Is a HTTPS webpage as secure as expected?

An Internet-wide study of Private Key Sharing in the HTTPS Ecosystem

A WhoisXML API Customer Success Story

November 2017.

Encrypted communication on the Internet is most commonly realized by Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Webpages communicating sensitive content, including internet banking, webshops, etc. use the HTTPS protocol which is based on this. E-mail servers, when communicating with client in a secure manner, use the relevant e-mail transfer protocols such as SMTP, IMAP or POP3 over the SSL/TLS, too.

The basis of such a communication is a public-key encryption is easy to understand. Suppose that Alice wants to communicate Bob confidentially. She needs a certificate binding Bob's name to a public key. Bob has a private key which is treated confidentially by him, and not revealed to anyone. With this key he can prove to Alice that it is indeed him on the other side. There is a risk, however: of course, any other (possibly malicious) entity who gets an access to Bob's private key can pretend that he was Bob.

Connecting to a website over HTTPS, when we see the "lock" icon in our browser we are confident that we are communicating the entity, say, our bank, in a secure manner. Implicitly we are confident that the other side is aware about the issue mentioned above and takes care about the private keys.

In current practice, however, the situation is more complicated. Webpages are often hosted at least in part by third-party hosting providers or content-delivery networks. Thus the hardware system we communicate belongs to this third party, which may host many other pages of completely different entities. And in order to establish the desired secure communication, this third party has to get hold of the private keys of these entities. In the current practice, many providers overtake even the management of the keys from their clients. Certainly all this gives rise to profound and possibly severe security implications.

F. Cangialosi and his coworkers [1] have recently performed the the first ever Internet-wide analysis of private key sharing between websites and third-party hosting providers. They have found that 76.5% of all organizations identified by them share at least one private key with a third-party hosting provider. Though 62.9% share with a single third party, but many organizations share one or more of their keys with tens to thousands. They have also studied the effect of this on the certificate management, such as revoking and reissuing compromised certificates. They find that *"Surprisingly, while sharing private keys with a third party is a clear violation of the semantics and security properties of online authentication, in practice, overall certificate management improves with outsourcing."* Altogether the research reveals a rather complex picture on the HTTPS ecosystem and its potential issues due to private key sharing and elucidates a number of challenges to cope with in the future to maintain the possibility of secure communication over the web.

To achieve these relevant results, F. Cangialosi and his coworkers [1] have developed a range of novel techniques of data analysis and applied them to a broad range of data. Amongst their datasets, WHOIS data are of utmost importance as they have to identify the ownership of the numerous analyzed Internet domains. However, as they point out, *"Unfortunately, the WHOIS infrastructure is distributed across registrars and resellers, and there is no standard format. Additionally, obtaining WHOIS data at scale is challenging, as most registrars rate-limit queries."* Luckily, they could rely on bulk WHOIS services, including WhoisXML API. The data purchased from us were one of the pillars of their investigations.

References

[1] Frank Cangialosi, Taejoong Chung, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. Measurement and analysis of private key sharing in the HTTPS ecosystem. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*. ACM Press, 2016. `https://doi.org/10.1145/2976749.2978301`