LTX – Verschlüsselung „easy“

Dieses Dokument erklärt im Kurzen die auf der LTX-Basis verwendeten Verschlüsselungstechnologien.

Vorab: „Verschlüsselung“ wird selten als interessantes Thema wahrgenommen. Doch hinter modernen Verschlüsselungsverfahren steckt eine unglaublich faszinierende und vielfältige Mathematik! Beispielsweise beschreiben die geometrischen Schnittflächen von einer Ebene und einem Kegel (die sogenannten „Kegelschnitte“) sowohl viele Aspekte moderner Verschlüsselungsverfahren, aber genauso auch beispielsweise physikalische Schwingungsprobleme oder Optimierungsprobleme.

Überblick Technologien

Beim Thema Verschlüsselung verliert man leicht den Überblick. Hier eine sehr einfache Erklärung der verwendeten Technologien:

Zuersteinmal muss unterschieden werden zwischen „symetrischen“ und „asymetrischen“ Verschlüsselungen.

Die asymetrische Verschlüsselungen werden überwiegend im öffentlichen Bereich eingesetzt. Beispielsweise für E-Mails, WWW, Kommunikationsgeräte. Schlagwörter hier sind „Öffentliche“ und „Private“ Schlüssel. Die meisten Angriffs-Szenarien beziehen sich auf asymetrische Verschlüsselungen, und sehr oft machen es „zu einfache“, mitgehörte oder gestohlene Schlüssel den Angreifern leicht.

Auf Geräte-Ebene (wie auch bei der LTX-Basis) werden meist symetrische Verschlüsselungen eingesetzt, wie etwa „AES“. Angriffe auf symetrische Verschlüsselungen sind zwar mathematisch besser beschreibbar, aber genau deshalb sind sie auch extrem sicher:

Funktionsprinzip AES

AES ist ein internationaler Standard und basiert auf mathematischen „Einweg-Funktionen“. Ein einfaches Beispiel dafür die die Quadratur: beispielsweise kann bei der Zahl 9 nicht gesagt werden, ob sie aus 3^2 oder $(-3)^2$ gebildet worden ist, bei 4 kann es 2^2 oder $(-2)^2$ sein, usw.

Es gibt also für jede Stelle, Zahl, Position (oder wie auch immer genannt) mehre Möglichkeiten.

Hier wäre das beispielsweise bei 4 Stellen und 2 Möglichkeiten Stelle 2*2*2*2 (also 2^4 = 16) Möglichkeiten. Bei 128 Stellen (wie etwas „AES-128“) wären das 2^128 = 3.4 * 10^38, also eine unglaublich hohe Anzahl.

Kleines Beispiel: Wenn ein aktueller und sehr moderner PC 1 Milliarde Kombinationen pro Sekunde prüfen könnte, bräuchte er 10790283070806014188970 Jahre (!!!) um die AES-128-Funktion „rückzurechnen“. Daher ist der Name „Einweg-Funktion“ absolut berechtigt.

Sämtliche Verschlüsselungen auf der LTX-Plattform basieren auf dem AES-128 Standard (Im Detail „AES-128-CBC“, das CBC steht für „Cipher Blockchain“, diese Blockchain garantiert die absolut sichere Verkettung der verschlüsselten Daten).

AES-128 wird aktuell z.B. vom BSI (Bundesamt für Sicherheit in der Informationsverarbeitung) empfohlen (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile) . Es gilt daher auch als sehr sicheres Verfahren.

Allerdings gilt obige Berechnung nur unter der Annahme eines Schlüssels mit maximaler (128 Bit) Länge.

Firmware

Um zu verhindern, dass modifizierte Firmware auf LTX-Geräten installiert werden kann, ist diese generell mit AES-128-CBC und Schlüsseln maximaler Länge verschlüsselt. Daher können Firmware-Updates auch problemlos z.B. per Bluetooth oder Mobilem Internet auf die Geräte übertragen werden. Es ist weder möglich den Code zu analysieren noch zu verändern! Nur absolut korrekte Firmware kann auf einem LTX-Gerät installiert werden.

Schwachstelle Schlüssel

In der Praxis reichen aber oft einfachere Schlüssel (z.B. für manuelle Eingabe) immer noch aus. Wichtig ist vor allem, dass dieser Schlüssel trotzdem nur mit unverhältnismäßig hohem Aufwand errechnet oder erraten und auf keinen Fall mitgehört werden kann.

Kommunikation über Bluetooth LE

Die LTX-Geräte verwenden eine sogenannte „Challenge-Response“ Authentifizierung, die auf dem Prinzip „Frage-Antwort“ basiert. Dabei stellt das Gerät bei jeder einzelnen Verbindung eine individuelle Frage, auf die es eine AES verschlüsselte Antwort erwartet. Als geheimen Schlüssel sind die Geräte werksmäßig mit einem (mindestens) 6-steligen PIN versehen (mit Abbruch und Zeit-Blockierung bei Falscheingaben). Ein Angriff darauf ist recht unwahrscheinlich, da rein rechnerisch selbst das (automatisierte) Durchprobieren (mit jeweiligen Verbindungsaufbau) mehrere Monate benötigt. Wichtig dabei ist, dass der geheime gemeinsame Schlüssel niemals mit übertragen wird. Daher ist dieses Verfahren selbst dann sicher, wenn ein Angreifer die Daten „mithört“: niemals stellt das Gerät dieselbe Frage.

Bei Fragen: j.wickenh@geo-precision.com