**Vulnerabilities in TLS and How to Overcome Them**

The Sudo Security Group recently revealed alarming news about some popular apps on the Apple App Store. When testing their security tool “verify.ly”, it discovered that 76 apps had same security loophole. More alarming is the fact that the applications have been downloaded approximately more than 18 million times worldwide, according to an estimate by Apptopia.

The vulnerability discovered in the apps was related to the usage of Transport Layer Security (TLS). When not configured properly by the developers, the encrypted information transmitted by TLS can be easily intercepted through Man-in-the-Middle attacks. With no security mechanism in place, this vulnerability could cause any party within the WiFi range of the app-using mobile device to conduct a successful attack and be able to steal passwords, credit card data or user identity. In technical terms, the apps can be sent a forced certificate through a proxy and successfully tricked into revealing critical information. The vulnerability is specifically a big threat for banking, healthcare, insurance and all businesses that need to protect critical data of their users.

Risk of having data compromised was relatively low in 33 apps, while 24 of them had medium risk. All of these apps were publicly disclosed. Remaining 19 apps posed a very high risk to user data and were not publicly named, but a notification was sent to their creators. The insecurity discovered in the apps is not exactly a new phenomenon and has been recurring in many apps that have used this protocol.

Currently, avoiding problems with TLS can be done by using hard coded “pinned” certificates, thus blocking fraudsters from using forged certificates. But for app developers this technique may not always be helpful. Because of this reason, Apple has been asking developers to instead use App Transport Security (ATS) for secure transmission of data.

In practice, TLS certificate implementation creates security holes because of its deviation from best practices of computer security. Mobile app developers therefore need a stable and secure platform to authenticate the identities of all parties involved in communication. TLS attempts to authenticate this by using digitally signed certificates by a trusted Certificate Authority. However, this attempt to authenticate communication between different parties creates security issues.

Third party services specialize in providing advanced digital security and can deliver mobile pinning at backend of mobile apps. Hence, developers do not need to think about this by themselves. Third party programs will ensure that the certificate gets encrypted, cannot be replaced, intercepted or changed, and is properly pinned to ensure the security of customer sessions.