

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1143

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Security architecture for message security in mobile web services

ITU-T Recommendation X.1143

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.1143

Security architecture for message security in mobile web services

Summary

ITU-T Recommendation X.1143 describes the security architecture and scenarios for message security in mobile web services.

Security services for messages are the most fundamental security requirements for mobile web services. Although the components for message security such as WS-Security have been standardized, standard architecture and service scenarios for providing message security for mobile web services have yet to be defined. Since simple object access protocol (SOAP) messages use hypertext transfer protocol (HTTP) ports, they cannot be filtered by firewalls; hence the need to provide a message filtering mechanism based on the message contents in the architecture for secure mobile web services as well as to integrate the security policy mechanism suitable for mobile web services message security and the message filtering mechanism into the architecture. Since many mobile terminals do not have sufficient processing power to support the web services protocol stack fully, and many back-end application servers are not based on web services, interworking mechanisms and scenarios between mobile web services and legacy non-web services applications should be provided.

This Recommendation seeks to establish a guideline for security architecture and security service scenarios for message security in mobile web services satisfying the above-mentioned requirements.

Source

ITU-T Recommendation X.1143 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Message security, mobile web services, security gateway, security policy, web services security.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	4
5	Conventions	5
6	Introduction of mobile web services security-related standards.....	5
7	Requirements of security architecture and scenarios for message security in mobile web services.....	7
8	Security model for mobile web services.....	8
8.1	Security threats to mobile web services	8
8.2	Security requirements	9
8.3	Security functions for mobile web services.....	10
8.4	Security architecture for mobile web services.....	12
8.5	Message security service scenario for mobile web services	14
8.6	Message filtering	17
9	Use cases for message security in mobile web services	18
	Appendix I – Reference security architecture for message security in mobile web services ..	20
I.1	Overall security architecture for message security in mobile web services...	20
I.2	Components of the mobile web services security gateway	23
	Appendix II – Use cases for message security in mobile web services.....	25
II.1	Use case 1	25
II.2	Use case 2	28
II.3	Use case 3	30
II.4	Use case 4	33
	Appendix III – Examples of security policy description	36
	Appendix IV – Comparison with other standards.....	38
IV.1	Parlay X	38
IV.2	AAA	39
IV.3	OMA.....	39
	Bibliography.....	41

Downloaded from

ITU-T Recommendation X.1143

Security architecture for message security in mobile web services

1 Scope

The scope of this Recommendation deals with the security architecture and security service scenarios for secure mobile web services as described below:

- Integrated security architecture for message security in mobile web services consisting of various mobile terminals and networks.
- Interworking mechanisms and service scenarios between applications that support the full web services security protocol stacks and legacy applications that do not support the full web services security protocol stack.
- Authentication, integrity and confidentiality mechanisms of the message in the mobile web services environment.
- Integrated security architecture that utilizes the security policy for message security in the mobile web services environment.
- Message filtering mechanism based on the message contents for the message security architecture.
- Reference message security architecture and security service scenarios for mobile web services.

The following objectives are not within the scope of this Recommendation:

- To define a new security policy language or an access control language.
- To define a new transport level security protocol or a message level security protocol.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.800]	ITU-T Recommendation X.800 (1991), <i>Security architecture for Open Systems Interconnection for CCITT applications</i> .
[ITU-T X.805]	ITU-T Recommendation X.805 (2003), <i>Security architecture for systems providing end-to-end communications</i> .
[ITU-T X.1141]	ITU-T Recommendation X.1141 (2006), <i>Security Assertion Markup Language (SAML 2.0)</i> .
[ITU-T X.1142]	ITU-T Recommendation X.1142 (2006), <i>eXtensible Access Control Markup Language (XACML 2.0)</i> .
[IETF RFC 2246]	IETF RFC 2246 (1999), <i>The TLS Protocol Version 1.0</i> . http://www.ietf.org/rfc/rfc2246.txt
[IETF RFC 2828]	IETF RFC 2828 (2000), <i>Internet Security Glossary</i> . http://www.ietf.org/rfc/rfc2828.txt

[IETF RFC 3075]	IETF RFC 3075 (2001), <i>XML-Signature Syntax and Processing</i> . < http://www.ietf.org/rfc/rfc3075.txt >
[IETF RFC 3198]	IETF RFC 3198 (2001), <i>Terminology for Policy-Based Management</i> . < http://www.ietf.org/rfc/rfc3198.txt >
[OASIS WSS]	OASIS Standard (2006), <i>Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)</i> . < http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf >
[OASIS WSS-SAML]	OASIS Standard (2006), <i>Web Services Security: SAML Token Profile 1.1</i> . < http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityTokenProfile.pdf >
[OASIS WSS-UsernameToken]	OASIS Standard (2006), <i>Web Services Security: UsernameToken Profile 1.1</i> . < http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf >
[OASIS WSS-X.509]	OASIS Standard (2006), <i>Web Services Security: X.509 Certificate Token Profile 1.1</i> . (Including errata) < http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf >
[OASIS WS-SecPol]	OASIS Standard, <i>WS-SecurityPolicy 1.2</i> (2007). < http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/ws-securitypolicy-1.2-spec-cd-01.pdf >
[W3C P3P]	W3C Recommendation (2002), <i>The Platform for Privacy Preferences 1.0 (P3P1.0) Specification</i> . < http://www.w3.org/TR/P3P/ >
[W3C WSDL]	W3C Recommendation (2007), <i>Web Services Description Language (WSDL) Version 2.0 Part 0: Primer</i> . < http://www.w3.org/TR/wsdl20-primer/ >
[W3C XML-Enc]	W3C Recommendation (2002), <i>XML Encryption Syntax and Processing</i> . < http://www.w3.org/TR/xmlenc-core/ >

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 **access control:** [ITU-T X.800]
- 3.1.2 **authentication:** [ITU-T X.800]
- 3.1.3 **authorization:** [ITU-T X.800]
- 3.1.4 **availability:** [ITU-T X.800]
- 3.1.5 **confidentiality:** [ITU-T X.800]
- 3.1.6 **data integrity:** [ITU-T X.800]
- 3.1.7 **data origin authentication:** [ITU-T X.800]

- 3.1.8 **key:** [ITU-T X.800]
- 3.1.9 **key management:** [ITU-T X.800]
- 3.1.10 **non-repudiation:** [ITU-T X.800]
- 3.1.11 **policy decision point:** [IETF RFC 3198]
- 3.1.12 **policy enforcement point:** [IETF RFC 3198]
- 3.1.13 **privacy:** [ITU-T X.800]
- 3.1.14 **security architecture:** [IETF RFC 2828]
- 3.1.15 **security policy:** [IETF RFC 2828]
- 3.1.16 **security service:** [IETF RFC 2828]
- 3.1.17 **trust:** [IETF RFC 2828]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

- 3.2.1 **application service:** This is an entity that provides various value-added services to the service requesters.
- 3.2.2 **artifact:** A piece of digital information. An artifact may be any size, and may be composed of other artifacts. Examples of artifacts: a message; a URI; an XML document; a PNG image; a bit stream. [b-W3C Glossary]
- 3.2.3 **discovery:** The act of locating a machine-processable description of a web service-related resource that may have been previously unknown and that meets certain functional criteria. It involves matching a set of functional and other criteria with a set of resource descriptions. The goal is to find an appropriate web service-related resource. [b-W3C Glossary]
- 3.2.4 **discovery service:** This is an entity that stores interface information for application services and related security policies for access to the application services by clients. Clients can get such information from the discovery service by sending queries that describe the services they want to access.
- 3.2.5 **end point:** An association between a binding and a network address, specified by a URI, that may be used to communicate with an instance of a service. An end point indicates a specific location for accessing a service using a specific protocol and data format. [b-W3C Glossary]
- 3.2.6 **gateway:** This is a network node that terminates a message on an inbound interface with the intent of applying some security processing or message conversions to the message, and presenting it to the target service through an outbound interface.
- 3.2.7 **identifier:** An identifier is an unambiguous name for a resource. [b-W3C Glossary]
- 3.2.8 **policy server:** This is an entity that manages security policies related to the security processing of messages and access control policies for the messages.
- 3.2.9 **principal:** This is an entity whose identity can be authenticated. Examples of principals include an end user or an organization.
- 3.2.10 **registry:** Authoritative, centrally controlled store of information. [b-W3C Glossary]
- 3.2.11 **service description:** A service description is a set of documents that describe the interface to and semantics of a service. [b-W3C Glossary]
- 3.2.12 **service interface:** A service interface is the abstract boundary that a service exposes. It defines the types of messages and the message exchange patterns that are involved in interacting with the service, together with any conditions implied by those messages. [b-W3C Glossary]

3.2.13 service provider: The person or organization that is providing a web service. [b-W3C Glossary]

3.2.14 service requester: A software agent that wishes to interact with a provider agent in order to request that a task be performed on behalf of its owner, the requester entity. [b-W3C Glossary]

3.2.15 SOAP intermediary: A SOAP intermediary is both a SOAP receiver and a SOAP sender and is targetable from within a SOAP message. It processes the SOAP header blocks targeted at it and acts to forward a SOAP message towards an ultimate SOAP receiver. [b-W3C Glossary]

3.2.16 SOAP message: The basic unit of communication between SOAP nodes. [b-W3C Glossary]

3.2.17 web service: A web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other web-related standards. [b-W3C Glossary]

3.2.18 XML schema: The possible arrangement of tags and text in a valid representation of information. A schema might also be viewed as an agreement on a common vocabulary for a particular application that involves exchanging information. [b-Walsh]

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
ASP	Application Service Provider
CA	Certification Authority
HTTP	Hypertext Transfer Protocol
P3P	Platform for Privacy Preferences
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public-Key Infrastructure
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security
TTP	Trusted Third Party
UDDI	Universal Discovery, Description, Integration
WSDL	Web Services Description Language
WS	Web Services
WTLS	Wireless Transport Layer Security
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
XKMS	XML Key Management Specification

5 Conventions

None.

6 Introduction of mobile web services security-related standards

Web services is a set of protocols based on eXtensible Markup Language (XML). Figure 1 illustrates the base web services protocols.

- Simple object access protocol (SOAP): Defines the message format in XML containing the service request and response; SOAP is independent of any particular transport and implementation technology.
- Web services description language (WSDL): Describes a web service; it provides a programmatic way of describing what a service does, thereby paving the way for automation.
- Universal discovery, description, integration (UDDI): A cross-industry initiative to create a standard for service discovery together with a registry facility that facilitates the publishing and discovery processes.

Core web services technologies such as SOAP, WSDL and UDDI do not directly provide the security mechanism. As such, a comprehensive security model for web services has been developed by the industry. The web services security model introduces a collection of individual inter-related specifications describing an approach to layering security facilities into a web service environment. The architecture is designed to allow the mixing and matching of the specifications, thereby enabling implementers to deploy only the specific parts they need.

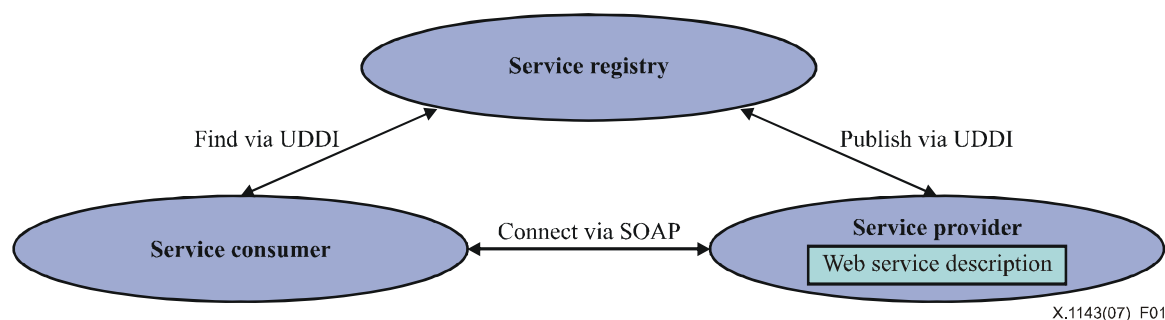


Figure 1 – Base web services protocols

The web services security roadmap that has been developed by the industry consists of an entire suite of specifications covering various facets of security (messaging, policies, trust, privacy, etc.). Figure 2 illustrates the roadmap.

The specifications build upon one another and are all built on top of a single specification, which is WS-Security (SOAP messages security). WS-Security defines a message security model.

The specifications are summarized as follows:

- WS-Security: Describes how to attach signatures and encryption headers to SOAP messages as well as how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages.
- WS-Policy: Describes the capabilities and constraints of the security and other business policies on intermediaries and endpoints (e.g., required security tokens, supported encryption algorithms, privacy rules).
- WS-Trust: Describes a framework for trust models that enables web services to interoperate securely.

- WS-Privacy: Describes a model for how web services and service requesters state their privacy preferences and organizational privacy practice statements.
- WS-SecureConversation: Describes how to manage and authenticate message exchanges between parties, including security context exchange and establishment and derivation of session keys.
- WS-Federation: Describes how to manage and broker the trust relationships in a heterogeneous federated environment, including support for federated identities.
- WS-Authorization: Describes how to manage authorization data and authorization policies.

WS-Security (SOAP messages security) is a base protocol in the web services security architecture; it is now an OASIS standard. WS-Security describes extensions to the SOAP protocol to provide secure messaging particularly to ensure message integrity and message confidentiality.

To accomplish this, the specification describes how to attach signature and encryption headers as well as binary-encoded security tokens such as X.509 certificates and Kerberos tickets to SOAP messages.

Message integrity is established through a combination of XML signatures and security tokens. By pairing digital signatures with security tokens that either contain or imply key data, the recipient of a message can be assured that the message has been transmitted without modification by a trusted party. Digital signatures support multiple signatures from multiple actors on the same document as well as multiple signature formats.

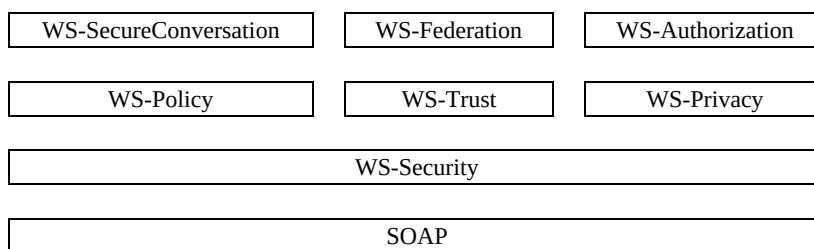


Figure 2 – Web services security roadmap

The security token mechanism defined by WS-Security is sufficiently extensible to support multiple security token formats (username-password pairs, X.509 certificates, etc.) and allow for the explicit inclusion of a token or an assertion regarding a security token that exists elsewhere.

Message confidentiality is established through a combination of XML encryption and security tokens. Similar to the case with digital signatures, the encryption mechanisms defined in WS-Security are designed to support a wide variety of encryption technologies, processes and operations by multiple actors. An encrypted element may also reference a security token.

The WS-Security specification also defines a mechanism for encoding binary security tokens such as X.509 certificates, Kerberos tickets and opaque encrypted keys, and for transmitting them with a SOAP message.

Figure 3 illustrates the structure of a message secured by WS-Security.

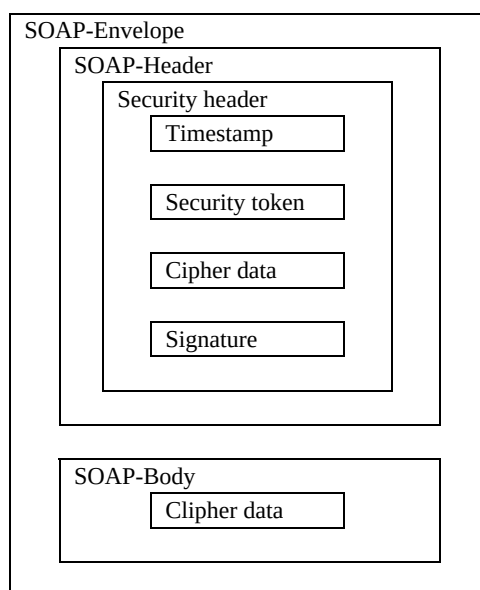


Figure 3 – Structure of a message secured by WS-Security

The XML signature for part of the SOAP message is generated and inserted into the security header element. Part of the SOAP message is encrypted using XML encryption, and its header information is inserted into the security header element; the encrypted part is then replaced by its cipher data. Security token(s) related to the digital signature or encryption is/are added to the security header element. A timestamp element used to determine the freshness of the message may be inserted into the security header element. The security header element is then inserted into the SOAP header part of the SOAP message.

WS-Security is a standard set of SOAP extensions that can be used when building secure web services for message-level integrity and confidentiality. It is a building block that can be used in conjunction with other web services extensions and higher-level, application-specific protocols. In the web services scenarios, SOAP messages may be exchanged via intermediary nodes and WS-Security can provide end-to-end security to the messages. The intermediary nodes may perform additional security processing on the SOAP messages if necessary.

The mobile industry is trying to apply web services technologies to the mobile domain since they can simplify the integration problems between operators, service providers and content providers. The convergence of mobile and web services technologies enables new services and business models and accelerates the development of mobile and fixed Internet technologies.

The mobile web services working group of Open Mobile Alliance (OMA) has developed a specification suite that will aid developers in applying web services to the mobile domain. A summary of the OMA specifications and the differences between the OMA specifications and this Recommendation are described in clause IV.3.

7 Requirements of security architecture and scenarios for message security in mobile web services

Applying existing security technologies to mobile web services directly is difficult because they have different security requirements. This clause analyses the security requirements for mobile web services.

In web services scenarios, SOAP messages may be exchanged via intermediary nodes. When SOAP

messages traverse between an originator and the final SOAP endpoint, it may be a requirement that information be kept secret from SOAP intermediaries. Transport level security protocols such as TLS cannot satisfy this requirement. WS-Security is adequate for such cases since it can provide end-to-end security to the messages. Although WS-Security and other web services security technologies have been standardized, applying the technologies to the mobile environment is difficult since most of the mobile terminals do not have sufficient processing power to support the web services protocol stack fully. Moreover, many back-end application servers are not based on web services; hence the need for a security service architecture that provides security interworking mechanisms between mobile web services and legacy non-web services.

Since mobile web services use HTTP ports, and they cannot be filtered by firewalls, it is required to provide message filtering mechanism based on message contents in the security service architecture. It is also necessary to integrate security policy mechanisms suitable for mobile web services and the message filtering mechanism into the architecture for secure message delivery in the mobile environment.

8 Security model for mobile web services

This clause describes the security model for mobile web services. This clause identifies security threats and security requirements, and then describes the security functions for mobile web services security. Then, the security architecture and message security service scenarios for mobile web services are described. Appendices I and II describe the detailed reference security architecture and service scenarios for message security in mobile web services, respectively, based on this model.

8.1 Security threats to mobile web services

8.1.1 General security threats

- Masquerade: In a masquerade, an entity pretends to be a different entity. An authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity having such privileges.
- Eavesdropping: Eavesdropping involves viewing information that should not be viewed, either by examining messages in transit or by examining the content stored in a server.
- Replay: A replay occurs when a message or part of it is repeated to produce an unauthorized effect.
- Modification of messages: The modification of a message occurs when the content of a data transmission is altered undetected, thereby resulting in an unauthorized effect.
- Man in the middle attack: A man in the middle attack is an attack wherein an attacker is able to read and modify at will the messages between two parties without either party knowing that the link between them has been compromised.
- Denial of service (DoS): Denial of service occurs when an entity fails to perform its proper function or acts in a manner that prevents other entities from performing their proper functions. Examples include overwhelming the server with requests requiring excessive processing or consuming excessive resources.

8.1.2 Security threats specific to mobile web services

- XML denial of service (XML-DoS): Since web services uses port 80, its XML traffic cannot be filtered by traditional firewalls. Traditional firewalls cannot detect content-level vulnerabilities. An attacker can make use of malicious XML messages, manipulate parts of XML data, or send an oversized XML payload that can trigger load-intensive operations at the target web services. Two of the most important DoS attacks in web services are "coercive parsing" and "oversize payload". A coercive parsing attack uses a deeply nested

XML document. On the other hand, an oversize payload attack uses an extremely large XML document to use up the memory of the service.

- XML message injection and manipulation: An attacker can modify parts of the XML messages or attachments to cause endless loops or failure of an XML parser. The attacker can also make use of recursive elements or XPath expression or unrelated message attachments to perform unintended processing that leads to service failure. This attack usually comes after a man in the middle attack.
- Session hijacking and theft: Some web services providers use session identifiers during communication to identify the service requesters. An attacker can steal and use the identifier information to hijack a session between the web services provider and the consumer.
- Parameter tampering: WSDL provides information on how to use parameters to execute a specific remote operation at the target web services. It is usually opened to the public. An attacker can manipulate different parameter options in order to execute an unauthorized operation.

8.2 Security requirements

- Access control: This is required to ensure that only authorized users or devices are allowed to access appropriate system resources or services.
- Authentication: This is required to confirm the identities of the communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication and provides assurance that an entity is not attempting a masquerade or an unauthorized replay of a previous communication. Authentication techniques may be required as part of access control.
- Non-repudiation: Non-reputation provides the means for preventing an individual or an entity from denying having performed a particular action related to data by making available proof of various network-related actions.
- Data confidentiality: This is required to protect data that is being transported, processed or stored by a network service against unauthorized access or viewing.
- Communication security: This ensures that information flows between authorized endpoints only. Communication security ensures that the information is neither diverted nor intercepted as it flows between these endpoints.
- Data integrity: Data integrity ensures the correctness or accuracy of data. Data is protected against unauthorized modification, deletion and replication, providing an indication of these unauthorized activities.
- Availability: This ensures that there is no denial of authorized access to network element, stored information flows, services, and applications due to events affecting the network.
- Privacy: Privacy refers to the right of individuals to control or influence which information related to them may be collected and stored and to whom such information may be disclosed.

Table 1 summarizes the relationship between the general security threats and security requirements.

Table 2 summarizes the relationship between the mobile web services-specific security threats and security requirements.

In each table, cells marked with "X" mean that a security requirement in the row is related to a threat in the column.