Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2015

D. Druta
AT&T
T. Fossati
Alcatel-Lucent
M. Ihlar
Ericsson
G. Klas
Vodafone
D. Lopez
Telefonica I+D
J. Reschke, Ed.
greenbytes

October 27, 2014

A Rationale for Fine-grained Intermediary-aware End-to-End Protocols
draft-reschke-objsec-01

Abstract

A tremendous growth in different uses of the Internet has let to a growing need to protect data sent over public networks, including data sent via http. Use of end-to-end TLS for the majority of traffic looks at first a most feasible response. However, the web architecture has become more sophisticated and as it has now gone beyond the simple client-server model, the end-to-end used of TLS is increasingly showing its downside. The end-to-end use of TLS excludes the use of beneficial intermediaries such as use of caches or proxies that provide instrumental services. Then need for greater privacy seems to collide with the equally growing desire for better end-to-end performance and user experience. As an example, the use of HTTP/TLS often appears to maximise the benefit for the combination of both.

This document describes the above dichotomy and lays out a number of objectives of what can ideally be achieved, namely catering for sufficient security and privacy whilst providing users with the opportunity to make use of intermediaries' services where considered beneficial. This document introduces a number of potential solutions towards use of suitable protocol mechanisms and data formats. End-to-end protocols which are aware of intermediaries should enable users and/or content providers to exercise fine-grained control over what intermediaries should be able to do and what exposure to data or metadata they shall be permitted to get. The document then highlights anticipated benefits to key stakeholders such as users, content providers and intermediaries. As elements such as object security can play a useful role, this document encourages the analysis of related work to discern their applicability, limitations,

and coverage of use cases. Such an effort may us espouse innovation to frame an overall architecture and motivate more detailed work on protocols and mechanisms in the future.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In the last decade, the generalization of network access, the cloud and the ubiquity of the Web as an application platform has translated into an unprecedented increase in the use of the Internet, facilitated by the development of new web standards and the innovations in mobile technologies. With this growth in use, there has been an increased amount of personal data being sent over multi hop public links.

In order to protect the integrity and confidentiality of the online transactions, HTTP traffic can be secured with transport layer security using https. While https is great for e-commerce and banking and while there is a sense of understanding in the user community around the secure nature of https, using TLS and https for the majority of the traffic has performance and functional drawbacks, mainly because the HTTP session is encrypted as a whole.

Looking from the privacy and security perspective, it is clear that users must be aware if and when an intermediary node is intercepting their traffic and they have the right to continue or demand higher levels of privacy by encrypting what they deem to be sensitive information. The privacy threshold depends on user's tolerance and the trust they put in the intermediary's reputation, as well as whether the user is the ultimate consent authority for a given connection: for example a parent or employer may take that role for a connection used by a child or employee.

Modern web architecture involves sophisticated caching schemes that involve fetching various objects (images, libraries, etc.) from various locations in the path to avoid latency and improve the overall user experience while reducing bandwidth use. This is an important aspect especially in the developing countries, remote locations and in general areas that lack fast network infrastructure.

Issues thus arise from the clash of two trends: One is towards enhanced privacy calling for integrity, confidentiality and

anonymity. The other one is towards improved performance and lower latency, calling for caching, compression, and adaptability.

This is also reflected in the views of important stakeholders. Users want to make informed decisions in regards to whom they trust with their data. They also want to have control over what data they share with whom.

Web site owners and content providers on the other hand are keen to get the most cost efficient and reliable way to deliver information and services to their users and customers, while preserving their confidentiality, protecting their privacy and the integrity of their data.

As different entities seek to meet the requirements of their stakeholders, they sometimes apply solutions which generate conflicts. Clients act on behalf of end users and solutions may include local caches and browser proxies. Servers act on behalf of content providers and solutions may include the use of CDNs and reverse proxies. Intermediaries operated by communication service providers and network operators act on behalf of users and/or content providers and solutions include means for access network optimization and content filtering.

In above context, the use of TLS and https looks like a "black and white approach", or an "all or nothing" approach which doesn't lend itself to resolving above-mentioned conflicts. The question arises: Can "color be added"?

TLS is a client server protocol and it serves its purpose perfectly in many client-server scenarios and use cases. But then the web has evolved to become a mesh. Average traffic flows now involve various intermediaries between clients and servers. They add value by performing different functions including multiple levels of optimization.

The application of TLS forces point-to-point flows which cuts out intermediaries and can lead to significant drawbacks. It reduces e.g. the optimization options which translates into increasing traffic volumes in access networks, higher latency and overall decreasing quality of experience for users.

It can be observed that ignoring the role of intermediaries on the Internet does not necessarily make the Internet more secure. In fact, in some cases it forces various parties to break the TLS promise of e2e integrity and confidentiality in order to meet their legal obligations (enterprises).

We suggest the solution to the challenge lies in "adding color". An example of this are fine-grained intermediary-aware end-to-end protocols.

Assuming the existence of such a fine-grained protocol, the following benefits could be imagined which leads to satisfying the justified needs of multiple stakeholders:

The ability to atomically encrypt objects or even HTTP frames should support this sophisticated caching mechanisms while allowing content providers to avoid distributing their server key material across the network nodes and prevent the risk of compromising their security.

2. Objectives

Given the short description of the problem above, the following objectives can be derived.

1. To improve security and user-controlled privacy.

2. To minimize passive interception and man in the middle attacks.

3. To allow the client (user) and the server (content provider) to negotiate what and whom they want to give (or not) visibility into their traffic flows.

4. To enable multiple levels of optimization that don't conflict with each other and either meet all parties expectations or maximise the benefit to as many involved parties as possible.

In a world of TLS and https only, it is difficult to achieve in particular objectives 3. and 4.

The challenge therefore is in finding mechanisms or protocols which meet objectives 1. and 2. (e.g. in the way TLS is delivering against those objectives) AND simultaneously provide the added flexibility to leverage the services of 3rd party intermediaries located between client and origin server.

3. Characteristics of Solutions

From above, one can draw some conclusions about the characteristics possible solutions or new protocols may have to show. Below is a non-exhaustive list. A new fine-grained intermediary-aware end-to-end protocol may need to feature:

1. a mechanism to enable users to choose their preferred level of privacy, adequate for a particular context and use case. The

context may be determined by the presence or absence of particular intermediaries or proxies which offer particular services (e.g. caching, data compression etc.).

2. mechanisms that enable certain communication data to be exchanged securely, whereby the end user shall be able to select the set of security services deemed adequate for a particular communication context (e.g. confidentiality, data integrity, entity authentication etc.).

3. mechanisms that enable the end user to select which communication data shall be subject to particular security services (like confidentiality, data integrity etc.). Note that this might be all application level data transferred between server and client, or it might be a subset of application level data. This refers to the notion of "fine-grained" control.

4. mechanisms that protect against passive interception and man-in-the-middle attacks.

5. mechanisms that allow the two ultimate communication end points, namely client and origin server, to negotiate whether and if so which intermediaries shall be permitted to play a role in delivering application data from origin server to client given particular end user expectations, requirements and preferences, and information about the status of the network between client and server. This refers to the notion of "intermediary-aware end-to-end protocol".

6. mechanisms that allow end users or origin server or both to determine in real-time which traffic optimizations are available at the time of communication setup.

7. mechanisms that allow end users or origin servers or both to eventually select zero or more optimizations to be applied to traffic flows between origin server and client.

8. mechanisms that allow the simultaneous or sequential application of optimizations such that those optimizations on traffic and traffic flow don't conflict with each other.

As said, above list is not exhaustive and additional characteristics may be either required or useful.

The intent of this draft is not to introduce a solution yet. However, it may help to consider possible elements which might play a role in any solution. One element is "object security".

4. Benefits for the content provider, for the users, for the intermediaries

An object security approach will allow the different parties to establis end-to-end and hop-by-hop security mechanisms to different data and metadata elements, and therefore address what can be seen as conflicting requirements in terms of optimization and security capabilitites.

The following benefits will arise for the different stakeholders:

Content providers:

- Can select the type of security service that is optimal and sufficient for particular types of content: e.g. confidentiality, integrity protection, entity authentication etc.

- Can select which parts of their content shall be secured or not and how content shall be securely retrievable.

- Can increase their confidence in secure temporary content storage during delivery through encrypting/signing sensitive content objects.

- Can leverage the business services of 3rd parties (intermediaries) through enabling the intermediaries to perform value-added services. Content providers may outsource particular tasks (like caching, or offering higher security level to users) to intermediaries.

- When using the services of content delivery networks, can benefit from faster, optimised delivery over the "last mile" (as seen from the perspective of a content delivery network). Content delivery networks can optimise delivery on behalf of content providers over the first and middle mile, however they often rely on other ISPs and mobile network operators to deliver content over the last mile. Intermediaries in the last mile can optimise traffic engineering.

Users:

- Are able to enjoy sufficient privacy and security as dictated by different use cases and equally their personal preferences (e.g. protection from traffic analysis, integrity of content).

- Can benefit from value-added services delivered by intermediaries on behalf of content providers.

- Can have access to services offered by intermediaries which enhance end user quality of experience (e.g. malware detection, parental controls).

- Can access web resources and services with lower latency and better response times (e.g. through intermediaries performing video pacing or traffic engineering to avoid congestion on particular networks).

Intermediaries:

- Can play their specific roles in content delivery and communication on behalf of content providers, like

  * Caching of content on behalf of content providers

  * Optimisation of content for optimal delivery on behalf of content providers

  * Video pacing on behalf of content providers.

- Can provide value-added services on behalf of users like parental control, malware detection etc.

- Can optimise content delivery and data communication within a network they are associated with or control e.g. through traffic engineering and traffic management by taking into account the inherent needs of content types and the explicit real- and non-real-time requirements of content providers and content delivery networks. Thereby, intermediaries contribute to an improved "end-to-end" user experience in the interest of both users and content providers.

  * Intermediaries are enabled to perform congestion management and can therefore reduce latency and response times.

- Can meet regulatory requirements as they may prevail in particular jurisdictions through an approach which is more open and transparent to both users and content providers, and which may be in the national interest.

5. Analysis of Related Work

The concept of object security is not something new, several approaches targeted at different application areas exist today, and we can even root them at the original S/MIME proposal ([RFC5751]).

As one of our first tasks, we intend to perform a detailed analysis of this related work, producing a list of the gaps of each technology solution in the scenarios we foresee. In particular, we have already identified at least a couple of such related work:

- JOSE, which stands for "JSON Object Signing and Encryption". It is a series of standards produced by the IETF under the JOSE charter ([1]) offering encryption, digital signatures, and Message Authentication Codes (MACs).

- Subresource Integrity ([SRI]), a W3C specification defining mechanisms by which user agents may verify that a fetched resource has been delivered without unexpected manipulation.

6. Architectural Considerations

The purpose of an object security architecture is to be able to provide more flexible security services than strict end-to-end encryption. A content owner should be able to express what security levels different objects should be associated with.

Such an architecture needs to define two types of logical channels between end-points. One channel is strictly end-to-end encrypted where sensitive data is transferred between end points without the risk of third-party access. The second channel is more relaxed in allowing third-party nodes be part of the flow (i.e hop-by-hop encrypted channel). The amount of information exposed in the second channel is determined by the content provider alone or in agreement with the end-user.

There are several ways to design an architecture that fulfills these requirements. An important question to analyze is whether an object security architecture should be designed at the application layer or further down the stack as an alternative to TLS.

7. Analysis of the Impacts on HTTP/2

[[CREF1: TBD]]

8. Analysis of the Impacts on TLS

[[CREF2: TBD]]

9. Impacts on the current browser architecture

[[CREF3: TBD]]

10. Impacts on the existing deployment / how to make this proposal coexist with the current

[[CREF4: TBD]]

11. Privacy Impact

[[CREF5: TBD]]

12. Security Considerations

[[CREF6: TBD]]

13. Contributors

The following people are not listed as authors, but contributed significantly to the discussions leading to this document: Liliana Dinale, Vijay Gurbani, Mike Jones, Eliot Lear, Salvatore Loreto, John Mattsson, Sanjay Mishram, Robert Moskowitz, Kevin Smith, Dan Wing.

14. References

14.1. Informative References

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[SRI] Braun, F., Akhawe, D., Weinberger, J., and M. West, "Subresource Integrity", W3C Working Draft WD-SRI-20140318, March 2014, <http://www.w3.org/TR/2014/WD-SRI-20140318/>.

Latest version available at [2].

14.2. URIs

[1] https://datatracker.ietf.org/wg/jose/charter/

Authors' Addresses

Dan Druta
AT&T

Email: dd5826@att.com

Thomas Fossati
Alcatel-Lucent

Email: thomas.fossati@alcatel-lucent.com

Marcus Ihlar
Ericsson

Email: marcus.ihlar@ericsson.com

Guenter Klas
Vodafone

Email: Guenter.Klas@vodafone.com

Diego R. Lopez
Telefonica I+D

Email: diego.r.lopez@telefonica.com

Julian F. Reschke (editor)
greenbytes GmbH

Email: julian.reschke@greenbytes.de