Long Term Cybersecurity research
Summaries of projects granted in the second NWO call for proposals (2014)

Project number	CYBSEC.14.008 / 628.001.019	
Main Applicant	Dr. B. Skoric	Technische Universiteit Eindhoven Faculteit Wiskunde en Informatica Informatica
Project title	ESPRESSO	

Scientific summary

In biometric authentication/identification systems, the best known protection of biometric information is to use a Helper Data System (HDS) such as a Secure Sketch or Fuzzy Extractor. Employing a HDS is equivalent to the best practice for storing password information, namely storing salted hashes instead of plaintext passwords; this protects even against insider attacks. However, the helper data inevitably leaks some information about the raw biometric, since some redundancy information must be provided for error correction. HDS research focuses a.o. on:
(i) Understanding and reducing the leakage
(ii) implementation efficiency
(iii) signal processing of sensor data.
Despite significant progress, we still have not reached the point where a HDS for fingerprints, the most widely used biometrics modality, can be implemented on a cheap smartcard. The aim of ESPRESSO will be to improve the state of the art on all fronts, by exploiting and further advancing recent developments: Enhance lightweight signal processing by outsourcing operations on non-confidential data and by compressed sensing techniques; improve error correction by maximally exploiting soft information about measurement component reliability; reduce leakage by helper data chaffing methods.
The processing of the raw sensor data, the error correction and the leakage reduction have strong interdependencies; ESPRESSO aims to take advantage of this.

Applicable NCSRA themes

- Identity, privacy and trust management
- Secure Design and Engineering