Attivo Cryptographic Module

Version 1.0

FIPS 140-2 Level 1
Non-Proprietary Security Policy

Version Number: 1.5
Date: June 23, 2017

Table of Contents

1. Module Overview 3
2. Modes of Operation 5
   2.1 Approved and Allowed Cryptographic Functions 5
   2.2 All other algorithms 6
3. Ports and interfaces 6
4. Roles and Services 7
5. Cryptographic Keys and CSPs 8
6. Self-tests 9
7. References 10

1. Module Overview

Attivo Cryptographic Module is a component of Attivo Networks' products such as the Attivo Central Manager 200, BOTsink 3200, and BOTsink 5100. These products constitute the Attivo ThreatMatrix Deception and Response Platform which detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving attackers into revealing themselves. The detections along with comprehensive attack analysis and actionable alerts empower accelerated incident response.

The cryptographic module is a software module that is executing in a modifiable operational environment by a general purpose computer.

This software module contains a single component:

- fipscanister.o (Linux and Mac OS)
- fipscanister.lib (Windows)

FIPS 140-2 conformance testing was performed at Security Level 1. The following configuration was tested by the lab.

Table 1.1: Configuration tested by the lab[1]

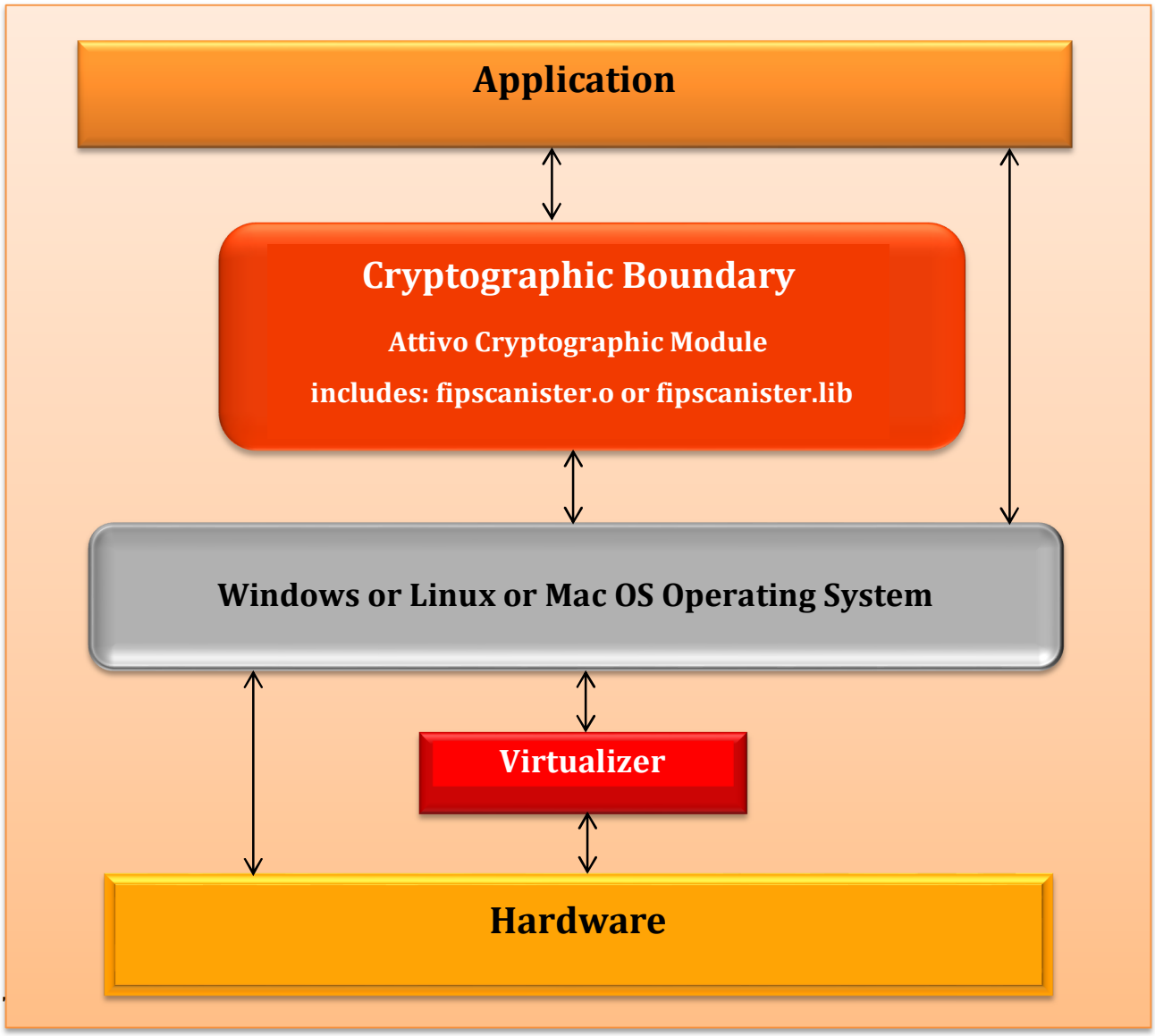
Software Component	Operating System	Processor(s)
● fipscanister.o (Linux and Mac OS) ● fipscanister.lib (Windows)	Mac OS X El Capitan 10.11.3	Intel Core i5 with AES-NI
	CentOS 6.5 on VMware ESXi 6.0.0	Intel(R) Xeon(R) CPU E5-2620 with AES-NI
	CentOS 6.5 on CentOS 6.5 - KVM	
	Ubuntu 12.04 LTS on VMware ESXi 6.0.0	
	Windows Server 2008 SP2 (32 bit) on CentOS 6.5 - KVM	
	Ubuntu 12.04 LTS on CentOS 6.5 - KVM	
	Windows Server 2008 SP2 32-bit on VMware ESXi 6.0.0	
	Windows 7 Professional 64-bit on VMware ESXi 6.0.0	
	Windows 7 Professional 64-bit on CentOS 6.5 - KVM	

[1] The module was also successfully tested without using AES-NI. However configurations without using AES-NI are not relevant to Attivo Networks.

Table 1.2: Module Security Level Statement

FIPS Security Area	Security Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Figure 1: Block Diagram for Attivo Cryptographic Module



2. Modes of Operation

The mode is selected implicitly based on the services used. In the FIPS approved mode of operation the operator must only use FIPS-approved and allowed security functions listed in the Section 2.1. The Module requires an initialization sequence per IG 9.5. The calling application enables FIPS mode by calling the FIPS_mode_set() function.

In the non-FIPS mode of operation the module performs non-approved functions listed in the Section "2.2 All Other Algorithms" of this security policy. These functions shall not be used in FIPS approved mode of operation.

2.1 Approved and Allowed Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.1: Approved Cryptographic Functions.

Algorithm	CAVP Certificate
AES (ECB, CBC, CFB, OFB, CTR, GCM, CCM and CMAC): 128/192/256 bits key AES XTS: 256/512 bits key	3983
SP 800-90A DRBG (CTR, Hash, HMAC)	1176
HMAC (SHA1, SHA224, SHA256, SHA384, SHA512)	2599
SHS (SHA1, SHA224, SHA256, SHA384, SHA512)	3288
ECC CDH (CVL), all NIST defined B, K and P curves except sizes 163 and 192	812
3 key Triple-DES (TECB, TCBC, TCFB, TOFB, CMAC)	2186
RSA (FIPS 186-2) SigVer ANSIX9.31, SigVer RSASSA-PKCS1_V1_5 , SigVer RSASSA-PSS (as specified on the CAVP Certificate) RSA (FIPS 186-4) SigGen ANSIX9.31, SigGen RSASSA-PKCS1_V1_5 , SigGen RSASSA-PSS (as specified on the CAVP Certificate)	2044
DSA (FIPS 186-4) (PQG Gen, PQG Ver, Key Pair Gen, Sig Gen, Sig Ver (as specified on the CAVP Certificate)	1083
ECDSA (FIPS 186-4) PKG, PKV, SigGen, SigVer (as specified on the CAVP Certificate)	881

The following non-FIPS approved but allowed cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.2: Non-FIPS Approved But Allowed Cryptographic Functions.

Algorithm
RSA encrypt/decrypt using RSA with keys ≥ 2048 bits
EC DH using all NIST defined B, K and P curves except sizes 163 and 192

2.2 All other algorithms

In the FIPS approved mode of operation the operator must not use the functions listed in the Table 2.3. These functions are available in the User role.

Table 2.3: Non-Approved Cryptographic Functions

Algorithm
(FIPS 186-2) RSA GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS
(FIPS 186-2) DSA PQG Gen, Key Pair Gen, Sig Gen
(FIPS 186-4) DSA PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA-1)
(FIPS 186-2) ECDSA PKG, SigGen
(FIPS 186-4) ECDSA PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384: (SHA-1) P-521:(SHA-1) K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283: (SHA-1) B-409:(SHA-1) B-571:(SHA-1))
(SP 800-56A) (§5.7.1.2) ECC CDH (CVL) All NIST Recommended B, K and P curves sizes 163 and 192
RSA encrypt/decrypt using RSA with keys < 2048 bits
ANSI X9.31 RNG(AES-128, AES-192, AES-256)

3. Ports and interfaces

The physical ports of the module are the same as those of the computer system on which it is executing. The logical interfaces of the module are implemented via an Application Programming Interface (API). The following table describes each logical interface.

Table 3: FIPS 140-2 Logical Interfaces.

Logical Interface	Description
Data Input	Input parameters that are supplied to the API commands
Data Output	Output parameters that are returned by the API commands
Control Input	API commands
Status Output	Return status provided by API commands

4. Roles and Services

The module supports a Crypto Officer role and a User Role. The Crypto Officer installs and loads the module. The Crypto Officer also uses the services provided by the module. The User uses the cryptographic services provided by the module. The module provides the following services.

Table 4: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Initialize	User Crypto Officer	N/A
Self-test	User Crypto Officer	N/A
Show status	User Crypto Officer	N/A
Zeroize	User Crypto Officer	All: Z
Installation	Crypto Officer	N/A
Random number generation	User Crypto Officer	DRBG CSPs: R, W
Asymmetric key generation	User Crypto Officer	DSA keys: W ECDSA keys: W
Symmetric encrypt/decrypt	User Crypto Officer	AES key: R Triple-DES key: R
Symmetric digest	User Crypto Officer	CMAC key: R
Message digest	User Crypto Officer	N/A
Keyed Hash	User Crypto Officer	HMAC key: R

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Key transport	User Crypto Officer	RSA keys: R
Key agreement	User Crypto Officer	EC DH keys: R, W
Digital signature	User Crypto Officer	RSA keys: R DSA keys: R ECDSA keys: R

Table 4: Roles and Services

Non-Approved cryptographic services are implementations of Non-Approved algorithms. They are listed in the Section 2.2.

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 5: Cryptographic Keys and CSPs

Key	Description/Usage	Origin	Zeroization
AES 128/192/256 bits Key AES XTS 256/512 bits key	Used during AES/XTS encryption, decryption, generation and verification Upon power cycle the calling application must ensure that any AES-GCM keys are refreshed	Generated using DRBG	Zeroized during power cycle or reboot
Triple-DES (3-Key) Key	Used during Triple-DES encryption, decryption, generation and verification	Generated using DRBG	Zeroized during power cycle or reboot
HMAC 160/224/256/384/ 512 bits Key	Used during calculation of HMAC	Generated using DRBG	Zeroized during power cycle or reboot
HMAC_DRBG CSPs: V(160/224/256/384/512 bits), Key(160/224/ 256/384/512 bits), and entropy input (length depends on security strength)	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot

Key	Description/Usage	Origin	Zeroization
CTR_DRBG CSPs: V(128 bits), Key(AES 128/192/ 256 bits), seed (232/256/ 320/384 bits) and entropy input (length depends on security strength)	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
Hash_DRBG CSPs: V(440/888 bits), C(440/888 bits), seed (440/888 bits) and entropy input (length depends on security strength)	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
RSA key pairs (1024 to 16384 bits)	Used for Sign/Verify and Key wrapping	Provided by user	Zeroized during power cycle or reboot
DSA key pairs (1024/2048/3072 bits)	Used for Sign/Verify	Generated using DRBG	Zeroized during power cycle or reboot
ECDSA key pairs (all NIST defined B, K, and P curves)	Used for Sign/Verify	Generated using DRBG	Zeroized during power cycle or reboot
EC DH key pairs (all NIST defined B, K, and P curves)	Used for Key agreement	Generated by the module or provided by user	Zeroized during power cycle or reboot

The Keys and CSPs are stored in plaintext in RAM within the module. CSPs enter the logical boundary in plaintext via API parameters without crossing the physical boundary. The module does not output CSPs, other than during key generation. However they don't cross the physical boundary. API commands automatically zeroize temporarily stored CSPs. The calling applications shall use entropy sources that meet the security strength required by [SP 800-90A]. These sources shall return an error if the minimum entropy requirement is not met.

Keys and CSPs used in the FIPS Approved mode of operation shall not be used while in the non-FIPS mode of operation. Keys or CSPs shall not be established while in the non-FIPS mode of operation.

6. Self-tests

The module performs the following power-up and conditional self-tests. Upon failure or a power-up or conditional self-test the module halts its operation.

Table 6: Self-Tests

Algorithm	Test
Software integrity	KAT using HMAC-SHA1
HMAC	KAT using SHA1, SHA224, SHA256, SHA384 and SHA512 to also cover SHA POST
AES	KAT(encryption/decryption)
Triple-DES	KAT(encryption/decryption)
RSA	KAT
	Pairwise consistency test on generation of a key pair
DSA	Pairwise Consistency Test (sign/verify)
	Pairwise consistency test on generation of a key pair
DRBG	KAT
	Continuous Random Number Generator test
ECDSA	Pairwise Consistency Test (sign/verify)
	Pairwise consistency test on generation of a key pair
ECC CDH	KAT
NDRNG	Continuous Random Number Generator test

7. References

Table 7: References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

Reference	Specification
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators