Overcoming the Friend-or-Foe Paradigm in Secure Communication

Sebastian Gajek, Jan Seedorf (NEC Laboratories Europe)
sebastian.gajek@neclab.eu, jan.seedorf@neclab.eu
Marc Fischlin, Özgür Dagdelen (TU Darmstadt)
marc.fischlin@cryptoplexity.de, oezguer.dagdelen@cased.de

Abstract

The existing paradigm to protect the network against pervasive monitoring via secure end-to-end channels usually conflicts with "user-friendly" operations by service providers, such as proxying, firewalling, or traffic optimisations performed by middleboxes. In this position paper we argue that future channel protocols should –and can– provide the possibility of a trade-off between security requirements and functionality.

1 Problem Statement

Secure communication protocols establish a channel between two entities in such a way that confidentiality and integrity of messages are preserved. The underlying cryptographic algorithms ascertain some strong *end-to-end security* guarantees (assuming computational hardness of the associated cryptographic problems). No party other than the two designated entities can infer significant information from the communication and any attempt of malicious alternation of messages can be detected. With these end-to-end security properties in mind, flagship protocols such as TLS, SSH, and IPSec have been designed, and proven to be an invaluable security provisioner for various applications like Voice-over-IP, Software Defined or Virtual Private Networks, to name a few.

However, since the 90ties when secure communication protocols have been designed, standardised, and implemented at a large scale, the network topology and service infrastructure has dramatically changed. With that came along also a change in requirements on security, management, and orchestration. Back then clients communicated with servers under the assumption that any kind of intermediary on the path between client and server that tries to modify the communication must be considered an adversary. Today, in many common scenarios the situation is different. In fact, we observe a fairly more complex involvement of multiple entities along the communication path as a result of optimisation, management, orchestration, or security efforts. Prominent examples include caching of network traffic to increase the quality of service, on-the-fly modification of html/javascript/css web content (so-called *Front End Optimization*), proxying content to mitigate congestion, or firewalling traffic to identify attacks.

While the aforementioned traffic optimisation mechanisms work well for unsecured communication, they fall short when it comes to communication over a secure channel. By the definition of a secure channel, any entity—be it a friend or a foe—other than sender and receiver is prevented from peeping into the communication. Clearly, if the entity is antagonistic, securing the communication is the right choice against illegitimate monitoring or modification. However as mentioned before, there are numerous situations of friendly monitoring or modification of traffic. The point to stress here is that present secure communication protocols make no differentiation between deliberate and agnostic network monitoring. As a result service providers are often forced to do a very security-critical move: they bypass the end-to-end security mechanisms. Given the inherent inability of intercepting communication over secure channels, they in certain cases de-facto annul the security of the channel by giving intermediate parties access to the cryptographic key material.

A prominent example that shows how critical such practices of service providers can be is the case of Nokia, mounting essentially Man-in-the-Middle attacks on TLS in order to optimise user traffic [1]. In this case, certainly Nokia's intentions are good (i.e. enhancing the user experience for their users), but the current secure networking paradigm (described above) forces Nokia to act as a malicious entity to improve the speed of otherwise encrypted traffic. Another, perhaps less controversial common practise is so-called *SSL-offloading* [3], offered by many CDN providers [2]. In this case, crucial keying material is spread to multiple edge servers, which—if compromised—could

impersonate an origin server. These are just some examples that exemplify the underlying problem: Intermediaries that are not an adversary to the client are effectively breaking a secure channel between client and server, thus—strictly speaking—acting maliciously. This makes them technically indistinguishable from actuall attackers that try to spy on users' traffic.

We argue that the following (technically solvable) problem exists with current state-of-affairs: There is (to the best of our knowledge) no standard solution of how to control the level of message disclosure and modification. Giving third parties access to the keying material implies giving away complete control of the message flow. In fact, any party in possession of the keying material may impersonate the end-point clients are communicating with.

2 Solution Ideas for the Standardisation Community

As a first and concrete step, we propose to enhance existing secure communication protocols (i.e. TLS, IPSEC) in a way that would allow *dedicated*, *controlled* modification of certain parts of the payload by intermediate entities, while preserving message confidentiality. This would allow third parties on the path between client and server to alter parts of the message, where it is under the control of the individual server to specify what parts exactly may be altered. Using such a mechanism, the server could allow certain traffic optimisation by intermediaries (e.g. allowing alternation of certain web content) while at the same time protecting overall message confidentiality as well as the integrity of the rest of the payload. With such a feature, however, it is important that clients can verify that any modification that has happened on the path was done with the consent of the server. In summary, with such "Interferable Secure Communication", a designated party would have the privilege to altering certain parts of messages in transit.

Note that having such a mechanism would allow—in contrary to today's status quo of secure communication protocols—to technically distinguish between dedicated intermediaries that are allowed to alter certain parts of messages and actual attackers that intend to monitor encrypted communications. This is because "good" intermediaries would no longer be in need of breaking the encryption channel. Thus, if there is an indication of some entity

breaking the secure communication channel, it would clearly be a sign of an actual adversary.

Techniques for enabling such *Interferable Secure Communication* exist, such as Sanitizable Signatures [4]. For protocols that achieve message integrity based on symmtric cryptography (i.e. Message Authetication Codes, MACs) such as TLS, similar mechanism can be designed. In particular, we believe that a standard extension of the TLS specification with the proposed functionality is feasible within the IETF with reasonable effort and within a reasonable timeframe.

Acknowledgement

This work has been partially supported by the mPlane project (mPlane: an Intelligent Measurement Plane for Future Network and Application Management), a research project supported by the European Commission under its 7th Framework Program (contract no. 318627). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the mPlane project or the European Commission.

References

[1] Nokia admits to implementing a Man-In-The-Middle flaw in HTTPS, `http://www.coderanch.com/t/602568/Security/Nokia-admits-implementing-Man-Middle`

[2] Akamai: *Secure Content Delivery*, `http://www.akamai.com/dl/feature_sheets/fs_edgesuite_securecontentdelivery.pdf`

[3] How Dynamic Site Acceleration Works, What Akamai and Cotendo Offer - Dan Rayburn - StreamingMediaBlog.com, `http://blog.streamingmedia.com/2010/10/how-dynamic-site-acceleration-works-what-akamai-and-cotendo-offer.html`

[4] G. Ateniese, D.H. Chou, B. de Medeiros, G. Tsudik: *Sanitizable Signatures*, ESORICS 2005, pp. 159-177