Workload Characterization of a Lightweight SSL Implementation Resistant to Side-Channel Attacks

Schlagworte: Kryptographie, Sicherheit mobiler Geräte, TLS/SSL Protokoll, effiziente Implementierung, Seitenkanalangriffe

Der Trend der letzten Jahre ging weg von großen, stationären, per Kabel vernetzten PCs und hin zu immer kleineren mobileren Geräten, die kabellos miteinander und mit dem Internet kommunizieren. Dies erfordert auch neue Algorithmen und Ansätze, um die Kommunikation dieser Geräte sowohl untereinander als auch netzübergreifend sicher, komfortabel und effizient zu gestalten. Ob es sich nun um Mobiltelefone, PDAs oder sogar Sensornetzwerke handelt: all diese Geräte verfügen nur über eingeschränkte Ressourcen, sollen aber trotzdem denselben Ansprüchen an Integrität, Vertraulichkeit und Authentizität der Datenübertragung genügen wie standortgebundene PCs mit einem Vielfachen an Speichergröße, Rechenleistung und verfügbarer Energie.

Hinzu kommt, dass herkömmliche Betrachtungen der Sicherheit in Netzwerken sich zumeist auf das Absichern der eigentlichen Kommunikationsverbindungen beschränkten, die Endpunkte einer solchen Verbindung allerdings für gewöhnlich als sicher angesehen wurden. Dieses Paradigma muss im Kontext mobiler Geräte überdacht werden, sind diese doch leicht zu entwenden und einfach zu manipulieren. Das Augenmerk ist nun also darauf zu richten, die in den Geräten gespeicherten Geheimnisse, die zum Herstellen einer gesicherten Verbindung notwendig sind, gegen das Abhören von Außen zu schützen. Vielfach ist es mittlerweile einfacher geworden, aus dem Stromverbrauch oder der benötigten Rechenzeit eines Gerätes auf die verwendeten Werte und damit letztendlich auch auf den geheimen Schlüssel einer Verbindung rückzuschließen (sogenannte *Seitenkanalattacken*), als zu versuchen, diese Informationen durch einen Angriff auf den verwendeten Algorithmus selbst zu extrahieren.

Unsere Arbeit beschäftigt sich mit der praktischen Implementierung einer gegen Seitenkanalangriffe resistenten Version des SSL/TLS Protokolls, das vor allem im Rahmen sicherer Kommunikation im Internet den aktuellen De-facto-Standard darstellt (erkennbar am „https://" vor der Adresse der Website). Der Fokus lag dabei vor allem auf der Eignung für kleine, in ihren Ressourcen stark eingeschränkte, mobile Geräte.

Der implementierte Softwareprototyp ermöglicht Einsparungen im Speicherbedarf (sowohl was die Größe der Bibliothek als auch den Verbrauch an Arbeitsspeicher betrifft) von 96%, verglichen mit herkömmlichen frei verfügbaren Lösungen wie OpenSSL. Die Verwendung der sogenannten *elliptischen Kurven Kryptographie* ermöglicht den schnellen Aufbau sicherer Verbindungen unter Nutzung beispielsweise eines handelsüblichen PDAs (< 160 Millisekunden für einen kompletten Verbindungsaufbau).

Die Verfügbarkeit einer solchen, dem Standard entsprechenden, effizienten und sicheren Implementierung gibt Anwendungs- und Geräteentwicklern nun ein Werkzeug in die Hand, die Sicherheit der Daten des Endanwenders ihrer Produkte einfach und ökonomisch zu erhöhen.