National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

For

Tripwire Manager ® 3.0 with Tripwire for Servers ® 3.0, Tripwire Manager ® 3.0 with Tripwire for Servers Check Point Edition ® 3.0

Report Number:	**CCEVS-VR-03-0035**
Dated:	**February 27, 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
Richard White
Mitretek Systems Inc.,
Falls Church, VA

Common Criteria Testing Laboratory

Evaluation Team
Cable and Wireless, Inc.
45901 Nokes Boulevard
Sterling, VA 20166

Table of Contents

1 Executive Summary

The evaluation of the Tripwire Manager ® Version 3.0 with Tripwire for Servers ® Version 3.0, and Tripwire Manager ® Version 3.0, with Tripwire for Servers Check Point Edition ® Version 3.0 was performed by Cable & Wireless CCTL in the United States and was completed on 17 February 2003. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Tripwire Manager ® product by any agency of the US Government and no warranty of the product is either expressed or implied.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The Cable & Wireless evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL1) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by Cable & Wireless.

1.1 Evaluation Details

Dates of Evaluation: September 05, 2002 through February 17, 2003
Evaluated Products: Tripwire Manager ® Version 3.0, Tripwire for Servers ® Version 3.0, and Tripwire for Servers Check Point Edition ® Version 3.0.
Developer: Tripwire Inc.
CCTL: Cable & Wireless Inc., Sterling VA
Validation Team: Richard White, Mitretek Systems Inc.,
Falls Church, VA
Evaluation Class: EAL1
PP Conformance: None

1.2 Interpretations

There are no interpretations that apply to this evaluation.

1.3 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

T.Capture: Eavesdropping data communication
An attacker may eavesdrop on, or otherwise capture, data being transferred between Tripwire for Servers ® and Tripwire Manager ®.

T.Deletion: TOE data deletion
An attacker may attempt to delete or destroy TOE configuration data.

T.Modification: TOE data modification
An attacker may attempt to modify the TOE configuration data.

T.Integrity: IT System data integrity
The integrity of the IT system data may be compromised as a result of an attacker action or due to software, hardware, or user errors.

2. Identification

2.1 ST and TOE Identification

ST: Security Target for Tripwire Manager ® Version 3.0 with Tripwire for Servers ® Version 3.0, and Tripwire Manager ® Version 3.0, with Tripwire for Servers Check Point Edition ® Version 3.0, Version 2.1 February 13, 2003

TOE Identification: Tripwire Manager ® Version 3.0 with Tripwire for Servers ® Version 3.0, and Tripwire Manager ® Version 3.0, with Tripwire for Servers Check Point Edition ® Version 3.0

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

Tripwire is a file system integrity checking tool designed to aid system administrators and users to monitor file system for unauthorized or unexpected modification. Tripwire can assure the integrity of critical data on the system(s) by detecting corrupted or altered files and reporting the occurrence to the system administrators, so corrective actions can be taken.

2.2 IT Security Environment

No requirements are placed on the IT Environment.

3. TOE Security Functions

3.1 Audit

The auditing function provides the ability to generate auditable events for the TOE. These auditable events will include: database initializations, integrity checks, database updates, policy file updates, and TFS commands executed. Each auditable event logged includes: date and time of the event, type of event, host identity, the authenticated OS user, event ID, and event description.

Audit data will be saved in suitable form for the administrator to interpret the information and will be protected from unauthorized deletion. The file protection is provided by changing the permissions for the Tripwire for Servers ® directory and files to full control for authorized administrators only in UNIX. In the Windows environment file protection is provide by giving write and execute permissions only to users who are authorized to administer Tripwire software in Windows (including Tripwire Agent service if it is specified as user). The audit records can be viewed using a proper OS editor.

In addition, the auditing function provides the ability to generate audit reports for violations discovered from the integrity check of a Tripwire for Servers ® machine. The TOE takes a snapshot of the files in a known good state and stores a hash value associated with each file being monitored in the integrity policy file. Violations are identified by comparing objects listed in the integrity policy file against the objects currently existing on the machine. Any object detected to be added, removed, or modified from the existing file system or registry structure is identified as a violation and is included in the audit report.

The following summary information is provided for each audit report:

- number of violations identified,
- maximum severity, total number of integrity errors,
- total number of objects scanned, location of policy file,
- location of configuration file, location of database file,
- location of Tripwire command issued,
- IP address of TFS, and

- date & time of last database update.

Date and time of the creation of the report, TFS host name, TFS host ID, TFS account name responsible for report creation will be part of audit report as well.

For each audit report, the TOE also provides the capability to view the audit reports on the screen and to store them in one, or a combination of, the following formats: HTML, XML, and/or sent via email.

3.2 Access Control

Tripwire for Servers ® uses a number of files to assess system security:

- Policy file (to specify how Tripwire software monitors the system);
- Database file (the center of integrity assessment);
- Report files (records the changes detected during an integrity check that violate the rules in the policy file);
- Configuration file (stores system-specific information that controls Tripwire operation);
- Site Key file and Local Key file (store public and private keys used to sign Tripwire files cryptographically);
- Agent Configuration file (stores information that each machine uses to communicate with the Tripwire Manager ®);
- Authentication Key file (stores the keys Tripwire Agent uses to authenticate connections with Tripwire Manger ®);
- Schedule file (stores scheduling information for integrity check);
- Task file (stores information about completed tasks); and Log file

Tripwire for Server ® implements the Configuration Policy (tw.cfg) and the Agent Configuration Policy (agent.cfg) to set the access rights to these critical security components. For each file, there is a parameter defined in the Configuration file or Agent Configuration file that can be used to set the TFS file permissions.

All these files are stored on the Tripwire for Servers ® machine in binary-encoded and signed form using El Gamal asymmetric cryptography with 1024 bit keys.

Access to the Tripwire files is controlled by the operating systems and additional Tripwire for Servers ® mechanisms. A user must first authenticate to the host operating system by providing the correct identification and authentication token. Additionally, the user must present the appropriate passphrase associated with the key to edit or modify signed Tripwire files.

TFS uses two keys for file encryption:

- Site key – used to protect the policy file and configuration files (*tw.cfg, agent.cfg)*, which can be used across an entire site.
- Local key – used to protect database and report files, which are specific to a particular system.

Additionally, the site key is used to protect the Authentication key file, Schedule file, Task file, and Log File.

When a Tripwire Manager ® sends a command to a Tripwire for Servers ® machine that requires a site or local passphrase, the Manager prompts the user for the Manager passphrase. This passphrase is for authentication to allow the Manager to access and send the appropriate passphrase for the Tripwire for Servers ® machine.

3.3 Authentication

To gain access to the TOE data and functionality, the authorized users must first successfully identify and authenticate themselves via the operating system (UNIX/Windows) login process.

The authentication function provides the definition of the security attributes identified for both the Tripwire Manager ® and Tripwire for Servers ® products. Security attributes for the Tripwire for Servers ® product include the local key and site key along with their associated passphrases. Security attributes for the Tripwire Manager ® product are the manager key along with its associated passphrase.

After successful authentication to the OS, in order to perform the TOE functionality, the user must authenticated to the TFS using the local key & passphrase or site key & passphrase. To authenticate to the TWM, the user must present the manager key & passphrase.

TWM can store the site and local passphrases for each machine registered to that Manager in the file console.dat. The passphrases are stored encrypted using Triple DES with 168 bit keys based on a manager passphrase. The Agent Configuration file stores information that each TFS machine uses to communicate with the TWM. When a TWM sends a command to a TFS machine that requires a site or local passphrase, the Manager prompts the user for the manager passphrase. This passphrase is used to de-crypt the passphrases in console.dat, allowing the Manager to access and send the appropriate passphrase for the Tripwire for Servers ® machine.

3.5 Communications

The communication function provides a secure communication channel between the Tripwire Manager ® and the Tripwire for Servers ® products. All communication between the Tripwire Manager ® and Tripwire for Servers ® machines is protected using the Secured Sockets Layer (SSL) protocol to prevent eavesdropping. The Tripwire implementation of SSL uses 168 bit Triple DES encryption.

The Tripwire Manager ® and Tripwire for Servers ® machines register each other by exchanging public authentication keys to facilitate secure communication. These keys are generated and distributed when each Tripwire for Servers ® machine is added to the Manager.

Once the Tripwire Manager ® and the Tripwire for Servers ® machines have exchanged keys, every time a connection is made between the two, each side authenticates the other by generating a random data packet and requesting that the other side digitally sign it. The signed packet can be verified using the public key of the signer.

Tripwire Manger ® uses the secure communication channel to perform integrity checks, update the database, retrieve audit report, edit configuration file, edit integrity policy file, edit policy enforcement schedule file, and send a request to a Tripwire for Servers ® machine to be registered.

3.6 Integrity Checking

The integrity checking function provides the Tripwire for Servers ® product with the capability of monitoring for any changes in the data stored within the system's file system. This process is provided by comparing hashed values of objects and object parameters stored within the system's most recently updated database against the hashed values of the objects currently in the file system. The list of objects to be monitored is determined by the integrity policy file.

When violations are identified, meaning an inconsistency between the hashed values of any object to be monitored, the details are writing to a report. The TOE stores the report and can send it to an administrator by email. In addition, Tripwire for Servers ® can automatically execute commands defined within the policy file in response to violations, or every time integrity checks are performed. Reviewing the report will help the administrator determine if the violations are actually authorized changes (such as installing an upgrade or new application) or if the changes are considered malicious or unauthorized. Based on that decision, the system administrator can update the database (so changes no longer show up as violations) or take steps to restore the correct files to the system.

4. Assumptions

A.No_Evil_Admin: Trustworthy Administrator

The Administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by TOE documentation.

A.HW/SW/FW_Func: Hardware/Software/Firmware function

The computer systems, software, and associated devices function correctly.

A. Phys_Acs: Physical Access

The TOE is located within a controlled access location that prevents unauthorized physical access by outsiders.

A. Peer: Connectivity to other systems

Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

A.Object_Cont: Object Control

It is assumed that only administrator(s) controls the objects (i.e. programs, scripts, etc) that the TOE calls using automated command execution.

5. Architectural Information

5.1 Overview

The Tripwire software is a data integrity assessment product that can assure the integrity of critical data on system(s) by monitoring the system files for unauthorized or unexpected modification. The TOE accomplishes this by detecting the corrupted or altered files and reporting the occurrence to the system administrators, so corrective actions can be taken. The following diagram describes in general terms the steps of checking the data integrity using Tripwire software.

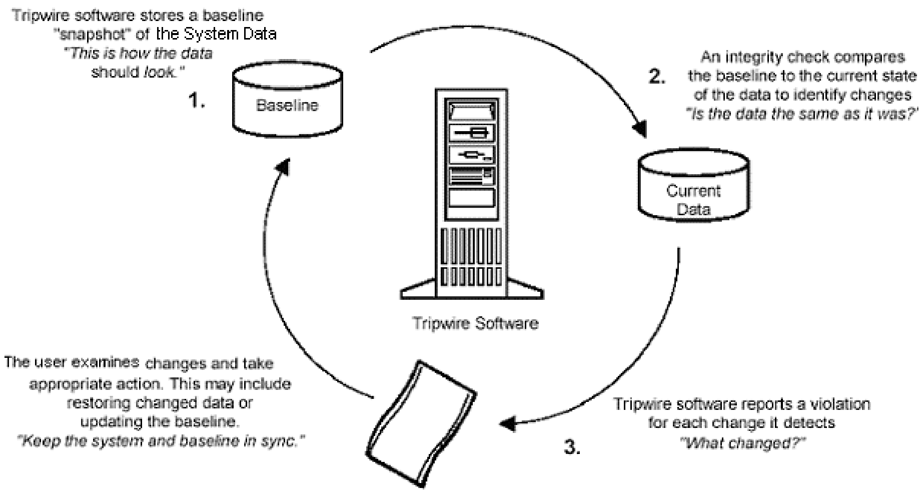
Tripwire software stores a baseline
"snapshot" of the System Data
"This is how the data should look."
1.
Baseline
2.
An integrity check compares the baseline to the current state of the data to identify changes
"Is the data the same as it was?"
Current Data
Tripwire Software
The user examines changes and take appropriate action. This may include restoring changed data or updating the baseline.
"Keep the system and baseline in sync."
3.
Tripwire software reports a violation for each change it detects
"What changed?"

Figure 1: Process of checking the data integrity using Tripwire software

Based on the configuration, the Tripwire software creates a baseline snapshot of the system data in a known good state.

After the baseline is established, the Tripwire software can regularly check the integrity of the system data. During an integrity check, Tripwire software compares the current state of data to the baseline and reports a violation or any change it detects.

The administrator (user) examines report files to evaluate changes to the system data and to take appropriate measures such as:

a. If the changes are considered malicious or unauthorized, then the system administrator may take steps to restore the correct files to the system.

b. If the changes are acceptable, than the baseline database can be updated to include them so that Tripwire software no longer detects them as violations.

5.2 Tripwire for Servers ®

Tripwire for Servers ® (TFS) is a self-contained integrity assessment system that can be installed on each machine that needs to be monitored. The TFS automatically verifies data and file integrity against a known good state in the Tripwire database and quickly notifies the administrator of any changes. The Tripwire for Servers ® software engine conducts subsequent file checks, automatically comparing the state of the system with the baseline database. Any inconsistencies are reported to Tripwire Manager ® and to the host system's log file. Reports can also be emailed to an administrator. In addition, Tripwire for Servers ® can execute commands automatically in response to violations, or every time when integrity checks are performed. If a violation is actually an authorized change (such as installing an upgrade or new application), a user can update the database so changes no longer show up as violations.

Tripwire for Servers ® detects changes to the system data, whether from outside the organization or from within it. Tripwire for Servers ® software can be used in the same way, whether it is used in conjunction with Tripwire Manager ® to manage the machines or managed by issuing commands from the command line.

5.3 Tripwire for Servers Check Point Edition ®

Tripwire for Servers ®, Check Point Edition ® (TFS CPE) establishes a baseline of data in known good state, detects and reports changes to the baseline, and enables rapid discovery and remediation when an undesired change occurs. It provides verification of the integrity of data within Check Point VPN-1 ® and Firewall-1 ® software against integrity violations. Such data may include: logs, firewall rules, configurations, or allowed VPN connections.

Tripwire for Servers CPE ® provides the capability to use Check Point Log Viewer as a means to review integrity checks run by Tripwire software; however, this functionality was excluded from this evaluation. All functions that the Tripwire of Server ® product uses to review the integrity check reports are also available in Tripwire for Servers CPE ®. Aside from the option to integrate Tripwire for Servers Check Point Edition ® with the Check Point ® Log Viewer, TFS CPE, and Tripwire for Servers ® provide the same security functions, and are therefore considered the same for this evaluation.

5.4 Tripwire Manager ®

Tripwire Manager ® (TWM) is a Java-based application with a graphical user interface (GUI) that allows the administrator to manage multiple installations of Tripwire for Servers ® software from a central location. The most basic configuration is a single Manager that controls all Tripwire for Servers ® machines.

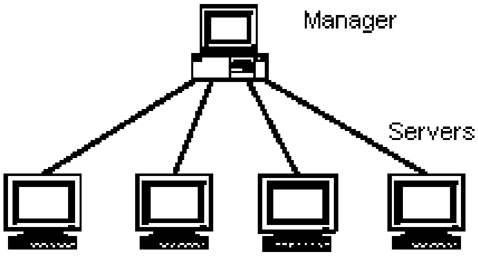

Figure 2: Tripwire configuration with one Manager

Multiple Managers can connect to the same Tripwire for Servers ® machine. However, only one Manager can issue commands to a Tripwire for Servers ® machine at a time.

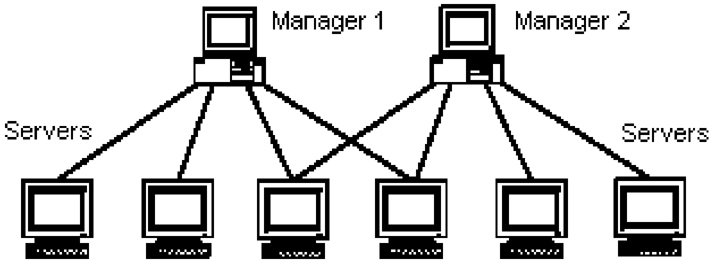

Figure 3: Tripwire configuration with multiple Managers

Tripwire Manager ® can manage many Tripwire for Servers ® installations from a central management console, from which an administrator can view and manage reports from all Tripwire-equipped machines. Secure Sockets Layer (SSL) is used to protect each communication link between the Tripwire Manager ® console and the Tripwire for Servers ® agents.

5.5 Logical Boundaries

Tripwire for Servers ® is an application for checking the integrity of stored data within a server's file system (or Windows registry). When violations are identified, audit reports are generated identifying the violations discovered from the integrity check of a Tripwire for Servers ® machine(s). Tripwire for Servers ® also generates auditable events for database initializations, integrity checks, database updates, policy file updates, and commands executed. Each auditable event includes the date and time of the event, event type, subject identity, and outcome of the event. All auditable events are stored and time stamped by the Tripwire for Servers ® underlying operating system.

Tripwire Manager ® allows the administrator to manage multiple installations of Tripwire for Servers ® software from a central location. The functions performed include performing integrity checks, updating the database, retrieving an audit report, editing the configuration file, editing the integrity policy file, and editing the policy enforcement schedule file.

As the Tripwire software is used to establish the security of machines throughout the network, it must itself be protected from intruders. The Tripwire Manager ® system provides internal security by using a combination of techniques, including Secured Sockets Layer technology, cryptographic signatures, and authentication.

All communication between the Tripwire Manager ® and Tripwire for Servers ® machines is protected using the Secured Sockets Layer (SSL) protocol to prevent eavesdropping. The Tripwire implementation of SSL uses 168-bit Triple DES encryption.

To prevent tampering and to protect against unauthorized modification, Tripwire files (policy file, database file, configuration file, site key file, local key file, agent configuration file, and (optionally) report files) on each Tripwire for Servers ® machine are stored on disk in a binary-encoded, signed form, using El Gamal asymmetric cryptography with 1024 bit keys. The Tripwire Manager ® and Tripwire for Servers ® machines register each other by exchanging public authentication keys to facilitate secure communication. These keys are generated and distributed when each Tripwire for Servers ® machine is added to the Manager.

Cryptographic techniques do not protect against all attacks, such as the deletion of Tripwire data files. For maximum security, important files are protected by the operating system enforcing access controls for authorized administrators only.

Every communication between the Tripwire Manager ® and Tripwire for Servers ® machines is authenticated, allowing each party to verify the identity of the other. Tripwire Manager ® can store the site and local passphrases for each machine registered to that Manager, and when it does, the passphrases are stored encrypted using Triple DES with 168 bit keys based on a Manager passphrase. Because the Manager passphrase controls access to all the machines on the network, neither the passphrase nor the 168 bit key that it generates is permanently stored on disk. Instead, they are stored encrypted in the buffer for 5 minutes after the Manager passphrase is entered, and it is required to periodically re-enter the passphrase.

5.6 Physical Boundaries

The complete TOE can consist of two physically separate machines to which are installed the Tripwire for Servers ®, and the Tripwire Manager ® products. Both products can also be installed on the same machine. Both products are software applications that reside on top of the operating system platform. With this in mind, the sole definition of the TOE includes both Tripwire software application components and their underlying Operating System(s).

The physical computers and network interfaces related to the product are outside the scope of this TOE.

The installation configuration of the TOE is as follows:

- Tripwire Manager ® with Tripwire for Servers ®
- Tripwire Manager ® with Tripwire for Server Check Point Edition ®.

This diagram shows the TOE boundary when the Tripwire products are installed on separate servers (a typical configuration).

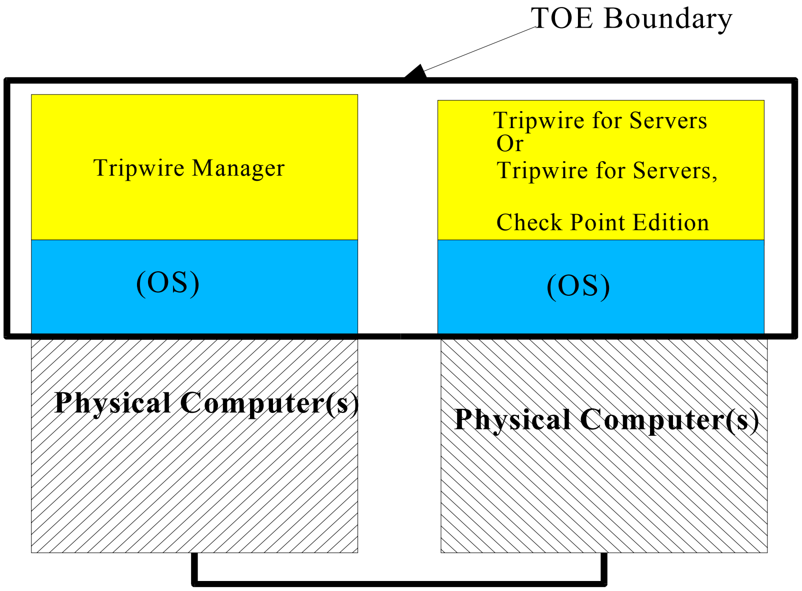

Figure 4: TOE Boundary

6. Documentation

Purchasers of the Tripwire Manager ® Version 3.0, Tripwire for Servers ® Version 3.0, and Tripwire for Servers Check Point Edition ® Version 3.0 will receive all OEM instruction and documentation manuals necessary for proper installation, maintenance, and secure use on the specifically requested platform.

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

As this was an EAL 1 evaluation, developer testing was not supplied as part of the documentation.

7.2 Evaluation Team Independent Testing

The Evaluation Team developed independent test sets that covered a range of conditions: some simply verify administrative or user guidance; some exercise boundary conditions that have been troublesome in other products; and some are highly technical flaw hypotheses that seem applicable to Tripwire Manager ® 3.0 with Tripwire for Servers ® 3.0, Tripwire Manager ® 3.0 with Tripwire for Servers Check Point Edition ® 3.0 platforms. As these scenarios were conducted, the actual tests performed by team members were documented in more detail along with the expected and actual test results. Any associated procedures have also detailed and documented. A total of seven different test configurations were tested. Each configuration was a single instance of the TOE installed on various platforms. Complete test configurations are contained within sections 4 & 5 of the Tripwire Manager ® 3.0 with TFS 3.0, Tripwire Manager ® 3.0 with TFS CPE 3.0, Test Report, January 21, 2003.

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

8. Evaluated Configuration

The evaluated configurations consisted of Tripwire Manager ® 3.0 with TFS 3.0, Tripwire Manager ® 3.0 with TFS CPE 3.0 running on one of the operating systems specified in the table below.

Configuration Name	Hardware Platform	Software Platform
Tripwire for Servers on Windows	Compaq Proliant 1850R	Windows 2000 with TFS 3.0
Tripwire for Servers CPE on Windows	Compaq Proliant 1850R	Windows 2000 with Check Point NG and TFS CPE 3.0
Tripwire Manager on Windows	Compaq Proliant 1850R	Windows 2000 with Tripwire Manager 3.0
Tripwire for Servers on UNIX	Sparc Ultra 5	Solaris 8 (32-bit) with patches with TFS 3.0
Tripwire for Servers CPE on UNIX	Sparc Ultra 5	Solaris 8 (32-bit) with patches with Check Point 4.1 and TFS CPE 3.0
Tripwire Manager on UNIX	Sparc Ultra 5	Solaris 8 (32-bit) with patches with Tripwire Manager 3.0

9. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL1 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Conclusions and Recommendations, in the Evaluation Team's ETR, Part 1, states:

"The TOE was evaluated against the ST and was found by this evaluation team to be conformant with the ST. The TOE was found to be CC Part 2 Extended and Part 3 Conformant. The overall verdict for this evaluation is a Pass."

10. Validation Comments/Recommendations

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11. Abbreviations

Abbreviations	Long Form
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSP	Functional Specification
I&A	Identification and Authentication
OR	Observation Report
QA	Quality Assurance
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Abbreviations	Long Form
TSFI	TOE Security Function Interface
TSS	TOE Summary Specification

12. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.