Protecting Transport Layer Security from Legacy Vulnerabilities

Karthikeyan Bhargavan

INRIA

Abstract. The Transport Layer Security protocol (TLS) is the most widely-used secure channel protocol on the Web. After 20 years of evolution, TLS has grown to include five protocol versions, dozens of extensions, and hundreds of ciphersuites. The success of TLS as an open standard is at least partially due its *protocol agility*: clients and servers can implement different subsets of protocol features and still interoperate, as long as they can negotiate a common version and ciphersuite. Hence, software vendors can seamlessly deploy newer cryptographic mechanisms while still supporting older algorithms for backwards compatibility.

An undesirable consequence of this agility is that obsolete and broken ciphers can stay enabled in TLS clients and servers for years after cryptographers have explicitly warned against their use. Practitioners consider this relatively safe for two reasons. First, the TLS key exchange protocol incorporates downgrade protection, so if a client and server both support a strong ciphersuite, then they should never negotiate a weaker ciphersuite even if it is enabled. Second, even if a connection uses a cryptographic algorithm with known weaknesses, it is typically hard to exploit the theoretical vulnerability to attack the protocol.

In this talk, we will see that both these assumptions are false. Leaving legacy crypto unattended within TLS configurations has serious consequences, as shown by a recent series of *downgrade attacks* including Logjam [1] and SLOTH [3]. We will show how these attacks expose protocol-level weaknesses in TLS that can be exploited with practical cryptanalysis. We will propose a new notion of *downgrade resilience* for key exchange protocols [2] and use this definition to evaluate the downgrade protections mechanisms built into the upcoming TLS 1.3 protocol.

References

1. D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J.A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. SZanella-Béguelin, and P. Zimmermann. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *ACM Conference on Computer and Communications Security (CCS)*, 2015.
2. K. Bhargavan, C. Brzuska, C. Fournet, M. Green, M. Kohlweiss, and S. Zanella-Béguelin. Downgrade Resilience in Key-Exchange Protocols. In *IEEE Symposium on Security and Privacy (Oakland)*, 2016.
3. K. Bhargavan and G. Leurent. Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH. In *Network and Distributed System Security Symposium (NDSS)*, 2016.