

Security Criteria for Service Delivery Network

CL-Security-Criteria-I01-090702

WORK IN PROGRESS

Notice

This specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs[®]) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

© Copyright 2009 Cable Television Laboratories, Inc.
All rights reserved.

Document Status Sheet

Document Control Number:	CL-Security-Criteria-I01-090702			
Document Title:	Security Criteria for Service Delivery Network			
Revision History:	D01 – Released January 25, 2009			
	D02 – Released May 8, 2009			
	I01 – Released July 2, 2009			
Date:	July 10, 2009			
Status:	Work in Progress	Draft	Issued	Closed
Distribution Restrictions:	Author Only	CL/Member	CL/ Member/ Vendor	Public

Key to Document Status Codes:

- Work in Progress** An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
- Draft** A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
- Issued** A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
- Closed** A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Contents

1	SCOPE	1
1.1	Introduction and Overview	1
1.2	Requirements	1
2	REFERENCES	2
2.1	Normative References	2
2.2	Reference Acquisition	2
3	TERMS AND DEFINITIONS	3
4	ABBREVIATIONS AND ACRONYMS	4
5	REQUIREMENTS	5
5.1	Documentation (D)	5
5.2	System Management (SM).....	5
5.3	Customer Interaction (CI)	6
5.4	Information Protection (IP)	6
5.5	Design Principles (DP).....	6
5.6	Technology Specific (TS)	7
5.7	Application (APP).....	7
5.8	Authentication (AUTH).....	8
5.9	Database (DB).....	8
	APPENDIX I ACKNOWLEDGEMENTS (INFORMATIVE)	11
	APPENDIX II REVISION HISTORY (INFORMATIVE)	12

This page left blank intentionally.

1 SCOPE

1.1 Introduction and Overview

This document specifies appropriate security practices and methods to protect cable service delivery networks. It provides initial guidance and sets expectations of minimal security functionality and features. Additional requirements may be specified by MSOs upon evaluation of the specific product or service.

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

“MUST”	This word or the adjective “REQUIRED” means that the item is an absolute requirement of this specification.
“MUST NOT”	This phrase means that the item is an absolute prohibition of this specification.
“SHOULD”	This word or the adjective “RECOMMENDED” means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
“SHOULD NOT”	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
“MAY”	This word or the adjective “OPTIONAL” means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

- [1] *Baseline Security Requirements for the Cox Service Delivery Network*, Network Intelligence & Security Engineering, August 06, 2007, Cox Communications, Inc.
- [2] *Application Requirements v1.1*, June 25, 2008, Comcast Cable Communications, Inc.
- [3] *Authentication Requirements v1.1*, June 05, 2008, Comcast Cable Communications, Inc.
- [4] *Database Security Requirements*, July 02, 2008, Comcast Cable Communications, Inc.
- [5] *My-SQL Security Requirements*, November 20, 2008, Comcast Cable Communications, Inc.
- [6] *Mysql Security Requirements*, July 24, 2008, Comcast Cable Communications, Inc.
- [7] *Operating System Requirements v1.0*, June 17, 2008, Comcast Cable Communications, Inc.
- [8] *Oracle Security Requirements*, July 02, 2008, Comcast Cable Communications, Inc.

2.2 Reference Acquisition

CableLabs Specifications:

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
Phone 303-661-9100; Fax 303-661-9199; Internet: <http://www.cablelabs.com/>

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Authentication	Process of establishing, to the required level of confidence, the identity of one or more parties to a transaction. Consists of identity management (establishing who you are) and logon management (confirming who you are). For this document, authentication is used in the commonly understood sense of logging on with a username and authentication key (e.g., password).
Password	Static secret, usually composed of keyboard characters, that is used as the authentication key
User	A person who uses a computer or Internet service. A user may have a user account that identifies the user by a username. To log in to an account, a user is typically required to authenticate with a password or other credentials.
Username	Construction of alphanumeric characters that is used to identify a customer within the authentication system (the username is used to identify the customer, or rather their authentication key, to the verifier as part of the authentication process)

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

3DES	Triple Data Encryption Algorithm
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
aLOM	Advanced Lights Out Manager
DBA	Database Administrator
DBMS	Database Management System
EDS	Enterprise Database System
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDEA	International Data Encryption Algorithm
IdM	Identity Management
iLO	Integrated Lights-Out
iLOM	Integrated Lights-Out Manager
IPv6	Internet Protocol Version 6
IdM	Identity Management
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial In User Service
RBAC	Role-Based Access Control
RC5	Rivest Cipher 5
SCP	Secure Copy
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access-Control System
TLS	Transport Layer Security
WPA	Wi-Fi Protected Access

5 REQUIREMENTS

5.1 Documentation (D)

ID #	Name	Description
D-01	Data flows	The vendor MUST supply detailed diagrams for all data flows associated with the system, including ports, protocols, and flow direction.
D-02	Proprietary protocols	The vendor MUST supply full documentation for any proprietary protocols utilized.

5.2 System Management (SM)

ID #	Name	Description
SM-01	Separation of management network traffic	The system MUST allow the separation of management network traffic from all other network traffic.
SM-02	Interactive management access	The system MUST force all interactive management access (i.e., Command line, GUI, etc.) over a network to traverse a secure encrypted channel.
SM-03	Configurable timeout/logoff	The system MUST provide a configurable timeout/logoff period for interactive access.
SM-04	External AAA systems	The system MUST fully support external AAA systems (TACACS+/RADIUS).
SM-05	Local management access without AAA	The system MUST allow the configuration of one local account for management access when external AAA is not available. The system MUST support iLOM, iLO, or aLOM.
SM-06	Local management access with AAA	The system MUST NOT allow management access using the local account when external AAA is available.
SM-07	Plaintext protocols	Plaintext protocols (e.g., Telnet and Http) Must not be used for any authentication on any network.
SM-08	No security feature circumvention	The system MUST NOT have management access interfaces that circumvent security features (such as unauthenticated console ports or default username/password backdoors).
SM-09	Password expiration and account lockout	The system SHOULD support password expiration and account lockout for management access.
SM-10	Strong passwords	The system MUST support strong passwords (i.e., minimum of 8 characters, at least one uppercase and lowercase character, one digit, and punctuation character).
SM-11	Multiple access levels	The system MUST support multiple access levels for management purposes (e.g., Role Based Access Controls). Common roles are: User, Operator, and Administrator.

5.3 Customer Interaction (CI)

ID #	Name	Description
CI-01	IdM authentication	The system SHOULD provide the ability to authenticate customers through an identity management system.
CI-02	Strong passwords	The system MUST support strong passwords (i.e., minimum of 8 characters, at least one uppercase and lowercase character, one digit, and punctuation character).
CI-03	User access	The system MUST authenticate and authorize users prior to granting access to services and resources.
CI-04	Configurable timeout/logoff period	The system MUST provide a configurable timeout/logoff period for interactive access.

5.4 Information Protection (IP)

ID #	Name	Description
IP-01	Customer identifiable information	The system MUST protect all customer identifiable information (e.g., name, address, login credentials, account numbers, etc.) at all times.
IP-02	Encryption methods	The system's encryption MUST utilize strong, open, peer reviewed methods (such as 3DES, AES, RC5, and IDEA).
IP-03	Secure file transfer	The system MUST support secure file transfers. (e.g., SFTP, SCP)

5.5 Design Principles (DP)

ID #	Name	Description
DP-01	Response to a failure	The system MUST NOT reduce security in response to a failure (i.e., "failclosed" design).
DP-02	Unnecessary services	The system MUST NOT have unnecessary services enabled (i.e., No compilers, extra packages, etc. Only those services required to run the application)
DP-04	Logging to an external facility	The system MUST support logging to an external facility (e.g., Syslog).
DP-05	Retrieval of local logs	The system MUST NOT provide a mechanism to retrieve local logs for external manipulation.
DP-06	Synchronization to external time source	The system MUST support synchronization to an external time source.

5.6 Technology Specific (TS)

ID #	Name	Description
TS-01	SNMP implementation	The system's SNMP implementation MUST be fully SNMPv2 compliant and support access control lists.
TS-02	Support for SNMPv3	The system's SNMP implementation SHOULD fully support SNMPv3.
TS-03	SSH implementation	The system's SSH implementation MUST be SSHv2 or higher.
TS-04	Support for WPA2	The system's 802.11 (wireless) interfaces MUST support WPA2.
TS-05	Support for SSL/TLS	The system MUST support SSLv3/TLSv1 on all HTTP/Web interfaces.
TS-06	Support for Ipv6	The system SHOULD have full support for IPv6 in all network interfaces, applications, and tools.
TS-07	Support for NTP	The system SHOULD support NTP for time synchronization.

5.7 Application (APP)

ID #	Name	Description
APP-02	Database Queries	Queries to sensitive backend data stores MUST be exposed through services on backend servers. For example, front end servers should never be allowed to talk directly to EDS.
APP-03	RFC Compliant	All application protocols MUST adhere to the protocol specifications.
APP-04	Malformed Packets	All applications MUST gracefully discard malformed packets without bringing down services or allowing additional functionality access to the box.
APP-06	Buffer Overflow	Application source code has been checked for buffer overflow vulnerabilities. Buffer overflow vulnerabilities discovered have been remediated.
APP-07	Error Handling	Application fails gracefully when confronted with an error.
APP-08	Bound Checking	All user input MUST be bound checked.
APP-09	Input Validation	All user input MUST be validated.
APP-10	Pointer Reference	All program pointers MUST reference a valid memory space (i.e. no pointers are referenced to NULL).
APP-11	Error Messages	Error messages SHOULD only contain the minimum amount of information required to trouble shoot the issue.
APP-12	User Writing Logs	Users MUST be prevented from writing directly to log.
APP-13	Trusted Data	Trusted and untrusted data MUST NOT be commingled.
APP-14	Compiling	Application MUST NOT and will not be compiled on production servers.
APP-15	Error Logging	At a minimum, the following security events MUST be logged: 1) failed logon attempts 2) configuration changes 3) user administration such as additions, deletions, and modifications
APP-16	Development Tools	All development materials MUST (source code, compile and link artifacts, uncompiled JSPs) have been removed from production servers.
APP-17	Sensitive Data Protection	Sensitive data transmitted across an untrusted network, or residing on hosts anywhere, MUST be protected. This includes data that has personally identifiable Information (PII) and other business sensitive information.

5.8 Authentication (AUTH)

ID #	Name	Description
AUTH-04	Application Authentication	All application interfaces MUST support application authentication, if there is a separate application on the element.
AUTH-05	Password Storage	Passwords MUST NOT be stored in plain text.
AUTH-07	Username	Unique usernames MUST be used for each user.
AUTH-08	Default Accounts	All default accounts SHOULD be removed. If default accounts cannot be removed, they should be locked. If locking is not possible, site password policy will come into effect.
AUTH-09	Direct OS Login	User direct login via root or application account MUST be prohibited on the OS.
AUTH-10	Application Local OS Accounts	All applications MUST have a dedicated system account and MUST NOT run as Root, user, or Run As; and MUST NOT allow interactive sessions.
AUTH-11	Application Role Base Security	The application MUST be able to allow system administrators to assign specific privileges (i.e., read, write, delete, and update) to system resources and assign them to roles or groups. Administrators SHOULD be able to add user IDs to the roles or groups.
AUTH-12	Least Privilege	All accounts MUST be created and given roles in accordance with the principle of least privilege to.
AUTH-14	Encrypted Login	The entire login transaction MUST be encrypted using HTTPS rather than just the password.
AUTH-17	Session Lifetime Limits	Session lifetime MUST be limited.
AUTH-18	Failed Login	Passwords provided during failed login attempts SHOULD NOT be recorded.
AUTH-19	Error Messages	The system SHOULD only indicate a login attempt failure from the specific user, it SHOULD NOT indicate what failed (e.g., username or password).
AUTH-21	Client Authentication	If HTTPS is being used, and the web server is configured for mutual authentication with client certificates, current certificate revocation lists have been installed and configured.

5.9 Database (DB)

ID #	Name	Description
DB-01	OS Partition	The database files SHOULD NOT reside on the same partition as the operating system or logging (var) partition.
DB-02	Database Local Account	The database servers SHOULD be run using a unique, local account used exclusively for the database. This SHOULD be the account used to install and run the database.
DB-03	Other Applications	No other applications SHOULD be installed on the same server as the database. If it is required that a 3 rd party application run on the database server it MUST be installed on a separate partition from the database software and associated data files.
DB-04	Database Creation Tools	Any database creation tools such as scripts or other procedures MUST be removed after installation.

DB-05	Password Decryption	The system MUST NOT allow anyone to decrypt and view encrypted passwords.
DB-06	Sensitive Information Storage	Scheduled jobs or scripts MUST NOT contain sensitive information such as database usernames and passwords. If exceptions need to be made they MUST be properly documented with the sensitive information identified and permission MUST be properly restricted.
DB-07	Environment Variables	Environment variables MUST NOT be used to store any unencrypted sensitive information such as database usernames and passwords.
DB-08	Batch Files	Batch files MUST NOT have unencrypted sensitive information such as database usernames and passwords.
DB-09	Default Accounts	Default accounts SHOULD NOT be used (e. g., scott account in Oracle, db2admin account in IBM DB2). If default accounts must exist, they MUST be locked and the default passwords MUST be changed.
DB-12	Unique UserIDs	Unique user ID/accounts MUST be assigned for each database user.
DB-13	Individual DBA Accounts	Individual DBA accounts MUST be set up to manage the database.
DB-14	Admin Password	The admin account MUST be configured with a strong password.
DB-15	SYSTEM tablespace	Users MUST NOT have the SYSTEM tablespace as their default or temporary tablespace.
DB-16	Operating System Authentication	The Operating System authentication option MUST be used for authentication.
DB-17	Database Link Password	Database link passwords SHOULD be encrypted.
DB-18	Initial Password Change	Newly created accounts MUST be prompted to create a new password at login.
DB-19	Password Expiration	Password expiration MUST be supported, be configurable and enforceable.
DB-20	Concurrent Sessions	The number of concurrent sessions MUST be 1 for individual users and set to minimal required number for application accounts.
DB-21	Privileges	Privileges MUST be assigned to roles and not directly to users.
DB-22	Application Privileges	The DROP, CREATE, UNLIMITED TABLESPACE, BECOME USER, GRANT ANY, SELECT ANY, EXECUTE ANY, and ALTER privileges MUST NOT be granted to any application.
DB-23	Well-Known Account	If well-known accounts exist, they MUST have the CONNECT privilege only.
DB-24	PUBLIC Roles and Privileges	All privileges and roles MUST be revoked from PUBLIC.
DB-25	Password Protected Roles	Applications MUST use password protected roles.
DB-26	Default Roles	Users MUST NOT be assigned any default roles.
DB-27	Connect and Resource roles	Connect and Resource roles MUST NOT be used for live database applications.
DB-28	DBMS command	Users, apart from the DBA, MUST be denied access to the DBMS command prompt on the database server.

	prompt	
DB-29	Views	Views MUST be used to enforce access restriction to tables.
DB-30	File Ownership and Permissions	Application files, including 3 rd party application files on the server accessing the database, MUST have proper ownership and minimal file permissions.
DB-31	GRANT All privileges	GRANT ALL MUST NEVER be used when assigning a user rights to an object.
DB-32	Database Initialization Files	The database initialization files MUST NOT be user readable.
DB-33	File Access Permissions	File access permissions on the database files MUST be set to the least permissions required for satisfactory functioning.
DB-34	Application Schema Owner	The account for the application schema owner SHOULD be locked where possible.
DB-35	Soft Quotas	Soft Quotas SHOULD be used.
DB-36	Fixed Database Links	There MUST NOT be any fixed database links that have a hard coded username and password.
DB-37	Database Connection Strings	Database connection strings MUST NOT be hard coded or stored in clear text in configuration files. They need to be encrypted and their access needs to be restricted.

Appendix I Acknowledgements (Informative)

We wish to heartily thank the MSO participants contributing directly to this document:

Comcast Cable Communications, Inc.

Cox Communications, Inc.

CableOne, Inc.

Cogeco Cable, Inc.

Cablevision Systems Corporation

General Communications, Inc. (“GCI”)

Time Warner Cable

Rogers Cable, Inc.

Vidéotron Ltée

Appendix II Revision History (Informative)

Table 1 Engineering Change Notices

ECN	Date Ratified	Summary