LTX – Encryption “easy”

This document briefly explains the encryption technologies used on the LTX basis.

First of all: "Encryption" is rarely perceived as an interesting topic. But behind modern encryption methods lies an incredibly fascinating and diverse mathematics! For example, the geometric intersections of a plane and a cone (the so-called "conic sections") describe many aspects of modern encryption methods, but also, for example, physical vibration problems or optimization problems.

Technologies overview

When it comes to encryption, it's easy to lose track. Here is a very simple explanation of the technologies used:

First of all, a distinction must be made between "symmetrical" and "asymmetrical" encryption.

Asymmetrical encryption is mainly used in the public sector. For example for e-mails, WWW, communication devices. Keywords here are "Public" and "Private" keys. Most attack scenarios relate to asymmetric encryption, and very often "too simple", eavesdropped or stolen keys make it easy for attackers.

At the device level (as with the LTX basis), mostly symmetrical encryption is used, such as "AES". Attacks on symmetric encryption can be better described mathematically, but that is exactly why they are extremely secure:

Functional principle AES

AES is an international standard and is based on mathematical "one-way functions". A simple example of this is squaring: for example, with the number 9 it cannot be said whether it was formed from 3^2 or $(-3)^2$, with 4 it can be 2^2 or $(-2)^2$, etc.

So there are several possibilities for each digit, number, position (or whatever it is called).

Here, for example, with 4 digits and 2 possibilities, digit 2*2*2*2 (i.e. 2^4 = 16) possibilities would be. With 128 digits (like something like “AES-128”), that would be 2^128 = 3.4 * 10^38, which is an incredibly high number.

Small example: If a current and very modern PC could check 1 billion combinations per second, it would need 10790283070806014188970 years (!!!) to "recalculate" the AES-128 function. Therefore the name "one-way function" is absolutely justified.

All encryption on the LTX platform is based on the AES-128 standard (in detail "AES-128-CBC", the CBC stands for "Cipher Blockchain", this blockchain guarantees the absolutely secure chaining of the encrypted data).

AES-128 is currently recommended, for example, by the BSI (Federal Office for Information Security) (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technische

Guidelines/TR02102/BSI-TR-02102. pdf?__blob=publicationFile) . It is therefore also considered a very safe procedure.

However, the above calculation only applies if a key is assumed to have a maximum length (128 bits).

Firmware

To prevent modified firmware from being installed on LTX devices, it is generally encrypted with AES-128-CBC and keys of maximum length. Firmware updates can therefore also be easily transferred to the devices, e.g. via Bluetooth or mobile Internet. It is neither possible to analyze nor to change the code! Only absolutely correct firmware can be installed on an LTX device.

Vulnerability key

In practice, however, simpler keys (e.g. for manual entry) are often sufficient. Above all, it is important that this key can only be calculated or guessed with a disproportionate amount of effort and that it cannot be overheard under any circumstances.

Communication via Bluetooth LE

The LTX devices use a so-called "challenge-response" authentication based on the "question-answer" principle. The device asks an individual question for each individual connection, to which it expects an AES-encrypted answer. The devices are provided with a (at least) 6-digit PIN as a secret key (with cancellation and time blocking in the event of incorrect entries). An attack on it is very unlikely, since mathematically even the (automated) trial and error (with the respective connection setup) takes several months. It is important that the secret shared key is never transmitted. Therefore, this method is secure even if an attacker "listens" to the data: the device never asks the same question.

For questions: j.wickenh@geo-precision.com