Research Topics in the National Cyber Security Research Agenda

'Trust and Security for our Digital Life'

About this document: This document summarizes the research topics as identified in the National Cyber Security Research Agenda, which is available in full from `http://www.iipvv.nl/IIP-VV-kanaal/IIPVV-Downloads.html`.

The NCSR Agenda identifies two over-arching goals:

Security and Trust of Citizens This includes privacy protection, security of mobile services, data and policy management, and accountability.

Security and Trustworthiness of Infrastructure This includes malware detection and removal, intrusion detection and prevention, trustworthiness of networks and hardware, software security, security of SCADA/industrial control systems(ICS), and secure operating systems.

Research projects that address these goals can

- target different *research topics* – explained in more detail below,
- target different *applications domains*, and
- range from short-term and more applied research to more fundamental research,

as illustrated in figures 2 and Fig 1.

Tackling cyber security is not just a matter of technical IT expertise. It requires collaboration between very different communities and *disciplines*:

- the β disciplines of computer science and engineering, and neighbouring areas of mathematics (notably cryptology) and electrical engineering.
- the α and γ disciplines of law, criminology, (business) economics, (information) management, applied ethics, psychology and sociology.

To structure the discussion on a potentially infinite list of research topics, the NCSR Agenda distinguishes the following research topics:

1. **Identity, Privacy and Trust Management**

   Managing the (digital) identities, protecting user's privacy and managing the trust in the online world are essential functionalities of the *future internet*[1], which are required in each of the application areas listed above. The application areas concern important but distinct aspects of the digital life of the citizen. In each of these, different authorities, and different numbers of authorities – sometimes one (e.g. the government), sometimes many, sometimes none – will be responsible for providing and controlling identities, and different authentication mechanism will be used. Therefore, different identity management solutions are needed to cater for the various needs. Research sub-areas include the computer science and

[1] See Future Internet Assembly: http://www.future-internet.eu/

Figure 1: Application domains and research topics

crypto techniques to ensure privacy and to handle identities securely, organisational rules and guidelines to delegate trust, and rules and legislation to deal with identity theft, privacy and anonymity rights, as well as private data retention and corresponding access rights.

2. **Malware**

   Malware, short for malicious software, denotes all forms of hostile, intrusive, or annoying software or program code. The ability to run malware is essential for many types of attack, serving as a *conditio sine qua non* for generating social and economic power for the attackers.

   Thus, the threat of malware will remain critical for the foreseeable future. Currently, we experience the threat of malware most saliently in the form of botnets – millions of infected machines tied together in networks at the disposal of attackers. But malware evolves with the ICT infrastructure. We are already seeing malware on social networks, in cloud computing and on mobile devices.

   In terms of research, it poses an interdisciplinary challenge. We need advances in technology, as well as arrangements to shape the socio-economic forces that fuel or mitigate the spread and impact of malware. Unless these issues are researched jointly, we will be stuck with partial solutions of limited value.

   Technological advances include attack detection and prevention, incident recovery, reverse engineering, and attack analysis. For instance, to detect and prevent attacks, we need techniques and tools to spot and remove vulnerabilities from software, and monitoring systems to raise an alarm when a program behaves in an anomalous manner.

   Analysis of malware requires reverse engineering techniques to help us understand what it is doing, as well as methods to estimate the number of infected machines and the effectiveness of counter-measures. From an historical perspective, we should study trends in malware–as doing so prepares us for new threats in time.

   While originating in criminal behaviour, the magnitude and impact of the malware threat are also influenced by the decisions and behaviour of legitimate market players such as Internet

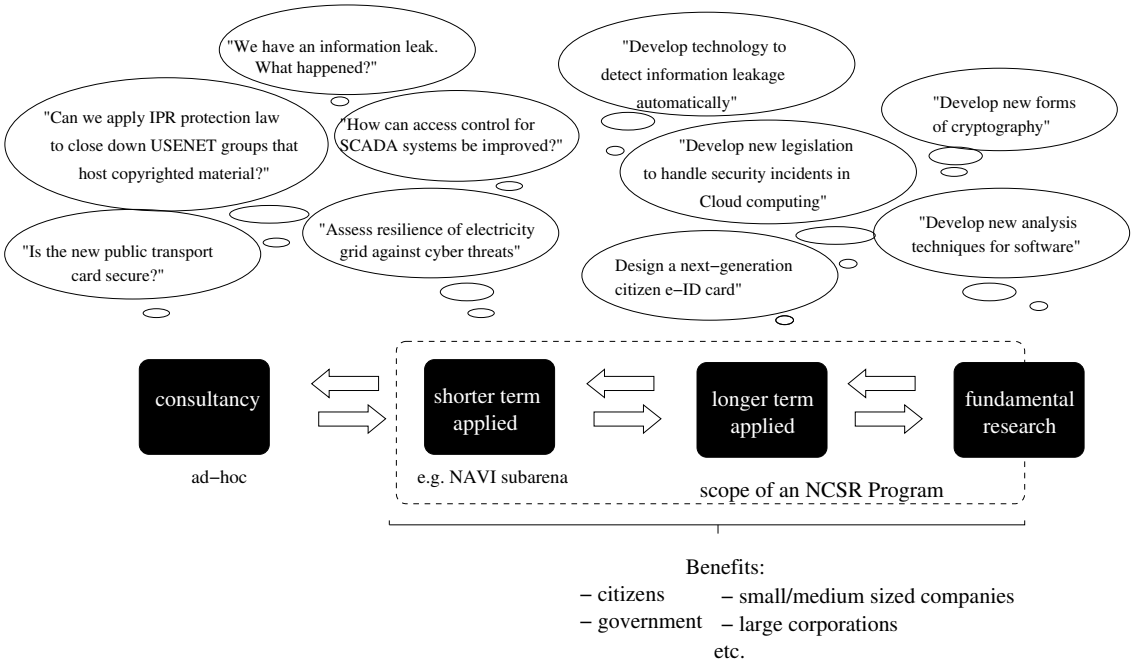

Figure 2: The spectrum of ICT security research problems – with examples

Service Providers (ISPs), software vendors, e-commerce companies, hardware manufacturers, registrars and, last but not least, end users. Here, critical questions focus on economic incentives for the variety of market players. These can be shaped by self-regulation, state regulation and liability assignment. At the organizational level, we need policies to govern the management of hardware and software (including purchase, configuration, updates, audits, decommissioning), and guidelines regarding the management of information.

In addition, we often lack understanding about the socio-cultural context of the malware. Why is it doing what it is doing? The threat posed by Anonymous (the loose group of netizens and hackers that attacked companies that interfered with WikiLeaks) is very different from that of criminal organisations herding massive botnets, and that of state-sponsored cyber espionage and warfare. Studying the origin of attacks and the nature of the victims, as well as the language and socio-cultural references in malware help linguists and sociologists to profile the attackers.

3. **Forensics**

The goal of cyber forensics is to examine digital media in a sound manner to identify, preserve, recover, analyse and present facts and opinions about the information. Forensics, and, more generically, Computer Security Incident Response (CSIR), is an important part of cyber security. It operates on the corrective or repressive side of security, i.e. it comes into play after a security breach has occurred and attempts either to correct the problem as quickly as possible, or to find evidence to be able to identify and prosecute the culprit.

The first decision after an incident is an economic one. How essential is the compromised system? For example, in a critical infrastructure setting such as a power station, it may be more important to get things up and running (without running the risk of a repeat) than to gather forensic evidence. If, however, the decision is made to consider the compromised system a crime scene, highly skilled digital forensics expertise is needed on-site as quickly as possible to collect evidence, in a way that provides evidence that is admissible in a court of law. This process requires deeply technical as well as legal knowledge. Legal expertise about digital forensic evidence is also very important in getting more visible cases where cyber

criminals are successfully prosecuted. Live forensics (forensics on a system that cannot be switched out, as in critical systems) and the attribution question (linking the criminal activity to the criminals behind it) are examples of issues that urgently require additional research. Forensic evidence has been used in a number of high profile cases and is becoming widely accepted as reliable within US and European court systems. However, this may be hampered by a lack of official standards for digital forensic evidence, especially with multiple parties providing digital forensic evidence.

4. **Data and Policy Management**

   In the application areas a variety of data plays a key role. However, the confidentiality, availability, authenticity and integrity requirements for different kinds of data can vary greatly, both in the technical as well as in the legal sense. For example, health records must be kept for 70 years, and therefore require strong security, whereas other data is almost ephemeral, such as the data kept by RFID tags. In this area, we need computer science research to develop data management techniques, but also organisational procedures, to ensure correct handling of sensitive data, and research to make sure that technical policies match with the user's mental models and understanding.

5. **Cybercrime and the underground economy**

   There is organised cyber crime, such as skimming, botnets, provision of child pornography and advance fee fraud, and unorganised (common) cyber crime, such as simple frauds, downloading child pornography, uttering threats, etc. In both cases we need to understand the (explaining) factors that lie behind the crimes, the modus operandi and the criminal careers of cyber criminals, and, in the case of organized crime, how their organisations work. We need to know more about patterns in cybercrime, who the victims are and how victimisation can be explained. Since money (and as a result of that goods and information with a monetary value) is a key factor in many crimes, it is important to better understand the underground economy, its size, its characteristics and how it is intertwined with the legal economic system. Also we need to know more about the effectiveness of measures against cyber crime and the cooperation between (private and governmental; national and international) parties against cybercrime. What works and why? Do law enforcement agencies use their special powers for crime fighting in a digital world and, if so, with what result? The aim of research into the cybercrime area, is to design crime prevention strategies and measures to effectively disturb/block criminal activities.

6. **Risk Management, Economics, and Regulation**

   Risk management aims to assess the economic value of security, to provide a rational basis for allocating resources to improve security after identifying and assessing risks – and to determine if we are doing enough, or too much, and if we are spending resources on the right things. One central problem here is that concrete data is often lacking, and more research could provide a more solid basis.

   A much more fundamental problem is that risk assessment is typically done by an individual party, one of the many parties that collectively provide a complex value chain. For an individual party in such complex value chain there may not be any economics incentives to fix a problem. Indeed, in cyber security there are many *externalities*: costs that borne by other parties and hence not incorporated in price. For example, someone whose home PC is part of a botnet might not notice any adverse effects, and hence not be motivated to go through all the hassle of cleaning it. Perverse incentives may be a more important cause of security problems rather than the lack of a suitable technical protection mechanisms. A better understanding of the economics of security – and the economic (dis)incentives that occur – is needed for more structural solutions of security problems.

   Understanding economic drivers – and where these fail – is also crucial to determine where regulation is needed, and more generally what the government's role should be in cyber

security. Different regulatory frameworks may apply in the various application domains, and at different levels: national, EU, and international.

7. **Secure Design, Tooling, and Engineering**

   Security engineering is a relatively new field and still lacks the methods and tools to design, build and cost-effectively test secure systems. ICT systems in use today are typically not designed and built with security in mind. As a result, security is often dealt with retrospectively, only after security problems arise. Security problems then have to be solved by an add-on in the design, when bad initial design decisions can no longer be reversed. When it comes to the software, fixing the problems requires costly bug fixes to patch implementations.

   Ideally, systems should be designed with security and privacy in mind from the start – ensuring **Security by Design** or **Privacy by Design**. They should then be implemented and tested using good engineering principles and analysis techniques to avoid security problems or detect them at an early stage. While considerable progress has been made in some niche areas, such as security protocol analysis, sound engineering methods for security are still a long way off, especially when it comes to providing secure software.

   Besides software engineering, the field of economics plays an important role in this area. The cost of a secure design may be initially higher and requires a trade-off between risks and expenses. In addition, the cost over time for a secure design is likely to be quite different from that of less secure systems.

Even if initially aimed at one specific application domain, research on the topics above can provide generic solutions that apply to other application domains. For this to happen it is important that NCSR Agenda helps to disseminate knowledge and project results across different application domains.