RTCWeb Working Group
Internet Draft

Intended status: Informational
Expires:August 8, 2014

Z. Cheng
M. Qi
J. Zhu
China Mobile
Feb. 8, 2014

Security Authentication of WebRTC Communication Service for Telephony Terminal
draft-cheng-rtcweb-teleauth-00

Abstract

The WebRTC use-cases and related requirements are defined in [draft-ietf-rtcweb-use-cases-and-requirements] that contains browser to browser use-cases and browser-GW/server use-cases (e.g., telephony terminal). In the use-case of telephony terminal, it is necessary for telephony terminal to be able to attest his identity to the telephony operator. Unlike the current authentication specified in [draft-ietf-rtcweb-security] such as PKI based authentication and web based peer authentication WebRTC communication is directly controlled by the telephony operator, which poses new authentication methods, including re-using existence authentication mechanism of telephony operator and authentication by using web credentials. This document presents the security authentication of WebRTC communication for telephony terminal.

http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

This Internet-Draft will expire on August 8, 2014.

Table of Contents

1. Introduction

The WebRTC use-cases and related requirements are defined in [draft-ietf-rtcweb-use-cases-and requirements] that contains a use-case titled telephony terminal. As shown in Figure 1, a mobile telephony operator allows its customers to use a web browser to access their services, so that WebRTC service is provided by the telephony operator

but not the web server. Therefore, the current authentication solutions (i.e., PKI based authentication and web based peer authentication) are only adaptive for service facilitated by web server, new authentication solutions due to a new exploited entity as operator server should be defined for the use case of telephony terminal, all telephony terminals can be authenticated to access WebRTC communication service provided by the telephony operator.

This document presents the security authentication of WebRTC communication for telephony terminal.

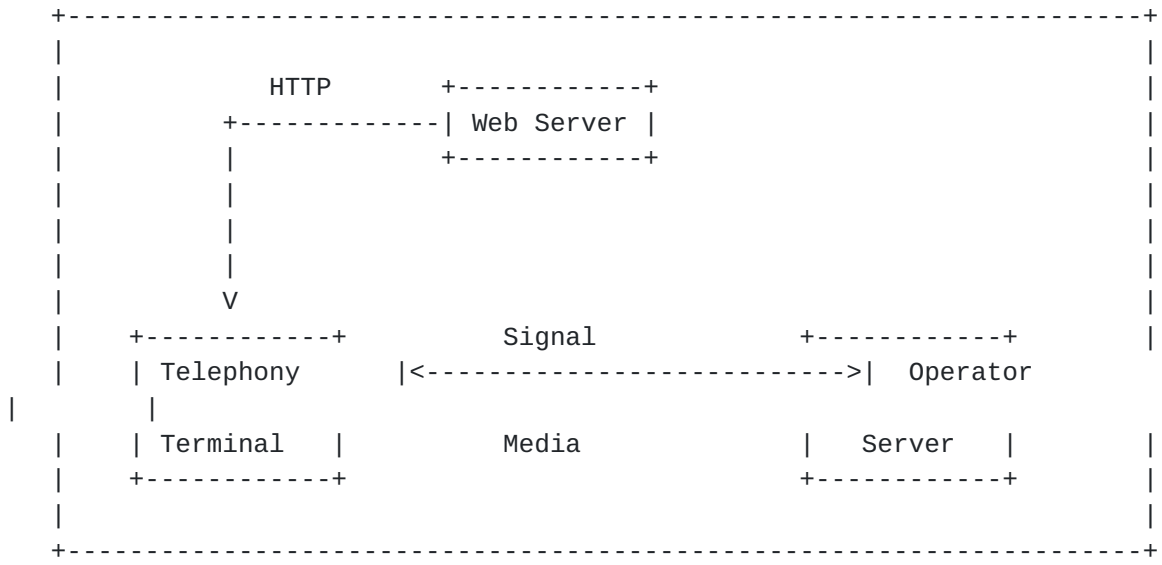

Figure 1. WebRTC system for telephony terminal

2. Conventions used in this document

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 RFC-2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

2.1. Definitions

Terminal: the terminal with browser that is equipped with a WebRTC JS application capable of interconnection with the operator server.

WebRTC application: The WebRTC application is downloaded from the Web server within the operator network or a third party network and provides access to the communications service from the telephony operator.

Web server: The Web Server is the initial point to contact in the Web that controls access WebRTC communications service for the terminal.

Operator server: The operator server is the point to verify any possible authentications of terminals and provide the specific WebRTC communication service for terminals.

3. Problem Statement

3.1 use cases

Nowadays, in current WebRTC use-cases (i.e., browser-to-browser use-cases), the terminals with WebRTC enable browsers visit some Web server which operates a calling service. The current authentication solution either uses PKI-style certificate or Web-based identity (e.g., Brower ID) to authenticate the terminals. In fact, not only the Web server but also the telephony operator can provide a calling service for their terminals.

As depicted in [draft-ietf-rtcweb-use-cases-and-requirements], there exists a specific use-case as follows:
Telephony terminal: A mobile telephony operator allows its customers to use a web browser to access their services. After a simple log in the user can place and receive calls in the same way as when using a normal mobile phone. When a call is received or placed, the identity is shown in the same manner as when a mobile phone is used.
The use-case of Telephony terminal supports two different solutions that differ in authentication methods and ownership of the web server (i.e., operator or the third party). The two solutions are depicted as follows:

Solution 1: The user has a subscription with an identity belongs to the telephony operator and uses an authentication method (e.g. SIP digest) to validate itself with the operator server.

Solution 2: The user has a subscription with an operator identity but uses a web identity and authentication scheme to authenticate with the Web server. The Web server assigns the user an operator credential in terms of the user's web credential for making authentication with the operator server. As aforementioned, the existing authentication solutions are no longer appropriate in the use-case of telephony terminals. When a telephony terminal requests for a calling service, it should prove its identity belongs to the telephony operator in advance, so that the operator permits it to access WebRTC service.

3.2 Current solutions analysis

In the browser-to-browser use-cases, each browser which attempt to communicate with exposes standardized JavaScript calling APIs (implemented as browser built-ins) which are used by the Web server to set up a call. The Web server also serves as the signaling channel to transport control messages between the browsers and service JS sets up some media.

In such use-cases, the conventional solution to providing communications identity usually uses third party identity system (e.g., PKI) to authenticate the browsers.
Furthermore, a new solution using Web-based identity technologies (e.g., BrowserID, Federated Google Login, Facebook Connect, OAuth, OpenID, WebFinger) has recently been developed to provide lightweight (from the user's perspective) third-party Web-based peer authentication. It uses systems of this type to authenticate WebRTC calls, linking them to existing third identity (e.g., Facebook adjacencies). Specifically, the third-party identity system is used to bind the user's identity to cryptographic keying material which is then used to authenticate the browsers.

3.3 problem statement

1. The current solution has the following problems:For PKI-based solution (i.e., PKI-style certificate), it needs to use certificate which is preset between the user and the server. But the certificate management is too cumbersome, including certificate application, issuance, updating, and dispose, it needs to setup the complicated certificate management module.

When AKA procedures using certificate need to check the validity of certificate, it costs extra complexity. However, for telephony user, it owns pre-shared key with operator rather than certificate. Therefore, PKI usage doesn't fit for telephony users.

2. For Web-based solution (i.e., Web-based peer authentication), it is suitable for browser-to-browser use-cases, since the browser is able to directly identify the other calling browser by connecting a Web-based (i.e., HTTP/HTTPS) identity provider without trusting the Web server which they are logged in. That means it is a general principle that the party which is being authenticated is NOT the signaling site (i.e., Web server) but rather the user with his browser. Refers to [draft-ietf-rtcweb-security-arch] However, it is necessary for operator server to authenticate its users with their browsers in the telephony terminal use-case. Therefore, Web-based solution can't address this requirements.

4. Requirement

In order to provide the secure WebRTC communication service from the telephony operator to its users/terminals, it is need to design new security authentication solutions for terminals to prove their identities through WebRTC methods in the use-case of telephony terminal.

5. Telephony Terminal Authentication Solution

5.1. Introduction

The security authentication of the use-case so-called Telephony terminal is the adaptive mechanism for the involved entities such as operator server, web server and the terminal to make authentication for WebRTC communication service.

There are two solutions for the authentication mechanisms:
Solution 1: The user has a subscription with an identity belongs to the telephony operator and uses an authentication method (e.g. SIP digest) to validate itself with the operator server.
Solution 2: The user has a subscription with an operator identity but uses a web identity and authentication scheme to authenticate with the

Web server. The Web server assigns the user a operator credential in terms of the user's web credential for making authentication with the operator server.

5.2. authentication solution 1

1. By using a WebRTC-enabled browser, the terminal accesses a URI to the Web server facilitating an HTTPS connection. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WebRTC application from the Web server.
2. The WebRTC application opens a WSS connection to the operator server using standard cross-origin resource sharing procedures to ensure that the application originated from a Web server authorized to access this operator server.
3. The WebRTC application launches a registration transaction with the operator server by sending a REGISTER request via the WSS connection. The REGISTER request includes authentication parameters as needed for proper registration. This request is translated in the operator core network as it is processed by the operator server. This process leverage user credentials in HSS.

5.3. authentication solution 2

1. By using a WebRTC-enabled browser, the terminal accesses a URI to the Web server facilitating an HTTPS connection. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WebRTC application from the Web server.
2. The Web server authenticates the terminal using a common web authentication procedure, determines the identity registered with the operator and assigned it to the terminal, issues a security token to the terminal and returns the identity as claims within the security token to the terminal's WebRTC application.
3. The WebRTC application opens a WSS connection to the operator server using CORS procedures to ensure that the WebRTC application originated from a Web server authorized to access the operator server.
4. The WebRTC application sends a REGISTER request to the operator server via the WSS connection. The request includes the user identity

extracted from the claims in the security token and the security token received from the Web server.

5. The operator server validates the contents of the security token and confirms that the identity being registered is authorized by the security token.
6. The operator returns an OK response to the terminal to announce that authenticates terminal successfully.

6. Security Considerations

This memo considers the security authentication for providing WebRTC service in use case of telephony terminal. So it would not introduce any additional security problems.

7. IANA Considerations

There are no IANA considerations associated to this memo.

8. Conclusions

This memo describes the problem raised by conventional authentication solutions for the use-case of telephony terminal. After that, the telephony terminal authentication requirement is raised and related security authentication solutions are proposed.

9. References

9.1. Normative References

9.2. Informative References

[I-D.ietf-rtcweb-use-cases-and-requirements]
C. Holmberg, et al., "Web Real-Time Communication Use-cases and Requirements", draft-ietf-rtcweb-use-cases-and-requirements-13 (work in progress), February 2014

[I-D.ietf-rtcweb-security-arch]
E. Rescorla, "WebRTC Security Architecture", draft-ietf-rtcweb-security-arch-07 (work in progress), July 2013

Authors' Addresses
Ziyao Cheng
China Mobile
Unit 2, 32 Xuanwumenxi Ave,
Xicheng District,
Beijing 100053, China
Email: chengziyao@chinamobile.com

Minpeng Qi
China Mobile
Unit 2, 32 Xuanwumenxi Ave,
Xicheng District,
Beijing 100053, China
Email: qiminpeng@chinamobile.com

Judy Zhu
China Mobile
Unit 2, 32 Xuanwumenxi Ave,
Xicheng District,
Beijing 100053, China
Email: Zhuhongru@chinamobile.com