Mobile Armor Mobile Armor™ Warp Drive 2.1.0.0

Security Policy

FIPS 140-2

Level 1

Version 5.1

September 23, 2005

Mobile Armor Mobile Armor™ Warp Drive 2.1.0.0 Security Policy

This document is provided for informational purposes about the non-proprietary structure of the Mobile Armor™ Warp Drive 2.1.0.0 as it pertains to FIPS 140-2 validation.

Any reproduction of this document must include the Copyright notice of Mobile Armor, LLC.

Document ID Number: DAWRPSP-51-01

Contact Mobile Armor

Mobile Armor, LLC.
400 South Woods Mill Road
Suite 110
St. Louis, MO, 63017 USA

Telephone: +1 (636) 449-0239
Fax: +1 (314) 205-2303

Website: http://www.mobilearmor.com

Email: mailto:sales@mobilearmor.com

Table of Contents

1. Security Policy Introduction

1.1 Security Policy, Product and Evaluation Identification

SP Title: Mobile Armor Warp Drive 2.1.0.0 Security Policy

SP Version: Version .5

Product Name: Mobile Armor Warp Drive

Product Version: 2.1.0.0

FIPS Evaluation Identification: FIPS 140-2

Evaluation Level: 1

1.2 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Mobile Armor Warp Drive 2.1.0.0. This security policy describes how the Mobile Armor Warp Drive 2.1.0.0 meets the Level 1 security requirements of FIPS 140-2. While the product will be evaluated on Windows XP Professional SP2, it is a cross-platform module also capable of running on Microsoft Windows 2000, Windows Mobile, and Red Hat Enterprise Linux 3.0 as well as other Linux distributions running the 2.6.8 or higher kernel. This policy was prepared as part of FIPS 140-2 validation of the Mobile Armor Warp Drive 2.1.0.0.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

1.3 References

This document deals only with operations and capabilities of the Mobile Armor Warp Drive 2.1.0.0 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Mobile Armor Warp Drive 2.1.0.0 application from the following sources:

- Overview information of Mobile Armor products and services as well as answers to technical or sales related questions, refer to: http://www.mobilearmor.com.

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
API	Application Programming Interface
OS	Operating System
PDA	Personal Digital Assistant
DLL	Dynamic Link Library

Table 1 – Acronyms

2. Mobile Armor Warp Drive

2.1 Overview

The Mobile Armor Warp Drive 2.1.0.0 provides cryptographic support for the Mobile Armor Mobile Armor products. The Warp Drive is used to perform disk encryption/decryption operations. The cryptographic keys which are used in these operations are provided by the Mobile Armor Crypto Module .

The Warp Drive does not have the ability to create, manage or delete keys; it can only utilize symmetric keys provided to it.

2.2 Cryptographic Module

The Mobile Armor Warp Drive 2.1.0.0 is classified as a multi-chip standalone module for FIPS 140-2 purposes. The cryptographic module is capable on running on any commercially available IBM compatible PC running the following list of Operating Systems (OS).

- Microsoft Windows XP SP2
- Microsoft Windows 2000 SP4
- Red Hat Enterprise Linux 3.0

Further, the module is capable of running on any commercially available Microsoft Windows Mobile-based PDA (note the PDA must be capable of running Windows Mobile, and not earlier versions of the Pocket PC OS). A partial list of devices currently available (in the United States) that meet this requirement can be found at http://www.microsoft.com/windowsmobile/devices/pocketpc/ppc/americas.mspx.

The module was tested for FIPS compliance on a generic PC running Windows XP Professional Service Pack 2 configured in the single user mode.

The module is compiled into libraries for each platform as a file driver which are used from within the OS to encrypt data being written to and decrypt data being read from the disk.

2.3 Module Ports and Interfaces

The Mobile Armor Warp Drive 2.1.0.0 is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the module's logical cryptographic boundary includes the driver binary, . The physical boundary is a PC or PDA running an operating system and interfacing with the device, and external components such as keyboard, mouse, touch screen, screen, floppy drive, CD-ROM drive, speaker, serial ports, parallel ports, USB ports and power plug.

The Mobile Armor Warp Drive 2.1.0.0 interacts with the operating system file system drivers and provides a logical interface via an Application Programming Interface (API). The API provided by the module is mapped to the FIPS 140-2 logical interfaces: data input, data output, control input, and status output. All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

FIPS 140-2 Logical Interface	Module Mapping
Data Input Interface	Parameters passed to the module via API calls
Data Output Interface	Data returned by the module via the API
Control Input Interface	Control input through the API function calls
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 computer itself

Table 2 – FIPS 140-2 Logical Interfaces

2.4 Roles, Services and Authentication

The Mobile Armor Warp Drive 2.1.0.0 does not provide any identification or authentication for any user that is accessing the module, and is only acceptable for FIPS 140-2 level 1 validation. The module provides the Crypto Officer and User roles which are combined into a single role. This role has access to all services, keys and CSPs of the module. The only available end-user services are encryption of written data and decryption of read data (both of which are required for the OS to function correctly).

The Mobile Armor Warp Drive 2.1.0.0 provides the following API calls for access to the functions of the module:

Exposed APIs	Description
MAWHDDAddDevice	responsible for creating functional device objects (FDO) or filter device objects (filter DO) for devices enumerated by the Plug and Play (PnP) manager
MAWHDDDispatchPnp	services IRPs containing the IRP_MJ_PNP I/O function code
MAWHDDIrpCompletion	The entry point for the driver-supplied IoCompletion routine, which is called when the next-lower driver completes the packet
MAWHDDStartDevice	function is the handler for IRP_MN_START_DEVICE
MAWHDDRemoveDevice	uses the IRP_MN_REMOVE_DEVICE to direct drivers to remove a device's software representation
MAWHDDSendToNextDriver	talks to next level driver layer by calling the function
MAWHDDDispatchPower	services IRPs containing the IRP_MJ_POWER I/O function code
MAWHDDForwardIrpSynchronous	called when the Irps have to be transferred to another DeviceObject synchronously
MAWHDDCreate	Handler for IRP_MJ_CREATE
MAWHddReadWriteWorkitem	the Queue item completion routine for MAWHDDIOcompletion
MAWHDDReadWrite	Main Handler routine for IRP_MJ_READ AND IRP_MJ_WRITE
MAWHDDIoCompletion	Main Handler routine for Completion routine for IRP_MJ_READ AND IRP_MJ_WRITE

Exposed APIs	Description
MAWHDDDeviceControl	Handler routine for Device IO calls done
MAWHDDShutdown	Shutdown Handler for the Driver
MAWHDDFlush	Flush handler for the driver
MAWHDDUnload	Unload handler for the Driver
MAWHDDRegisterDevice	Registers the Device object to handle WMI requests later
MAWHDDIrpCompletion	The IRP completion routine for Asynchronous IRP Completion
MAWHDDLogError	Error log for the Driver
MAWHDDDebugPrint	Outputs to the debug window

Table 3 – Application Programming Interface

2.5 Physical Security

The Mobile Armor Warp Drive 2.1.0.0 is a software module intended for use with Microsoft Windows 2000, Microsoft Windows XP and Red Hat Enterprise Linux 3.0 in single user modes on a PC, and Microsoft Windows Mobile on a PDA. Since the module is implemented solely in software, the physical security section of FIPS 140-2 is not applicable.

2.6 Operational Environment

The Warp Drive is implemented as a loadable module compiled into three forms, one for each OS platform where it is installed: a Windows SYS for Windows 2000/XP, a Linux DLL for the Red Hat Enterprise Linux 3.0, and a Windows Mobile SYS for the PDA platform. The only differences in these Driver versions are those necessary to port the Driver to each OS.

The Mobile Armor Warp Drive 2.1.0.0 is a single user module that is always distributed in binary form to discourage unauthorized access or modification to source. Additionally, a software integrity check is run when the modules are loaded to help ensure that the code has not been accidentally or ineptly modified from its validated configuration.

2.7 Cryptographic Key Management

The Mobile Armor Warp Drive 2.1.0.0 implements the following algorithms. The FIPS approved column specifies whether the algorithm is available in the FIPS-mode

.

Algorithm	FIPS Approved
AES (ECB-256-bit keys)	Yes
TDES (ECB,Keying Options 1,2,3)	Yes
HMAC-SHA-1	Yes
SHA-1	Yes
SHA-256	Yes

Table 4 – FIPS Cryptographic Algorithms

The following is a list of keys is used by the module. They are inserted into the module and stored within the Warp Drive protected memory as necessary.

Name	Created	Size(s)	Purpose
AES-disk	Inserted	256-bits	Encryption, Decryption
3DES-disk	Inserted	168-bits	Encryption, Decryption
HMAC-SHA-1 integrity check key	Hard coded	128-bits	Verify driver integrity

Table 5 – Key Generation

Encryption/Decryption Keys are stored in the Driver's internal data structures, which are not exposed to external access. When keys are set for deletion, the key is zeroized by overwriting the key multiple times to ensure it cannot be retrieved. The HMAC-SHA-1 key can be zeroized by deleting the driver binary and reformatting the hard disk

The HMAC-SHA-1, SHA-1 and SHA-256 algorithms are only used to perform startup integrity check and are not available once the Driver has started.

2.8 Self-Tests

The Mobile Armor Warp Drive 2.1.0.0 performs several power up self-tests including known answer tests and monte carlo tests. The crypto module also performs a self-integrity check to verify the module has not been damaged or tampered with.

Algorithm	Known Answer Tests	Monte Carlo Tests
AES	Yes	Yes
TDES	Yes	Yes
SHA-256	Yes	No
SHA-1	Yes	No
HMAC SHA-1	Yes	No

Table 6 – FIPS Algorithm Self Tests

2.9 Design Assurance

Mobile Armor maintains versioning for all source code and associated documentation through Microsoft Visual SourceSafe 6.0.

2.10 Mitigation of Other Attacks

The Mobile Armor Warp Drive 2.1.0.0 does not employ security mechanisms to mitigate specific attacks.

3. Operation of the Mobile Armor Warp Drive

The Mobile Armor Warp Drive 2.1.0.0 contains only FIPS-approved algorithms and operates only in FIPS mode after installation.

The Mobile Armor Warp Drive 2.1.0.0 is designed for installation and use on a computer configured in single user mode, and is not designed for use on systems where multiple, concurrent users are active.