All Your SSL Are Belong To Us

SSL/TLS is the de facto standard for secure Internet communications. Deployed widely in Web browsers and non-browser software, it is intended to provide end-to-end security even against active, man-in-the-middle attacks. This security fundamentally depends on correct validation of X.509 certificates presented when the connection is established.

I will first demonstrate that many SSL/TLS deployments are completely insecure against man-in-the-middle attacks. Vulnerable software includes cloud computing clients, merchant SDKs responsible for transmitting payment information from e-commerce sites to payment processors, online shopping software, and many forms of middleware. Even worse, several popular SSL/TLS implementations do not validate certificates correctly and thus all software based on them is generically insecure. These bugs affect even common Web browsers, where minor validation errors such as recent certificate expiration can mask serious issues such as failure to authenticate the Web server’s identity.