Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 3, 2020

I. Symeonidis
University of Luxembourg
B. Hoeneisen
Ucom.ch

October 31, 2019

Privacy and Security Threat Analysis for Private Messaging draft-symeonidis-pearg-private-messaging-threats-00

Abstract

Modern email and instant messaging applications offer private communications between users. As IM and Email network designs become more similar, both share common concerns about security and privacy of the information exchanged. However, the solutions available to mitigate these threats and to comply with the requirements may differ. The two communication methods are, in fact, built on differing assumptions and technologies. Assuming a scenario of untrusted servers, we analyze threats against message delivery and storage, the requirements that these systems need, and the solutions that exist in order to help implement secure and private messaging. From the discussed technological challenges and requirements, we aim to derive an open standard for private messaging.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 3, 2020.

Copyright Notice

Table of Contents

1. Introduction

Private messaging should ensure that, in an exchange of messages between (two) peers, no one but the sender and the receiver of the communication will be capable of reading the messages exchanged at any (current, future or past) time. Essentially, no one but the communicating peers should ever have access to the messages during transit such as Telecom, Internet providers, or intermediary parties, and storage such as messaging servers. As private messaging, we are referring to Instant Messaging (IM) [RFC2779], such as WhatsApp and Signal, and Emailing applications, such as the centralized Protonmail and the fully decentralized pEp [I-D.birk-pep].

The aim of this document is to provide an open standard for private messaging requirements, as well as a unified evaluation framework. The framework catalogues security and privacy threats and the corresponding, to threats, requirements. IM and Email applications have common feature design characteristics and support a common set of information assets for transmission during communication between peers. For example, applications for both systems should support message exchange of text and files (e.g., attachments) in a private messaging manner.

Despite having common characteristics, IM and Email have network design divergences in areas such as responsiveness and synchronicity. For example, low-latency and synchronous were the common features for instant messaging and high-latency and asynchronous for email. As IM and Email network designs become more similar, approaches to security and privacy should be able to address both types of communications. Current IM applications tend to be asynchronous, allowing delivery of messages when the communicating parties are not at the same time online.

Solutions available to implement private messaging in the two types of applications may call for different mitigation mechanisms and design choices. For instance, confidentiality can be preserved in multiple ways and with various cryptographic primitives. As design choices, it depends on the expected level of protection and the background of the user. For instance, for users whose lives may be at stake, such as journalists, whistleblowers, or political dissidents, the design choices for requirements and mitigation mechanisms can be (and often are) much more advanced than those for organizations and general end-users. Despite this distinction, privacy and security on the internet are Human Rights, and easily-enabled means to protect these rights need to exist. But in cases where stronger protections are required, usability may come second to more robust protection.

The objectives of this document are to create an open standard for secure messaging requirements. The open standard for private messaging aims to serve as a unified evaluation framework, including an adversarial model, threats, and requirements. With this document, we catalogue the threats and requirements for implementing secure and private messaging systems. In this current version, we discuss two key design features of IM and Email, message delivery and storage/ archival. This draft is an ongoing work in progress, and the list of requirements discussed here are not exhaustive. However, our work already shows an emerging and rich set of security and privacy challenges.

Of course, IM additionally can support voice/video calls, which is an additional feature/asset under which a threat assessment and requirements can be evaluated.

1.1. Requirements Language

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].

1.2. Terms

The following terms are defined for the scope of this document:

- Man-in-the-middle (MITM) attack: cf. [RFC4949], which states: "A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association."

2. System Model

2.1. Entities

- Users: The communicating parties who exchange messages, typically referred to as senders and receivers.

- Messaging operators and network nodes: The communicating service providers and network nodes that are responsible for message delivery and synchronization.

- Third parties: Any other entity who interacts with the messaging system.

2.2. Assets and Functional Requirements

This section outlines a private messaging system. It describes the functionalities that needs to support and the information that can be collected by the system as assets from users. We follow the requirements extracted from real world systems and applications as well as from the academic literature for email and instant messaging [Unger] [Ermoshina] [Clark].

Assets:

- Content: text, files (e.g., attachments), voice/video
- Identities: sender/receiver identity, contact list
- Metadata: sender/receiver, timing, frequency, packet size

Functionalities:

- [Email/IM] Messages: send and receive text + attachments
  - Peer or group: more than 2 participants communicating
- [IM] Voice / video call
- [Email/IM] Archive and search: of messages and attachments
- [Email/IM] Contacts: synchronisation and matching
- [Email/IM] Multi-device support: synchronisation across multiple devices

3. Threat Analyses and Requirements

This section describes a set of possible threats. Note that typically not all threats can be addressed in a system, due to conflicting requirements.

3.1. Adversarial Model

An adversary is any entity who leverages threats against the communication system, whose goal is to gain improper access to the message content and users' information. They can be anyone who is involved in communication, such as users of the system, message operators, network nodes, or even third parties.

- Internal - external: An adversary can seize control of entities within the system, such as extracting information from a specific

entity or preventing a message from being sent. An external adversary can only compromise the communication channels themselves, eavesdropping and tampering with messaging such as performing Man-in-the-Middle (MitM) attacks.

- Local - global: A local adversary can control one entity that is part of a system, while a global adversary can seize control of several entities in a system. A global adversary can also monitor and control several parts of the network, granting them the ability to correlate network traffic, which is crucial in performing timing attacks.

- Passive - active: A passive attacker can only eavesdrop and extract information, while an active attacker can tamper with the messages themselves, such as adding, removing, or even modifying them.

Attackers can combine these adversarial properties in a number of ways, increasing the effectiveness - and probable success - of their attacks. For instance, an external global passive attacker can monitor multiple channels of a system, while an internal local active adversary can tamper with the messages of a targeted messaging provider [Diaz].

3.2. Assumptions

In this current work, we assume that end points are secure such that the mobile devices of the users. Moreover, we assume that an adversary cannot break any of the underline cryptographic primitives.

3.3. Security Threats and Requirements

3.3.1. Spoofing and Entity Authentication

Spoofing occurs when an adversary gains improper access to the system upon successfully impersonating the profile of a valid user. The adversary may also attempt to send or receive messages on behalf of that user. The threat posed by an adversary's spoofing capabilities is typically based on the local control of one entity or a set of entities, with each compromised account typically is used to communicate with different end-users. In order to mitigate spoofing threats, it is essential to have entity authentication mechanisms in place that will verify that a user is the legitimate owner of a messaging service account. The entity authentication mechanisms typically rely on the information or physical traits that only the valid user should know/possess, such as passwords, valid public keys, or biometric data like fingerprints.

3.3.2. Information Disclosure and Confidentiality

An adversary aims to eavesdrop and disclose information about the content of a message. They can attempt to perform a man-in-the-middle attack (MitM). For example, an adversary can attempt to position themselves between two communicating parties, such as gaining access to the messaging server and remain undetectable while collecting information transmitted between the intended users. The threat posed by an adversary can be from local gaining control of one point of a communication channel such as an entity or a communication link within the network. The adversarial threat can also be broader in scope, such as seizing global control of several entities and communication links within the channel. That grants the adversary the ability to correlate and control traffic in order to execute timing attacks, even in the end-to-end communication systems [Tor]. Therefore, confidentiality of messages exchanged within a system should be guaranteed with the use of encryption schemes

3.3.3. Tampering With Data and Data Authentication

An adversary can also modify the information stored and exchanged between the communication entities in the system. For instance, an adversary may attempt to alter an email or an instant message by changing the content of them. As a result, it can be anyone but the users who are communicating, such as the message operators, the network node, or third parties. The threat posed by an adversary can be in gaining local control of an entity which can alter messages, usually resulting in a MitM attack on an encrypted channel. Therefore, no honest party should accept a message that was modified in transit. Data authentication of messages exchanged needs to be guaranteed, such as with the use of Message Authentication Code (MAC) and digital signatures.

3.3.4. Repudiation and Accountability (Non-Repudiation)

Adversaries can repudiate, or deny, the status of the message to users of the system. For instance, an adversary may attempt to provide inaccurate information about an action performed, such as about sending or receiving an email. An adversary can be anyone who is involved in communicating, such as the users of the system, the message operators, and the network nodes. To mitigate repudiation threats, accountability, and non-repudiation of actions performed must be guaranteed. Non-repudiation of action can include proof of origin, submission, delivery, and receipt between the intended users. Non-repudiation can be achieved with the use of cryptographic schemes such as digital signatures and audit trails such as timestamps.

3.3.5. Elevation of Privilege and Authorization

An adversary may attempt to elevate privileges aiming to gain access to the assets of other users or the resources of the system. For instance, an adversary may attempt to become an administrator of a message group or a superuser of the system aiming at retrieving users' messages or executing operations as a superuser. Therefore, authorization mechanisms such as access control lists that comply with the principle of least privilege for user accounts and processes should be applied.

3.4. Privacy Threats and Requirements

3.4.1. Identifiability - Anonymity

Identifiability is defined as the extent to which a specific user can be identified from a set of users, which is the identifiability set. Identification is the process of linking information to allow the inference of a particular user's identity [RFC6973]. An adversary can identify a specific user associated with Items of Interest (IOI), which include items such as the ID of a subject, a sent message, or an action performed. For instance, an adversary may identify the sender of a message by examining the headers of a message exchanged within a system. To mitigate identifiability threats, the anonymity of users must be guaranteed. Anonymity is defined from the attackers perspective as the "attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set" [Pfitzmann]. Essentially, in order to make anonymity possible, there always needs to be a set of possible users such that for an adversary the communicating user is equally likely to be of any other user in the set [Diaz]. Thus, an adversary cannot identify who is the sender of a message. Anonymity can be achieved with the use of pseudonyms and cryptographic schemes such as anonymous remailers (i.e., mixnets), anonymous communications channels (e.g., Tor), and secret sharing.

3.4.2. Linkability - Unlinkability

Linkability occurs when an adversary can sufficiently distinguish within a given system that two or more IOIs such as subjects (i.e., users), objects (i.e., messages), or actions are related to each other [Pfitzmann]. For instance, an adversary may be able to relate pseudonyms by analyzing exchanged messages and deduce that the pseudonyms belong to one user (though the user may not necessarily be identified in this process). Therefore, unlinkability of IOIs should be guaranteed through the use of pseudonyms as well as cryptographic schemes such as anonymous credentials.

3.4.3. Detectability and Observability - Undetectability

Detectability occurs when an adversary is able to sufficiently distinguish an IOI, such as messages exchanged within the system, from random noise [Pfitzmann]. Observability occurs when that detectability occurs along with a loss of anonymity for the entities within that same system. An adversary can exploit these states in order to infer linkability and possibly identification of users within a system. Therefore, undetectability of IOIs should be guaranteed, which also ensures unobservability. Undetectability for an IOI is defined as that "the attacker cannot sufficiently distinguish whether it exists or not." [Pfitzmann]. Undetectability can be achieved through the use of cryptographic schemes such as mix-nets and obfuscation mechanisms such as the insertion of dummy traffic within a system.

3.5. Information Disclosure - Confidentiality

Information disclosure - or loss of confidentiality - about users, message content, metadata or other information is not only a security but also a privacy threat that a communicating system can face. For example, a successful MitM attack can yield metadata that can be used to determine with whom a specific user communicates with, and how frequently. To guarantee the confidentiality of messages and prevent information disclosure, security measures need to be guaranteed with the use of cryptographic schemes such as symmetric, asymmetric or homomorphic encryption and secret sharing.

3.6. Non-repudiation and Deniability

Non-repudiation can be a threat to a user's privacy for private messaging systems, in contrast to security. As discussed in section 6.1.4, non-repudiation should be guaranteed for users. However, non-repudiation carries a potential threat vector in itself when it is used against a user in certain instances. For example, whistle-blowers may find non-repudiation used against them by adversaries, particularly in countries with strict censorship policies and in cases where human lives are at stake. Adversaries in these situations may seek to use shreds of evidence collected within a communication system to prove to others that a whistle-blowing user was the originator of a specific message. Therefore, plausible deniability is essential for these users, to ensure that an adversary can neither confirm nor contradict that a specific user sent a particular message. Deniability can be guaranteed through the use of cryptographic protocols such as off-the-record messaging.

3.6.1. Policy Non-compliance and Policy compliance

Policy non-compliance can be a threat to the privacy of users in a private messaging system. An adversary, can attempt to process information about users unlawfully and not-compliant to regulations. It may attempt to collect and process information of users exchanged in emails without the users' notification and explicit consent. That can result in unauthorized processing of users information under the General Data Protection Regulation resulting in of such as profiling, advertisement and censorship. Therefore, data protection policy compliance must be guaranteed. It can be achieved with auditing such as with Data Protection Impact Assessment considering [GDPR].

4. Security Considerations

Relevant security considerations are outlined in Section 3.3.

5. Privacy Considerations

Relevant privacy considerations are outlined in Section 3.4.

6. Future Key Challenges

Reducing metadata leakage and standardization (i.e. prevent further fragmentation).

7. IANA Considerations

This document requests no action from IANA.

[[RFC Editor: This section may be removed before publication.]]

8. Acknowledgments

The authors would like to thank the following people who have provided feedback or significant contributions to the development of this document: Athena Schumacher, Claudio Luck, Hernani Marques, Kelly Bristol, Krista Bennett, and Nana Karlstetter.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

9.2. Informative References

[Clark] Clark, J., van Oorschot, P., Ruoti, S., Seamons, K., and D. Zappala, "Securing Email", CoRR abs/1804.07706, 2018.

[Diaz] Diaz, C., Seys, St., Claessens, J., and B. Preneel, "Towards Measuring Anonymity", PET Privacy Enhancing Technologies, Second International Workshop, San Francisco, CA, USA, April 14-15, 2002, Revised Papers, pp. 54-68, 2002.

[Ermoshina] Ermoshina, K., Musiani, F., and H. Halpin, "End-to-End Encrypted Messaging Protocols: An Overview", INSCI 2016: pp. 244-254, 2016.

[GDPR] "General Data Protection Regulation 2016/680 of the European Parliament and of the Council (GDPR).", Official Journal of the European Union, L 119/89, 4.5.2016 , April 2016, <https://eur-lex.europa.eu/eli/dir/2016/680/oj>.

[I-D.birk-pep] Marques, H., Luck, C., and B. Hoeneisen, "pretty Easy privacy (pEp): Privacy by Default", draft-birk-pep-04 (work in progress), July 2019.

[Pfitzmann] Pfitzmann, A. and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management", 2010, <https://nyuscholars.nyu.edu/en/publications/sok-secure-messaging>.

[RFC2779] Day, M., Aggarwal, S., Mohr, G., and J. Vincent, "Instant Messaging / Presence Protocol Requirements", RFC 2779, DOI 10.17487/RFC2779, February 2000, <https://www.rfc-editor.org/info/rfc2779>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[Tor] Project, T., "One cell is enough to break Tor's anonymity", June 2019, <https://blog.torproject.org/one-cell-enough-break-tors-anonymity/>.

[Unger] Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., and M. Smith, "SoK: Secure Messaging", IEEE Proceedings - 2015 IEEE Symposium on Security and Privacy, SP 2015, pages 232-249, July 2015, <https://nyuscholars.nyu.edu/en/publications/sok-secure-messaging>.

Appendix A. Document Changelog

[[RFC Editor: This section is to be removed before publication]]

- draft-symeonidis-pearg-private-messaging-threats-00:
  - Initial version
  - this document partially replaces draft-symeonidis-medup-requirements-00

Appendix B. Open Issues

[[RFC Editor: This section should be empty and is to be removed before publication]]

- Add more text on Group Messaging requirements
- Decide on whether or not "enterprise requirement" will go to this document

Authors' Addresses

Iraklis Symeonidis
University of Luxembourg
29, avenue JF Kennedy
L-1855 Luxembourg
Luxembourg

Email: iraklis.symeonidis@uni.lu
URI: https://wwwen.uni.lu/snt/people/iraklis_symeonidis

Bernie Hoeneisen
Ucom Standards Track Solutions GmbH
CH-8046 Zuerich
Switzerland

Phone: +41 44 500 52 40
Email: bernie@ietf.hoeneisen.ch (bernhard.hoeneisen AT ucom.ch)
URI: https://ucom.ch/