Prof. dr. B.P.F. Jacobs (RUN), E4A

English scientific summary

This project addresses the fundamental societal problem that encryption as a technique is available since decades, but has never been widely adopted, mostly because it is too difficult or cumbersome to use for the public at large. PGP illustrates this point well: it is difficult to set-up and use, mainly because of challenges in cryptographic key management. At the same time, the need for encryption has only been growing over the years, and has become an urgent problem with stringent requirements – for instance for electronic communication between doctors and patients – in the General Data Protection Regulation (GDPR) and with systematic mass surveillance activities of internationally operating intelligence agencies.

The interdisciplinary project "Encryption for all" addresses this fundamental problem via a combination of cryptographic design and user experience design. On the cryptographic side it develops identity-based and attribute-based encryption on top of the attribute-based infrastructure provided by the existing IRMA-identity platform. Identity-based encryption (IBE) is a scientifically well-established technique, which addresses the key management problem in an elegant manner, but IBE has found limited application so far. In this project it will be developed to a practically usable level, exploiting the existing IRMA platform for identification and retrieval of private keys. Attribute-based encryption (ABE) has not reached the same level of maturity yet as IBE, and will be a topic of further research in this project, since it opens up attractive new applications: like a teacher encrypting for her students only, or a company encrypting for all employees with a certain role in the company.

On the user experience design side, efforts will be focused on making these encryption techniques really usable (i.e., easy to use, effective, efficient, error resistant) for everyone (e.g., also for people with disabilities or limited digital skills). To do so, an iterative, human-centred and inclusive design approach will be adopted. On a fundamental level, scientific questions will be addressed, such as how to promote the use of security and privacy-enhancing technologies through design, and whether and how usability and accessibility affect the acceptance and use of encryption tools. Here, theories of nudging and boosting and the unified theory of technology acceptance and use (known as UTAUT) will serve as a theoretical basis. On a more applied level, standards like ISO 9241-11 on usability and ISO 9241-220 on the human-centred design process will serve as a guideline. Amongst others, interface designs will be developed and focus groups, participatory design sessions, expert reviews and usability evaluations with potential users of various ages and backgrounds will be conducted, in a user experience and observation laboratory available at HAN University of Applied Sciences. In addition to meeting usability goals, ensuring that the developed encryption techniques also meet national and international accessibility standards will be a particular point of focus. With respect to usability and accessibility, the project will build on the (limited) usability design experiences with the mobile IRMA application.

English public summary

Encryption is a technology to protect the confidentiality of messages. New data protection regulation makes this more urgent than ever. However, existing techniques are too complicated. This project aims at broad adoption of encryption via a combination of advanced cryptographic techniques and humancentred design.

Dutch public summary

Versleuteling is een techniek voor het beschermen van de vertrouwelijkheid van berichten. Dat wordt vereist in nieuwe wetten voor gegevensbescherming. Echter, bestaande technieken zijn te ingewikkeld. Dit project richt zich op brede adoptie van versleuteling via een combinatie van geavanceerde cryptografische technieken en mens-gericht ontwerp.