords, which are stored in the user database (encrypted with 3DES). A more detailed description of the application's key lifecycle can be found in the *Pointsec Software Architecture* document. To view this proprietary document, please contact Pointsec.

2.10 Self-Tests

Upon startup, the program will run 3DES-MAC an integrity check to ensure that no malicious code has been loaded and will perform cryptographic known answer tests for the DES and 3DES algorithms. Other tests run at startup include a power on self-test run by the BIOS and a virus scan/partition scan run by Pointsec 4.1. The module implements a continuous random number generator test on the ANSI X9.17 PRNG. To manually initiate these self-tests, the operator should power-cycle the computer.

3 Operation of Pointsec 4.1

Pointsec 4.1 is validated with the Microsoft Windows operating system(s); therefore, the application must be installed on a Microsoft Windows machine to maintain compliance to the FIPS 140-1 standard. Windows NT (SP6a) installations must be configured for single-user. Pointsec 4.1 is designed to meet FIPS 140-1 Level 1 requirements, and it does not require any special configuration to meet these requirements once installed. Although the module supports non-FIPS approved algorithms (AES, BLOWFISH, and CAST), the license number supplied by the vendor with Pointsec 4.1 enables only FIPS approved algorithms and functions. To enable FIPS mode, the customer should use only FIPS license numbers when installing the application.