Project in Penetration testing

Exploration of new techniques to penetrate the USB interface

The Crypto Stick is a USB stick in a small form factor containing an integrated OpenPGP smart card to allow easy and high-secure encryption e.g. of e-mail or for authentication in network environments. As opposed to ordinary software solutions, private keys are always inside the Crypto Stick so that their exposure is impossible. All cryptographic operations (precisely: decryption and signature because of public key cryptography) are executed on the PIN-protected Crypto Stick. In case the Crypto Stick was stolen, got lost, or is used on a virus-contaminated computer (e.g. Trojan horse) no attacker is able to access the private keys so that all encrypted data stays secure.

The Crypto Stick is developed by the German Privacy Foundation as a non-profit open source project and ensures a very high level of security due to verifiability and an attractive price. The open interface of the used OpenPGP smart card allows optimal compatibility with various software applications (e.g. GnuPG, Mozilla Thunderbird + Enigmail, OpenSSH, Linux PAM, OpenVPN, Mozilla Firefox).

In its current version the Crypto Stick does not contain ordinary data storage. The version 2 which is currently being developed shall contain data storage.

Features:

- Three independent RSA keys (signature, encryption, authentication) with a length of up to 3072 bit
- Keys can be generated on the stick itself or already existing keys can be imported. Afterwards the private keys can never leave the Crypto Stick to protect against Trojan horses, viruses, and in case of theft or loss.
- Compatible to Windows, GNU/Linux and Mac OS
- High security, due to the usage of a smart card based on a Common Criteria 5-high certificated one
- LED light to signalize activity
- Small and handy form factor

Further details about Crypto Stick are available at http://www.crypto-stick.org

Short task description

Penetration testing

Penetration testing usually refers to the test of IP connected devices and exploitation of their security vulnerabilities. The Crypto Stick is not an IP device but an USB device. Hence the security testing of the Crypto Stick should include the exploration of new techniques to penetrate the USB interface and the CCID as well as mass storage interfaces on top of it.

Longer and more detailed description will be provided on demand.

Point of contact: info@nlnet.nl

For more technical details you may also contact cryptostick@privacyfoundation.de directly.