CS 105

TA Lecture Notes

April 27, 2015

TLS provides identity of website; it guarantees that the website is Amazon. It also guarantees security—it ensures that only you and Amazon can read any transactional information.

Identity verification is achieved through a system of private and public keys used by a trusted third party auditor that provides legitimacy to a website's claim of identity. The trusted party's (e.g. Verisign) entire business model is to verify other company's identity. Verisign uses a private key, known only by VeriSign, which is required to sign certificates. The public key, known by everyone, is used to validate that it is indeed VeriSign verifying Amazon's identity.

Identities can be tricked by malicious parties with a forged signature.
Note: When https: is crossed out in red, Google Chrome has detected that the site is using an outdated encryption technique, which has a potential that it could have a faked signature.

Security is achieved through a shared secret (a key). The user and the website transmits only encrypted text and the key is encrypted and decrypted using an exclusive OR (XOR) operation. The XOR operation and other commonly security algorithms have the advantageous property of reversibility. The key is encrypted by applying the XOR algorithm and decrypted by applying the operation again.

Heartbleed was an exploit that was discovered after 13 years. It had the ability to ask any server for its secret. Attacker with server secret can decrypt or encrypt any messages sent between the user and the website.