Bodacion Technologies' HYDRA Server 1.4 Security Target
February 14, 2003
Document No. F1-0203-003

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Phone: 301-498-0150
Fax: 301-498-0855

DOCUMENT INTRODUCTION

Prepared By:	Prepared For:
COACT, Inc.	Bodacion Technologies’
9140 Guilford Road, Suite G	18-3 Dundee Rd Suite 300
Columbia, Maryland 21046-2587	Barrington, IL. 60010

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Bodacion Technologies’ HYDRA Server 1.4. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC	Common Criteria
CPCI	Compact Peripheral Component Interconnect
EAL	Evaluation Assurance Level
EIDE	Enhanced Integrated Drive Electronics
EXT3	Third Extended File System (Linux)
FAT32	32-bit File Allocation Table
FLASH	Flashable non-volatile memory
FSP	Functional Specification
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure sockets
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NTFS	New Technology File System
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
RCR	Representative Correspondence
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSS	TOE Summary Specification

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Bodacion Technologies' HYDRA Server 1.4. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.1*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) interpretations through July 16, 2002. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the HYDRA Server 1.4 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target Name

Bodacion Technologies' HYDRA Server 1.4 Security Target

1.1.2 TOE Reference

Bodacion Technologies' HYDRA Server 1.4

1.1.3 Security Target Evaluation Status

This ST is has been evaluated. The results of which can be seen in the ST ETR.

1.1.4 Evaluation Assurance Level

Functional and assurance claims conform to EAL1 (Evaluation Assurance Level 1) from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

1.1.5 Keywords

Internet, Intranet, Web Server, HTTP Server, HTTPS Server, FTP Server and Secure Server

1.2 TOE Overview

This Security Target defines the requirements for the Bodacion Technologies' HYDRA Server 1.4. HYDRA Server 1.4 is an internet server built without an operating system from the ground up to be totally secure. It contains everything you need to run a high-performance, secure Web site including HTTP, HTTPS, and FTP servers, Web-based administration, and Java/JSP capabilities.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the HYDRA Server 1.4 to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

The Bodacion Technologies' HYDRA Server 1.4 is compliant with the Common Criteria (CC) Version 2.1, functional requirements (Part 2) extended and assurance requirements (Part 3) conformant for EAL1.

1.4 Protection Profile Conformance

The Bodacion Technologies' HYDRA Server 1.4 does not claim conformance to any registered Protection Profile.

CHAPTER 2

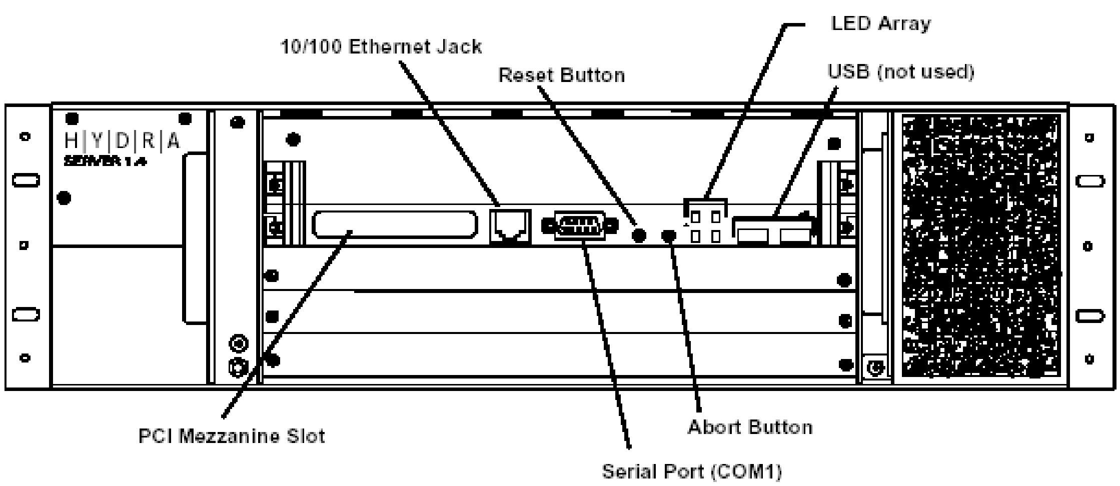
2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 HYDRA Server TOE Description

The Target of Evaluation is the Bodacion Technologies' HYDRA Server version 1.4. HYDRA Server 1.4 is a hard, real-time, embedded system that provides secure Web services including HTTP, HTTPS, FTP, and FTPS. A PowerPC based CompactPCI system card executes HYDRA Server's firmware after loading it into RAM from FLASH memory. The HYDRA Server system card is contained in a standard 3U high CPCI chassis, along with a mass storage shelf containing an EIDE disk drive. This 3U high CPCI chassis has the capability to house and operate three HYDRA Server's. In addition, the HYDRA has the ability to operate with an additional FLASH memory device; a FIPS approved SSL accelerator and a 4-port Ethernet NIC, all which are outside the scope of this evaluation. The HYDRA's firmware will detect if any of these devices are used. The figure below identifies the TOE housed in the CPCI chassis.

Figure 1 - HYDRA CPCI Chassis Front Panel



The HYDRA Server 1.4 eliminates much of the vulnerability in typical web servers through its design. The HYDRA Server 1.4 does not contain a general purpose Operating System; it includes a kernel that operates as a resource manager. The kernel contains no shell or command line that could lead to a hack attack. Since the HYDRA Server 1.4 does not execute on a Hard-Drive, the HYDRA does not contain a standard file system (e.g. EXT3, NTFS, FAT32) that would be vulnerable to virus attacks. The HYDRA Server 1.4 contains a proprietary file system embedded within the hardware/firmware design and is not vulnerable to virus attacks. The HYDRA Server 1.4 was designed to help mitigate vulnerability attacks.

2.1.1 Physical Boundary

The physical boundary of the HYDRA Server includes the entire HYDRA Server PowerPC based CompactPCI system card. On this one system card, the interfaces include a 10/100 Ethernet Jack that connects the HYDRA Server to the internet or intranet. A Serial Port (COM1) that allows for some administrative duties to be performed. LEDs show the status of the HYDRA Server. Restart and Abort buttons that allow the operation of the HYDRA Server to be restarted and halted. A PCI Mezzanine Slot and USB Ports are seen but as not used in the evaluated configuration of the HYDRA Server. The HYDRA Server executes along with a mass storage shelf containing an EIDE disk drive. This hard drive system is within the TOE boundary because it stores the web content that the HYDRA serves.

2.1.2 Logical Boundary

The logical boundary of the HYDRA Server is the entire HYDRA Server PowerPC based CompactPCI system card. The information flow stays within the system card. The HYDRA has the capability to operate without any external devices except the CPCI chassis in that it is housed. The logical structure of the HYDRA Server allows for identification and authentication of the administrators, and allows for a secure trusted path via an HTTPS server and dedicated Serial Port connection. The HYDRA includes a web GUI interface that allows the administrator to configure the TOE. The administrator can also do some initial configuration via a Serial Port connection. Web developer administrators can manage web page content via the FTP connection.

2.2 HYDRA Server Evaluated Configuration

The CPCI chassis has the capability to house multiple HYDRA systems. In the evaluated configuration, only one HYDRA Server will be installed in the chassis. The HYDRA Server will use the mass storage Hard Drive system database for web content storage. The HYDRA has the optional ability to work along side with a FLASH memory device; a FIPS approved SSL accelerator card or a 4-port Ethernet port. In the evaluated version, the HYDRA Server will not use these features. The HYDRA Server will be configured to operate with a test network.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation countered by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organisational security policies for the TOE as appropriate.

Using the above listing, this chapter identifies assumptions (A), threats (T) and organisational security policies (P). For assumptions, threats or policies that apply to the environment, the initial character is followed by a period and then an 'E'. For example, A.E.LOCATE is a security environmental threat of unauthorised physical access.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

3.2.1 Connectivity Assumptions

A.TIME	The HYDRA Server 1.4 shall be connected to an Ethernet interface such that the TOE has access to a NTP timeserver to obtain the current time.

3.2.2 Personnel Assumptions

A.ADMIN	Administrators of the HYDRA Server 1.4 shall be trained and trusted to enforce the security aspects of the HYDRA Server 1.4 relevant to them.
A.SETUP	The security administrator of the TOE shall immediately, upon installation, change the configuration of the TOE so the Web Console GUI operates on a HTTPS server and change the password after the first successful connection to the HTTPS Web Console GUI so it shall remain secure.

3.2.3 Physical Assumptions

A.E.LOCATE The HYDRA Server 1.4 shall be located in a secure facility that mitigates against unauthorised physical access.

A.E.CONSOLE The environment and security mechanisms of the environment must ensure that only an authorised administrator has access to the TOE via the Serial Interface Port.

3.3 Threats

3.3.1 Threats Against the TOE

T.HACK A malicious computer user, or Hacker can compromise the TSF and TOE security through a Hack attack on the Server's operating environment (the HYDRA Server 1.4 Kernel/OS).

T.VIRUS A computer virus could infect the TOE's operating environment's file-system (proprietary file system within the HYDRA Server 1.4) and compromise the TSF and TOE security data.

T.ADMIN A non-administrative user could attempt to configure and manage the TOE/TSF as an administrator.

3.4 Organisational Security Policies

There are no Organisational Security Policies required for the TOE.

CHAPTER 4

4. Security Objectives

4.1 Security Objectives for the TOE

All of the objectives listed in this section ensure that all of the security threats listed in Chapter 3 have been countered. The security objectives (O) for HYDRA Server are:

O.ADMIN The TOE will allow the administrators the capability to securely configure and manage the TOE/TSF data.

O.DESIGN The TOE will be designed in such a way as to prevent unauthorised users and data (i.e. files that could contain a virus) access to the TOE.

4.2 Security Objectives for the non-IT Environment

O.E.ACCESS Those responsible for the TOE must ensure that only users authorised to use the TOE are allowed physical access to the TOE and that the TOE is properly initially configured.

O.E.NET Those responsible for the TOE must ensure that the TOE is physically connected to an Ethernet interface such that it can server web pages, and have access to an NTP timeserver.

4.3 Security Objectives Rationale

Table 1 demonstrates the correspondence between the security objectives listed in Sections 4.1 and 4.2 to the assumptions, threats and policies identified in Sections 3.2, 3.3 and 3.4.

Table 1 - Correspondence Between Assumptions, Threats and Policies to Objectives

Table Legend		
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment		
Assumption, Threat or Policy	**Security Objectives**	**Rationale**
A.TIME – The HYDRA Server 1.4 shall be connected to an Ethernet interface such that it has access to a NTP timeserver to obtain the current time.	O.E.NET – Those responsible for the TOE must ensure that the TOE is physically connected to an Ethernet interface such that it can server web pages, and have access to an NTP timeserver.	The TOE must be connection to a network via the ethernet interface otherwise it cannot performs its primary objective, to serve web pages. The TOE also needs this connection for access to a NTP timeserver.
A.ADMIN – Administrators of the HYDRA Server 1.4 shall be trained and trusted to enforce the security aspects	O.E.ACCESS – Those responsible for the TOE must ensure that only users authorised to use the TOE	The Administrator is the only authorised user of the HYDRA Server 1.4, and is a trusted individual. They will

Table Legend		
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment		
Assumption, Threat or Policy	**Security Objectives**	**Rationale**
of the HYDRA Server 1.4 relevant to them.	are allowed physical access to the TOE and that the TOE is properly initially configured.	have the capability to manage and configure the TOE/TSF data.
A.SETUP – The security administrator of the TOE shall immediately, upon installation, change the configuration of the TOE so the Web Console GUI operates on a HTTPS server and change the password after the first successful connection to the HTTPS Web Console GUI so it shall remain secure.	O.E.ACCESS – Those responsible for the TOE must ensure that only users authorised to use the TOE are allowed physical access to the TOE and that the TOE is properly initially configured.	Upon the intial configuration, the security administrator will configure the TOE to use the HTTPS server for Web Configuration. The security administrator will then change their password following the first login via the HTTPS Web Console GUI so the password will again be secure.
A.E.LOCATE – The HYDRA Server 1.4 shall be located in a secure facility that mitigates unauthorised physical access.	O.E.ACCESS – Those responsible for the TOE must ensure that only users authorised to use the TOE are allowed physical access to the TOE and that the TOE is properly initially configured.	It is the responsibility of those accountable for the TOE to apply appropriate measures to mitigate against possible physical attacks of the HYDRA Server 1.4.
A.E.CONSOLE – The environment and security mechanisms of the environment must ensure that only an authorised administrator has access to the TOE via the Serial Console Port.	O.E.ACCESS – Those responsible for the TOE must ensure that only users authorised to use the TOE are allowed physical access to the TOE and that the TOE is properly initially configured.	It is the responsibility of those accountable for the TOE to ensure that the TOE will be physically off limits for non-administrative users of the TOE. Therefore no non-administrators can gain access to the Serial Console Port connection.
T.HACK – A malicious computer user, or Hacker can compromise the TSF and TOE security through a Hack attack on the Server's operating environment (the HYDRA Server 1.4 Kernel/OS).	O.DESIGN – The TOE will be designed in such a way as to prevent unauthorised users and data (i.e. files that could contain a virus) access to the TOE.	The design of the HYDRA Server 1.4 does not include a standard OS that would include a shell or command line vulnerable to hack attacks.

Table Legend		
A = Assumption, P = Policy, T = Threat, O = Objective, .E = Environment		
Assumption, Threat or Policy	**Security Objectives**	**Rationale**
T.VIRUS – A computer virus could infect the TOE's operating environment's file-system (proprietary file system within the HYDRA Server 1.4) and compromise the TSF and TOE security data.	O.DESIGN – The TOE will be designed in such a way as to prevent unauthorised users and data (i.e. files that could contain a virus) access to the TOE.	The design of the HYDRA Server 1.4 does not include a standard File System that would be vulnerable to virus attacks.
T.ADMIN – A non-administrative user could attempt to configure the TOE as the administrator.	O.ADMIN – The TOE will allow the administrator the capability to securely configure and manage the TOE/TSF data.	Only an authorized administrator can perform management and configuration of on the HYDRA Server 1.4.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 Security Functional Requirements

Table 2 lists the functional and assurance requirements and the security objectives each requirement enforces. All functional and assurance dependencies associated with the components in Table 2 have been satisfied.

Table 2 - Functional Components

CC Component	Name	Hierarchical To	Dependency	Objectives Enforced / Rationale
EXP_FIA_UAU.2	User Authentication before any action	No Other Components	EXP_FIA_UID.2	O.ADMIN – This SFR verifies that the identified administrators are authenticated and are given access to the TSF/TOE data.
EXP_FIA_UID.2	User Identification before any action	No Other Components	None	O.ADMIN – This SFR distinguishes the administrative and non-administrative users from one another by requiring a login ID when accessing the TOE.
FMT_MOF.1	Management of security functions behaviour	No Other Components	FMT_SMR.1	O.ADMIN – This SFR allows the security administrator to configure the TOE.

CC Component	Name	Hierarchical To	Dependency	Objectives Enforced / Rationale
FMT_MTD.1	Management of TSF data	No Other Components	FMT_SMR.1	O.ADMIN – This SFR allows the web developer administrators to manage the TSF data.
FMT_SMR.1	Security Roles	No Other Components	FIA_UID.1	O.ADMIN – This SFR requires the TOE to have administrative and non-administrative users.
FTP_TRP.1	Trusted Path	No Other Components	None	O.ADMIN – This SFR allows for a secure path that will ensure that only trusted administrators have access to the configuration of the TSF/TOE.
ADV_FSP.1	Informal Functional Specification	No Other Components	ADV_RCR.1	O.DESIGN – The Development Assurance Requirements will show that the HYDRA is designed using a bottom up approach that mitigates against virus and hack threats.

CC Component	Name	Hierarchical To	Dependency	Objectives Enforced / Rationale
ADV_RCR.1	Informal Correspondence Demonstration	No Other Components	None	O.DESIGN– The Development Assurance Requirements will show that the HYDRA is designed using a bottom up approach that mitigates against virus and hack threats.

The functional requirements that appear in Table 2 are described in more detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.1* with the exception of italicised items listed in brackets. These bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces.

5.1.1 Identification and Authentication (FIA) (EXP)

Justification: The HYDRA server has three security roles. However, the HYDRA has four classes of users that comprised those three roles. The CC Part 2 requirements for Identification and Authentication are designed for all uses of the TOE, not classes of users, therefore these requirements are explicitly stated for the four classes of users, the non-administrative web user, the web developer administrator and the administrative web based console user and the administrative serial interface user, which comprise the security administrator.

5.1.1.1 EXP_FIA_UAU.2 (EXP) User authentication before any action

Hierarchical to: No other components.

EXP_FIA_UAU.2.1 (1) The TSF shall require each *administrative web based console user* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that *administrative web based console user*.

Dependencies: EXP_FIA_UID.1

Rationale: The HYDRA Server 1.4 requires the administrative web based console user to be authenticated using a password. The administrative web based console user is identified automatically since there is only one security administrator of the TOE. This user has the name *hydra-admin* and is authenticated via the password, but the user name is hard-coded within the HYDRA Server and automatic in the web based administrative console.

EXP_FIA_UAU.2.1 (2) The TSF shall require each *administrative serial interface user* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that *administrative serial interface user*.

Dependencies: EXP_FIA_UID.1

Rationale: The HYDRA Server 1.4 requires the administrative serial interface user to be authenticated using the HYDRA Server 1.4 Enabler Code. The Enabler code is similar to that of a password. The initial enabler code is supplied by Bodacion Technologies. Because it is assumed that the administrator is the only user who has access to through the administrative serial interface port, the dependency of EXP_FIA_UID.1 is met trivially and therefore considered satisfied.

EXP_FIA_UAU.2.1 (3) The TSF shall require each *web developer administrator* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that *web developer administrator*.

Dependencies: EXP_FIA_UID.1

Rationale: The HYDRA Server 1.4 requires the web developer administrator to be authenticated via a password when accessing the TOE via the FTP server. The web developer administrator can either use their respective password for their login, or use an assigned one-time password assigned by the security administrator. One-time passwords are assigned via the Administrative Web Based Console connection, and are only valid for specified users in a specified time frame.

5.1.1.2 EXP_FIA_UID.2 (EXP) User identification before any action

Hierarchical to: No other components.

EXP_FIA_UID.2.1 The TSF shall require each *web developer administrator* to be successfully identified before allowing any other TSF-mediated actions on behalf of that *web developer administrator.*

Dependencies: No dependencies.

Rationale: The HYDRA requires all web developer administrators to be identified via a login name when attempting to access the TOE's administrative FTP Server.

5.1.2 Security Management (FMT)

5.1.2.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *disable, enable*] the functions [assignment: *the web server configuration, and web developer administrator accounts*] to [assignment: *the security administrative user*].

Dependencies: FMT_SMR.1

Rationale: Only authorised security administrators will be able to enable and disable web developer administrator accounts. Only authorised security administrators will be able to configure the web server by means of enable and/or disable of system services, such as the FTP, and HTTP servers.

5.1.2.2 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *modify, delete,* [assignment: *upload web content*]] the [assignment: *web pages and additional web content*] to [assignment: *web developer administrator*].

Dependencies: FMT_SMR.1

Rationale: Only authorised web developer administrators have the access to manage the web content through the FTP Server connection.

5.1.2.3 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *security administrative user, web developer administrators and non-administrative users*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of Identification.

Rationale: The HYDRA Server 1.4 allows for Administrative and Non-Administrative users to access the TOE. Non-Administrative users can access and view web pages on the HTTP and the HTTPS servers. These users are oblivious to the fact that they are using the HYDRA Server, from their standpoint, they are just browsing the World Wide Web. The non-administrative user has no access to the security functionality of the TOE. The Security Administrative User can configure the TOE and must be Identified and Authenticated. The Web Developer Administrator (also known as FTP users in the vendor documentation) can access the TOE via the FTP Server to upload and modify the web pages to which they have administrative access. This Security Functional Requirement's dependency on FIA_UID.1 is satisfied by the explicitly stated requirement, EXP_FIA_UID.2 that requires the users of the TOE to be identified.

5.1.3 Trusted Path/Channels (FTP)

5.1.3.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

FTP_TRP.1.1 (1) The TSF shall provide a communication path between itself and [selection: *remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 (1) The TSF shall permit [selection: *remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 (1) The TSF shall require the use of the trusted path for [selection: [assignment: *administration of the TOE*]].

Dependencies: No dependencies.

Rationale: During administration of the HYDRA Server 1.4, the security administrator can configure the TOE via an HTTPS Web based Administration Console. The SSL encryption makes this path logically different than other ethernet connectivity because all data will be unrecognizable in plaintext.

FTP_TRP.1.1 (2) The TSF shall provide a communication path between itself and [selection: *local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 (2) The TSF shall permit [selection: local *users*] to initiate communication via the trusted path.

FTP_TRP.1.3 (2) The TSF shall require the use of the trusted path for [selection: [assignment: *administration of the TOE*]].

Dependencies: No dependencies.

Rationale: During administration of the HYDRA Server 1.4, the administrator can configure the TOE via a Serial Port Interface. This connection is the only local interface of the TOE for the security administrator. Only one user at a time can use the Serial Port Interface connection based on its design, and that connection is reserved for the security administrator only.

5.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL1. These requirements are summarised in Table 3.

Table 3 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.1	Version Numbers
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Tests	ATE_IND.1	Independent Testing - Conformance

5.3 Security Requirements for the IT Environment

There are no security requirements on the IT environment.

CHAPTER 6

6. TOE Summary Specification

6.1 TOE Security Functions

The major functions implemented by the TOE are:

IDENTIFICATION and AUTHENICATION (I&A)	The TOE performs Identification and Authentication for the administrative user of the TOE. The identification of the security administrator is done automatically and a password is required when the administrator uses the web console and an Enabler Code, which is similar to a password, is required via the Serial Port Interface. Web developer administrators are identified and authenticated by a user name and password when accessing the TOE via the FTP server. Non-administrative users of the TOE are identified via their computers IP address strictly for communication purposes and are not part of the security functionality of the TOE.
SECURE	The TOE provides a trusted communication path to allow the security administrator to configure the TOE. A HTTPS Server allows the security administrator to securely administer the TOE via a web GUI. A dedicated Serial Console connection allows the security administrator to do some preliminary configuration of the TOE.

Table 4 - Functions to Security Functional Requirements Mapping

Functions	Security Functional Requirements	Rationale
I&A	EXP_FIA_UID.1, EXP_FIA_UAU.1, FMT_MOF.1, FMT_MTD.1, FMT_SMR.1	The HYDRA Server requires the administrators of the TOE to be identified and authenticated before management and configuration of the TOE can begin. This can be done multiple ways as discussed above.
SECURE	FMT_MOF.1, FTP_TRP.1	The HYDRA Server supplies a trusted path either through

		an HTTPS Web Administrative Interface or from an isolated Serial Port Connection that allows the security administrator to configure the TOE.

Table 5 shows the mapping between the security functional requirements and the functions listed above.

Table 5 - Security Functional Requirements to Functions Mapping

Security Functional Requirement	Functions	Rationale
EXP_FIA_UAU.1	I&A	The TOE requires the administrators to be authentication before any configuration or management of the TOE is allowed with the use of a password or Enabler Code.
EXP_FIA_UID.1	I&A	The TOE requires the administrators to be identified with a login ID.
FMT_MOF.1	I&A, SECURE	The TOE requires the security administrator to be identified and authenticated before allowing configuration of the TOE. The TOE supplies a trusted path for the security administrator to configure the TOE.
FMT_MTD.1	I&A	The TOE requires the web developer administrators to be identified and authenticated before any management of the web content can take place via the FTP server.
FMT_SMR.1	I&A	The TOE allows for administrative and non-administrative users of the TOE. Security Administrative Users: Can configure the TOE/TSF data through a

Security Functional Requirement	Functions	Rationale
		Serial Port Connection and Administrative web based Console Interface. Web developer administrators: Web developers who have pages and content on the HYDRA Server 1.4 can be granted access to the HYDRA by the Security Administrator and can manage the TSF data through an FTP server. Non-Administrative Users: Are transparent to the fact that they are using the HYDRA Server. These users simply can download and view HTTP and HTTPS web pages. They are oblivious to the fact that the HYDRA Server is the web Server being used and have no access to the security functionality of the TOE.
FTP_TRP.1	SECURE	The Security Administrator of the TOE configures the TOE/TSF through an isolated Serial Port connection or via a Secure HTTPS Administrative Web Based Console Interface.

6.2 Assurance Measures

The assurance measures provided by the TOE satisfy all of the assurance requirements listed in Chapter 5, Table 3. Table 6 provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 6 - Assurance Measures

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.1	HYDRA Versioning	Contains a description of the configuration management of the HYDRA Server 1.4
ADO_IGS.1	HYDRA Server 1.4 User Manual	The Manual includes instructions on installing and configuring the HYDRA Server 1.4
ADV_FSP.1	HYDRA System Architecture, HYDRA Server 1.4 User Manual	Between the two documents, all interfaces and functionality of the HYDRA Server 1.4 are covered in detail.
ADV_RCR.1	TOE Summary Specification to Informal Functional Specification Correspondence	Contains a correspondence between the TSS and FSP.
AGD_ADM.1	HYDRA Server 1.4 User Manual	Describes the management and configuration of the HYDRA Server 1.4
AGD_USR.1	N/A	The non-administrative users are not aware they are using the HYDRA Server 1.4. Non-administrative users can simply view web pages in read only mode. The non-administrative users have no access to the security functions of the TOE and therefore this SAR is met trivially.
ATE_IND.2	Test Activity	Describes test procedures conducted by the developer.

6.2.1 Rationale for TOE Assurance Requirements

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL1 from part 3 of the Common Criteria.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any registered Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any registered Protection Profile.

7.4 Protection Profile Rationale

This Security Target does not claim conformance to any registered Protection Profile.

CHAPTER 8

8. Rationale

The IT Security Objectives are met through Security Functional and Assurance requirements as a mutually supportive whole.

8.1 Security Objectives Rationale

The rationale for the security objectives of the TOE is defined in Chapter 4, Section 4.3 Security Objectives Rationale.

8.2 Security Requirements Rationale

The rationale for the security requirements of the TOE is defined in two sections. Rationale for the security functional requirements is given after each functional component description in Chapter 5, Section 5.1 Security Functional Requirements. Rationale for the security assurance requirements is given in Chapter 6, Section 6.3 Rationale for the TOE Assurance Requirements.

8.3 TOE Summary Specification Rationale

The rationale for the TOE Summary Specification is defined in Chapter 6, Section 6.1 TOE Security Functions.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.