Who evaluates evaluators: assessing cryptography evaluators assessing a secure messaging application security

Marion Videau*[1]

[1]Quarkslab – Quarkslab – France

Résumé

Secure messaging applications are the natural companion of smartphones that occupy almost everyone's pocket. Cryptography plays a huge role in providing the security features. One of the enjoyable aspects of security is that a system can only be supposed secure until a vulnerabilty is found. Which implies that among other activities to ensure a reasonnable level of trust in security claims, having security evaluators actually looking for vulnerabilities is a fundamental one. But who evaluates evaluators? In France it is done through ANSSI which certifies ITSEF (CESTI in French) and regularly check for their actual competencies through challenges. The last one has been centered on cryptography with CRY.ME a secure messaging platform based on matrix. In our talk we will describe the challenge through the lense of the CESTI Quarkslab and reflect on the vulnerabilties introduced and found, their categories, their difficulties and their surprises.

*Intervenant