Journal of Theoretical and Applied Information Technology
31st October 2015. Vol.80. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# REVIEW OF WEB-BROWSER COMMUNICATIONS' SECURITY

**ANTON PAVLOVICH TEYKHRIB**
Company Naumen (Nau-Service)
E-mail: ateyhrib@naumen.ru

**ABSTRACT**

The issues of Internet communications' security are considered in the article. The causes of security violation and the main threats to communications' security were defined. As a result, it became clear that protection against threat of listening, interception, and data alteration is determined by technology of data transmission, while other threats are connected with organizational issues and infrastructure. Further, security aspects in modern web browsers communications' technologies such as WebRTC and RTMFP are considered. As a result, it became clear that both technologies provide similar protection capabilities based on AES encryption against unauthorized access to data.

**Keywords:** *WebRTC, RTMFP, Internet Communications, Internet Communications' Security Threats, Encryption*

## 1 INTRODUCTION

Nowadays much attention is paid to the Internet communications security issues, both on the part of IT community, and on the part of regulatory authorities. Particularly in 2005, there were published security considerations of US National institute of standards and technologies [1], in which security issues of VoIP means and signaling protocols, such as SIP and H.323, were considered.

The interest in VoIP security is a consequence of the fact that VoIP hacking is easy to monetize [2]. So, finding an error in the service, a hacker can make calls to fee-paying services, "sell line" or to send audio spam. Insecurities were found in solutions of Cisco, Skype, Asterisk and others at different times [3].

Today, there is continued growth of communications over the Internet. At the same time, the use of web browsers, as a unified access point to various information systems and services, is one of the leading trends. The combination of these trends leads to the growth of communications through the web browser. However, the security issue of such communications arises. The study of this issue is the subject of this article. The goal of this article is to review security considerations adopted in two main technologies of communications through web-browser: WebRTC and Adobe Flash RTMFP. Before actual review of technologies, there is necessity to observe causes of security violation and main types of Internet communications threats. This observation will provide criterion for technologies comparison.

## 2 THE CAUSES OF SECURITY VIOLATION

The main reasons for security violation of voice communication at the level of the last mile through the Internet include [4]:

1. Unskilled actions of IP-PBX service specialists.
2. Weak passwords of telephone numbers or their absence.
3. The use of standard passwords for telephone equipment.
4. The use of out-of-date software versions.
5. Lack of the IP-PBX protection against classic hacking techniques such as search of passwords, etc.
6. Lack of network access control system.
7. The incorrect configuration of the IP-PBX, allowing to skip unauthenticated calls.

According to scientific and engineering publications, the attention is paid to two levels of the security organization: a) at the level of functioning of VoIP-systems and intersystem interaction, b) at the level of the security organization within "the last mile" (from the client device to the server of provider).

Potential security threats at the level of the last mile are divided into four groups:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. Interception of communication session, assignment of other people's rights, confidentiality compromise and misrepresentation.
2. Intrusion into an organization's network via flaws, which appeared as a result of VoIP system deploying.
3. Use of IP-PBX fraudulently or through unauthorized access.
4. Improper activities, directed on deterioration of voice services.

Key elements of the information security of IP-telephony networks can be classified as follows: [5]:

1. Privacy: the need of the transmitted information (voice and data) protection in order to prevent the listening or interception of conversations, alteration of a talking or signaling traffic, passwords theft.
2. Integrity: ensuring that unauthorized users don't affect the transmitted information (voice or data), and certain tasks or functions requests (for example, initialization of a voice call or change of configuration parameters) are initiated only by authorized users or applications.
3. Availability: provision of smooth functioning of the corporate IP-telephony system in the conditions of DoS-attacks (Denial of Service), various "worms", "viruses", etc.

Security of the VoIP-systems functioning and intersystem interaction is offered to be organized at the following levels:

1. Security of the public communications network interface (PCN) – such main threats, as substitution of a user and unauthorized access to functions of the corporate information system, are carried out on this level.
2. Security of media stream (voice and video information, transferred in VoIP system) – the main threats of this level are unauthorized listening and activity, leading to the communication quality degradation.
3. Security of signal system – threats of violation of communication system's normal operation (DoS), substitution of a user, theft of access codes to overcome the corporate information system users' restrictions, frauds in DLD / ILD are created on this level.
4. Safety of control system – control interfaces can be attacked on this level in order to thieve users' personal information (username and password) or to organize some attack, for example, DoS-attacks. Supervision and listening of certain ports is sometimes used for obtaining various information (for example, call accounting), which can contain access codes to various services (an exit to the PCN, etc.), or information on the last made calls. In addition, there may be cases of applications substitution and malicious system changes.

## 3 THE MAIN TYPES OF INTERNET COMMUNICATIONS THREATS. CRITERIA OF SECURITY.

The aim of this section is to describe and classify the main security issues, which arise when performing Internet communications.

In order to determine the issues, connected with security of communication systems it is necessary to define the threats of information security, arising in the course of such systems' operation. Information Security Threat (IST) – set of the conditions and factors creating potential or factual danger of information security violation. However, the realization of this or that threat is defined on the basis of insecurities of information system. Security vulnerability is the property of information system causing implementability of security threats.

The following ISTs of communications system can be distinguished:

1. Human factor – problems, associated with actions of a person, incorrect equipment and software adjustment, software errors, problems of protocols, which can lead to the situation when an attacker acts as an ordinary user and carry out such subsequent attacks, as a phishing, spam attacks, stealing of a service.
2. Listening, audio interception, and alteration are situations, in which a hacker could interfere in the process of session's establishing or direct transmission of data flow, remaining unidentified.
3. Denial of service (DoS) – situation in which users lose access to information and communication system.Within this threat, users can lose all opportunities for communication. Such attacks can be specialized both for communication systems, and generalized, can be associated with physical damage of the equipment, as well as, at the level of computing infrastructure (for example, violation of the DNS service).
4. The unauthorized use of some communication services, as an example, a violator's calls at the expense of a subscriber.
5. Physical damage of communication hardware or physical level of network (in the 7-level OSI model).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. The unintentional termination of service's work, leading to communications' quality degradation. The example of such threats may be overload of the service, the power off in consequence of force majeure, etc.

Within the article, it is necessary to concentrate on determination of those Information Security Threats against which protection will be directed.

The attacks' distribution by the Information Security vulnerabilities' [7] types, is presented 4 main types:

1. Denial of service (56%).
2. Listening, audio interception and traffic alteration (20%).
3. The human factor (18%).
4. Unlawful use of service, physical violation of equipment operability (4%).

We will consider these vulnerabilities in more detail.

### 3.1 Denial Of Service

The attacks, leading to denial of service, are one of the most common types of attacks. They are quite different from each other. In particular, there is [8] the following classification of attacks:

1. Specific to Internet communications'systems.
2. Overload of equipment and software by enquiries.
3. Sending of incorrect enquiries.
4. Incorrect use of the traffic preference settings (QoS).
5. Sending of fictitious enquiries.
6. Destruction of messages.
7. Network level.
8. Level of an operating system, hardware firmware.
9. Distributed traffic overload from a set of infected computers.

### 3.2 Listening, Audio Interception And Change Of Traffic

This type of attacks is used to receive unauthorized access to the transmitted data, in particular:

1. Listening to voice, video, graphic and text data.
2. Analysis of communications' lines.
3. Determination of network's participants, their presence in a network.

As well as altering of network traffic, such as:

1. Interception (suppression) of transmitted data.
2. Unauthorized redirection of communications.
3. Substitution of a caller's identity.
4. Change of voice, video, graphic and text data.

### 3.3 Human Factor

The human factor is one of the most complex vulnerabilities that any information system faces. Complexity can be explained by the reason that influence of this factor is related to the all lifecycle phases of information system:

1. Design – there are errors in software's architecture.
2. Development – there are errors in implementation of data communication protocols and data processing.
3. Testing – not covered software use cases allows mistakes from the previous phases to remain unnoticed.
4. Deployment – there are errors at the level of configuration.
5. Operation – the mistakes connected with disregard of rules of safe use of information system, work with registration data, etc.

Work with exposures of this class demands direct work with people, involved in the life cycle of information systems. This work should be aimed at improving the culture of information security and discipline of adherence to safety rules. Direct development of these rules and organization of the development process and design, directed on minimization of mistakes in information systems, is required.

### 3.4 Selection Of The Research Direction In The Field Of Security

Among the considered ISTs types for communication systems, 96% of cases of the realized IST's can be reduced to three types (in decreasing order of a share): denial of service; listening, interception and data alteration; human factor. Thus, it should be taken into account that the work with a human factor is more organizational in its nature, than realization of any principles in the information system. The only thing that can reduce this ISC is the maximum simplification of the software configuration and operation, which will reduce quantity of user errors and administrators of information system.

At the same time it is worth noting that for ensuring protection against attacks, leading to a denial of service, it is necessary to consider the whole infrastructure context of the communication information system's use, because this type of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attacks can be carried out both on the level of information system, and also on the transport and network levels.

Protection against IST on listening, interception and data alteration can be carried out on the level of Internet communications system and can be technologically realized due to use of protocols and technologies.

We will compare the listed threats by the following criteria:

- Realization on the level of Internet communications system.
- Realization on the infrastructure level.
- Realization on the organizational level.

Comparison of the specified IST by the specified criteria is presented in Table 1.

*Table 1 – Comparison of Information Security Threats*

| | Denial of service | Listening, audio interception and data change | Human Factor |
|---|---|---|---|
| Realization on the level of Internet communications' system | + | + | - |
| Realization on the level of infrastructure | + | - | - |
| Realization on the level of organization | - | - | + |

Only the direction associated with listening, audio interception and change of data is localized in the system of Internet communications. Therefore, security from the attacks, related with interception and change of transmitted data, for further studies in the framework of the article, will be considered. Moreover, this type of security is defined by the following characteristics:

- Protection of session's setup process.
- Protection of transmitted data flow.

In this regard, in accordance with [8] by the protection is meant:

- Preserving the integrity of packages or violation indication.
- Ensuring access to contents of the package only to authorized participants of a transfer.

Providing these protection characteristics is achieved by addressing the following questions. On the one hand, it is necessary to have opportunity to identify a user and to define the user's rights for access to the transferred stream data and process of a session establishment; on the other hand, it is necessary to hide transmitted data from users, who aren't relating to this transmission. For solution of the first problem, it is necessary to solve a problem of development of the decentralized signaling protocol, supporting establishment of a session, authentication and authorization of users, in turn, consideration of possible options and a choice of the most suitable one for this purpose is required. To solve the second problem, it is necessary to provide encryption of the transmitted data. For this purpose it is necessary to consider possible methods and algorithms of the transmitted data's encryption. One of the direct data encryption procedures is a procedure of a key exchange, which also should be considered within this research.

## 4 COMPARISON OF WEBRTC AND RTMFP BY SAFETY CRITERIA

We will carry out comparison of security parameters of voice Internet communications by means of WebRTC and RTMFP in the aspect of encryption facilities.

Considering security of particular way of communications in the Internet, it is necessary to pay attention to the solution of the following issues:

- Encryption methods and algorithms.
- Keys exchange methods.
- Authentication and authorization of users.

Realization of these methods, in the considered technologies, is required for ensuring security of the considered levels.

### 4.1 WebRTC

The WebRTC technology doesn't regulate procedure of the streaming session establishment. It only determines directly the transfer process. Therefore, we will separately consider procedure of a session establishment and data transmission.

#### 4.1.1 Encryption methods and algorithms

When establishing a streaming session, methodical literature from the manufacturers of specialized solutions recommends using a variety of solutions, in particular Microsoft recommends in most cases to use a WebSocket secure (WSS) connection [9]. On the one hand, it makes possible to provide connection security, on the other hand, it

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

increases the chances of a successful connection, because many proxy servers reject WebSocket's unencrypted connection.

In the notation of "WebSocket Security" [10] from Heroku (one of the world's most popular PaaS platform), the use of the protected WSS protocol is also recommended.

WSS is based on TLS [11] (Transport Layer Security) which is a cryptographic protocol that provides a protected data communication between network nodes using asymmetric cryptography for authentication, symmetric encryption for privacy and authenticity codes of messages to preserve the integrity of messages. TLS establishes a tunnel, which provides low-level TCP connection like point-to-point via the HTTP proxy server between WebSocket Secure client and WebSocket server.

Another version of the procedure of establishing securely a thread-specific data transfer session within the WebRTC technology is the use of HTTPS requests with long timeout (long polling). In this case, protection is also provided due to the use of transport layer protocol - TLS.

Therefore, both approaches can be used to establish a secure data transfer session. For secure voice and media data communication within the WebRTC traditional Secure Real- time Transport Protocol (SRTP) must to be used. AES encryption algorithm (symmetric algorithm of block encryption) makes possible to implement function of cryptographic protection for voice messages. It is a real-time protection of voice data and it has little effect on the key characteristics of data transmission such as exchange time.

#### 4.1.2 Key exchange methods

Key exchange at the signal level takes place within the TLS protocol. For the streaming data, it is reasonably to use protocols, which are applied to RTP protocol. To generate and distribute encryption keys of media information among the communication subjects SDES, ZRTP, DTLS protocols may be used. We will give a brief description of them.

SDES protocol description is provided in RFC 4568. According to this approach, the key is transmitted in the SIP-message through the signaling channel, and the recipient uses it to encrypt the traffic (the exchange of signaling messages must also be protected). Thus, the possibility to use SDES protocol is limited by obligatory SIP/TLS connection security (described above). Another limiting factor is an inability to use this protocol to ensure the "point-to-point" security, for example, when using a virtual PBX, SDES will distribute keys between the first communication subject and virtual PBX and between the second communication subject and virtual PBX, but not directly between the communicating parties.

ZRTP protocol is designed specifically for VoIP and standardized in RFC 6189. The protocol provides secure authentication and data exchange. During ZRTP-call initialization a Diffie – Hellman key exchange method is used (a cryptographic protocol that allows two or more parties to get a shared secret key using covertness-unprotected channel), which does not protect against attacks such as "man in the middle" (man in the middle). To overcome this problem for authentication purposes it is used SAS (Short Authentication String) that is a short-cut representation of cryptographic hash of received Diffie – Hellman keys.

DTLS protocol for SRTP is described in RFC 5764 specification. It describes the exchange of voice traffic in "point-point" mode with rigid fixation of UDP ports that communication subjects have. Protocol messages are transmitted together with the RTP-packets. To organize the communication session, participants exchange messages. Since the DTLS protocol is based on TLS (Transport Layer Security), that uses public key infrastructure (PKI), then the application of DTLS may be possible also only with infrastructure issue nodes, storage and verification of communication subjects' certificates.

It should be noted that according to the draft standard [12] only DTLS is required to support information systems that implement WebRTC.

#### 4.1.3 User authentication and authorization

The WebRTC technology doesn't determine the method of user authentication and authorization, so this issue demands an independent solution.

### 4.2 RTMFP

In the case of the RTMFP, the approaches, considered in the context of the WebRTC technology, can't be used due to the fact that one protocol is used both for establishment of data transmission session and direct transmission.

#### 4.2.1 Encryption methods and algorithms

We will consider opportunities of encryption within the RTMFP. Use of any encryption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

algorithm isn't set in the RTMFP protocol. The need for its use is only indicated [13]. However, over time after publication of this protocol, there was a description of its specific realization, which is used in products of the Adobe Company. We will consider this realization. The encryption by means of the AES code with 128 bit keys is used in this realization [14]. Packages of a session establishment for stream data transfer and directly transmitted data are encrypted in the same way and with the same keys.

#### 4.2.2 Key exchange methods

Key exchange is carried out in two stages:

- Session is established on the first stage and common key (symmetric encryption) is used, which is set in [14]: "Adobe Systems 02" in the UTF-8 coding, thus the cryptographic 16-bit checksum is used for check of the package's integrity. There is an exchange of asymmetric keys for subsequent work within establishment of a session;
- further, an establishment of the common confidential key is carried out on the basis of the Diffie-Hellman's algorithm that becomes possible due to the established connection, protected from alteration (but available for listening).

After establishment of the common key, all newly transmitted data are coded with its help.

#### 4.2.3 User authentication and authorization

There is no support for authentication and authorization in implementation of the RTMFP protocol. In accordance with [14], any well-encoded certificate will be considered as valid. In this regard, when using the RTMFP protocol, it is required to develop a separate algorithm for user authentication and subsequent authorization that will operate over the RTMFP protocol.

Thus, in the case of using the RTMFP protocol, the issues, related to the key exchange and encryption of transmitted data, have a solution, but has not addressed issues, related to user authorization and authentication. The solution of this issue within this protocol shall be executed in the next stage.

### 4.3 Final Comparison

Final comparison is presented in Table 2.

*Table 2. WebRTC And RTMFP Security Comparison*

| | WebRTC | RTMFP |
|---|---|---|
| Encryption algorithm | AES | AES |
| Key exchange | DTLS | Own algorithm based on Diffie-Hellman |
| Authentication and authorization | Should be developed separately | Should be developed separately |

Thus, it is visible from comparison of security settings of the described technologies that the algorithm of AES in both technologies is used for direct encryption, but the mechanism of key exchange differs. So, use of the DTLS protocol is mandated for the WebRTC technology (also other algorithms can be used additionally) for key exchange, while an own algorithm is supposed for the RTMFP. At the same time, there is no regulation of the protocol for establishment of a communication session for WebRTC, so it is necessary to develop independent solutions for such session establishment. At the same time, both technologies do not allow organizing the process of user authentication and authorization, and this process should be developed independently.

## 5 FURTHER RESEARCH

This research shows that both technologies are security aware and shows usage of widely adopted algorithms and methods. Unfortunately, developer should make own solution for user authentication and authorization. This is a topic for further research.

## 6 CONCLUSIONS

Security aspects in Internet communication were considered in this article. The main threats to such communications were identified, namely:

- Denial of service.
- Listening, interception and alteration of transmitted data.
- Human factor.

Attacks on vulnerabilities of the listed types make up to 96% of all attacks on Internet communications. Based on consideration of these threats, it was determined that only work with threat of listening, interception and alteration of transmitted data is determined by communication technology; other threats are connected with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

organizational moments and used infrastructure. Further, the technologies of Internet communications, applied in web browsers, were considered: Adobe Flash RTMFP and WebRTC and ways of protection in them against threat of listening, interception and alteration of transmitted data. The research found that encryption by the AES algorithm is used for protection against this threat within these technologies. However, the protocols of a streaming data session establishment and user authorization and authentication should be developed separately.

## 7 ACKNOWLEDGEMENTS

The article is published under financial support of the Ministry of Education and Science of the Russian Federation. The unique identifier of the applied scientific research RFMEFI57614X00086.

## REFERENCES

[1] D. R. Kuhn, T. J. Walsh and S. Fries, "Security Considerations for Voice Over IP Systems. Recommendations of the National Institute of Standards and Technology", *National Institute of Standards and Technology*, Gaithersburg, 2005.

[2] G. Gritsay, "VOIP security", [On the Internet]. Available: http://www.ptsecurity.ru/ics/%D0%93.%D0%93%D1%80%D0%B8%D1%86%D0%B0%D0%B9_%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_VoIP.pdf . [Access date: June 5, 2015].

[3] S. Yaremchuk, "Securing of VoIP-service and protection against listening", [On the Internet]. Available: https://xakep.ru/2014/09/08/safe-voip. [Access date: June 3, 2015].

[4] D. Balashov, "Security of VoIP-connections", 2010. [On the Internet]. Available: http://www.lastmile.su/files/article_pdf/3/article_3898_39.pdf. [Access date: May 6, 2015].

[5] V. Dokuchayev, "Information security in the corporate VoIP networks", *Telecommunication*, No. 4, pp. 5-8, April, 2012.

[6] A. Keromytis, "A Comprehensive Survey of Voice over IP Security Research", *Communications Surveys & Tutorials,* b. 14, No. 2, pp. 514-537, 2012.

[7] A. Keromytis, "Voice-over-IP Security: Research and Practice", *Security & Privacy,* n. 8, No. 2, pp. 76-78, 2010.

[8] "VoIP Security and Privacy Threat Taxonomy", *VoIP Security Alliance*, October 2005.

[9] Microsoft, "How to protect the WebSocket connections by means of the TLS/SSL protocol (XAML)", Microsoft, [On the Internet]. Available: https://msdn.microsoft.com/ru-ru/library/windows/apps/xaml/hh994399.aspx. [Access date: June 9, 2015].

[10] Heroku, "WebSocket Security", [On the Internet]. Available: https://devcenter.heroku.com/articles/websocket-security. [Access date:June 13, 2015].

[11] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol", *Internet Engineering Task Force (IETF)*, 2008.

[12] C. S. Perkins, M. Westerlund and J. Ott, "Web Real-Time Communication (WebRTC): Media Transport and Use of RTP", *Internet Engineering Task Force (IETF)*, 2015.

[13] M. Thornburgh, "Adobe's Secure Real-Time Media Flow Protocol", *Internet Engineering Task Force (IETF)*, 2013.

[14] M. Thornburgh, "Adobe's RTMFP Profile for Flash Communication", *Internet Engineering Task Force (IETF)*, 2014.