A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring

https://www.w3.org/2014/strint/

Strengthening the path and strengthening the end-points

Xavier Marjou, Emile Stephan, Jean-Michel Combes, Iuniana Oprescu

Internet data is more and more subject to pervasive monitoring. This paper investigates ways of enhancing this situation depending on where such pervasive monitoring may occur.

There are two different locations to secure: the endpoints and the path between these endpoints.

In the present document, we also emphasize the fact that encryption, although bringing additional data confidentiality, might in some cases contradict security's two other pillars, which are availability and integrity.

Strengthening the path

Although the Internet was designed for end-to-end communication between clients and servers without packet retransmission by routers, its architecture has adapted. The Internet can support applications that require some degree of retransmission like voice, video or file sharing while still protecting the end points (client and server) with firewalls. Scalability is achieved through the use of reverse proxies, content is cached in the enterprise proxies first then subsequently in Content Delivery Network (CDN) nodes. Other intermediary nodes include modules that handle IPv4 addresses shortage (CGN) and user mobility… Likewise, whilst in the past, intermediaries were essentially limited to routing/relaying the content, nowadays intermediaries store or cache information on those requests to improve routing and user experience.

In most cases, the two end-points expect that the data exchanged during their communication remain secret, which requires a private room for exchanging data in a secure manner. Today, this private room is either brought by application encryption (HTTP over TLS) [1] or not possible at all (HTTP) [2]. From the user perspective, it is generally better to use application encryption versus transactions in the clear.

One can never be 100% sure that TLS [3] encryption cannot be broken (cf. Bruce Schneier's talk at the IETF plenary [4], the reservations on some "elliptic curves" encryption, on "general factoring and discrete logs advances", or on "attack against RC4"). From a monitoring perspective, however, encryption is always better than no encryption at all, as it strongly decreases the risk posed by passive attacks (such as tampering with the physical layer) and greatly inflates the attack cost, rendering it unprofitable for most attackers. Encryption with the strongest ciphering suites is even highly recommended in order to decrease again such probability.

The Web is bimodal. A communication is either in-the-clear or encrypted end-to-end. The first mode is the HTTP scheme; the second mode is the HTTPS scheme. A new scheme must be added to HTTP or to TLS for allowing the cacheability of content carried over encrypted communication in explicit locations. Such intermediaries must be explicitly authorized and their discovery and selection should be configurable by end-points. HTTP2 [5] and TLS are wonderful toolboxes that must be adapted to achieve this purpose.

Strengthening the end-points

In addition to encrypting the path, it is also important to consider the security of the end-points themselves. Indeed, the end-points can be compromised too: the endpoint device, or the endpoint administrator may redistribute - intentionally or not - the data exchanged during web communications to another (potentially pervasive) third-party player.

Ensuring the privacy of digital data is not an easy task. So far, there is no technology for solving this problem. Of course, some tools exist to try and mitigate privacy concerns like the private browsing, W3C Do No Track (DNT) field, W3C Platform for Privacy Preferences Project (P3P) field, or proprietary features implemented in browsers. However, it does not fully solve the problem given that it is not possible for the end-users to remain anonymous on all web sites: merchant web sites require identification; hiding identities in social networks is a hard problem (an anonymous identity can be disclosed by a friend among the contacts within the social network).

Depending on the country, citizens may be concerned about privacy given a number of factors: culture, regulations (or not) protection of personal data (e.g. Directive 95/46/EC [6]). In a same way, companies generally set up security policies regarding the use of devices and networks by their employees. Therefore, we think that there should be a framework in the Internet allowing to take into account the regulation applying to a company, country or to a federation of countries.

Avoiding weakening the current (or future) security mechanisms

However, strengthening the internet against pervasive monitoring should be done carefully. Not all internet data has to be systematically encrypted. For instance, security mechanisms are based on monitoring as well like malware propagation detection, intrusion detection or IP address spoofing prevention (i.e., SAVI [7]). Assuming that data used by these mechanisms are encrypted, this would weaken their efficiency. This impact should be strongly taken into account in any security policy involving encryption of data.

References

[1] E. Rescorla, “HTTP Over TLS”, RFC 2818, IETF, May 2000.

[2] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners Lee, “Hypertext Transfert Protocol – HTTP/1.1, RFC 2616, IETF, June 1999.

[3] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, IETF, August 2008.

[4] IETF, "IETF 88 Plenary Meeting Materials", URL: https://datatracker.ietf.org/meeting/88/materials.html, Nov 2013.

[5] M. Belshe, R. Peon, M. Thomson (Ed.) and A. Melnikov (Ed.), “Hypertext Transfer Protocol version 2.0”, draft-ietf-httpbis-http2, IETF, December 2013.

[6] Directive 95/46/EC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[7] J. Wu, J. Bi, M. Bagnulo, F. Baker and C. Vogt, (Ed.), “Source Address Validation Improvement (SAVI) Framework”, RFC 7039, IETF, October 2013.