ESPOO 2007 VTT RESEARCH NOTES 2368

Technology roadmap of security research

VTT TIEDOTTEITA – RESEARCH NOTES 2368

Technology roadmap of security research

Veikko Rouhiainen (ed.)

ISBN 978-951-38-6894-9 (soft back ed.)
ISSN 1235–0605 (soft back ed.)

ISBN 978-951-38-6895-6 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455–0865 (URL: http://www.vtt.fi/publications/index.jsp)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 3, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 3, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 3, P.O.Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 4374

VTT, Tekniikankatu 1, PL 1300, 33101 TAMPERE
puh. vaihde 020 722 111, faksi 020 722 3499

VTT, Teknikvägen 1, PB 1300, 33101 TAMMERFORS
tel. växel 020 722 111, fax 020 722 3499

VTT Technical Research Centre of Finland, Tekniikankatu 1, P.O. Box 1300, FI-33101 TAMPERE, Finland
phone internat. +358 20 722 111, fax +358 20 722 3499

Technical editing Leena Ukskoski
Cover picture: Kaarina Takkunen
Illustrations: Clip Art and VTT

Edita Prima Oy, Helsinki 2007

Technology roadmap of security research. Rouhiainen, Veikko (ed.) Espoo 2007. VTT Tiedotteita – Research Notes 2368. 33 p.

Keywords energy distribution, telecommunication networks, embedded systems, water supply, transportation, citizens, business, manufacturing systems, security, terrorist attacks

Abstract

VTT has a broad range of security research ongoing in many areas of technology. The main areas have been concentrating on public safety and security, but VTT is also participating in several research projects related to defence technology.

To identify and define expertise and research goals in more detail, the Security research roadmap was developed. The roadmap identified three particularly significant areas related to security. The assurance of a critical infrastructure emphasises the protection of energy networks, information networks, water supply, traffic and transport, and obviously also the citizens. For assuring the activities of entrepreneurship, significant areas include the security of production and services, the security of sites and assets, and information security for embedded systems. The most important security products and technologies needed are, for example, management of total security, detection, identification, localisation and communication, protection of information networks and systems, as well as physical protection.

In the EU's Security programme, which aims at ensuring the security of society and its vital functions, it is stated that “Technology alone can not assure security, but security can not be assured without the support of technology.” VTT is conducting security research in all its areas of expertise and clusters. The area has a significant research potential. The development of products and systems designed for the improvement of security has just started. There is still room for innovation.

This report presents knowledge and development needs in more detail,as well as future development potential seen in the area of security.

Preface

The need for increasing security has arisen in Europe after some highly visible and tragic events. While responsibility for security rests largely on national activities, the EU has also started planning a security programme as a part of the 7th Framework Programme. The justification for this research area has been presented as “Technology alone can not assure security, but security can not be assured without the support of technology.” Furthermore, this justification highlights the fact that security and military research are becoming ever closer. The old distinction between civil and defence research is diminishing, because both areas are nowadays using the same knowledge.

In Finland, noteworthy entrepreneurship related to security already exists. Although some of the companies are already international leaders in their area, others are currently operating only in Finland. The importance of the security industry is increasing and remarkable potential for new growing business areas can already be identified. This, however, also requires an increase in research efforts.

The improvement of products and systems requires the development, combination and wide-scale application of technologies. The Security research roadmap is based on this assumption. The roadmap concentrates especially on the following key areas: the assurance of critical infrastructure, the assurance of the activities of entrepreneurship and security technologies and services. The publication identifies VTT's key areas of expertise and their possibilities with regard to the development prospects of society and entrepreneurship as far as they are relevant for VTT's Security research, and proposes plans to develop the new knowledge. VTT's expertise in the field of critical technologies improving security is good, so VTT should strive to take a leading role in large-scale security projects in Finland. VTT has good chances of widening its participation in international networks and in the development of security in production.

This publication is a shortened version of the publication VTT Research Notes 2327 (2006), which was published in Finnish.

Contents

1. Introduction

During the last few years, the development of products and systems designed for the improvement of security has increased sharply. In this publication, these products and services, some of which still lie in the future, are examined from the aspects of the assurance of critical infrastructure and the assurance of the activities of entrepreneurship. The potential security technologies are viewed through their areas of application. The emphasis is on describing development potentials and the attainable benefits.

1.1 Need for security

The assurance of critical infrastructure emphasises the protection of energy networks, information networks, water supply, traffic and transport and citizens. A summary of the goals, visions and development potentials related to these aspects can be found in Table 1.

For assuring the activities of entrepreneurship, significant areas include the security of production and services, the security of sites and assets, and information security for products and systems. A summary of the goals, visions and development potentials related to these aspects can be found in Table 2. The purpose of this report is to examine security research from the perspective of general security, so it does not include all the subjects of security research.

1.2 Need for security technologies

In general, the short-term goal is to analyse the risks and to apply the existing technologies to the area of security research. In the medium term, the goal is to develop the support systems of decision making and to integrate security with larger systems. In the long term, the goal is to build intelligent and reliable security systems.

Generic technologies maintaining safety include technologies used in total security, alarm and monitoring systems and information security. In the management of total security, the key areas are the analysis, evaluation and management of risks, safety information management, the cooperation of the different parties and the methods and models used in security management. Converting the risk into a form measurable by business indicators (due diligence) is becoming more important. In detection, the development is expected to shift from the detection of chemical factors (the establishment of motives) to the observation and identification of biological factors, the development of analysis systems and to the application of detected information in practice. Sensor technology, definition methods and communication must be fast. The roles of information security monitoring and the protection

of information networks and systems are emphasised in many application areas of information security.

In information security management, it is important to understand the role of information security risks, threats and vulnerabilities with regard to a company's business, its products and its services. Digital convergence on the level of information networks, equipment and services poses special challenges for work related to information security. The convergence development threatens general safety as well, when interfaces to open networks are built into the control systems of critical basic structures. With regard to security, it is important to be able to develop proactive monitoring and protective methods, instead of reactive ones.

Table 1. The goals of the assurance of critical infrastructure in selected applications in the short term (under 5 years) and in the medium term (10 years).

Functionality	Goals and vision (short term)	(medium and long term)
Energy networks	To analyse the threats related to the networks and the possibilities to improve security with current technologies.	To develop the technologies that are necessary to protect the networks from expected threats and to improve the security thinking of owners and users.
Information networks	To ensure the functionality and availability of services, i.e. that the security service is available when it is needed and it functions as well. The definition and value network analysis of security objectives in mobile service.	Actual and extensive basic information security services in telecommunications. Proactive and transparent information security. Intelligent information security monitoring.
Water supply	To analyse the critical areas of water supply, and related risks and threats, as well as the options for improving security by means of new monitoring, measuring and analysing techniques.	To develop technologies that are necessary to protect the critical points of the drinking water network against threats and to support the necessary decision making process. To develop the usability and the fault tolerance of the water supply in all circumstances.
Traffic and transport	Definition of the security area in traffic and logistics. Development of risk identification methods and evaluation models. Adding security thinking to research methods.	Application of risk management models. To ensure the usability, functionality and security of logistics networks.
Protection of citizens	Processing the risk assessment of threats. Analysis of the detection methods of chemical and biological agents. Harmonisation of the protection of rescue teams, development of decontamination solutions for shelters and indoor spaces that can be taken into use quickly.	Utilisation of microbiological risk evaluation knowledge and models, application of detection methods of biological agents. Creation of a reliable definition concept for air samples and the management of CBR agents (filtration, protection, decontamination).

The products and systems designed for the improvement of security have a number of economic advantages. These pertain to assuring the security of critical objects and preventing downtimes in production, among others. Reliability and availability improve usability. As an example, water supply is related to a number of other systems. Ensuring the security of transports (e.g. food, fuel and electricity) supports the assurance of critical infrastructure. The solutions developed for the protection of citizens may improve the quality of inside air in general.

Table 2. The goals of assuring the activities of entrepreneurship in selected applications in the short term (under 5 years) and in the medium term (10 years).

Functionality	Goals and vision (short term)	(medium and long term)
Security of production and operations	Integrating the security perspective into vulnerability analyses, e.g. HACCP hazard analyses and other risk analysis tools. Development of IT tools used in risk analysis and risk management, and their application in the security area. Development of security and risk indicators. Development of information security risk management methods.	Adding security risk management to the management of companies. Integration of security management and risk management into the different phases of the product's life cycle and more clearly as part of the business. Methods of information security management (evaluation, design, realisation, follow-up).
Security of sites and assets	Risk analyses of the sites, risk analyses of the reference buildings. Development of the risk management methods of the sites: the information security risks related to the use of the automation, alarm and control systems of the IP networks have been analysed. Building Reporting to the Emergency Vehicle system (PARK).	Identification, prevention and control of risk behaviour. Alarm systems using RF sensor networks. Secure information security solutions related to the use of the automation, alarm and control systems of IP networks. Information system of the sites' security management.
Information security of products and systems	Management of the state-of-the-art technology of mobile devices and embedded systems. Information security analysis of the digital TV application platform and the IP-based return channel. Management and application of content protection (DRM) methods.	Development of new information security architectures for mobile devices and embedded systems. Information security management in the data terminal (e.g. protection of the mass memory and the return channel). Testing of content protection methods, method development.

2. Security as a research area

This chapter presents the research and development potential that security provides from a technological point of view. Security as a research area (2.1) introduces the basis for the report and the security aspect selected. The benefits obtained from security research are discussed in Chapter 2.2 and the new products and services in Chapter 2.3. The benefits and the new products and services are analysed in the light of the report's two key aspects: how they assure the critical infrastructures and how they assure the activities of entrepreneurship. The technologies used in the security industry, the services enabled by them and their connection to different application areas are presented in Technologies and services of the security industry (2.4).

2.1 Scope of the research

Starting point

Ensuring safety in society and critical operations has become a considerable challenge in Europe. The description of the EU´s security programme says: “Technology alone can not assure security, but security can not be assured without the support of technology.” This description also emphasises that security and defence research are now nearing each other more than ever. The old division into civil and military research is fading, because it has been established that both utilise the same knowledge. This was also emphasised with the technology projects commenced by the Finnish Defence Forces in 2005.

As the scope of the Security research is very wide, the EU has started a preliminary project, the first sub-projects of which started in 2004. Their purpose is to guide the Commission in targeting the Security programme. This is the reason why VTT, along with some other companies and research organisations, is involved in the IMPACT and SeNTRE projects. SeNTRE is a network project which makes it possible for VTT experts to influence the targeting of the EU's future Security programme and at the same time build the necessary networks.

VTT's security research roadmap

VTT as a research institution specialised in multidisciplinary, confidential and impartial research has good opportunities and resources to take charge of large security-related projects. VTT also has the necessary cooperation networks, such as EARTO and EUROTECH, through which it can get in touch with the best experts in Europe. VTT has also created functional links within the industry in Finland, e.g. through defence

research. Its versatile knowledge and networks allow an active participation in international networks and development within the industry.

The technology roadmap of VTT's Security research examines the area of security from the following aspects (possible research and development areas):

- Assurance of critical infrastructure
- Assurance of the activities of entrepreneurship
- Security technologies and services.

There is great research potential in the area, as the development of products and systems designed for the improvement of security has just started. There is still room for new innovations and they are needed. The improvement of products and systems requires the development, combination and wide-scale application of technologies. The goal is to create new products and business. The industry and especially the companies operating in the defence industry are directing their operations towards the area of security more than ever. The research has a considerable social impact.

Areas of security research

In Finnish, the word ”turvallisuus” refers to both ”safety” and ”security”. This publication mainly deals with the area of security. It is not our intention to define the terms strictly. In general, it can be said that the concept of safety refers to unintentional damage, that relate to occupational, traffic, home, fire and product accidents and losses. On the other hand, the concept of security refers to intentional damage, such as crime, terror and crisis management. An exception to this is information security, as both intentional and unintentional risks are referred to as information security risks. It must be pointed out that in communications jargon, ”security” usually refers to information security. In order to avoid confusion, VTT uses the term “network and information security.” This naming convention is based on an example provided by the European Network and Information Security Agency.

The Foreign Affairs Committee proposes in the EU's CORDIS publication that the research areas of security and safety should not be separated from each other. In this publication, we have attempted to outline wholes that support both of these elements. In VTT's Security roadmap project, no effort was made to define the terms exactly.

Tekes (Finnish Funding Agency for Technology and Innovation) is preparing to launch a safety and security technology programme. Earlier, Tekes ran a programme called “TURVA 2003 Turvatuotteet, -teknologiat ja -palvelut” (SECURITY "2003 Security products, technologies and services). Its subject areas are the following:

- intelligent security products and systems for the following sub-areas of security: personal safety, ensuring the safety of property, safety of property and sites, information security
- methods of safety and security management
- knowledge-intensive service business in the field of security.

However, security research is conducted in numerous other programmes as well. Often security is regarded as such an inherent part of the products and the services that the research given relates to their development. The issues relating to security are horizontal, meaning that they can be applied to different vertical application areas.

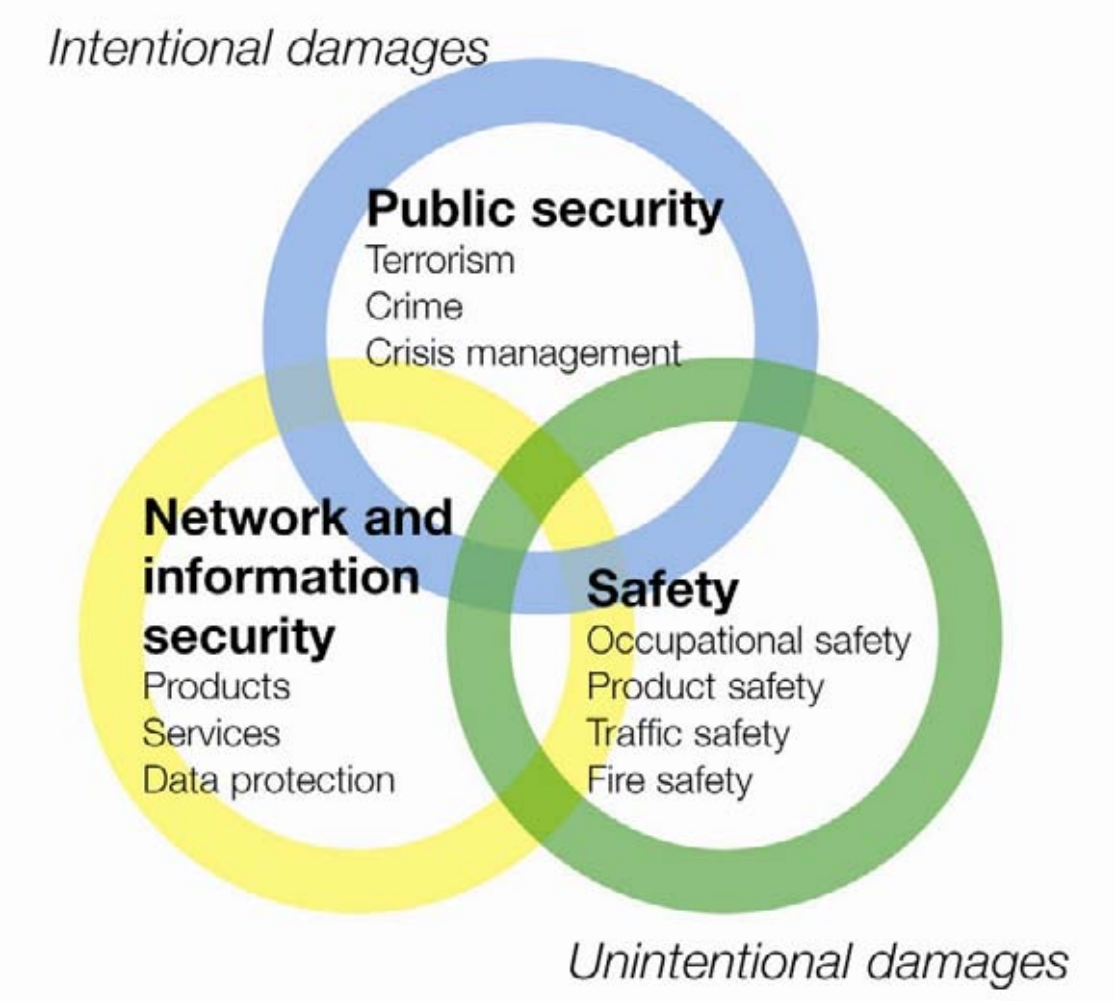


Figure 1. The sub-areas of research that fall within the scope of the Security research roadmap. VTT's traditionally strong areas of expertise in the field of safety have been considered in this roadmap only if they bring new aspects to the Security research as well.

The sub-areas discussed in the publication are shown in Figure 1. The roadmap covers the subjects of the EU's Security programme, as well as safety and information security research (including security management, human activity and especially information security related to products and services). VTT's expertise is based on the analysis of earlier unintentional risks, and with regard to information security, also of intentional risks. Adding intentional risks to unintentional risks is relatively straightforward, but at the same time very challenging in its details. VTT also carries out other research in the field of security that is not covered in this roadmap, such as nuclear research. One purpose of the security roadmap project is to develop cooperation between information security research and safety research.

VTT carries out information security research in several knowledge centres. Information security research is co-ordinated horizontally by a network and information security research coordination group (NIS). Information security as a technological area is discussed in the chapter *Protection of information networks and systems* and as an application area in chapters *Security of production and operations* (including services and their information security) and *Information security of products and systems*. Information security is also included in a number of other application areas.

2.2 Benefits obtained from the security research

Ensuring the security of critical objects provides financial benefits, such as preventing downtimes in production. Reliability and availability improve usability. As an example, water supply is related to a number of other systems. Ensuring the security of transports (e.g. food, fuel and electricity) supports the assurance of critical infrastructure. The solutions developed for the protection of citizens may improve the quality of inside air in general. The benefits of ensuring security have been listed in Table 3 by application area.

Table 3. Benefits of ensuring security.

Application area	Benefit
Assurance of critical infrastructure	
Energy	Better product (electricity), image and social responsibility for the network companies, assuring the availability of a commodity necessary for society, improvement of general security (electricity-dependent functions, e.g. locks). Understanding and analysing interdependencies is crucial. Dimensioning of the backup system. Optimisation of the network for Europe.
Information networks	Information security can be managed and used more extensively, securely, efficiently and easily. Improved information security enables the advanced management of the network. In the long term, communications can be made invisible to the users. The reliability of information networks is improved. The dimensioning and selection of backup systems.
Water supply	The security and reliability of water supply is improved at the level of watersheds, communities and industrial plants. The effects are important: The security and reliability of communities (inhabitants and companies) and industrial plants are improved. The same methods can provide a warning of disturbances that are caused by intentional threats, the aging of the system or by natural disasters.
Traffic and transport	Elimination of risks and threats, better management of logistics. Improvement of delivery reliability. Ensuring business-critical deliveries (valuable transports, electronics, etc.). Operational prerequisites of traffic and transport businesses. Transport equipment, transport network, usage of the network, analysis based on these factors.
Protection of citizens against the consequences of terrorist attacks	Early warning system (biological and chemical agents), better protective clothing and equipment. Fast reaction and alarm, prevention. Interfaces of other systems to the healthcare systems, e.g. to hospitals. Special requirements in protection. Financial optimisation of the bomb shelter structure. Possibility of preventing the contamination of spaces.
Assurance of the activities of entrepreneurship	
Security of production and services	Comprehensive risk management, benefits of synergy and a wider perspective on support development, management of information risks, targeting of risk management in a cost-efficient way, quick reaction in the face of threats. Digital payment transactions. Digital control of production and logistics. Ensuring the security of digital and mobile services. Ensuring the security of automated systems. Development of processes.
Security of sites and assets	Improved security for working alone (e.g. in health centres, security and industrial control functions). Clearer compensation responsibilities, easier to solve crimes. Ensuring the operational capacity of people. Personal security devices integrated into the security systems of sites.
Information security of products and systems	The management of the information security of products is probably the largest and most important single application area of information security. The security and reliability of equipment and embedded systems is improved.

2.3 New products and services

Investing in security creates a number of new products and services. Such products and services ensuring critical infrastructure have been listed in Table 4. New products and services ensuring the activities of entrepreneurship have been listed in Table 5.

Table 4. New products and services created by ensuring critical infrastructure.

Application area	New products and services
Energy	• New products: energy storages • Protected communications solutions • Possibly new structural solutions • New services: interference detection solutions • Improvement of measuring technology • Vulnerability analyses
Information networks	• Information security can be managed more extensively, securely, efficiently and easily, and in the long term, it can also be made invisible to the users • Consultancy services in the research and development of information security: goal setting, protocols, identification, context-dependent information security (digital convergence), evaluation, validation, integration, maintenance of best practice rules, information security management in organisations and international value networks • Information security of services provided by society, information security of administration (availability, preservation, integrity, confidentiality, uncontestability and authentication of information) • Reliability of information systems used in healthcare and the automation industry
Water supply	• Network-wide monitoring systems for extensive condition monitoring • New analysis systems for water quality and security • System-wide movement monitoring systems • New modelling, simulation and visualisation systems to support monitoring • Risk analysis, evaluation and management systems and tools
Traffic and transport	• Transport monitoring systems • Ensuring passenger traffic (flight safety, biometric passport) • Security management as a service in traffic and logistics • Security tools in traffic and logistics
Protection of citizens against the consequences of terrorist attacks	• Biodetection technologies, sensors of dangerous agents • Risk assessment methods • Better and compatible chemical alarm systems • Protective materials and structures • Governmental (regional) alarm and warning systems

Table 5. New products and services created by ensuring the activities of entrepreneurship.

Application area	New products and services
Security of production and operations	• Information security of payment and financial services • Risk analysis, evaluation and management systems and tools • Operation planning concepts, management and operation systems, evaluation of financial effects, converting the risk into a form measurable by business indicators (due diligence) • Management of the risks of outsourcing and networking • Development and indicators of diagnostics and analysis methods • Situational awareness, visualisation, communications • Consultancy services in the research and development of information security: goal setting, protocols, identification, context-dependent information security (digital convergence), evaluation
Security of sites and assets	• Protective structures and technologies, filters • Detectors and alarm systems (system reporting to the emergency vehicle) • Risk management concepts • Evaluation of financial effects, converting the risk into a form measurable by business indicators (due diligence)
Information security of products and systems	• Development of the information security properties of data terminals • Development of the information security properties of devices operated by service providers • Information security testing and monitoring • Information security management process for the whole duration of the product's life cycle

Some of the products and services described above can be realised on a tight schedule, others require more time. The products designed for improving security often require the combination of technologies and the assembly of systems. This is a slow and time-consuming task.

3. Technologies utilised in the security area

3.1 Technologies in application areas

The security industry technologies discussed in the roadmap have been divided into four main categories. These are the management of total security, identification, localisation and communication, protection of information networks and systems, and physical protection.

The management of total security deals with technologies related to risk analysis methods, the management of general security and alarm and monitoring systems. The category of identification, localisation and communication includes a large number of technologies, including RFID, sensor networks (active tags), detection technologies, such as millimetre wave imaging, immunological techniques, as well as pattern recognition and biometric user authentication techniques. The protection of information networks and systems is concerned with technologies related to intrusion prevention, software platforms and architectures, network and Internet security, as well as information security testing. Physical protection includes both structural protection and technologies involving protection against CBR agents in the air.

3.2 Management of total security

Risk analysis methods[1]

In this context, risk analysis methods refer to

- The application and development of risk analysis methods for the assessment of security risks
- The identification of objects to be protected, the identification of threats (scenarios)
- Vulnerability analysis, risk quantification, risk management
- Microbiological risk management strategies in the industry, microbiological qualitative and quantitative risk evaluation
- Self-control and new risk analysis methods like, e.g. HACCP hazard analyses in the food industry.

Risk analyses serve as the basis for systematic risk management. They include the elimination and mitigation of risks, as well as monitoring the situation. New technologies have been developed for this purpose, such as the analysis of weak signals.

[1] Commented by Teuvo Uusitalo, Marinka Lanne, Laura Raaska and Gun Wirtanen.

Benefits and potentials: New products and services based on risk analysis methods can include risk and vulnerability analysis methods, decision making models based on risk evaluation, information technology instruments related to risk analyses, as well as microbiological qualitative and quantitative risk analysis and management methods and tools.

Information security management in companies and organisations[2]

In this context, information security management in companies and organisations refers to

- Processes, practices and technical solutions that are used for information security management in organisations
- The development of information security management processes and practices
- Information security management as part of the companies' business processes
- The definition of the goals and requirements of information security (e.g. by using a common criteria approach)
- Risk, threat and vulnerability analysis
- Continuous information security management during the system's life cycle.

Benefits and potentials: The services based on information security management in companies and organisations can include auditing and definition services or "standardisation". The products can include information security monitoring systems, the development of auditing and monitoring metrics, and risk, threat and vulnerability analyses.

[2] Reijo Savola and Anni Sademies

3.3 Detection, identification, localisation and communication

RFID (Radio Frequency Identification)[3]

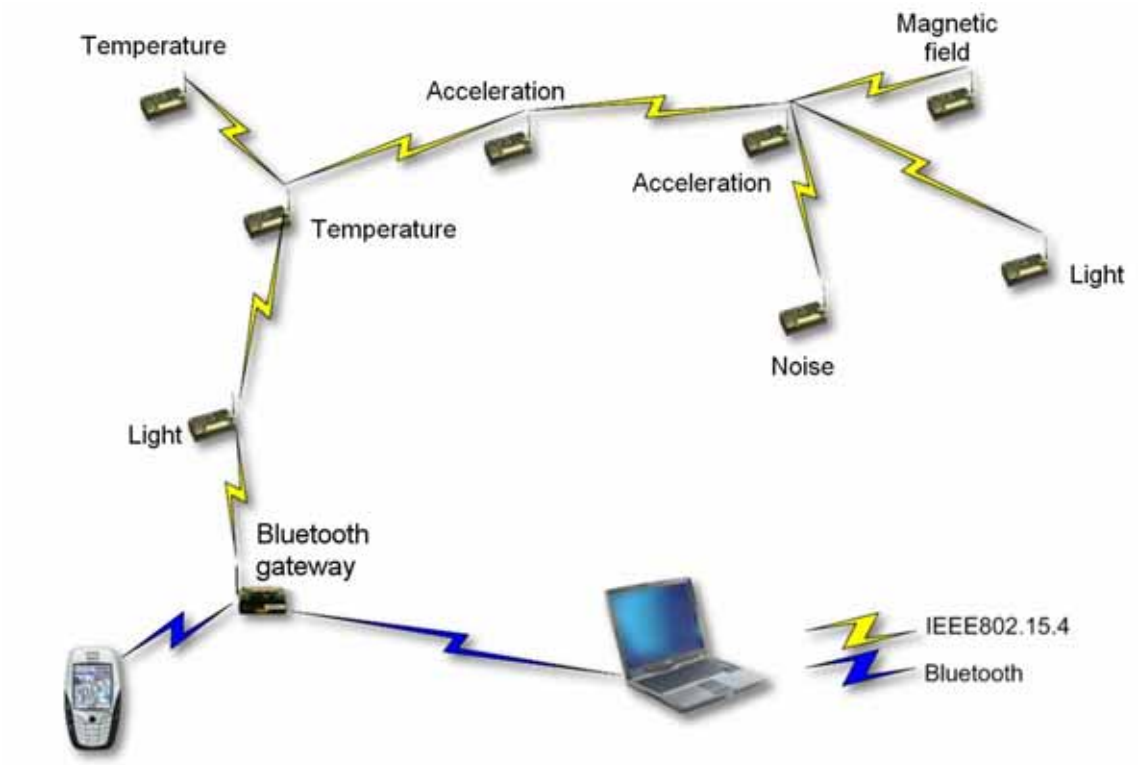
RFID (Radio Frequency Identification) is a cheap radio technology that makes it possible to identify objects, usually consumer goods, pallets and other transport units as well as vehicles and people. The use of RFID is becoming more common as an alternative to the bar code, because RFID does not require eye contact. The RFID reader has an antenna and a transceiver, while the object is equipped with a passive or active RFID tag that provides the information stored in the tag and other information when required from the net.

An example of the application of RFID is the information system based on escort memories developed by Prosec Tietoturvapalvelu, used for the accurate handling of locked collected containers. Each secure container has a unique RFID tag. The tag helps in recording when the container was taken away, inspected and returned, registering the time of the activities and the people carrying them out, and identifying the container when it is weighed. The drivers have PDA devices that are used for registering the service activities related to the containers.

Benefits and potentials: It is possible to identify people or goods electronically fast or in real time without physical or eye contact. Relatively cheap and automated identification makes it possible to establish new businesses, automate functions, enable automatic access control and real-time monitoring of transports and goods.

[3] Pasi Ahonen and Antti Permala

Active tags[4]



The active tag is a cheap simple tag that unlike the passive RFID can carry out measuring and radio communication activities independently. The tag has its own energy source or it generates energy from the environment. Active tags can monitor their own status continuously and forward information, if necessary.

Benefits and potentials: By creating a network of active tags, it is possible to build different monitoring and identification systems. The possible new products include sensor networks and sensory detectors.

Detection[5]

The sensor probes the physical or chemical quantity and generates a corresponding signal. For example, the leaks of shut-off valves and the wear of bearings can be detected more easily by means of a micromechanical silicon sensor. Both faults cause a vibration in the structures in the ultrasound range. The failure, wear and service need of the actuator can be established by embedding the sensor into the device to measure vibration.[6]

---

4 Henrik Huovila
5 Pasi Ahonen, Antti Permala and Laura Raaska
6 Aarne Oja

The new technologies can offer numerous benefits and potentials. As an example, a detecting package may be able to monitor its own status (temperature, humidity, corrosion, ESD, oxygen etc.) and possibly also be able to communicate with the operator. The measurements can be carried out by means of sensors or other techniques. It is also possible to monitor the operational capacity of people.

Detection of chemical and biological factors [7]

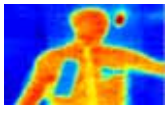
The purpose of large-scale international research and development projects is to develop a good, functional and fast biodetector for the most important bioagents. As an example, the United States invests 1 billion dollars a year in this area.[8] B detection is usually based on mass spectrometry, PCR-technology and immunological techniques. C detection uses traditional analytical chemical techniques or an ion movement detector.

VTT has decades of experience in building bomb shelters, which have always included CBNR protection as well, along with filtering techniques. The IMPACT project is concerned with reviewing the current technologies used for B and C detection and carrying out a SWOT analysis, as well as with evaluating the benefits of the new biotechnical methods in developing multi-analytical B and C detection methods. The goals of the development of PCR-based detection methods for harmful microbes in industrial samples include among others the following: [9]

- The definition of unwanted microbes in the process and end product samples of the food and paper industry
- The application of fast molecular biological methods to new sample matrices
- Concentration on selected key microbe types and groups occurring in industrial processes.

Benefits and potentials: By using new microbiological and chemical methods, results can be obtained faster, which means that the industry can react faster in case of problems (e.g. recall of polluted food before delivery, adjustment of a paper mill's processes before the occurrence of problems caused by microbes).

Millimetre wave and Terahertz imaging technology[10]



Millimetre wave and Terahertz imaging technology refers to passive or active imaging in the millimetre and sub-millimetre range by using very sensitive

[7] Kristiina Takkinen
[8] Veikko Komppa
[9] Outi Priha, Laura Raaska, Kirsi Kujanpää and Hanna Miettinen
[10] Arttu Luukanen

radiometers or radars. By combining a relatively short wavelength with good transparency e.g. in traditional clothing materials, it it possible to detect weapons, other similar objects or explosives remotely from a distance of up to 100 metres.

In the short term, the purpose of millimetre wave imaging technology is to demonstrate a practical and reasonably-priced imaging equipment that is sensitive enough for positive detection and identification with low false positive alarm rates.. The demonstration would include a few pixel elements combined with mechanical scanning. In the medium term, the number of pixel elements would be increased to hundreds of pixels and combined with mechanical or electro-mechanic scanning, which would enable imaging with video frame rates. Alternatively, the demonstration would involve imaging equipment based on aperture synthesis. In the long term, the goals are the following: complete electronical scanning, camera operating in the video frequency range (mm range); a focal plane with thousands of pixel elements, a "CCD"camera operating in the video frequency range (sub-mm range); for longer distances (e.g. military applications), a camera based on aperture synthesis producing a video frequency picture. The millimetre wave imaging technology is being developed by VTT, NIST, DHS, DARPA, HSARPA, the University of Delaware and a number of other companies.

Benefits and potentials: Under the current airport security measures, many threats go undetected: Metal detectors do not indicate items such as ceramic kitchen knives. By means of current X-ray devices, it is difficult to detect thin sheet explosives. Millimetre cameras are able to detect both of these threats. In the long term, the resonances of macromolecules in the millimetre and sub-millimetre ranges may enable the remote detection of biological threats. The monitoring of earth traffic at airports will be possible in all circumstances, as the mm-waves will be able to penetrate all obstacles, such as fog. The remote detection of threats will also make it possible to mitigate their effects before they are localised in the object to be protected. Military applications are also possible. Finally, it is foreseen that the overall success of stand-off detection of CBE threats will be only achieved with the efficient integration of multiple detection modalities of which mm-wave or Terahertz imaging is one.

Pattern recognition[11]

Pattern recognition aims at recognising, classifying or modelling objects based on their properties or observations made of them. Pattern recognition uses methods of signal processing, neurocomputing, statistics and artificial intelligence, among others. They make it possible to process different kinds of information, including pictures, speech, texts, measurements of industrial processes,

[11] Pasi Ahonen, Heikki Ailisto and Jouko Viitanen

intelligence information and statistical data. Possible monitoring objects for the methods are e.g. underground stations, licence plates and suspicious “behaviour”.

During the last 25 years, VTT has carried out numerous projects in almost all sub-areas of pattern recognition. The fields include industrial automation, process automation, robotics, mobile technology, recycling, medicine, biotechnology, logistics, laboratory automation, remote mapping, security technology, facility management, traffic control, electronics and microelectronics.

Benefits and potentials: Understanding the state of security, alarms, recognising change; simplifying the interaction between man and machine; digital picture archives, searches etc.; medicine: automatic review of patient pictures; robotics: moving, automatic working; industrial automation: manufacturing, moving; verifying the person's identity (arrival in the country, air traffic, other critical objects). The new products and services include the following:

- Inventions related to the computer's or the mobile phone's interface
- Software products designed to speed up the development and deployment of recognition systems
- Sensors tailored to special applications (e.g. wide-spectre detection).

Biometric authentication[12]

Identifying people on the basis of their physical properties (e.g. fingerprint) or behaviour pattern (e.g. walking style). Typically the user of the system is first registered (taught, enrolled) into the system, e.g. by taking a fingerprint sample, after which the identification information provided in normal circumstances is compared to the learnt model (template). Biometric authentication can be divided into one-to-one recognition (verification) and one-to-many recognition (identification). A separate method is the so-called watch list activity, which is used for authenticating only certain people.

Typical products and services are the following:

- Information security: PCs, information networks
- ATMs, other banking activities
- Biometric locks and access control: restricted areas in airports, offices, factories, hospitals, agencies, homes
- Security: defence forces

[12] Pasi Ahonen, Heikki Ailisto

- Aid in emergency areas
- Immigration: passport control
- Work of the authorities, official documents.

Possible applications in the future are the following:

- E-business
- Mobile data terminals, Internet mobile phones, mobile payments
- Cars, household appliances, gym equipment
- Home entertainment systems recognise who came into the room, and select the person's favourite channel, volume etc.
- Security and convenience of senior citizens.

3.4 Protection of information networks and systems

Compatibility with regard to information security[13]

The networks of different organisations, companies and the government have to be combined in different value networks in order to provide comprehensive services or to improve the cooperation between the companies. These organisations may have very different information security policies and the level of information security in the networks may also vary. If public Internet is utilised in combining the networks, it also involves a component for which no information security has been defined. For this reason, the level of information security may vary or it may even be unknown. In the future, special attention must be paid to ensuring an adequate level of information security, as the services, devices and networks will converge more and more. In particular, connecting closed old systems to open systems will pose significant challenges for information security.

Benefits and potentials: The safe connection between the networks of different organisations, companies and the government in order to provide comprehensive services or to improve the cooperation between the companies. Integrating information security into the company's business process.

[13] Jarkko Holappa

Intrusion prevention, detection and prevention systems and measurement of information security in the networks[14]

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) monitor network traffic and its nature. The purpose of the IDS system is to detect intrusion attempts and to minimise any possible damage. The earlier the attack is detected, the less damage it can cause. These systems also make it possible to collect information about attack patterns. This information can be used in developing more efficient intrusion prevention methods and measuring systems.

Benefits and potentials: The system detects intrusion attempts and minimises any possible damages by blocking or slowing down the intrusion or by limiting its effects. IDS and IPS systems must be developed so that they become more comprehensive and intelligent - "Beyond IDS".

Software platforms and architectures[15]

In this context, software platforms and architectures refer to

- Information security management mechanisms in embedded software products from an architecture or platform point of view
- Especially middleware solutions are important

Benefits and potentials: Information security management solutions, content protection. Developing information security testing techniques for software platforms and architectures is important, so that they can provide a good enough basis for equipment and embedded systems.

Network and Internet information security[16]

In this context, network and Internet information security refers to

- The identification, prevention, blocking, monitoring and management of threats inherent in a network environment
- Comprehensive information security management and information security solutions for IP networks that relate to the Internet and its services
- Protecting the network and its management
- Protecting the overlay networks supported by the network

[14] Jarkko Holappa and Reijo Savola
[15] Reijo Savola
[16] Reijo Savola, Arto Juhola and Juuso Pesola

- Information security management solutions in an Internet application environment. It is evident that IP network technology will be dominant in almost all network solutions. Other technologies will be used only in special applications (e.g. for connecting very simple devices, such as sensors, to wider networks).
- Special problems of IP networks.

Benefits and potentials: Autonomous operation and manageability; information security as a transparent part of the network and its services. Manageability results in traceability. It is possible to influence who does what. Suitability for demanding applications. The new products and services can include support services for network information security, which are characterised by dynamic and comprehensive features, active elimination of interference and overlay networks.

Information security testing[17]

Information security testing refers to the testing or approval of the product or system that ensures that the goals set for information security are met. If the goals of information security have not been defined on an adequate level, information security testing also includes the definition of these goals. Information security testing consists of robustness testing and information security analysis (i.e. comparison with the goals of information security).

Benefits and potentials: Improving the testing knowledge. Better understanding of information security phenomena. Synergy of information security monitoring (especially the metrics). Certainty that the product complies with the requirements. Information security testing also provides material for research.

3.5 Physical protection

Structural protection[18]

In this context, structural protection refers to

- The protection of people and the functions within the building from mechanical blows, such as
  - pressure waves (explosions)
  - kinetic loads (car crashes, fragments)
- The protection of people and the functions within the building in case of fire

[17] Reijo Savola
[18] Auli Lastunen

- The protection of electrical devices and electric circuits within the building from
  - electromagnetic pulses (EMP)
  - high power microwave (HPM) weapons.

Benefits and potentials: Prevention and slowing down of intrusion. Weaker effect on people in exceptional circumstances. Electromagnetic protection. The new products include more durable and secure products (e.g. window glass that does not break into fragments) and services (e.g. a testing method for examining the effect of blows on wall and intermediate floor structures).

Protection against CBR agents in the air[19]

Protection against CBR agents in the air refers to

- The detection of CBR agents in the air
- The cleaning of incoming and breathing air of CBR agents
- A decentralised air conditioning system, tightness of structures etc.
- The air quality of a controlled space and the necessary filtration methods
- Air microbiology and the detection of biological agents in the air.

Benefits and potentials: In normal circumstances, the improved filtration of incoming air also removes the other impurities in the air that are detrimental to health (outside pollution), while tighter wall structures save heating energy. In exceptional circumstances, the effects on people are less serious. After a possible blow, the need for cleaning is smaller. The new products include more efficient, versatile, intelligent and economical filters and analysis systems that last longer and require less maintenance. The development in the field is slowed down by the fact that there are no grounds for it, unless the authorities provide instructions regarding the security issues or the threat is considered serious enough to be taken into consideration. The builders play a significant role in the deployment of new products. The actual deployers are filter and detector manufacturers.

[19] Auli Lastunen, Laura Raaska and Gun Wirtanen.

4. Conclusions

Ensuring safety in society and vital operations has become a considerable challenge in Europe. The EU's advisory board has stated that technology alone can not assure security, but security can not be assured without the support of technology. There is great research potential in the area, as the development of products and systems designed for the improvement of security has just started. There is still room for new innovations and they are needed.

The improvement of products and systems ensuring security requires the development, combination and wide-scale application of technologies. The Security research roadmap is based on this assumption. The roadmap concentrates especially on the following key areas: the assurance of critical infrastructure, the assurance of the activities of entrepreneurship and security technologies and services. The publication identifies VTT's key areas of expertise and their possibilities with regard to the development prospects of society and entrepreneurship as far as they are relevant for VTT's Security research and proposes plans to develop the new knowledge. One of the goals of the work is to serve as a basis for the coordination of information security research and for developing the cooperation with other security research carried out at VTT.

For VTT, key application areas of technologies provided by the security industry are energy networks, information networks, water supply, traffic and transport, the protection of citizens, the security of production and services, the security of sites and assets, and information security for products and systems. The most important findings of the report are presented below by application area.

Energy networks

Important technologies designed to ensure the operation of energy networks include different backup plans for total security, the increased decentralisation of energy production in general and new structural solutions.

The key knowledge in ensuring the security of energy networks is related to the management of risk analysis methods and information security. In addition to the above,

the technological knowledge related to the detection of threats and disturbances is important for ensuring the operation of the energy networks. Information security emphasises intrusion prevention and the protection of information networks and systems.

Information networks

In the short term, important technologies ensuring the operation of information networks are a secure middleware layer, a simplified and robust key management solution and programmable networks. In the medium term, the requirements regarding the functionality of the Internet are emphasised, and a number of technologies are required to develop it, including an automatic and autonomous policy-based information security management solution for the network, programmable networks, reliable components, utilisation of the context and overlay security. The importance of measuring information security and monitoring will become more pronounced.

The key knowledge in ensuring the safety of information networks is related to information security management and naturally to the protection of the information networks and systems. The knowledge related to sensor networks and biometric authentication is also useful for ensuring the operation of the information networks.

Water supply

Important technologies for ensuring the operation of the water supply as part of total security include the evaluation of process phases and the development of control systems that are crucial to the product safety of waterworks, the design of threat scenarios and the analysis of potential risks. In the medium and long terms, the role of different modelling, simulation, visualisation and localisation techniques, as well as management and decision making systems, becomes more important. Important technologies related to the detection and monitoring of problems are the chemical, biological and radioactive analysis and detection techniques. In the medium term, microbiological diagnostics are developed for the target microbes. In the long term, the speed of microbe diagnostics (results in under two hours) and its application in practice will become more marked. Sensor technology and communication must be fast.

Traffic and transport

In ensuring the operation of traffic and transport, detection, localisation and communication technologies have a key role. In the short term, these include the tracking technologies of vehicles and transports, as well as GIS applications. In the middle term, the development concentrates on system development, including control

and monitoring systems, while in the long term, the emphasis is shifted to the integration of the different systems.

The key knowledge in ensuring the security of traffic and transports is related to geographic information systems (GPS, Galileo), RFID, sensor networks, pattern recognition and biometric authentication. In addition to the above, knowledge in protecting information networks and systems and familiarity with risk analysis methods are important for ensuring the safety of traffic and transports.

Protection of citizens

Important technologies for protecting citizens include technologies of physical protection, as well as different detection, localisation and communication technologies. The latter can also involve millimetre wave imaging and immunological techniques in C and B detection. The development is expected to shift from the detection of chemical factors to the observation and identification of biological factors, the development of analysis systems and to the application of detected information in practice.

In total security management, the development of risk and vulnerability analyses and monitoring the situation by observing people's deviant behaviour by statistical means will become pronounced in importance. Among other things, this requires finding out the availability of data necessary for risk quantification, the development of questionnaire and interview methods, risk quantification and decision making models, as well as real-time monitoring, interpretation and control of the situation.

On the one hand, the key knowledge in protecting citizens is related to physical protection, i.e. structural protection and protection against the CBR agents in the air, while on the other hand, it is about the development of detection technologies. Knowledge related to alarm and monitoring systems, as well as system integration, is also crucial.

Security of production and services

The security of production and services is a broad area. It involves almost every technology that has been discussed in this publication. The appropriate technologies vary depending on the field of business and the company, but it can be generally stated that in the short term, information technology, facility technology, protection technologies, risk analysis, risk assessment and management systems, as well as microbe diagnostics are of crucial importance. In the medium and long terms, the application of these technologies in practice becomes pronounced. Total security

management is based on the application of safety and information security knowledge and experience to the field of security.

It is possible that in some respects, Finland is overprotective. On the other hand, the risk management measures within the industry may be inadequately targeted and their maintenance costs have not been properly studied. There are certainly inadequacies in the maintenance of the risk management systems as well. The coordination of operations at the company level is still disorganised and the focus areas within corporate security have mainly been chosen traditionally. There is little experience of the benefits resulting from synergy between the different areas of security. The realisation of the security level should be more closely monitored and the definition of the focus areas should be based on analyses.

Companies rely very much on information security management and their vulnerability increases as malicious damages become more common. Globalisation and networking bring threats and requirements to information security. The wider use of information technology and electronics (ICT) in all processes and systems increases the need to detect and control risks in order to improve reliability.

Ensuring the security of production and services requires extensive technological knowledge. For VTT, key areas of expertise are for example total security management and the protection of information networks and systems. In addition to these, knowledge in detection, localisation and communication is very important.

Security of sites and assets

Important technologies related to the security of sites and assets include passive or structural security solutions, as well as different alarm and monitoring systems, and their integration and connection to facility systems, alarm control rooms and governmental emergency systems. In the total security management of the site, risk analysis, evaluation and management, reviews, approvals, scenarios, management of security-related information, cooperation between the different parties and the methods and models of security management have a crucial role. The improvement of safety is based on covering the whole lifecycle of the site (design, construction, use, maintenance, development and security management).

The security of assets is crucial, among other reasons to prevent crime and to ensure the security of information. In certain areas, it has also become crucial to prepare for terrorist attacks. The current monitoring systems are integrating with each other. Joint risk management of companies is necessary in for example industrial parks.

Information security in embedded systems

The information security management of products and systems is mainly based on information security architectures and middleware components and platforms. In the short term, such software platforms and architectures include Symbian + IP (mobile data terminals), Java (embedded systems) and the MHP1.0.x environment (digital TV). In the medium and long terms, the use of Linux in mobile data terminals and embedded systems will become more prevalent in addition to the above. A new challenge for digital TV technologies in the medium term are the applications that are loaded through and use the return channel.

The key knowledge in the information security of embedded systems is related to software platforms and architectures, as well as to information security testing. A general knowledge of network and Internet information security is important for protecting the operation of embedded systems.

Generic technologies

The generic technologies ensuring security include the technologies used in total security management, alarm and monitoring systems and information security. Total security management is based on the application of safety knowledge and experience to the security area. Actions emphasise the analysis, evaluation and management of risks, safety information management, the cooperation of the different parties and the methods and models used in security management. Converting the risk into a form measurable by business indicators (due diligence) is becoming more important. Risk and vulnerability analysis methods are being developed. In order to manage risks, methods such as observing people's abnormal behaviour by statistical means and analysing weak signals are being developed.

Knowledge related to alarm and monitoring systems, as well as system integration, is crucial. In the detection of threat situations, the development is expected to shift from the detection of chemical factors to the observation and identification of biological factors, the development of analysis systems and to the application of detected information to the practice. Sensor technology, definition methods and communication must be fast. The goal is to develop fast definition methods and integrated, miniaturised measuring systems, as well as to verify their reliability.

The roles of information security monitoring and the protection of information networks and systems are emphasised in many application areas of information security. The improvement of information security is based on information security architectures, such as middleware components and platforms. Important technologies ensuring the operation

of information networks are a secure middleware layer, a simplified and robust key management solution and programmable networks.

However, technologies cannot ensure security by themselves. Therefore, in addition to technology development, we also focus on developing practices that ensure and promote security.

Series title, number and
report code of publication

VTT Research Notes 2368
VTT–TIED–2368

Author(s)
Rouhiainen, Veikko (ed.)

Title
Security research roadmap

Abstract
VTT has a broad range of security research ongoing in many areas of technology. The main areas have been concentrating on public safety and security, but VTT is also participating in several research projects related to defence technology.

To identify and define expertise and research goals in more detail, the Security research roadmap was developed. The roadmap identified three particularly significant areas related to security. The assurance of a critical infrastructure emphasises the protection of energy networks, information networks, water supply, traffic and transport, and obviously also the citizens. For assuring the activities of entrepreneurship, significant areas include the security of production and services, the security of sites and assets, and information security for embedded systems. The most important security products and technologies needed are, for example, management of total security, detection, identification, localisation and communication, protection of information networks and systems, as well as physical protection.

In the EU's Security programme, which aims at ensuring the security of society and its vital functions, it is stated that “Technology alone can not assure security, but security can not be assured without the support of technology.” VTT is conducting security research in all its areas of expertise and clusters. The area has a significant research potential. The development of products and systems designed for the improvement of security has just started. There is still room for innovation.

This report presents knowledge and development needs in more detail,as well as future development potential seen in the area of security.

ISBN
978-951-38-6894-9 (soft back ed.)
978-951-38-6895-6 (URL: http://www.vtt.fi/publications/index.jsp)

Series title and ISSN	Project number
VTT Tiedotteita – Research Notes 1235–0605 (soft back edition) 1455–0865 (URL: http://www.vtt.fi/publications/index.jsp)	4790

Date	Language	Pages
February 2007	English	33 p.

Name of project	Commissioned by
Yhteiskunnan turvallisuuden varmistaminen tutkimuksen ja teknologian avulla (VTT:n strateginen hankealue)	

Keywords	Publisher
energy distribution, telecommunication networks, embedded systems, water supply, transportation, citizens, business, manufacturing systems, security, terrorist attacks	VTT P.O.Box 1000, FI-02044 VTT, Finland Phone internat. +358 20 722 4404 Fax +358 20 722 4374

VTT has a broad range of security research ongoing in many areas of technology. The main areas have been concentrating on public safety and security as well as information security. VTT is also participating in several research projects related to defence technology.

To identify and define expertise and research goals in more detail, the Security research roadmap was developed. The roadmap identified three particularly significant areas related to security. The assurance of a critical infrastructure emphasises the protection of energy networks, information networks, water supply, traffic and transport, and obviously also the citizens. For assuring the activities of entrepreneurship, significant areas include the security of production and services, the security of sites and assets, and information security for embedded systems. The most important security products and technologies needed are, for example, management of total security, detection, identification, localisation and communication, protection of information networks and systems, as well as physical protection.

VTT is conducting security research in all its areas of expertise and clusters. The area has a significant research potential. The development of products and systems designed for the improvement of security has just started. There is still room for innovation.

This report presents knowledge and development needs in more detail, as well as future development potential seen in the area of security.

Julkaisu on saatavana
VTT
PL 1000
02044 VTT
Puh. 020 722 4404
Faksi 020 722 4374

Publikationen distribueras av
VTT
PB 1000
02044 VTT
Tel. 020 722 4404
Fax 020 722 4374

This publication is available from
VTT
P.O. Box 1000
FI-02044 VTT, Finland
Phone internat. + 358 20 722 4404
Fax + 358 20 722 4374

ISBN 978-951-38-6894-9 (soft back ed.)
ISSN 1235-0605 (soft back ed.)
ISBN 978-951-38-6895-6 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)