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

Project number	CYBSEC.14.028 / 628.001.017	
Main Applicant	Dr. A. Peter	Universiteit Twente Faculteit der Elektrotechniek, Wiskunde en Informatica
Project title	Critical Infrastructure Protection through Cryptographic Incident Management (CRIPTIM)	

Scientific summary

Critical Infrastructure Protection (CIP) mechanisms are commonly based on complex models of interdependencies between the many operators in our critical infrastructure. Particularly due to the rapid emergence of new cyber-threats, the sharing of incident information is indispensable for the functioning of such mechanisms. However, the high sensitivity of this information prevents operators from sharing it.

CRIPTIM introduces the new paradigm of 'cryptographic incident management' for CIP that ensures data confidentiality with cryptographic guarantees, thereby reducing the operators' fears of information leakage. The underlying idea is to monitor and analyze incident data in the encrypted domain, while an alarm is set off only when a certain failure or alarm state is detected. The subsequent alarm resolution is facilitated through novel access control mechanisms for the selective disclosure of alarm-related information. CRIPTIM realizes this paradigm by developing novel custom-tailored cryptographic techniques in Secure Multiparty Computation, Homomorphic- and Functional Encryption, as well as Oblivious RAM. The intended technology will, for the first time, allow external parties, like intelligence agencies, to feed threat-related top-secret information into the monitoring system which may be the missing piece for the early detection of potentially major disasters.

The new paradigm will be validated with different incident models through a prototype implementation in collaboration with three national actors in CIP: TNO, NCSC, and AIVD. CRIPTIM sets the foundations for this innovative approach to CIP and contributes to an effective and confidential incident management that leads to a more secure and reliable critical infrastructure.

Applicable NCSRA themes

- Attack detection, attack prevention and monitoring
- Forensics and incident management
- Data, Policy and Access Management
- Secure Design and Engineering