Karlsruhe Institute of Technology

KASTEL - Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
`https://crypto.kastel.kit.edu`

OpenLI: From a security perspective

Master's Thesis

Some governments require network operators by law to intercept their customers' traffic in order to prevent crime. The ETSI Lawful Interception (LI) standard has been developed for this purpose, adding important metadata to the intercepted traffic, for example, to provide admissible evidence in court. Interception must be seamless so that customers are unaware they are being monitored. However, the cost of the right equipment, a solution, and LI's in-house expertise can be prohibitive for small network providers. In response, an open source solution called OpenLI has been developed by a very small team that implements the ETSI LI standard. Being open source provides transparency and allows the community to help find problems, but it also makes it easier for attackers to find vulnerabilities. Especially since it is developed by a small team and also has a small community behind it, it is potentially vulnerable to security problems. Intercepting customer traffic is a very security-critical application, and existing security issues potentially allow an attacker to intercept any customer's traffic.

Scope of the work

- Get an overview of the OpenLI code.
- Provide an overview of the architecture and the standard that is implemented through the code.
- Compare your results with the OpenLI documentation and the ETSI LI standard.
- Analyze OpenLI's security features
- (optional) Find security issues

Requirements

Following prior knowledge or skills are useful (or have to be acquired) for the thesis:

- Familiarity with programming, particularly the C programming language
- Basic knowledge of cryptography & cryptographic protocols (IP-Sec & TLS)
- Familiarity with network security
- Interest in the topic is strongly recommended

Contact

In case of interest or for further information, please contact Dennis Faut, `dennis.faut@kit.edu`.