National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

TippingPoint Technologies, Inc.
UnityOne™ Version 1.2

Report Number: CCEVS-VR-03-0045

Dated: 21 August 2003

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jandria Alexander

John Nilles

The Aerospace Corporation

Columbia, Maryland

William Jones

National Security Agency

Ft. Meade, Maryland

Common Criteria Testing Laboratory

Cable and Wireless

Sterling, Virginia

Table of Contents

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of the TippingPoint, Technologies Inc. UnityOne ™, Version 1.2 intrusion detection system. The evaluation was performed by the Cable and Wireless (C&W) Common Criteria Testing Laboratory. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by C&W and submitted to the validators. The evaluation determined that the product conforms to the Common Criteria Version 2.1, Part 2 extended and Part 3.

The TOE is a TippingPoint Technologies intrusion detection system that monitors network data flows for inappropriate, incorrect, or anomalous activity. UnityOne ™ performs the IDS functionality of a scanner, sensor and analyzer. It uses two detection techniques: static signatures and anomaly algorithms. Signatures are used to detect indications of known attacks. Anomaly algorithms detect types of attacks rather than known implementations of the attack. The TOE consists of the following logical components: the Network Discovery (ND), the Intrusion Protection System (IPS), the Local Security Manager (LSM), the Command Line Interface (CLI), the UnityOne™ OS (operating system), and the UnityOne™ hardware.

The IPS and ND interact with each other through a central component, the Local Security Manager (LSM) agent. The two components report observed events to the LSM agent and the LSM agent takes action based upon the preconfigured administrative settings. The LSM agent also reports this information on the LSM console, through which the authorized administrator is able to monitor and review observed events.

The validation team observed the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team's observations support the conclusion that the product satisfies the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that the findings of the evaluation team are accurate, and the conclusions justified.

2 IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if applicable);
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	TippingPoint Technologies, Inc. UnityOne™ Version 1.2
Protection Profile	Intrusion Detection System Analyzer Protection Profile, Version 1.1, December 10, 2001; Intrusion Detection System Scanner Protection Profile, Version 1.1, December 10, 2001; Intrusion Detection System Sensor Protection Profile, Version 1.1, December 10, 2001; Intrusion Detection System System Protection Profile, Version 1.4, February 4, 2002.
Security Target	TippingPoint Technologies, Inc. UnityOne™ Version 1.2 Security Target, Version 2.3
Evaluation Technical Report	TippingPoint Technologies, Inc. UnityOne™ Version 1.2 Evaluation Technical Report, Version 1.2, 18 August 2003
Conformance Result	Part 2 extended, Part 3 conformant, EAL2

Sponsor	CORSEC Security, Inc.
Developer	TippingPoint Technologies, Inc.
Evaluators	Cable & Wireless
Validators	The Aerospace Corporation The National Security Agency

Table 1: Evaluation Identifiers

3 SECURITY POLICY

The Tipping Point Technologies, Inc. UnityOne™ does not implement a security policy in the traditional sense of enforcing a set of access control rules. The TOE stores and manages all IDS System, Analyzer, Scanner and Sensor records.

The Security Objectives for the TOE state that

- The TOE must protect itself from unauthorized modifications and access to its functions and data.
- The TOE must include a set of functions that allow effective management of its functions and data.
- The TOE must allow authorized users to access only appropriate TOE functions and data.
- The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
- The TOE must respond appropriately to analytical conclusions.
- The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
- The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
- The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
- The TOE must appropriately handle potential audit and Analyzer, Scanner, Sensor, and System data storage overflows.
- The TOE must record audit records for data accesses and use of the Analyzer, Scanner, Sensor, and System functions.
- The TOE must ensure the integrity of all audit and Analyzer, Scanner, Sensor, and System data.
- When any IDS component or the TOE makes its data available to another IDS component, the TOE will ensure the confidentiality of the Analyzer, Scanner, Sensor, and System data.

3.1 Roles

The product supports three roles: the Superuser role, an Administrative role and an Operator role.

- **Superuser** – Full access to the TOE. This role is able to manage the users of the TOE and to view/modify the configuration of the TOE and the logs. This role corresponds to the "authorized administrator" role that is called out in the FMT_SMR.1 requirement in each of the 4 IDS PPs.

- **Administrator** – Write access to the TOE. This role is able to view/modify the configuration of the TOE (with the exception of managing user accounts) and the logs (with the exception of selection of auditable events and clearing of the audit log).

- **Operator** – Read-only access to the TOE. This role is able to view the logs and configuration of the TOE, but is not permitted to modify any information other than his/her own password.

Each authorized user of the TOE is assigned to one and only one role.

A user account cannot be created without an associated role; if this is attempted, the action is denied and the interface enforces that a role be specified before proceeding with account creation.

Superusers are permitted to change their role or the roles of other users.

3.2 Security Management

The TOE provides security management functionality necessary to manage TOE and IDS data. This includes the ability to query TOE data, schedule scans and enable/disable signatures, clearing of Alert, Block, Fault, and System logs, and setting the clock.

4 ASSUMPTIONS

4.1 Usage Assumptions

The evaluation made the following assumptions concerning product usage.

- The TOE has access to all the IT system data and resources it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.

4.2 Physical Assumptions

The evaluation made the following environmental assumptions:

- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.3 Personnel Assumptions

The evaluation made the following personnel assumptions:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

5 ARCHITECTURAL INFORMATION

The TOE consists of six logical components, the Network Discovery, the Intrusion Protection System (IPS), the Local Security Manager (LSM), the Command Line Interface (CLI), the UnityOne™ OS (operating system), and the UnityOne™ hardware. Together the subsystems provide the following security functionality:

- Audit Generation, Selection, Review and Protection
- Identification and Authentication
- Management of Security Functions
- Protection of TOE Security Functions
- Intrusion Detection System data collection, sensing, analysis, reaction and protection.

Network Discovery

The **network discovery (ND)** component of the TOE is used to collect information on a network, including detecting active hosts, the services running on those hosts, and identifying the hosts' operating systems. This is essentially an IDS Scanner.

The Network Discovery Service (NDS) is the primary data collector for IDS system and scanner data. The NDS probes a targeted network through the Data Network Interface for the purpose of detecting services running on machines attached to the targeted network. The NDS utilizes the system-support API to record the collected scanner data to the IDS logs. The NDS supports the scanner data collection by scanning the hosts monitored by the device and storing the results of the scan in an internal database.

Additionally, the NDS scans the hosts monitored by the IDS in order to determine the information about those hosts that relates to IDS functionality. The results of the scans are used to populate a database, which in turn is used by the IDS to determine what signatures apply to which hosts.

Intrusion Prevention System

The intrusion prevention system (IPS) component of the TOE monitors network data flows for inappropriate, incorrect, or anomalous activity. It uses two detection techniques: static signatures and anomaly algorithms. Signatures are used to detect indications of known attacks. Anomaly algorithms detect types of attacks rather than known implementations of the attack. The IPS also compensates for various techniques used to bypass an IPS, such as TCP packet fragmentation. The IPS can be dynamically configured based on the findings of the ND.

Local Security Manager (LSM)

The IPS and ND interact with each other through a central component, the Local Security Manager (LSM) agent. The two components report their findings to the LSM agent and the LSM agent is able to react upon these findings as configured. The LSM agent will pass this information along to the LSM console, an http interface, through which the authorized administrator is able to monitor everything that is happening in real time. If configured to automatically react to new information (such as attacks or a newly detected host), the LSM agent is able to modify the IPS rules based on the newly gathered information.

Command Line Interface (CLI)

In addition to the LSM, the UnityOne™ provides a Command Line Interface to access some security management functions.

UnityOne™ OS (Operating System)

The **UnityOne™** operating system, based on a third-party embedded real-time operating system, provides the basic execution environment for the UnityOne™ product software. The UnityOne™ application relies on the following services the OS provides:

- Boot processing and system initialization;
- File system services;
- Process scheduling services;
- POSIX library implementation;
- Network and other hardware device drivers; and
- Network (TCP/IP, HTTPS) protocol implementations.

UnityOne™ Hardware

The 400/1200/2400 appliance models have a fixed set of 4 (network interfaces). The 2000 system model has a variable ("bladed") set of 5 data segments per blade with a capacity of up to 4 blades, allowing 20 data segments. A firmware switch controls the speed at which a particular appliance model will operate. At boot-up, the software references internal information to determine which model it is and sets the parameter accordingly.

6 DOCUMENTATION

Following is a table of the evaluation evidence issued by the vendor:

Evidence

Category	Title(s)
Security Target	TippingPoint Technologies, Inc. UnityOne™ Version 1.2 Security Target Document Version 2.3, August 14, 2003
Configuration Management	TippingPoint UnityOne™ version 1.2 Configuration Management Description v1.4
Delivery and Operation:	TippingPoint UnityOne™ version 1.2 Secure Delivery and Installation v1.5
	Common Criteria Certified Installation and Configuration Guidelines for UnityOne™ Version 1.2; TECHD-

Category	Title(s)
	0000000030; Publication Control Number 070103
	Quick Start UnityOne™ Intrusion Prevention System; Part Number TECHD-0000000003; Publication Control Number 062603
	UnityOne™ Model 400/1200/2400 Intrusion Prevention Appliance Installation and Configuration Guide Version 1.2; Part Number TECHD -00000000015; Publication Control Number 030503
	UnityOne™ Model 2000 Intrusion Prevention System Installation and Configuration Guide Version 1.2; Part Number TECHD -00000000004; Publication Control Number 021303
	UnityOne™ Command Line Interface Reference Version 1.2; Part Number TECHD-0000000013; Publication Control Number 062503
	UnityOne™ Local Security Manager User Guide Version 1.2; Part Number TECHD-00000000014; Manufacturing Revision A07; Publication Number 021903
	Licensing V1.2; Part Number TECHD-0000000005
Design Documentation:	TippingPoint UnityOne™ version 1.2 Functional Specification v1.9
	UnityOne™ Command Line Interface Reference Version 1.2; Part Number TECHD-0000000013; Publication Control Number 062503
	UnityOne™ Local Security Manager User Guide Version 1.2; Part Number: TECHD-0000000014; Manufacturing Revision:A07; Publication Control Number: 021903
	Common Criteria Certified Installation and Configuration Guidelines for UnityOne™ Version 1.2; TECHD-0000000030; Publication Control Number 070103
	TippingPoint UnityOne™ version 1.2 High-Level Design v1.5
	UnityOS™ Draft High Level Design Document; Pub Number: Not Assigned; Revision unpub 2002-10-28.
	TippingPoint UnityOne™ version 1.2 Informal Correspondence Analysis v1.3
Guidance Documentation:	Common Criteria Certified Installation and Configuration Guidelines for UnityOne™ Version 1.2; TECHD-0000000030; Publication Control Number 070103
	UnityOne™Local Security Manager User Guide Version

Category	Title(s)
	1.2; Part Number: TECHD-0000000014; Manufacturing Revision:A07; Publication Control Number: 021903
	UnityOne™ Command Line Interface Reference Version 1.2; Part Number TECHD-0000000013; Publication Control Number 062503
Test Documentation:	UnityOne™ v1.2 CC test package - June 26 2003.zip.pgp
	TippingPoint Technologies, Inc. UnityOne™ Version 1.2 Functional Specification Manifest Document Version 1.7
Vulnerability and Assessment Documentation:	TippingPoint UnityOne™ version 1.2 Vulnerability Assessment v1.2

7 IT PRODUCT TESTING

7.1 Vendor Testing

At EAL2 testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TSF have been tested."[1]

The vendor testing included at least 1 test for each security function, and included:

- Creation of administrator, superuser, and operator accounts;
- Protection and review of audit log;
- Identification and authentication functionality;
- Configuration of IDS Attack Filters; and
- Detection and logging of intrusion events.

7.2 Evaluator Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation and Startup documentation. The test configuration is depicted in Figure 1 below.

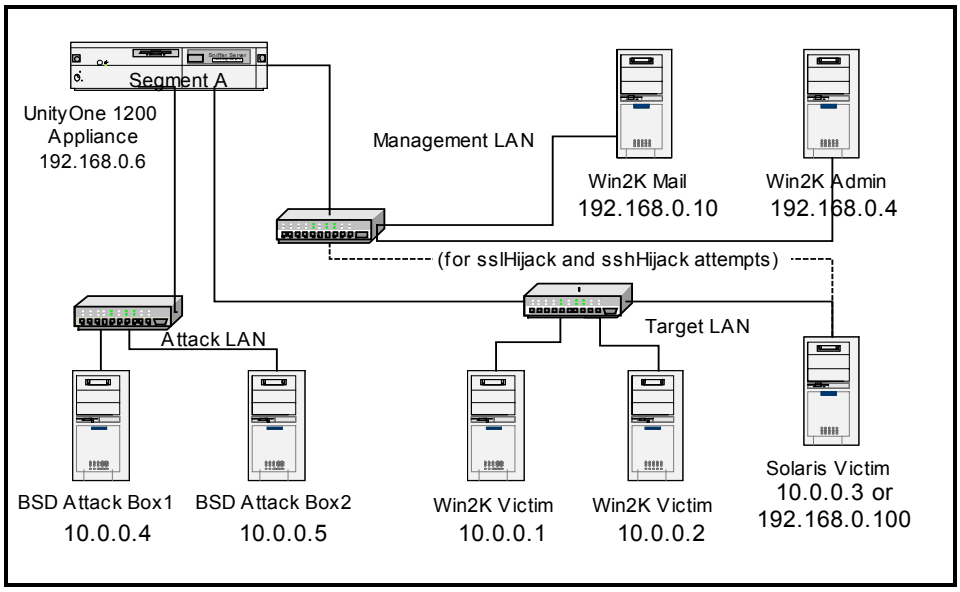

Figure 1

[1] CEM, V1.0, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

Evaluator testing covered the following areas:

- Collection and detection of fragmented and non-fragmented intrusion attacks;
- Detection and Blocking of intrusion attacks;
- TSF Self protection;
- Audit pre- and post-selection;
- Password rule enforcement

8 EVALUATED CONFIGURATION

The evaluation configuration consists of TippingPoint UnityOne™ version1.2 software which can reside in one of four hardware models. Three of these models are identified as appliances and one is identified as a system. These models are identified as follows:

- UnityOne™-400 Appliance (intrusion prevention performed at 400 Megabits per second);
- UnityOne™-1200 Appliance (intrusion prevention performed at 1.2 Gigabits per second);
- UnityOne™-2400 Appliance (intrusion prevention performed at 2.4 Gigabits per second); and
- UnityOne™-2000 System (intrusion prevention performed at 2.0 Gigabits per second).

In addition UnityOne™-intrusion detection system must be installed and operated as described in the Common Criteria Installation and Configuration Guidelines for UnityOne™-Version 1.2.

9 RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [5]; and all applicable National and International Interpretations in effect on 6 December 2001. The evaluation confirmed the product as being Part 2 extended and Part 3 EAL 2 compliant. The details of the evaluation are recorded in the Evaluation Technical Report, which is controlled by the Cable and Wireless CCTL. The evaluation determined the product to be **Part 2 extended conformant, Part 3 conformant,** and to meet the requirements of **EAL 2**. The product was evaluated and tested against the claims presented in the *TippingPoint Technologies, Inc. UnityOne™ Version 2.3 Security Target;* dated 14 August 2003.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

Evaluation of the TippingPoint UnityOne™ V1.2 Security Target (ST) (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the TippingPoint UnityOne™ product that are consistent with the Common Criteria; and product security function descriptions that support the requirements.

Evaluation of the Configuration Management capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items were considered configuration items: TOE implementation, design documentation, test documentation, and user guidance.

Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during these events.

Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the developer strength of function analysis and the developer vulnerability analysis as well as the evaluation team's performance of penetration tests.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy (or veracity) of the claims in the ST.

10 VALIDATOR COMMENTS AND RECOMMENDATIONS

The validators observations support the evaluation teams conclusion that the TippingPoint UnityOne™ V2.1 meets the claims stated in the Security Target. In particular, the product provides the functionality cited in the four Protection Profiles (an IDS Sensor, Scanner, Analyzer and System) to which it claims conformance. However, the TOE is not separable into distinct IDS components , but is only available with the scanner, sensor, analyzer, and system functionality integrated into a single product.

11 SECURITY TARGET

The ST, *TippingPoint Technologies, Inc. UnityOne™ Version 2.3 Security Target;* dated 14 August 2003 is included here by reference.

12 GLOSSARY

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LSM	Local Security Manager
ND	Network Discovery
NDS	Network Discovery Service
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

13 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements; dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes; dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements; dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology; dated August 1999, version 1.0.

[7] TippingPoint Technologies, Inc. UnityOne™ Version 2.3 Security Target; dated 14 August 2003.

[8] TippingPoint Technologies, Inc. UnityOne™ Version 1.2 EAL 2 Team Test Report Version 2.9, Release Date August 4, 2003

[9] TippingPoint Technologies, Inc. UnityOne™ Version 1.2 Functional Specification Manifest Document Version 1.7

[10] UnityOne™ v1.2 CC test package - June 26 2003.zip.pgp

[11] Evaluation Technical Report, for TippingPoint UnityOne™ Ver. 1.2; 18 August 2003

[12] TippingPoint UnityOne™ version 1.2 Vulnerability Assessment.