General SIM Security Guidelines

June 2013

The SIM is a key security element for authentication in mobile networks. This paper presents general guidelines that are intended to ensure that a SIM's security levels are optimally maintained.

Mechanisms to break security systems become more sophisticated over time. As with any other security system, SIM security must, at a minimum, evolve at the same pace as potential threats in order to maintain a sufficiently high security margin.

Below are the security factors which should be regularly reviewed.

- The security policies of Mobile Network Operators (MNOs) should adhere to guidelines that are provided by the following organisations: NIST, BSI and ANSSI [(1)]. Some indications for protocols used on the internet are also given in relevant RFCs by IETF.

- SIM configurations and profiles should also adhere to the guidelines provided by the above organisations.

  A good SIM configuration requires the selection of cryptographic algorithms which are capable of withstanding attacks well beyond the maximum expected lifetime of the SIM. Up-to-date information on the security levels of cryptographic algorithms is provided by the organisations mentioned above. Cryptographic algorithms are subject to cryptanalysis and to brute force attacks. Attack scenarios based on cryptanalytic results are usually first discussed in the academic community before an attack is seen in the field. Brute force attacks can be expected to become more powerful, according to Moore's Law. To be successful on a first attempt, an attack usually requires massive computing power, but as they become easier to execute over time, they become more common in the field. In recent years, deprecated algorithms that have shown this weakness include Comp128-1, DES and MD5. It is the responsibility of MNOs to select strong algorithms.

- Security of SIM Operating System and application implementations must also be considered and SIM security implementation countermeasures improve with each new generation of SIM cards.

- The SIM chip hardware implements protection mechanisms against a whole range of attacks. As time goes on, however, new attack methods become known and consequently new protection mechanisms, as available in the latest smart card chip generation, become required.

Conclusion

Due to the evolution of security, MNOs should ensure that their SIM profiles and products are regularly upgraded to keep ahead of security threats.

MNOs should specifically focus on the security of NFC-enabled SIMs. Due to the convergence of banking and telecommunications, payment applications will increasingly reside on the same smart card chip as network access applications. In the payment sector, cards are cyclically replaced after a few years. This guarantees that only cards with recognised and up-to-date security levels are used. A similar regular replacement cycle is therefore recommended for SIMs to ensure they benefit from the latest security improvements. In addition, NFC SIM cards should comply with existing certification processes such as EMVCo and Common Criteria.

(1)

- NIST SP 800-57 Part 1, http://csrc.nist.gov/publications/PubsSPs.html
- BSI TR-02102, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
- ANSSI RGS http://references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf