Client Side Content Screening Framework Requirements

Candidate Version 1.0 – 18 Jan 2006

Open Mobile Alliance

OMA-RD-Client_Side_CS_FW-V1_0-20060118-C

Contents

Tables

1. Scope (Informative)

This document presents use cases and requirements for a content screening framework for mobile terminals that detect and screen against malicious content. This document contains information applicable to terminal manufacturers and independent software vendors. Additionally, related functionality not described here may involve requirements outside the scope of this document. This additional functionality shall not interfere with the core requirements described in this document.

2. References

2.1 Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[Privacy] "OMA Privacy Requirements for Mobile Services" , Version 1.0., Open Mobile Alliance™, OMA-RD_Privacy-V1_0, URL:http://www.openmobilealliance.org/

2.2 Informative References

[CSBOFTR] "Technical Report – OMA Content Screening BOF", Version 1.0, Open Mobile Alliance™, OMA-CSBOF-TR-V1_0_0, URL:http://www.openmobilealliance.org/

[OMA-DICT] "Dictionary for OMA Specifications", Version 2.3, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_3, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

For the purposes of this document, the terms and definitions given in [OMA-DICT] apply and the following also apply:

Content	Data or code delivered to an end-user and/or end-user’s terminal.
Content Screening	The act of protecting an end-user and/or end-user’s terminal from undesirable content by blocking access to the said content. This act may be in the form of warning message, confirmation of deletion, notification of deletion, silent deletion without notification, etc. Exact detail would vary according to severity level reported, I/O capability of mobile terminal, user preferences, etc.
Client Side Content Screening	Content screening performed at the mobile terminal.
Server Side Content Screening	Content screening performed at the network by servers with content screening functionality. E.g. Proxy server, mail server, firewall, etc.
Undesirable Content	Content that should be screened because it is malicious, unsolicited or inappropriate.
Malicious Content	Content that will have a detrimental impact upon end-user’s terminal or overall mobile system. E.g. Viruses, worms, vulnerability exploits, etc.
Unsolicited Content	Content that an end-user and/or end-user’s terminal has not requested. E.g. SPAM and denial-of-service attacks.
Inappropriate Content	Content that is unsuitable for an end-user based on user profile, regulation or local law. This includes illegal content. E.g. Adult materials for minors, non-work related sites for enterprise customers, pirated softwares, etc.
Content Scanning	The actual operation of looking at the data to determine whether it is a potential candidate for screening and level of severity if found to be as such. What this operation consist of would vary according to how content scanning functionality is implemented and falls outside the scope of this document.
Scan Engine	Component of client side content screening framework that performs content scanning service to OMA/non-OMA enablers related to end-user content delivery and/or processing.
Content Scanning Functionality	Content scanning performed for OMA/non-OMA enabler wishing to determine whether a content under consideration is undesirable or not. This performance is accessed by a set of interfaces specified by the content screening framework.
User Profile	Lists end user sensitivities and/or requirements. The profile may include age, sexual, religious, and cultural sensitivities, as well as specific requirements regarding the forms of communication that are acceptable/unacceptable (e.g. SPAM, Unsolicited), Type of content (e.g. Premium Rated content, text, Picture, etc) and means of access (e.g. WLAN, Bluetooth, UE Memory card). Note that the determination of the suitability of specific content will require a comparison of that content against a combination of end user sensitivities (e.g. age and sexual).
Vulnerability Exploits	Content that deliberately or non-deliberately causes various misbehaviors on a mobile terminal because of a glitch in the content itself, or in an enabler processing the content, or in an execution environment executing the enabler processing the content, or in the mobile network system serving the terminal.

Misbehaviors (on mobile terminal)	Any undocumented or unspecified functioning of a mobile terminal. E.g. System freeze, system crash, performance degradation, unintended communications, misrepresented content, unusual power consumption, etc.
Client Side Content Screening Framework	An abstract conceptual structure used as the basis for contructing interaction model between OMA/non-OMA enablers and content scanning functionality through a set of interfaces with the ultimate goal of bringing forth content screening capability to the mobile terminal.
Screening Action	The act of blocking an undesirable content (see 'Content Screening').
SPAM	Unsolicited commercial electronic messages sent indiscriminately to a large number of recipients, usually to promote products or services.

3.3 Abbreviations

OMA	Open Mobile Alliance
DOS	Denial-of-Service
P2P	Peer to Peer
VPN	Virtual Private Network
SSL	Secure Socket Layer
Web	World Wide Web
WLAN	Wireless LAN
UE	User Equiment (a.k.a. mobile terminal)
SMS	Short Message Service
MMS	Multimedia Message Service
IM	Instant Message
PC	Personal Computer

4. Introduction (Informative)

Currently, OMA is developing a number of enablers which provide the means to deliver content to users. With client side content screening framework OMA provides the means to screen content delivered to mobile terminals that is malicious, unsolicited, and/or inappropriate. According to "7.1 Recommendation for Client-Side Content Screening" of the Content Screening BOF ([CSBOFTR]), client side content screening framework should be standardized by OMA. An OMA specified framework for mobile terminals will facilitate adaptation of existing, or the development of, client-side content screening technologies to the mobile environment, providing a timely solution for an effective countermeasure to malicious content.

This document presents use cases and requirements for development of the specification for OMA client-side content screening framework that detect and screen malicious content. The framework will specify interfaces to OMA/non-OMA enablers for utilizing content scanning functionality. The framework will also specify how such enablers interact with the content scanning functionality through these interfaces.

There is an urgent market demand for an effective countermeasure to the growing amount of malicious content delivered to mobile terminals before more lethal variants, such as self-spreading viruses and worms create havoc for networks and users as richer content become available. This document provides requirements on a client-side content screening framework for countering these threats.

5. Use Cases

The following use cases are provided to illustrate the functions and roles of the various system elements in the content framework in mobile terminals.

5.1 Content that connect to premium sites

5.1.1 Short Description

Email with a link connecting to a premium site or number.

5.1.2 Actors

End-user using an email client software to access an email message containing a link to a premium site or number.

Email client software residing in the mobile terminal.

Scan engine residing in the mobile terminal providing content scanning functionality to enablers participating in the content screening framework.

5.1.2.1 Actor Specific Issues

End-user is not aware of the undesirable effects of accessing a particular link embedded in an email message.

5.1.2.2 Actor Specific Benefits

End-user is warned that a particular email message contains a link to a premium site or number.

5.1.3 Pre-conditions

End-user receives an email containing a link to a premium site which may result in unintended phone bill.

5.1.4 Post-conditions

End-user is presented with a warning when he/she tries to access the link in the email message.

5.1.5 Normal Flow

1. End-user notices a new email message.
2. End-user uses the email client software on the mobile terminal to view the received message.
3. Before displaying the content of the message, the email client software passes the content to the scan engine for content.
4. Scan engine analyzes the content and determines that contains a link to a premium site or number
5. Email client software warns the end-user that the message contains a link to a premium site or number.
6. End-user chooses to cancel viewing the message.

5.1.6 Alternative Flow

7. Instead of cancelling, the end-user chooses to go ahead and view the message.
8. While viewing the content of the message, the end-user chooses to access a particular site without knowning that it is an address of a premium site.
9. Before establishing connection to the site, email client software passes the address of the site to the scan engine for scanning.

10. Scan engine scans the address and determines that the address is a known target of prank messages.
11. Email client software displays a warning dialog that the site is a premium service site.
12. End-user chooses to cancel connection to the premium site.

5.1.7 Operational and Quality of Experience Requirements

In cases where the site is a known target of such messages (i.e. target of DOS attack), the severity level reported by the scan engine can be set to, for example, "High Severity" so that instead of warning the user, the email client may chooses to deny access without asking for user confirmation.

5.2 Content that causes misbehaviors on mobile terminals

5.2.1 Short Description

Content that causes various mishaviors on mobile terminals because of glitch in the content itself or glitch in the enabler processing the content.

5.2.2 Actors

End-user using a browser to view a malformatted Web page that causes the browser to misbehave.

Browser software residing in the mobile terminal.

Scan engine residing in the mobile terminal providing content scanning functionality to enablers participating in the content screening framework.

5.2.2.1 Actor Specific Issues

End-user is not aware of the undesirable effects of accessing a particular malformatted Web page.

5.2.2.2 Actor Specific Benefits

End-user is warned that a particular Web page may cause the mobile terminal to misbehave in various ways.

5.2.3 Pre-conditions

End-user accesses a malformatted Web page which may cause the mobile terminal to misbehave in various ways.

5.2.4 Post-conditions

End-user is presented with a warning when he/she tries to access the malformatted Web page.

5.2.5 Normal Flow

1. End-user uses the browser to access a particular Web page, either by clicking on a link in a given Web page or by manually entering the URL addresss.
2. Browser retrieves the Web page.
3. Before processing the content of the retrieved Web page, the browser passes the content to the scan engine for scanning.
4. Scan engine scans the content and determines that it contains a code that may cause the mobile terminal to misbehave.
5. Browser warns the end-user that the Web page being accessed may cause the mobile terminal to misbehave.
6. End-user chooses to cancel accessing the Web page.

5.2.6 Alternative Flow

The Web page itself is properly formatted but the browser has a glitch that causes it to misrepresent the Web page. Flow is same as above.

5.2.7 Operational and Quality of Experience Requirements

In cases where the malformatted Web page causes significant misbehavior, such as crashing the terminal, the severity level reported by the scan engine can be set to, for example, "High Severity" so that instead of warning the user, the browser may chooses to deny access without asking for user confirmation.

5.3 Content received from local environment

5.3.1 Short Description

Malicious content received from local environment, such as via Bluetooth, wireless LAN, removable media, etc.

5.3.2 Actors

End-user using a mobile terminal capable of file transfers from local environment, such as via Bluetooth, wireless LAN, removable media, etc.

File installer residing in the mobile terminal responsible for handling file transfers or installations.

Scan engine residing in the mobile terminal providing content scanning functionality to enablers participating in the content screening framework.

5.3.2.1 Actor Specific Issues

End-user is not aware of the undesirable effects of installing a particular malicious content retrieved from the local environment.

5.3.2.2 Actor Specific Benefits

End-user is warned that a particular content retrieved from the local environment is malicious.

5.3.3 Pre-conditions

End-user tries to install a content that is malicious, such as a virus, from the local environment.

5.3.4 Post-conditions

End-user is presented with a warning when he/she tries to access the malicious content.

5.3.5 Normal Flow

1. End-user uses the file installer to install a content that was received via Bluetooth message.
2. Before installing the content, file installer passes the content to the scan engine for scanning.
3. Scan engine scans the content and determines that it is a virus.
4. File installer notifies the end-user that the file is a virus.
5. End-user chooses to terminate the installation process.

5.3.6 Alternative Flow

Instead of the file installer passing the content to the scan engine for scanning, Bluetooth message handler passes the content to the scan engine. If the content is found to be safe and if the content is an installation file, then it is forwarded to the file installer for further processing.

5.3.7 Operational and Quality of Experience Requirements

The file installation may choose to deny installation without asking for user confirmation if the content is set to, for example, "High Severity" such as that of viruses and other malicious content.

5.4 Content accessed while in roaming mode

5.4.1 Short Description

End-user surfs the Web using the mobile terminal while traveling abroad. The end-user accesses a malicious image file that infects the user's mobile terminal with a virus. The end-user would not be exposed to such malicious content when using the mobile terminal in his/her country as the home mobile operator performs server side content screening.

5.4.2 Actors

End-user using a mobile terminal while traveling abroad.

Browser client software residing in the terminal.

Scan engine residing in the mobile terminal providing content scanning functionality to enablers participating in the content screening framework.

Home mobile operator that provides mobile service to the end-user and provides content screening functionality by scanning their network traffic.

Visited mobile operator that provides mobile service to the end-user when the end-user is traveling abroad (i.e. when the end-user is out of the service area of his/her home mobile operator). Visited mobile operator does not offer any content screening functionality in their network.

5.4.2.1 Actor Specific Issues

End-user is protected from malicious content when he/she is receiving mobile service from home mobile operator because they provide server side content screening service. End-user is not protected from malicious content when he/she is in roaming mode as the visited mobile operator does not provide server side content screening service.

5.4.2.2 Actor Specific Benefits

End-user is warned that a particular image file contains a virus.

5.4.3 Pre-conditions

End-user accesses a malicious image file while in roaming mode that infects the mobile terminal with a virus.

5.4.4 Post-conditions

End-user is presented with a warning when he/she tries to access the malicious image file.

5.4.5 Normal Flow

1. End-user is using a mobile terminal in roaming mode.
2. End-user accesses the Web using the browser.

3. End-user accesses a malcious image file in a Web page.
4. Before displaying the image, the browser passes the content to the scan engine for scanning.
5. Scan engine analyzes the content and determines that it is a malicious image file.
6. Browser warns the end-user that the retrieved image file contains a virus instead of displaying the content.
7. End-user chooses to delete the image file.

5.4.6 Alternative Flow

5.4.7 Operational and Quality of Experience Requirements

In cases where the malicious image file causes significant misbehavior, such as crashing the terminal, the severity level reported by the scan engine can be set to, for example, “High Severity” so that instead of warning the user, the browser client software may chooses to delete the message without asking for user confirmation.

5.5 Content received via end-to-end encrypted connections

5.5.1 Short Description

End-user retrieves a content via end-to-end encrypted connection (e.g. SSL, VPN, WTLS, P2P, etc.) that is malicious.

5.5.2 Actors

End-user using a mobile terminal.

Browser software residing in the terminal with an end-to-end encrypted communication capability.

Scan engine residing in the mobile terminal providing content scanning functionality to enablers participating in the content screening framework.

Mobile operator that provides content screening functionality to the end-user by scanning their network traffic but only applies to scanning of unencrypted traffic.

5.5.2.1 Actor Specific Issues

End-user is protected from malicious content when he/she is using the browser in unencrypted mode because his/her mobile service operator provides server-side content screening service. End-user is not protected from malcious content when he/she is using the browser in encrypted mode.

5.5.2.2 Actor Specific Benefits

End-user is warned that a particular content retrieved via browser communicating in encrypted mode is malicious.

5.5.3 Pre-conditions

End-user tries to access a malicious content via browser communicating in encrypted mode.

5.5.4 Post-conditions

End-user is presented with a warning when he/she tries to access the malicious content.

5.5.5 Normal Flow

1. End-user clicks on a link using a browser.
2. Browser retrieves the content via encrypted connection.

3. Before processing the content to the end-user, the browser passes the content to the scan engine for analysis.
4. Scan engine analyzes the content and determines that it is a malicious content that may cause the mobile terminal to misbehave.
5. Browser warns the end-user that the content is malicious instead of processing the content.
6. End-user chooses to cancel accessing the content.

5.5.6 Alternative Flow

5.5.7 Operational and Quality of Experience Requirements

In cases where the malicious content causes significant misbehavior, such as crashing the terminal, the severity level reported by the scan engine can be set to, for example, "High Severity" so that instead of warning the user, the browser may instead choose to delete the content without asking for user confirmation.

5.6 Content received within trusted domain

5.6.1 Short Description

End-user receives a malformatted email message from its service provider that provides server side content screening service to its users (the message may be a new product announcement or a Welcome message in roaming mode). The message was not screened because it was generated within the trusted domain.

5.6.2 Actors

End-user using an email client software to access an email message generated from a trusted domain.

Email client software residing in the terminal.

Scan engine residing in the mobile terminal providing content scanning functionality to enablers participating in the content screening framework.

Mail service provider that provides server side content screening functionality by scanning their incoming traffic.

5.6.2.1 Actor Specific Issues

End-user is protected from malicious content when the email is sent from non-trusted domain because the mail server scans incoming emails for existence of any malicious content. End-user is not protected from malicious content when the email message itself is generated by the mail server itself or by trusted domain.

5.6.2.2 Actor Specific Benefits

End-user is warned that a particular email message is malformatted and may cause various misbehaviours on the mobile terminal.

5.6.3 Pre-conditions

End-user receives an email message from a trusted domain that may cause various misbehaviours on the mobile terminal.

5.6.4 Post-conditions

End-user is presented with a warning when he/she tries to access the malformatted email message.

5.6.5 Normal Flow

1. End-user is using a mobile terminal.

2. End-user receives a malformatted MMS message
3. End-user uses MMS client software to view the received message.
4. Before displaying the content of the message, the MMS client software passes the content to the scan engine for scanning.
5. Scan engine analyzes the content and determines that it is a malformatted email message that may cause the mobile terminal to misbehave.
6. Email client software warns the end-user that the email is a malformatted instead of displaying the content.
7. End-user chooses to cancel viewing the message.

5.6.6 Alternative Flow

5.6.7 Operational and Quality of Experience Requirements

In cases where the malformatted email message sent from a trusted domain causes significant misbehavior, such as crashing the terminal, the severity level reported by the scan engine can be set to, for example, “High Severity” so that instead of warning the user, the email client software may chooses to delete the message without asking for user confirmation.

5.7 Open Issues

None.

6. Requirements (Normative)

6.1 General

6.1.1 Framework

1. Client side content screening framework SHALL specify interfaces and interaction to OMA/non-OMA enablers in mobile terminal related to end-user content delivery and/or processing.
2. The framework SHALL have interfaces for allowing enablers to pass the content to the content scanning functionality for scanning.
3. The framework SHALL NOT assume nor exclude the use of server-side content screening solutions placed on the network or gateways.
4. The framework SHALL NOT specify internal mechanisms (such as the scan engine, scanning rules, and updating of such engine and rules) of content scanning functionality.
5. The framework SHOULD specify informative section on the use of the interfaces in particular execution environments.
   A) The framework SHALL NOT restrict their use implicitly or explicitly to said execution environments.
6. The framework SHOULD specify informative section on recommended interface invocation times for use by enablers.
7. The framework SHOULD specify informative section on recommended screening actions for use by enablers.

6.1.2 Interfaces

1. The interfaces SHALL adhere to the principle of execution environment neutrality.
2. The interfaces SHOULD be extensible in order to address new content screening requirements in the future.
3. The interfaces MAY accept information on type of the content being passed for scanning.

6.1.3 Scanning

1. The content scanning functionality SHALL return the result of the scan to the calling enabler.
2. The result of the scan SHALL indicate whether the content was found to be malicious or not.
3. The result of the scan MAY include severity level if the content was found to be malicious.

6.1.4 Screening

1. The calling enabler SHOULD perform the screening action if the content was found to be malicious.
2. Other system element besides the calling enabler (e.g. user interface handler, operating system, scan engine, etc) MAY perform the screening action if the content was found to be malicious.
3. The result of the screening action MAY be conveyed to the end-user (in the form of warning message, confirmation of deletion, notification of deletion, silent deletion without notification, etc).

6.2 High-Level Functional Requirements

1. Malicous content	Client side content screening framework SHALL have a set of interfaces for OMA/non-OMA enablers to determine whether a particular content is malicious.

Table 1: High-Level Functional Requirements

6.2.1 Security

1. Content scanning	Content scanning functionality and its interfaces SHALL be trusted by the clients residing within the mobile terminal.

Table 2: High-Level Functional Requirements – Security Items

6.2.2 Charging

	Editor's note: None had been identified so far.

Table 3: High-Level Functional Requirements – Charging Items

6.2.3 Administration and Configuration

1. Configuration	Enable and disable of content scanning functionality MAY be configurable by the end-user.

Table 4: High-Level Functional Requirements – Administration and Configuration Items

6.2.4 Usability

1. End-user	Mobile terminal equipped with content screening capability SHOULD NOT interfere with normal usage of the terminal by the end-user.
2. End-user	The end-user MAY be notified of content scanning that is about to be performed, is being performed, or has performed.
3. End-user	The end-user MAY be notified of content screening action that was performed.

Table 5: High-Level Functional Requirements – Usability Items

6.2.5 Interoperability

1. Interoperability	Content scanning functionality SHALL be interoperable with the calling enablers through a set of interfaces specified by the client side content screening framework.

Table 6: High-Level Functional Requirements – Interoperability Items

6.2.6 Privacy

1. Privacy	Privacy requirements SHALL be compliant with requirements stated in [Privacy].
2. Informational privacy	Content scanning functionality SHALL NOT expose personal data.

Table 7: High-Level Functional Requirements – Privacy Items

6.3 Overall System Requirements

	Editor's note: None had been identified so far.

Table 8: High-Level Functional Requirements – Security Items

6.4 System Elements

	Editor's note: None had been identified so far.	

Table 9: System Elements

6.4.1 System Element A

	Editor's note: None had been identified so far.	

Table 10: Requirements for System Element

6.4.2 Network interfaces

		Editor's note: None had been identified so far.

Table 11: Requirements for Network Interfaces

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD_Client_Side_CS_FW-V1_0	16 Aug 2004		First Draft
	20 Aug 2004	9.2.2.2, 11.3	Incorporates input to committee: OMA-MAE-2004-0107-Meeting-Minutes-20040818PM
	03 Sep 2004	3.2, 4, 6.1	Incorporates input from informal RD review conducted in REQ group on September 2, 2004.
	10 Sep 2004	3.2., 3.3, 6.1, 6.2	Revised according to comments in MAE confcall on Sep. 7, 2004.
	28 Sep 2004	4, 6.2.1	Revised according to comments in MAE F2F meeting on Sep 28, 2004.
	19 Oct 2004	2.1, 2.2, 4, 5.4, 6.2	Inclusion of agreed RDRR as per OMA-Client-Side-CS-Framework-RDRR-20041019-D
Candidate Version OMA-RD_Client_Side_CS_FW-V1_0	18 Nov 2004	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2004-0385-Client_Side_CS_FW-RD4Approval
	18 Jan 2006	2.1, 2.2, 6.4.1	Revised according to consistency review report: OMA-CONRR-Client_Side_CS_FW-V1_0-20060117-D