ON THE FEASIBILITY OF FINE-GRAINED TLS SECURITY CONFIGURATIONS IN WEB BROWSERS BASED ON THE REQUESTED DOMAIN NAME

Eman Salem Alashwali and Kasper Rasmussen
University of Oxford, UK
{eman.alashwali,kasper.rasmussen}@cs.ox.ac.uk

In proc. of the 14th International Conference on Security and Privacy in Communication Networks (SecureComm 2018).

PROBLEM

Version and ciphersuite downgrade attacks in the TLS protocol that circumvent handshake authentication.

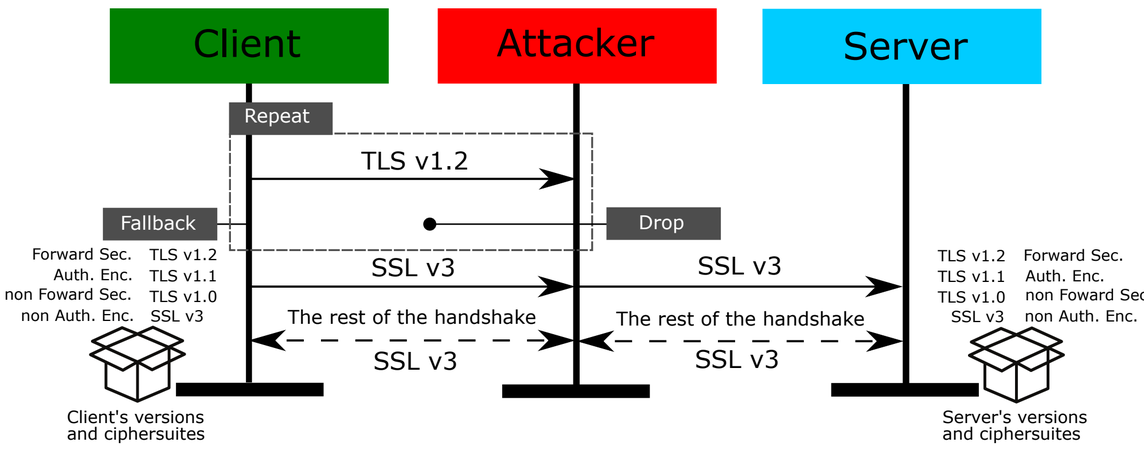

Fig. 1. The POODLE version downgrade attack [1].

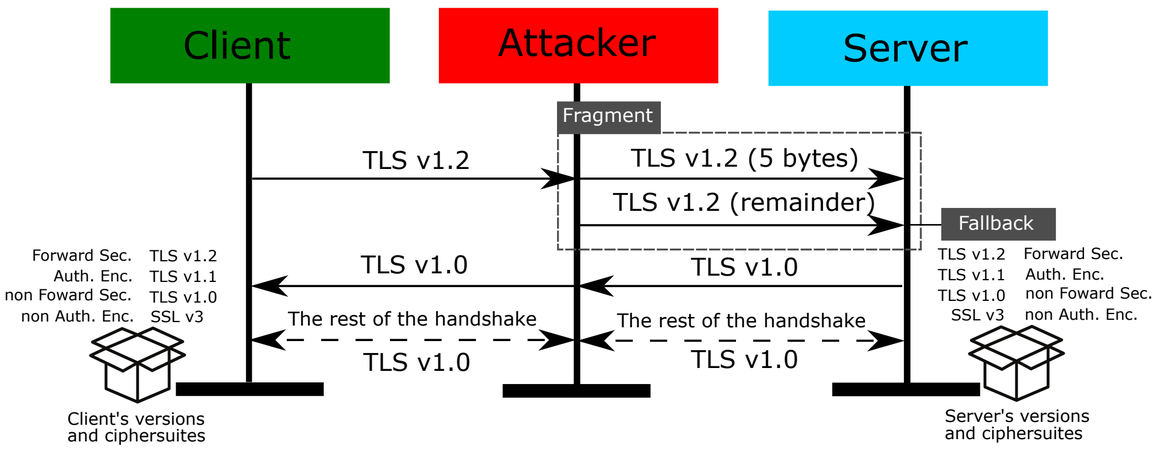

Fig. 2. The ClientHello fragmentation version downgrade attack [2].

OBSERVATION

- If the client supports only the latest version (TLSv1.3), Forward Sec. and Auth. Enc. ciphers, the client will refuse to continue a downgraded handshake (i.e. no fallback).
- This will reduce the downgrade attacks surface, provide additional layer of security, which is highly desirable for sensitive websites (e.g. e-banking).
- Since enforcing `strict` TLS client configurations is not practical to all websites, fine-grained configurations provide a balance between security and backward compatibility.

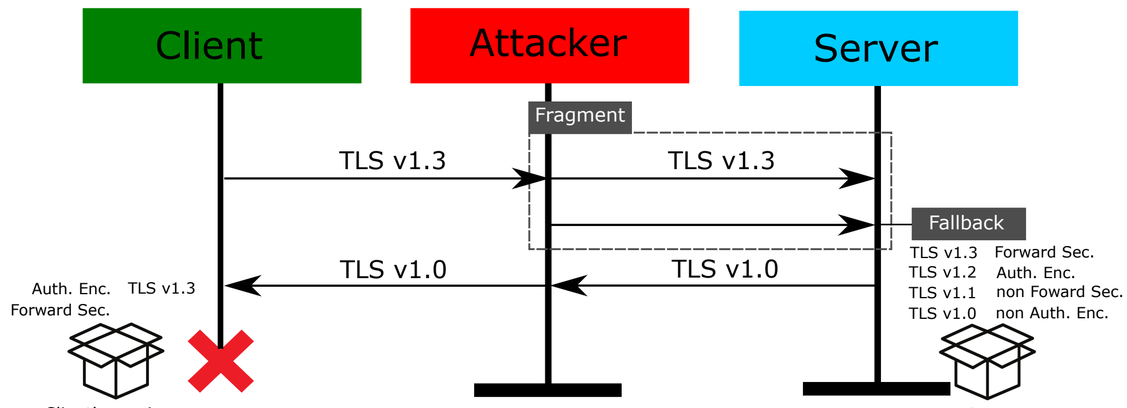

Fig. 3. Illustration of a failed version downgrade attempt when the client enforces `strict` (latest version only) TLS configurations.

QUESTION

How can we guide the browser into making an informed decision on whether to enforce `strict` or `default` TLS configurations?

OUR PROPOSED SOLUTION

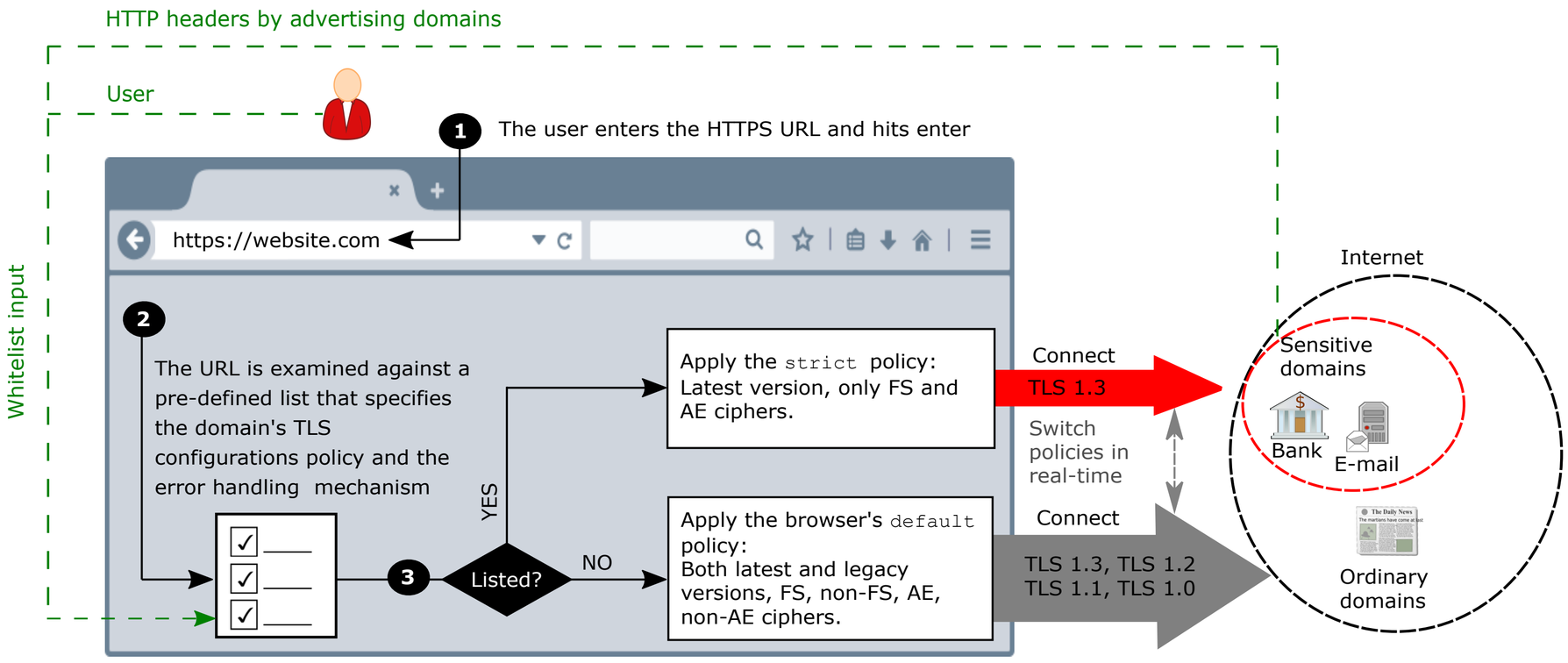

Fig. 4. Illustration of the proposed fine-grained TLS configurations mechanism.

We envision this mechanism as a built-in security feature in web browsers, e.g. a button similar to the "Bookmark" button in most browsers, and as a standardised HTTP header, to augment browsers security.

CONCLUSION

Our proposal enables web browsers to learn about websites sensitivity and enforce `strict` TLS configurations when connecting to sensitive websites while enforcing `default` configurations when connecting to the rest of the websites. This is an improvement over the "one-size-fits-all" coarse-grained TLS configurations mechanism that is used in most mainstream web browsers today.

[1] Moller, B., Duong, T., Kotowicz, K.: This POODLE Bites: Exploiting the SSL 3.0 Fallback (2014), https://www.openssl.org/~bodo/ssl-poodle.pdf
[2] Beurdouche, B., Delignat-Lavaud, A., Kobeissi, N., Pironti, A., Bhargavan, K.: FLEXTLS A Tool for Testing TLS Implementations. In: Proc. 9th USENIX Workshop on Oensive Technologies (WOOT) (2014)