ACM 200

Version 1.0

FIPS 140-2 Level 2 Non-Proprietary Security Policy

Version Number: 1.7
Date: October 15, 2021

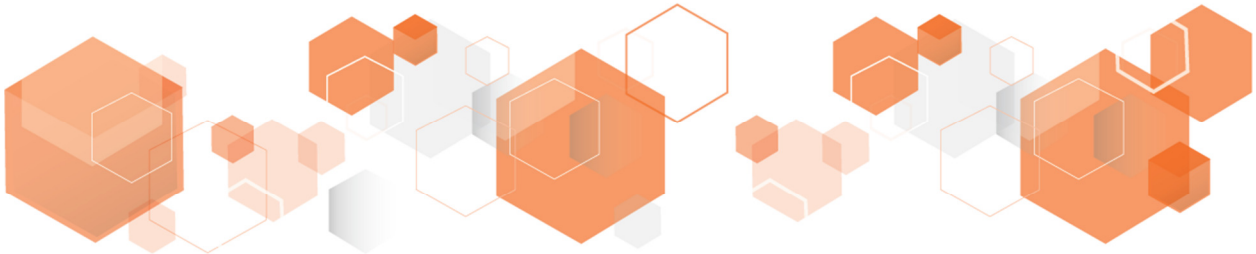

Table of Contents

1. Module Overview

The Attivo BotSink solution uses dynamic deception techniques and a matrix of distributed decoy systems to turn an entire network into a trap, which is designed to deceive and detect attackers and their automated tools into revealing themselves. Whether the attack vector is zero day, stolen credential, ransomware, phishing or an insider threat, the BotSink system provides an effective and efficient solution to detect these threats in real-time. Prevention-based detection does not reliably detect signature-less attacks, the use of stolen credentials, and the lateral movement of attacks that have bypassed firewall, anti-virus and other prevention solutions. Not reliant on known attack patterns or signatures, Attivo will instead use deception to lure the attacker into interacting with the decoy systems. Once the attacker engages, an alert is immediately created with the substantiated attack detail required to block the attacker and quarantine the infected device. The attack details can be viewed in the Attivo Threat Intelligence Dashboard, through a variety of reports, and can be automatically uploaded into 3rd party prevention solutions dramatically improving incident response.

The ACM is designed to manage several BotSinks in a centralized manner. ACMs cannot be managed by other ACMs, and each BotSink can be programmed to use one and only one ACM.

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

Table 1: Configuration tested by the lab.

Module Name and Version	Firmware version
ACM 200	3.3

The Cryptographic Module meets FIPS 140-2 Level 2 requirements.

Table 2: Module Security Level Statement.

FIPS Security Area	Security Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

The cryptographic boundary of the module is the enclosure that contains components of the module. The enclosure of the cryptographic module is opaque within the visible spectrum. The module uses tamper evident labels to provide the evidence of tampering.

Figure 1: ACM 200

2. Modes of Operation

The module always operates in the FIPS approved mode.

2.1 Approved Cryptographic Functions

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

Table 3: Approved Cryptographic Functions

CAVP Cert	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
4134 4417	AES	FIPS 197, SP 800-38D	ECB, CBC, CTR, GCM[3]	128, 192, 256	Data Encryption/ Decryption
1251 1426	DRBG	SP 800-90A	HASH_Based DRBG HMAC_Based DRBG CTR_DRBG		Deterministic Random Bit Generation[4]
941	CVL Partial DH	SP 800-56A	ECC	P-256 P-384 P-521	Shared Secret Computation
2706 2933	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384,	160, 256, 384, 512	Message Authentication

CAVP Cert	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
			HMAC-SHA-512		
2259 2379	Triple-DES	SP 800-67	TECB, TCBC	168	Data Encryption/ Decryption[1]
3403 3638	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384 SHA-512		Message Digest
2250 2405	RSA	FIPS 186-4, FIPS186-2	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 ANSIX9.31; PKCS1 v1.5; PSS	1024 (verification only), 1536 (verification only), 2048, 3072, 4096	Digital Signature Generation and Verification
1228 1229 1230	CVL TLS 1.2, SSH	SP 800-135			Key Derivation[2]
1130	RSASP1 Signature Primitive	FIPS 186-4 PKCS#1v2.1	PKCS 1.5	2048	Signature Primitive

Note 1: any software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Note 2: not all CAVS tested modes of the algorithms are used in this module.

[1] Operators are responsible for ensuring that the same Triple-DES key is not used to encrypt more than 2^16 64-bit data blocks

[2] No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

[3] The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288. AES-GCM is only used in TLS version 1.2.

[4] The module directly uses the output of the DRBG.

2.2 Non-FIPS Approved But Allowed Cryptographic Functions

Algorithm	Caveat	Use
RSA Key Wrapping using 2048 bits key	Provides 112 bits of encryption strength.	Used during TLS handshake
DH using 2048 bits key	Provides 112 bits of encryption strength.	Used during TLS handshake and SSH session establishment.
EC DH	Provides between 112 and 256 bits of encryption strength	Used during TLS handshake

2.3 All other algorithms

Algorithm	Use
MD5 (no security claimed)	Checksum
Blowfish (no security claimed)	Obfuscation

3. Ports and interfaces

The following table describes physical ports and logical interfaces of the module.

Table 4: Ports and Interfaces.

Port Name	Count	Interface(s)
Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output
VGA Port	1	Data Output, Status Output
Serial Port	1	Data Input, Data Output, Control Input, Status Output
USB Port	4	Data Input, Control Input
Power Receptacle	2	Power Input
IPMI	1	Not used
LEDs	multiple	Status Output
Power button	1	Control Input
Reset button	1	Control Input

4. Roles, Services and Authentication

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

Table 5: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Self-test	Crypto Officer	N/A
Reboot	Crypto Officer	N/A
Zeroization	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update key: R
Show status	Crypto Officer	N/A
Installation	Crypto Officer	Password: R, W SSH Keys: R, W TLS Keys: R,W DRBG seed: R, W
SSH	User Crypto Officer	Password: R, W SSH Keys: R,W DRBG seed: R, W
HTTPS	User Crypto Officer	Password: R, W TLS Keys: R,W DRBG seed: R, W
Device Management	User Crypto Officer	Password: R, W TLS Keys: R,W SSH Keys: R,W DRBG seed: R, W
Central Management	Crypto Officer	Password: R, W TLS Keys: R,W DRBG seed: R, W

The module supports the following authentication mechanisms.

Role	Authentication Mechanisms
User	Passwords (Minimum 8 characters)
Crypto Officer	Passwords (Minimum 8 characters)

5. Cryptographic Keys and CSPs

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

Table 6: Cryptographic Keys and CSPs

Key	Description/Usage	Storage
TLS pre-master secret	Used to derive TLS master secret	RAM in plaintext
TLS master secret	Used to derive TLS encryption key and TLS HMAC Key	RAM in plaintext
TLS AES or Triple-DES key	Used during encryption and decryption of data within the TLS protocol	RAM in plaintext
TLS HMAC key	Used to protect integrity of data within the TLS protocol	RAM in plaintext
TLS RSA public and private keys	Used during the TLS handshake to encrypt the TLS pre-master secret	RAM in plaintext Magnetic media in plaintext
TLS Diffie-Hellman public and private keys	Used during the TLS handshake to establish the shared secret	RAM in plaintext
TLS EC Diffie-Hellman public and private keys	Used during the TLS handshake to establish the shared secret	RAM in plaintext
CTR_DRBG CSPs: entropy input, V and Key Hash_DRBG CSPs: entropy input, V and C HMAC_DRBG CSPs: entropy input, V and Key	Used during generation of random numbers	RAM in plaintext
Passwords	Used for user authentication	RAM in plaintext Magnetic media in plaintext
Firmware update key	Used to protect integrity during firmware update	RAM in plaintext Magnetic media in plaintext
Client certificates	Used for connection authentication	RAM in plaintext
SSH AES key	Used during encryption and decryption of data within the SSH protocol	RAM in plaintext
SSH HMAC key	Used to protect integrity of data within the SSH protocol	RAM in plaintext

SSH RSA public and private keys	Used to authenticate the SSH handshake	RAM in plaintext
SSH Diffie-Hellman public and private keys	Used during the SSH handshake to establish the shared secret	RAM in plaintext

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.

The following table describes self-tests implemented by the module.

Table 7: Self-Tests

Algorithm	Test
AES	KAT (encryption/decryption)
Triple-DES	KAT (encryption/decryption)
SHS	KAT
HMAC	KAT
SP800-90A DRBG	KAT
	Continuous Random Number Generator test
NDRNG	Continuous Random Number Generator test
RSA	KAT
ECC CDH	Shared secret computation
Firmware integrity	RSA
Firmware update	RSA

7. Physical Security

The cryptographic module consists of production-grade components. The enclosure of the cryptographic module is opaque within the visible spectrum. The removable covers are protected

with tamper-evident seals that leave residue when peeled from the surface of application. The labels have unique serial numbers which can be used to track a specific label or set of labels in terms of position and orientation to further detect attempts to cover up physical device interference. The tamper-evident seals are applied at the factory. The tamper-evident seals must be inspected periodically by the Crypto Officer. If the tamper-evident seals are missing or there are other signs of tampering, the Crypto Officer must take necessary steps as called for in the organizational security policy and procedure. The steps must include zeroization and making the module non-operational.

8. References

Table 8: 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 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[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

Reference	Specification
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions