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

Project number	CYBSEC.14.001 / 628.001.020	
Main Applicant	Prof. dr. R.J. Wieringa	Universiteit Twente Faculteit der Elektrotechniek, Wiskunde en Informatica Informatiesystemen
Project title	Learning from Incidents (LINC)	

Scientific summary

Dutch public telecom providers are required by law to register availability incidents with the Dutch Telecom regulator Agentschap Telecom (AT). Yearly summaries are submitted to ENISA, which compiles annual reports of telecom availability incidents in Europe. The incident database could be a lot more useful if it could be shared among telecom providers to help them improve the resilience of their infrastructure. However, the information in it is often incomplete, and it is extremely confidential. The goal of the LINC project is to develop techniques to extract reusable lessons learned about causes and resolutions of availability incidents from the database, that preserve confidentiality.

We will develop an incident analysis method and an incident model that is usable in practice to report on the analysis and recovery of availability incidents. To ensure confidentiality, these lessons learned will be stated in terms of statistical information about the failure mechanisms of incidents without referring to the entire incident, and will be stored in a separate database that is readable by telecom providers. Use of this database must be confidential. Failure mechanisms are diverse, and may include technical as well as organizational mechanisms, as well as natural disasters. Furthermore, we will develop a risk assessment method by which telecom providers will be able to relate these lessons to their own infrastructure in order to identify possible improvements.

To ensure usability, we will develop the methods and database iteratively together with AT and with close cooperation with telecom providers and other stakeholders such as ENISA.

Applicable NCSRA themes

- Forensics and incident management
- Risk Management, Economics and Regulation
- Secure Design and Engineering

Project number	CYBSEC.14.003 / 628.001.016	
Main Applicant	Prof. dr. ir. C.T.A.M. de Laat	Universiteit van Amsterdam Faculteit der Natuurwetenschappen, Wiskunde en Informatica Instituut voor Informatica
Project title	Security Autonomous Response in programmable Networks (SARNET)	

Scientific summary

The ever wider use of ICT in our society is reflected in the growing complexity of ICT systems and probably, the growing number of cyber criminals. These growing numbers impact the risk of cyber criminality adversely. Risk is an important concept in our research, it is the average impact of a given malicious interaction with an ICT infrastructure. As one of the partners of this proposal, Air France-KLM, has experienced these impacts, which can be enormous.

Basically our research goal is to obtain the knowledge to create ICT systems that model their state (situation), discover by observations and reasoning if and how an attack is developing and calculate the associated risks. In addition, our goal is to have the knowledge to calculate the effect of counter measures on states and their risks, and to choose and execute one. In short, a we research the concept of a networked computer infrastructures exhibiting SAR: Security Autonomous Response.

Based on prior research, we are capable to use the new technologies of Software Defined Networking (SDN), cloud computing and Network Function Virtualisation (NFV) for SAR, e.g. to adapt a network topology as a response to a threat. In earlier research we learned how to create software (control programs) that continuously control ICT infrastructures.

Multi country test beds, visualisation centres, public workshops and whitepapers are part of our validation and valorisation activities. The research is supported by Ciena, a network equipment manufacturer and will be validated in the context of Air France-KLM.

Applicable NCSRA themes

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

Project number	CYBSEC.14.007 / 628.001.011	
Main Applicant	Prof. dr. P.H. Hartel	Universiteit Twente Faculteit der Elektrotechniek, Wiskunde en Informatica
Project title	SEcurity RequIrements for seriOUS apps (SERIOUS)	

Scientific summary

A serious App is used for serious business such as tele-treatment, or tele-learning. Serious Apps process important data that must only be shared with authorised parties. End-users find it difficult to manage the security and privacy risks of Apps because current platforms such as Google Android, Apple iOS and Windows Phone do not provide the end-user with usable tools. For example the Android permission system has a large number of system oriented permissions that do not necessarily mean much to the end-user. The aim of the SERIOUS project is to help end-users to manage security and privacy risks of serious Apps. To achieve this aim we will build software that will enable a human guardian to manage the risks for the end-user. The guardian could be a nurse in the case of a tele-treatment App, or a teacher in the case of a tele-learning App. The software will be developed in three phases. In the first phase the guardian has to be involved in every security and privacy decision. We will conduct social science experiments with end-users of serious Apps in three different domains to research how end-users and guardians manage security and privacy risks. This knowledge will be codified in subsequent version of the software to lighten the work of the guardian. The final version should operate with no, or minimal assistance of the guardian. The main research challenge is to understand how to manage security and privacy risks and how to codify that knowledge into usable tools.

Applicable NCSRA themes

- Attack detection, attack prevention and monitoring
- Data, Policy and Access Management
- Risk Management, Economics and Regulation
- Secure Design and Engineering

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

Project number	CYBSEC.14.014 / 628.001.012	
Main Applicant	Prof. dr. ir. B.R.H.M. Haverkort	Universiteit Twente Faculteit der Elektrotechniek, Wiskunde en Informatica Ontwerp en Analyse van Communicatiesystemen (DACS)
Project title	More secure SCADA networks through self-awareness (MOSES)	

Scientific summary

SCADA (Supervisory Control And Data Acquisition Systems) networks control physical processes, such as electricity grids, and are increasingly vulnerable to cyber attacks, due to unauthenticated and non-encrypted communication protocols. However, the continuous operation (dependability) of the physical processes is of utmost importance to society and industry. SCADA security has mainly been considered separately from the physical processes they control, even though attacks and countermeasures have a direct impact on the physical process. We propose to use predictive knowledge of the physical process (i) to improve intrusion detection capabilities, (ii) to assess the impact of security breaches, and (iii) to justify countermeasures.

The key idea of this proposal is to build process-aware intrusion detection techniques for Smart Grids, which requires, next to state-of-the-art network intrusion detection, an accurate model of the physical processes that can be evaluated in real time. Due to the complex nature of Smart Grids, the model of the physical process has to combine discrete and continuous characteristics with stochastic behaviour (so-called 'stochastic hybrid models'). This model is then combined with a model that describes 'normal' network traffic. Together this allows for anomaly detection in both the network traffic and the behaviour of the physical system.

This so-called self-awareness monitor (SAM) will detect malicious behaviour that cannot be detected solely from SCADA traffic. Furthermore, it can predict future behaviour of the smart grid and quantify the impact of security breaches and different counter-measures on the physical process.

Applicable NCSRA themes

- Malware and malicious infrastructures
- Attack detection, attack prevention and monitoring

Project number	CYBSEC.14.016 / 628.001.010	
Main Applicant	Prof. dr. ir. P.H.A.J.M. van Gelder	Technische Universiteit Delft Subfaculteit Wijsbegeerte en Technische Maatschappijwet Veiligheidskunde
Project title	Secure Our Safety: Building Cyber Security for Flood Management	

Scientific summary

Cyber attacks on critical infrastructures can have devastating consequences for environment, health and even human lives. To improve the protection and resilience, various approaches for security risk assessment, attack detection and safety monitoring have been developed. The existing approaches, however, fail to fully incorporate the specifics of these systems for cyber security. On the one hand, security monitoring has little understanding of the safety context that is in place. On the other hand, procedures for safety response do not include knowledge about the security status of IT system components. In a broader perspective, the links between cyber security and safety management are poorly understood, and relevant information is not shared, creating space for malicious activities to pass undetected.

This proposal aims at improving the cyber security of critical infrastructures by bridging the gap between safety and security risk management and monitoring. In particular, we use the context of flood management to provide integrated decision support for incident response related to cyber threats, based on both safety and security science. The project has two objectives. Firstly, the project will enrich network security monitoring with safety context information. Here, the context consists of static information about the underlying physical process, as well as dynamic information about safety threats (i.e., extreme hydrometeorological conditions). Secondly, the project will improve safety incident response by procedures that include information from security monitoring in assessing the expected effectiveness of responses. The integration of the two innovations will enable adequate responses to flood defence security threats.

Applicable NCSRA themes

- Attack detection, attack prevention and monitoring
- Risk Management, Economics and Regulation
- Secure Design and Engineering

Project number	CYBSEC.14.023 / 628.001.015	
Main Applicant	Prof. dr. B.J. Koops	Tilburg University Faculteit Rechtswetenschappen TILT-Recht, Technologie en Samenleving
Project title	Public-private actions against botnets: establishing the legal boundaries	

Scientific summary

Combatting botnets, which facilitate many forms of cyber-attacks, is a key challenge in cybersecurity. The classic crime-fighting approach of prosecuting perpetrators and confiscating crime tools fails here: botnets cannot be simply 'confiscated', and law-enforcement's reactive focus on prosecuting offenders is ill-suited to deal effectively with botnet threats. A wider set of anti-botnet strategies, including pro-active strategies and public-private co-operation, is needed to detect and dismantle botnets. Public-private anti-botnet operations, however, raise significant legal questions: can data about (possibly) infected computers be shared among private parties and public authorities? How far can private and public actors go in anti-botnet activities? And how legitimate are public-private partnerships in which private actors partly take up the intrinsically public task of crime-fighting?

This project aims to enhance legal certainty for stakeholders and the legitimacy of public-private anti-botnet operations in two key sectors involved in botnet-fighting (telecommunications/Internet and higher-education), and therewith to stimulate lawful and legitimate anti-botnet operations. The objectives are to investigate the legal limits and possibilities for public-private anti-botnet operations, to raise awareness among stakeholders of the legal room for anti-botnet operations, and to develop guidelines and sectoral codes of conduct that clarify and establish the boundaries of anti-botnet operations.

The overall research question is: under which conditions can efficacious public-private anti-botnet operations be lawfully and legitimately undertaken? The methodology combines legal analysis (Dutch and European law), comparative law (Germany, England) and social-scientific methods of stakeholder analysis. National and international collaboration will foster a wide dissemination of best practices in combating botnets.

Applicable NCSRA themes

- Malware and malicious infrastructures
- Attack detection, attack prevention and monitoring
- Risk Management, Economics and Regulation

Project number	CYBSEC.14.024 / 628.001.014	
Main Applicant	Prof. dr. B.P.F. Jacobs	Radboud Universiteit Nijmegen Faculteit der Natuurwetenschappen, Wiskunde en Informatica Computer Science
Project title	Own Your Own Identity	

Scientific summary

Over the past fifteen years, research in cryptography has demonstrated that attribute-based credentials (ABCs) can be used for flexible, secure and privacy-friendly authentication. Such credentials may be either identifying or anonymous; they allow users to gain access to resources without revealing any information about themselves other than the fact that they are authorized, e.g. by only proving that they are over 21, or have such-and-such social security number. More recent research within the "IRMA project'' at Nijmegen has shown that the advanced cryptographic protocols supporting ABCs can actually run on modern smart cards. This non-trivial achievement forms a breakthrough towards an innovative eIdentity infrastructure.

A crucial aspect of ABCs is that they need to be closely bound to the user, via a secret cryptographic key. This key needs to be stored securely, under direct (physical) control of the user, in special hardware.

The project outlined in this proposal builds on this existing IRMA work and aims to make a next step, going outside academia into the world of eIdentity providers and customers. Together with project partners KPN and SURFnet this proposal aims to design and develop new realisations of ABCs in (secure hardware in) mobile phones and tablets that are so important in modern workflow.

The combined scientific and engineering challenges lie in integrating the subtle and computationally-intensive cryptographic protocols for ABCs in constrained environments like SIM cards, Trusted Execution Environments (TEEs) in mobile phones and tablets, and in a newly designed "homebox''.

Applicable NCSRA theme

- Identity, privacy and trust management

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

Project number	CYBSEC.14.029 / 628.001.018	
Main Applicant	Prof. dr. ir. A. Pras	Universiteit Twente Ontwerp en Analyse van Communicatiesystemen (DACS)
Project title	D3 - Distributed Denial-of-Service Defense: protecting schools and other public organizations	

Scientific summary

The goal of this project is to develop an architecture to detect and mitigate Distributed Denial of Service (DDoS) attacks on public organizations, e.g., schools. Since summer 2013 the number of such attacks has increased rapidly, primarily due to availability of booters, i.e., web-based facilities that offer "DDoS-as-a-service". Booters find their origins within the Internet gaming community, and can be used for a few euros by people without any technical skills. Since booters use general Internet services such as DNS and NTP to amplify their attacks, they can operate without an underlying botnet.

Although DDoS attacks are well-known in literature, it took the Wikileaks "operation payback" (2010) until the general audience understood the potential power of such attacks. Since then we've witnessed attacks on banks and crucial Internet services; some of these attacks even reached traffic peaks of 400 Gbps. Since summer 2013 the Dutch Research Network provider (SURFNet) sees a trend that students use booters to attack schools, often at times of exams. Also other public organizations and services, e.g., tax offices, DigiD, municipalities, hospitals are increasingly being targeted.

The novel approach of this project is to detect DDoS attacks at an early stage, within the core network. The scientific contribution is in two areas. First, Software Defined Networking (SDN) principles (OpenFlow) will be applied to re-route at an early stage attack traffic towards filtering systems that employ sophisticated anomaly detection mechanisms (e.g., HMM and SVM). Second, business modeling will be an integral part of the research, including economic, regulatory and ethical aspects.

Applicable NCSRA themes

- Malware and malicious infrastructures
- Attack detection, attack prevention and monitoring

Project number	CYBSEC.14.030 / 628.001.013	
Main Applicant	Dr. J.H. Hoepman	Radboud Universiteit Nijmegen Subfaculteit Informatica Security of Systems
Project title	Patterns for Privacy (P4P)	

Scientific summary

The World Economic Forum [20] has recognized that the economic value of personal data is threatened by a steady decline in trust by all stakeholders, and recommends to develop principles to encourage the trusted flow of personal data. The proposal for a new European data protection regulation [6] explicitly requires data protection by design and by default. This shows that privacy by design [4] is becoming a significant economic and regulatory factor. It is therefore crucial to support developers in satisfying these requirements with practical tools and guidelines.

This proposal aims to achieve just that.

During our study of privacy design strategies [d, e] we discovered that a comprehensive and readily applicable set of tools to support system designers to design for privacy does not exist. In particular, a systematic study of privacy design patterns is wanting. Only a small, incomplete and inconsistent patchwork of privacy design patterns exists [10, 11, 15, 14, g].

To bridge this gap, the project will:
- develop a framework to express and study privacy design patterns,
- develop a comprehensive catalogue of such privacy design patterns, and
- develop tools to support system designers to apply privacy design patterns throughout the system development lifecycle.

TNO, our industrial project partner, is busy raising a consortium that will implement a national health data infrastructure. It will use our results in the development of such personal health information providers.

Applicable NCSRA theme

- Identity, privacy and trust management