National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Gilian Technologies, Incorporated
G-Server Version 2.5

Report Number: CCEVS-VR-03-0044
Dated: 11 August 2003

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

Paul Bicknell
The MITRE Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory

CygnaCom Solutions, an Entrust Company
McLean, Virginia

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the CCEVS evaluation of Gilian G-Server. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by CygnaCom Solutions, an Entrust Company and was completed on August 11, 2003. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by Cygncom and submitted to the validator. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 1, resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The Gilian G-Server under evaluation is Version 2.5.

The Target of Evaluation (TOE) includes the G-Server Series 200XL machine with no bypass card, running G-Server Version 2.5 software, including the Maintenance Tool, Administration Tool, Signing Tool, and also the G-Agent.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that CygnaCom's findings are accurate, the conclusions justified, and the conformance results correct.

Disclaimers: The information contained in this Validation Report is not an endorsement of Gilian G-Server by any agency of the U.S. Government and no warranty of Gilian G-Server is either expressed or implied. In addition, the cryptography used in the Gilian G-Server 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.

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 who desire 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 organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Gilian G-Server Version 2.5
Protection Profile	None
Security Target	Gilian G-Server Version 2.5 Security Target, Version 1.0, July 30, 2003
Evaluation Technical Report	Evaluation Technical Report for Target of Evaluation Gilian G-Server Version 2.5, Version 1.3, August 7, 2003
Conformance Result	Part 2 conformant, Part 3 conformant, and EAL 1
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable National and International Interpretations effective on May 5, 2003
Version of CEM	CEM Version 1.0 [5], [6] and all applicable National and International Interpretations effective on May 5, 2003
Sponsor	Standards Institution of Israel
Developer	Gilian Technologies, Inc.
Evaluators	CygnaCom Solutions, an Entrust Company Ms. Robin Medlock Mr. Steve Brackin
Validators	Mr. Paul Bicknell (The MITRE Corporation)

3 SECURITY POLICY

The Gilian G-Server is an appliance that is placed between one or more Web Servers and connections to external networks (see Figure 1). Its purpose is to detect and prevent invalid data from being sent out from Web Servers that have arranged to be protected by the G-Server. Requests for Web Server actions made by End-Users from the external network are intercepted by the G-Server, are inspected and if permitted, are forwarded to the Web Servers on the protected, internal, network. Server responses from the protected Web Servers are also inspected, and if determined to

be valid by the G-Server, are released onto the external network. In the event that invalid responses are issued by a protected Web Server, generic responses can be released to the external network in their place.

To accomplish its functions, the Gilian G-Server recognizes three distinct groups of subjects: Protected-Sites, End-Users, and Administrators. The Protected-Sites are Web Server hosts on the internal network that attempt to send responses to End-Users on external networks in response to incoming HTTP requests. The End-Users are entities on external networks that send HTTP and HTTPS requests to Protected-Sites via the TOE. Administrators are privileged users that interact directly with the TOE, using specific administrative tools to configure and manage the TOE. Protected-Sites and End-Users are subject to information flow control and Administrators are subject to access control.

The Gilian G-Server provides integrity validation services for static and dynamic web pages. Protections are established by the Administrator registering hashed and digitally signed records of static protected web pages in the TOE. Responses to requests from End-Users are compared against the signed records and if found to be valid are returned to the End-Users. Responses that are not valid, and which may indicate some sort of security breach at a protected Web Server, result in the creation of alarm messages and other alerts. However, a copy of the original web page is returned to the End-User without their being notified that anything out of the ordinary has occurred.

Dynamic web pages are also protected by registering hashed and digitally signed records of scripts or programs that generate dynamic Web Server responses. On receipt of a request for a dynamic web service protected Web Servers, via the G-Agent, send a signed image of the script or program to the TOE where it is validated against a pre-established image. Any differences will cause alerts to be created and a generic response to be sent to the End-User.

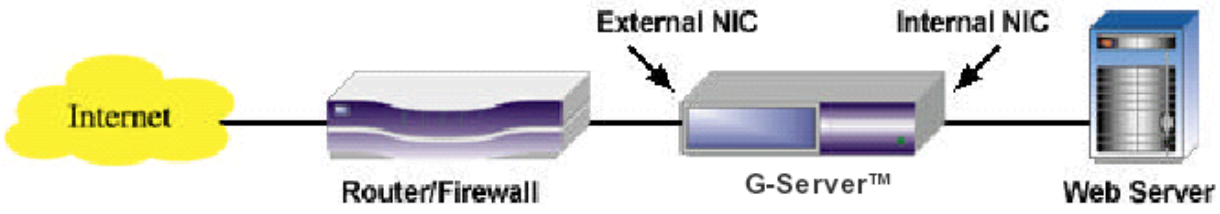

Figure 1: Traffic Mediation Architecture

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 Usage Assumptions

The evaluation made the following assumptions concerning product usage:

- Administrators may establish connections with the TOE either from a directly connected terminal or from an administration workstation located on either the internal or external networks and the administrative workstation is part of the TOE.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- There is no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The TOE does not host public data other than pre-established generic response information.

4.2 Environmental Assumptions

The evaluation made the following environmental assumptions:

- The TOE is physically secure.
- Information cannot flow among the internal and external networks unless it passes through the TOE.
- Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

4.3 Clarification of Scope

Gilian G-Server provides a level of protection that is appropriate for protecting the contents of requests for service that are submitted by external End-Users to protected internal Web Servers. G-Server is not designed to provide protection to Web Servers from End-Users located on the same, internal, network. Likewise, G-Server is not designed to provide any protection unless the network is configured so that all information flows that are controlled by TSP pass through the TOE.

All TOE security objectives, categorized as either Security Objective for the TOE or Security Objectives for the Environment, reflect the stated intent to counter identified threats in light of specific assumptions.

5 ARCHITECTURAL INFORMATION

This section provides a high level description of the TOE and its subsystems as described in the Gilian G-Server 2.5 design documentation.

Gilian G-Server provides six security functional services in the TOE, TSF Protection, Exit Control, Entry Control, Security Management, Audit, Alerts, and Trusted Path Channel. Together these security functions provide the following protections:

- Audit Generation, Review, and Protection
- Information Flow Policy Enforcement
- Identification and Authentication

- Management of Security Functions
- Protection of TOE Security Functions

5.1 TOE Security Functions

The following subsections describe the security functions of the TOE that provide the protections listed above.

5.1.1 TSF Protection Function

The TSF Protection security function is provided by the operating system, and a proprietary networking subsystem that allows the G-Server to be transparently inserted between end-users and protected sites. The G-Server is an application-level service running on a Microsoft Windows 2000 server SP3. It uses the capabilities provided by Windows for file and process management services. No non-G-Server applications are allowed to run on the Windows system.

The proprietary networking subsystem is logically and physically placed between internal protected Web Servers and the external network. The G-Server has two, physically distinct, network connections, one of the protected internal network and one for the unprotected external network. Every network packet received on the external interface is examined by the G-Server. Traffic is separated into three categories: Mediated; Fast-Forward; and Administrative. Mediated traffic consists of HTTP and HTTPS requests for services from protected Web Servers. Such traffic is processed for security policy enforcement by the G-Server. Fast-Forward traffic consists of traffic that is outside the TSC, i.e., HTTP/HTTPS that is not intended for a protected Web Server, or is other IP traffic. Fast-Forward traffic is directly sent to the internal network interface for release onto the internal network. Administrative traffic is traffic directed at the G-Server itself and can arrive from either the external or the internal network. It is distinguished by specific G-Server IP and port numbers and this traffic results in administrative services being initiated.

5.1.2 ExitControl

The central security function provided by the G-Server is that of ExitControl, namely the control of information flow from protected sites on the internal network for release onto the external network. Protection is offered for both static and dynamic resources. Static resources are protected by the G-Server recording security attribute information about the resource, as well as recoverable instances of the resource itself. When a resource request is received from the external network a request identifier is recorded by the G-Server prior to forwarding the request to the internal network. Once the response from the protected Web Server is received, security attributes of that response are compared against attributes the G-Server previously stored (done at a prior time when protections were initialized). If the attributes compare and an open request identifier exists the response is released to the external network by the G-Server. In the event that the security attributes do not match then the recoverable instance of the resource is released to the external network in place of the response from the Web Server. Audit entries are also created and processed.

In the case of a dynamic resource, similar processing takes place. However, a difference is that recoverable instances of dynamic resources cannot be stored on the G-Server. Also the security attributes of the resource have a different form and are not of the resource itself but are derived from the process or script that creates the resource. Whenever differences in the attributes of a resource

are detected by the G-Server, assisted by the G-Agent that is running on the protected server to create representations of processes or scripts for use in attribute checking by the G-Server, a default error response is returned to the requestor on the external network. Appropriate audit records and audit record processing also takes place.

5.1.3 EntryControl

An additional security function provided by the G-Server is EntryControl where requests received from the external network can be examined for certain information that may indicate hostile intentions by users on the external network. When an HTTP request is received by the G-Server for a protected site, it can be tested against a set of predefined signature patterns. When an anomalous request is detected, the connection is closed, and audit record processing is performed. Administrators can define certain predefined request limits or constraints on request properties. EntryControl mechanisms can also analyze requests looking for predefined attack signatures coded as strings. These patterns can be matched to HTTP headers, the query, the content part of the HTTP request, or the URL (Universal Resource Locator). EntryControl provides the capability to detect known attacks that can be characterized by recurring string patterns in a request.

5.1.4 Security Management

Security Management is provided in the G-Server with the establishment of three security roles: G-Master; Signer; and Viewer. The G-Master is the primary G-Server administrator, is responsible for initial setup and system management, and uses the G-Server Maintenance Tool on the G-Server console or the client-server G-Server Administration Tool running on a remote workstation. Using either of these tools the G-Master initializes the G-Server, establishes protected sites and resources, and configures protections. The Signer utilizes the G-Server Signing Tool to initialize security attributes of protected resources. This function can also be done by the G-Master with the Maintenance or Administration Tools. The third security role can only view settings and audit records, they have no ability to enter or change security-related information. Identification and Authentication is performed using user identifiers and passwords. Audit records of security role actions are captured.

5.1.5 Audit

The G-Server maintains comprehensive audit trails composed of four different logs:

- The **System Log** contains events related to G-Server functionality and a record of TOE administration events;
- Site **Signing Log**s contain resource management events such as resource signing;
- Site **Verification Log**s contain information flow events that match administrator-defined event logging patterns.
- The **Alerts Log** contains Alerts that were triggered by the ExitControl and EntryControl mechanisms;

The logs can be viewed, filtered, and sorted. The administrator can export the log to an external file, and can purge the log. Log sizes are configurable by the administrator.

5.1.6 Alerts

The G-Server supports two levels of alerts: G-Server alerts, such as requested attempts to log in with a bad password; and site alerts, such as notifications about resource security attribute check failures. G-Server alerts include errors related to problems in the system itself. The three types of Alerts

mechanisms exist: Email Alerts; SNMP Alerts; and Execution of Preinstalled Executables. The E-mail Alert sends an e-mail alert to a predefined list of recipients when security attribute check failures are detected. The SNMP (Simple Network Management Protocol) G-Module sends alert messages to an external device, such as a Network Management System or a pager, when security attribute check failures are detected. The Executables Alert can trigger commands in other applications installed on the G-Server, such as an audible alarm or an instant messaging program, when a security attribute check failure is detected. This is determined by the exception and verification rules for the site.

5.1.7 Trusted Path/Channel

When an administrator accesses the G-Server using the Administration Tool or the Signing Tool, the G-Server sets up a trusted channel between the client and the server. Integrity and confidentiality protection are achieved using the Secure Sockets Layer (SSL) protocol. Once the session has been established, the client signs a server challenge using the administrator's password protected private key, authenticating the administrator.

6 DOCUMENTATION

This section provides a complete listing of the documentation that was issued by the developer (and sponsor).

Design documentation:

1) Introduction, Version 1.03, July 15, 2003.
2) Alert Log Functional Specifications, Version 1.04, July 15, 2003.
3) Application Protection G-Module Functional Specifications, Version 1.03, July 15, 2003.
4) Email G-Module Functional Specifications, Version 1.03, July 15, 2003.
5) Executables G-Module Functional Specifications, Version 1.03, July 15, 2003.
6) G-Agent Functional Specifications, Version 1.04, July 13, 2003.
7) GHTTP & Management Module Functional Specifications, Version 1.05, July 13, 2003.
8) G-Server G-Modules Functional Specifications, Version 1.03, July 15, 2003.
9) HTTP[S] Session Management Functional Specifications, Version 1.04, July 13, 2003.
10) Logging G-Module Functional Specifications, Version 1.04, July 15, 2003.
11) Management Sessions and Authentication Functional Specifications, Version 1.04, July 15, 2003.
12) Platform Functional Specifications, Version 1.03, July 21, 2003.
13) Recovery G-Module Functional Specifications, Version 1.03, July 15, 2003.
14) Redirect G-Module Functional Specifications, Version 1.03, July 15, 2003.
15) Signature Management Functional Specifications, Version 1.06, July 15, 2003.
16) SNMP G-Module Functional Specifications, Version 1.03, July 15, 2003.
17) Transparency Envelope Functional Specifications, Version 1.04, July 13, 2003.
18) User Management Functional Specifications, Version 1.03, July 15, 2003.

Guidance documentation:

1) G-Server User Guide, Version 2.5, August 2003.

Delivery and Operation documentation:

1) G-Server Installation and Getting Started Guide, Version 2.5, April 2003.

Security Target:

1) Gilian G-Server Version 2.5 Security Target, Version 1.0, July 30, 2003.

7 IT PRODUCT TESTING

7.1 Evaluator Testing

The evaluators performed testing based on a test suite developed to cover the Security Functional Requirements and Security Functions as documented in the Gilian G-Server Version 2.5 Security Target, Version 1.0, and to test the Target of Evaluation (TOE) to the degree that was consistent with the EAL 1 level of assurance. The objective was to demonstrate that the TOE security functions perform as specified and to confirm that the TOE security functional requirements are met.

The testing involved the Gilian G-Server appliance, G-Server 200XL, with no bypass card and the following tools pre-installed. (G-Server was configured in Single Mode as part of testing.) It included:

- Maintenance Tool,
- Administration Tool,
- Signing Tool, and
- CCTL provided resources:
  - Monitor,
  - Keyboard, and
  - Mouse

It also utilized two CCTL-provided Web Servers:

- An Apache version 1.3 website running on Red Hat Linux 6.2, installed on a Dell Optiplex GX110, with G-Agent software installed, and configured to support the HTTP protocol.
- An IIS version 5.0 website running on Windows 2000 Server, installed on a Dell Optiplex GX1, configured to support the HTTPS protocol, and
- A Dell Latitude C600 laptop computer running Windows NT Workstation 4.0 with Internet Explorer version 5.5. (The following G-Server software was installed as part of testing: Administration Tool, Signing Tool.)

Tests were created to cover most, but not necessarily all, of the security functions identified in the Security Target TOE Summary Specification. During the ADO evaluation activities, it was

concluded that most of the security functions could be tested by following the instructions described in the Installation, Generation, and Start-up documentation. However, additional tests were developed to augment these tests; for example, tests were added to verify role separation and entry control functions, to verify areas that were not were not otherwise adequately covered. Together these two test suites were considered to be sufficient for the evaluation assurance level.

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.

8 EVALUATED CONFIGURATION

The evaluated configuration consists of a G-Server Series 200XL machine with no bypass card, running G-Server Version 2.5 software, including the Maintenance Tool, Administration Tool, Signing Tool, and with the G-Agent running on protected Web Server machines.

9 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.1 [1], [2], [3], [4] and CEM version 1.0 [5], [6] and all applicable National and International Interpretations in effect on May 5, 2003. The evaluation determined the product to be Part 2 conformant, and to meet the Part 3 EAL 1 requirements. The details of the evaluation are recorded in the Evaluation Technical Report [8] that is controlled by CygnaCom.

9.1 Evaluation of the Gilian G-Server Security Target (ST) (ASE)

The evaluation team applied each EAL 1 ASE CEM work unit. The ST evaluation ensured that the ST contains description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Gilian product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 1 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE.

9.3 Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 1 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to install, and configure the TOE securely.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a set of functional specification documents. 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.

9.5 Evaluation of the guidance documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE.

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

The evaluation team applied each EAL 1 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 team tests substantiated the security functional requirements in the ST.

9.7 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 independent tests also demonstrates the accuracy (or veracity) of the claims in the ST.

10 VALIDATOR COMMENTS

The Gilian G-Server TOE satisfies the Gilian G-Server Version 2.5 Security Target Revision 1.0, when configured according to the Installation Guides listed in Section 8, and the Gilian G-Server ST is a CC compliant ST.

The cryptography used in the Gilian G-Server 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 SECURITY TARGET

The Security Target, "Gilian G-Server Version 2.5 Security Target Revision 1.0", July 30, 2003 is included here by reference.

12 GLOSSARY

CC	Common Criteria

CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I&A	Identification and Authentication
I/O	Input/Output
IP	Internet Protocol
NIAP	National Information Assurance Program
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation

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] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

[8] Evaluation Technical Report for a Target of Evaluation Gilian G-Server 2.5, Version 1.3, August 7, 2003.

[9] Gilian G-Server Version 2.5 Security Target Revision 1.0, July 30, 2003.