Research Priorities in Information Security

Report prepared by

Norsk Ressursnettverk for Informasjonssikkerhet

http://www.nisnet.no/

October 2008

NISNet Partners:	
Universitetet i Bergen	Thales Norway
Universitetet i Stavanger	DnBNor
Universitetet i Tromsø	EDB Businesspartner
Høyskolen i Gjøvik	Kongsberg Defence and Aerospace
NTNU – Telematikk	CONAX
NTNU - Q2S	Mnemonic
Universitetet i Agder	AbelDRM
UNIK - Universitetet i Oslo	Det Norske Veritas
Nasjonal Sikkerhetsmyndighet	HDD
FFI	Avenir
Norsk Regnesentral	Movation (Norman/Birdstep/Comperio/ Fast/Nera/Opera/Radionor/Telenor)
SINTEF IKT	

Document Version:	2.0
Document Status:	Official
Version Date:	27 October 2008
Editor:	Audun Jøsang, UNIK

Executive Summary

This document articulates research priorities in the area of information security as seen by NISNet (Norsk Ressursnettverk for Informasjonssikkerhet) (Norwegian Information Security Network). The document is intended as input to discussions in the IT security community, and to provide advice to Government bodies responsible for defining research policies and for allocating research funding.

Information security research should focus on global research challenges where significant contributions by Norwegian research institutions can be achieved, either alone or in collaboration with other national or international partners. Information research should also prioritize specific national challenges, e.g. in case specific security threats, vulnerabilities and risks are relatively more severe within the national domain than elsewhere.

Given the diversity of expertise among national research groups in the area of information security, research efforts should be allowed and encouraged to focus on different areas. This diversity is also reflected by the many national and international collaborative industry and academic links that our national research groups maintain. To reflect this diversity while at the same time preserving coherence and structure, the research priorities have been grouped under the two main themes *fundamental information security* and *application oriented information security.* A selection of research challenges is briefly outlined below.

For fundamental information security, it is a particularly serious problem that criminals and attackers control a considerable proportion of hosts in Norway. According to Symantec’s Internet Security Threat Report of April 2008, hosts in Norway are the main source of network attacks targeting European countries, and the 8th largest source of attacks worldwide. To mitigate this problem both technical and regulatory controls should be considered. Network security is a related problem, where the relatively uncontrolled nature of the Internet has allowed malicious traffic to flourish. Metaphorically, our networks must evolve from the present situation of fortresses protected by walls, to civilised networks where the traffic between towns and cities is policed. For sensitive commercial, government or military applications, research into secure software development methodologies and security architectures for highly trusted systems is needed. Cryptography continues to be a research challenge, and there is a particular need for new lightweight cryptographic algorithms and protocols in order to provide adequate security with limited processing power for ubiquitous computing. It is well known that humans represent the weakest link in information security. Of particular concern are people who traditionally have difficulties in adopting and using IT. In the face of the European and Norwegian initiatives for e-inclusion, security usability for all users is an urgent security research priority. CIIP (Critical Information Infrastructure Protection) is a strategically important topic that requires investigation in information risk management to better understand the uncertainty around assessments of risk. Digital forensics is a key element for law enforcement against computer and cybercrime and also for supporting CIIP. Research challenges in forensics include the establishment of accepted standardized principles for representation, collection and preservation of forensic evidence, inclusion of tracing and non-repudiation techniques in network architectures, and the establishment of training programs in our educational institutions to produce graduates who can become skilled forensics professionals. Research in fundamental security should also focus on creating new types of privacy enhancing technologies for the Internet age and Web 2.0 where the practice of sharing and exposing personal information challenges traditional privacy principles. Biometric identification and authentication of persons can offer many advantages over traditional methods, but still suffers from having certain vulnerabilities and potential negative impacts on safety and privacy. The research challenges are to improve the reliability and find adequate mitigation strategies against privacy and safety threats.

In the area of application oriented information security, current identity management systems suffer from not being scalable for the users, e.g. by requiring separate identifiers and corresponding credentials for different service providers. This creates security vulnerabilities because users are unable to securely manage their many different identities and credentials. The concept of the semantic web assumes the existence of policies for confidentiality, integrity and availability where rights with respect to access to, and that the use of data are respected/enforced, and that no intentional or accidental semantic misrepresentation exists. These assumptions rest on partly non-existent security and trust technologies that are yet to be developed, and therefore pose a research challenge. The convergence of mobile and Internet environments poses challenges and also offers opportunities for security, i.e. to combine the flexibility of IP based networks with the relatively strong identity management of mobile networks. Trust and reputation systems have emerged as a key element for providing soft security, i.e. as collaborative method for moderating and civilising markets and communities on the Internet. The challenge is to take advantage of IT and the Internet to create efficient and reliable networks for collecting trust related information, for deriving measures of trust and reputation in order to support decision making, and last but not least to make trust and reputation systems robust against strategic and malicious manipulation and attacks. Mobile ad-hoc networks and sensor networks can be particularly useful in special situations such as emergency and military operations, but their dynamic and distributed nature pose particular security challenges. Well integrated eHealth solutions have the potential of radically improving efficiency and quality of health care. A crucial factor for the sustainable eHealth development is information security where the challenges are to define adequate policies for access management, privacy and consent, and to design security technology to enforce those policies. RFID (Radio Frequency Identification) is a rapidly growing technology used for tracking of goods and people. RFID security research challenges include access control to prevent unauthorised access, privacy protection policies and architectures, and the prevention of interference with other systems. SCADA networks (Supervisory Control And Data Acquisition) represent a crucial element in the national critical infrastructures and therefore constitute an unavoidable aspect in any critical infrastructure security consideration. Design of security mechanisms for SCADA networks is challenging because it must satisfy particular security requirements not found in general purpose computing. The long term preservation of information poses security challenges that so far have received little attention. This is an area where solutions must have a perspective of thousands of years. The success of e-Government programs will be judged on the public’s trust in the technology used. A large-scale security breach on an e-Government system would undermine the entire political process. The robustness of e-Government relies on traditional security elements such as platform, software, communication and web security, but also includes particular requirements for privacy protection and trust management. A relevant research challenge is to investigate whether e-voting systems can be made sufficiently reliable to be practical.

The NISNet study group recommends that funding be provided for research programs that express innovative research visions and that articulate sound approaches to investigating and developing new security solutions. This includes multidisciplinary research as well as the integration of multiple types of information security technology to solve relevant problems. While a single research project with a limited budget necessarily will have a limited scope, it should always be seen in the light of high level societal goals. Constant technology innovation and the changing threat environment make information security an ongoing process that always requires new solutions. For that reason, it should be noted that information security research topics other than those directly described in this document can also have merit and be fundable. Project proposals should always be assessed by impartial experts who through their continuous engagement in the information security community stay constantly updated and informed about the changing information security landscape.

Table of Contents

1 Introduction

Scientific and industrial research consumes considerable resources in the national economy. It is in the interest of all parties to focus this research on areas with the highest potential impact and outcome for the national and the global community.

This document summarizes current research challenges in the area of information security and indicates research priorities seen from a global perspective in general and from a national perspective in particular. Information security research should focus on global research challenges where significant contributions by Norwegian research institutions can be achieved, either alone or in collaboration with other national or international partners. Information research should also prioritize specific national challenges, e.g. in case specific security threats, vulnerabilities and risks cause more concern nationally than in other countries.

Given the diversity of expertise among national research groups in the area of information security, research efforts should be allowed and encouraged to focus on a wide spectre of topics. This diversity is also reflected by the many national and international collaborative industry and academic links that our national research groups maintain. To reflect this diversity while at the same time preserving coherence and structure, the research priorities have been grouped under the two main themes *fundamental information security* and *application oriented information security.* Fundamental information security, which consists of 11 specific topics, covers the design and engineering of fundamental security building blocks. Application oriented information security, which also consists of 11 specific topics, covers security in services and applications. From a global perspective, some of the described topics have been research priorities for 30 years or more, whereas others are more recent. Although many security problems have been successfully solved, it may seem as a paradox that the international research community and prominent global IT companies have not been able to effectively solve serious endemic security problems like e.g. virus infections and spam. While theoretic solutions to these problems exist, it is important to recognize that a security solution not only depends on the technical innovation itself, but also on user acceptance, on compatibility with legacy technology, on the existence of appropriate business models and on the right political environment for its implementation and introduction to be successful. Research in information security must therefore have a wide enough scope to cover issues such as policies, governance and economic models for security.

Constant technology innovation and the changing threat environment make information security an ongoing process that always requires new solutions. Research in information security must therefore be adapted to the current technology and threat environment, and the research priorities articulated here represent a selection of important and timely topics.

2 Recent Articulations of Security Research Priorities

International experts, the European Union and the Norwegian Government have published documents that articulate needs in terms of security and security research. These are briefly described below to provide a background and reference for the research priorities expressed by NISNet. Verbatim quotes are emphasized in *italics.*

2.1 Recent Expert Opinion Security Research Priorities

Sean W. Smith and Eugene Spafford, two internationally renowned security experts, published an article in IEEE Security and Privacy entitled *"Grand Challenges in Information Security: Process and Output"*, [Smith&Spafford 2004] wherein they define the four main research challenges below.

1. Epidemic-style attacks

We must stop epidemic-style attacks in 10 years. Computing is plagued by epidemic-style attacks. Spam makes it hard to read email; denial-of-service (DOS) attacks bring down critical sites at inopportune times; and viruses and worms continue to plague systems - and are starting to plague critical infrastructure (such as ATMs and emergency response systems) that previously had resisted them. Attacks are propagating increasingly faster, and humans (and automated systems) cannot respond. The problem is asymmetric - attackers can be local, and they require few resources and entry points, whereas defenders must be global and organized. This problem is "grand" because it's important. Such attacks are high cost and will grow as more critical infrastructure is affected. (IEEE Security & Privacy's own Bruce Schneier has recently speculated that, in part, a worm might have caused the 2003 blackout.) Solving this problem requires overcoming many technical and logistical challenges, but success can be easily and tangibly demonstrated: DOS attacks or worms, for example, simply would no longer halt the infrastructure on a regular basis.

2. Trustworthy large-scale systems

We must build trustworthy large-scale systems for important societal applications. We use computers for important tasks, such as voting, health records, and law enforcement. However, something about the way we build large, networked software systems leads to vulnerabilities - again, witness the state of the CERT curve, or the fact that computer scientists were reputed to have said the same thing at the 1968 NATO Conference on Software Engineering. As we move sensitive operations onto networked general-purpose machines, on what grounds can stakeholders trust that the networks can resist dedicated attackers? What's going to happen when remote code-injection vulnerability is shown to exist - and has been used - in the commodity OS supporting a presidential election? As before, this problem is grand because it's important, and because solving it will require solving software engineering, production, and composition problems whose solutions have eluded the field since its inception.

3. Quantitative information systems risk management

We must make quantitative information systems risk management as good as quantitative financial risk management. At first glance, the credit-card system baffles security students. The authentication is so weak, but somehow the credit-card industry remains afloat. Part of the answer here is the way this technology embeds in a larger financial system, where decisions about risks and defenses are supported by well-understood risk management techniques. In the financial realm, corporate officers can gauge what they are getting for their investment, and when they are spending too much or too little. However, in information security it's all black magic. Corporate chief information officers do not have well-founded techniques to evaluate whether they are spending too much or too little on security technology, or whether they are incurring more or less risk than they did a year earlier. To paraphrase Lord Kelvin, "we cannot manage what we cannot measure". We need a sound quantitative risk-management theory for information technology risk. Such a thing *would enable government, industry, and consumers to make rational decisions about security investment and provide a basis for both the free market and public policy to seek out a stable, trustworthy state.*

4. End users security and privacy

We must give end users security they can understand and privacy they can control. Two recent trends in computing seriously impact the human end user. First, technology is becoming complex to the point of incomprehensibility. Even an experienced user has trouble conceptualizing exactly what services his or her machine offers right now on the network and what pull-down menus and configuration files to change to steer those services into a more acceptable state. This situation will only get worse as we continue to extend the analysis to less savvy users or to designers and integrators - or to the complex, pervasive computing environments looming just around the corner. Second, you manage your privacy by making free choices about your actions. However, moving activity into a networked computing environment, with machines and software representing many stakeholders (potentially remote and invisible) makes it much harder to delineate exactly what's involved in these actions. Where is your private information going today? Did you know it was going there? Reconciling these trends is a grand challenge. Human users must make rational choices about their computing actions, but cannot make such choices if they cannot understand the systems. All stakeholders should have thorough discussions of the range of potential privacy policies for computing services - but they can't do that if the default policy offered by the default technology is accepted as the only solution technology can offer. Technology dictates social values, when it should be the other way around. At the end of the day, if our computing systems are not serving the needs of human users, then what's the point of building them?

2.2 Recent EU Security Research Priorities

ICT Challenge 1: "Pervasive and Trusted Network and Service Infrastructures" of EU's "ICT element of the Cooperation programme in the Seventh Framework Programme" describes relevant information security objectives [CORDIS 2007]. This document follows the rather typical style of EU research policies where the density of key words is so high that the text is almost is hard to read.

- Objective 1.4: Secure, dependable and trusted Infrastructures
  - o *Security and resilience in network infrastructures: building and preserving flexible, scalable and context-aware, secure and resilient architectures and technologies to enable dynamic management policies that ensure end-to-end secure transmission of data and services across heterogeneous infrastructures and networks, including dynamic networks of tiny insecure devices, and multiple provider, business and residential domains; real time detection and recovery capabilities against intrusions, malfunctions and failures;*
  - o *Security and trust in dynamic and reconfigurable service architectures supporting assured and scale-free composition of services and service coalitions with managed operation across several administrative or business domains, enabling flexible business models;*
  - o *Trusted computing infrastructures ensuring interoperability and end-to-end security of data and services; increased security and dependability in the engineering of software and service systems to ensure the design and development of trustworthy applications and services; Identity management and privacy enhancing tools with configurable, context dependent and user-controlled attributes in static and dynamically changing*

  - *environments; trust policies for managing and assessing the risks associated to identity and private data;*
  - *Longer term visions and research roadmaps ; metrics and benchmarks for comparative evaluation and open technology competitions, in support of certification and standardization; international cooperation and co-ordination with developed countries; coordination with related national or regional programmes or initiatives and; coordination of FP7 projects addressing security, dependability, privacy and related ethical issues across different challenges and objectives of this work programme.*

- Objective 1.6 : New Paradigms and Experimental Facilities
  - *Advanced networking approaches to architectures and protocols, designed to cope with increased scale, complexity, mobility and requirements for security, resilience and transparency of the Future Internet coupled with their validation in large scale testing environments based on a combination of physical and 'virtual' infrastructures.*
  - *Interconnected test beds addressing novel distributed and reconfigurable protocol architectures; novel distributed service architectures, infrastructures and software platforms; and advanced embedded or overlay security, trust and identity management architectures and technologies. Test beds for systems that provide trusted access to e-services with users requiring no administration and security skills.*

- Objective 1.7: Critical Infrastructure Protection
  - *The interoperability and interconnectivity of communication and supply networks and systems is one of the cornerstones of the functioning of our modern society. The vulnerabilities in the intercommunication of systems, equipment, services and processes and their resilience against malicious attacks of terrorism and (organized) crime are elementary to the security of the citizens. The objective of the joint call is to make key infrastructures of modern life, such as energy production sites and transmission systems, storage and distribution, information and communication networks, sensitive manufacturing plants, banking and finance, healthcare, or transportation systems more secure and dependable. The aim is to protect such critical infrastructures that can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, mismanagements, accidents, computer hacking, criminal activity and malicious behaviour and to safeguard them against incidents, malfunctions and failures.*

2.3 Recent National Security Research Priorities

2.3.1 BAS5 (Protection of Society)

In the final report of the BAS5 project (Beskyttelse av Samfunnet) (Protection of Society), the following list is presented as "future work"
(page 40-41) of [FFI 2007]:

- Prioritering og identifisering av ulike forhold
  - *Metodikken for identifisering og prioritering av samfunnskritisk IKT inneholder foreløpig ikke prosesser eller teknikker som er spesielt rettet mot oppdagelse av hittil*

ukjent risiko, for eksempel scenarioteknikker, foresight-teknikker eller horizon scanning-teknikker. Hvordan slike best kan inngå i prosessen er en viktig avklaring. I parallell med dette bør et foreslått hierarki over ulike scenarier som kan inngå i prioriteringsarbeidet utvikles videre og underkastes nærmere analyse, med hensyn på å identifisere de viktigste scenariene og sile fra scenarier som er mindre plausible.

  - *Det er også behov for en nærmere kritisk gjennomgang av på hvilke områder en prioritering faktisk gir mening. En spesiell problemstilling er hvorvidt på forhånd fastsatte prioriteringer faktisk vil avhjelpe en krisesituasjon, eller om det kan være til hinder for krisehåndteringen der og da.*
  - *I tillegg kan prioritering overfor en spesifikk situasjon sies å være relativt enkelt. Men hvordan kan man best prioritere hensyn på tvers av et bredt spekter av scenarier?*

- Risikoanalyser
  - *Hvordan kan tilsiktede hendelser best inkluderes i risikoanalyser? En spesiell utfordring er hvordan sannsynlighets- og usikkerhetsvurderinger av slike hendelser bør behandles metodisk.*
  - *Hvordan kan strategiske sikkerhetsinitiativer og lokale ROS-analyser best kobles? Resultatene fra BAS5-prosjektets delmål 1 og 2 bør derfor viderebehandles og integreres i større grad enn nå.*
  - *Hvordan kan andre sikkerhetsteknikker inngå i og understøtte en risikoanalyse av samfunnskritisk IKT? Eksempler på slike teknikker er bruk av sjekklister, penetrasjonstester, tradisjonelle sårbarhetsanalyser av IKT-systemer osv.*
  - *Hvordan kan følgekonsekvenser utenfor IKT-systemet best behandles i en risikoanalyse? Spesielt problematisk er konsekvensene for storsamfunnet som er avhengige av tjenester understøttet av IKT-systemet. Den enkelte virksomhet vil sjelden ha tilstrekkelig kompetanse om slike forhold eller ressurser til å gjennomføre en detaljert analyse.*

- Arbeid med nasjonal IKT-sikkerhet
  - *Rapportens forslag til tiltak og prosess for det nasjonale IKT-sikkerhetsarbeidet er basert på erfaringer fra FFIs arbeid med IKT-sikkerhet i flere år, og presenteres som et innspill til debatt. Denne debatten er svært viktig for å bringe arbeidet med IKT-sikkerhet i Norge et nødvendig steg videre. I forlengelsen av dette kan det imidlertid være behov for ytterligere utredninger, for eksempel knyttet til hvilket trusselbilde man skal planlegge IKT-sikkerhetsarbeidet mot, hvilke roller og oppgaver ulike aktører bør ha og hvilke tiltak og virkemidler som er best egnet for det nasjonale sikkerhetsarbeidet i tiden fremover.*

2.3.2 National Guidelines for Strengthening of Information Security

The Norwegian Government published "Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010" in December 2007 (National Guidelines for Strengthening of Information Security) [N.Gov. 2007] which states the following on page 6:

- *Etter lanseringen av Nasjonal strategi for informasjonssikkerhet i 2003, er det først og fremst fire teknologiske og bruksmessige utviklingstrekk som er blitt mer fremtredende:*
    - *Samfunnets avhengighet av IKT og Internett har økt. Samfunnet som helhet er blitt mer sårbart for selv kortere driftsavbrudd i systemer og nett.Den økte sårbarheten skyldes blant annet økt kompleksitet i systemer og nett.*
    - *Det er en økt tendens til målrettede, skreddersydde, og profesjonelle angrep.*
    - *Finansiell vinning fortsetter å være den viktigste motivasjonsfaktoren for angriperne, som i økende omfang arbeider i det skjulte og stjeler konfidensielle data. Det er klare tegn på profesjonalisering av den kriminelle virksomheten. Det eksisterer i dag et illegalt marked for omsetning av verktøy for å begå sikkerhetsbrudd.*
    - *Den store økningen i antall brukere av PC og Internett, med varierende kompetanse, har medført et økende behov for bevisstgjøring, informasjonsdeling og opplæring. Det er nødvendig at alle brukere får en bedre forståelse av sitt ansvar overfor andre brukere av nettet, og kunnskap til å ivareta dette ansvaret på en god måte.*

2.3.3 SAMRISK (Samfunnnssikkerhet og Risikoforskning)

The SAMRISK Committee (Utredningsgruppe for Samfunssikkerhet og Risikoforskning) published a report [SAMRISK 2005] to the Norwegian Research Council recommending the establishment of a research program in the area of Community Security and Risk Governance.

SAMRISK recommended undertaking research on a relatively high level, articulated in terms of the themes in the table below and the explanation underneath.

<table>
<tr><th colspan="2">Eksempler på forskningsoppgaver for SAMRISK. Hovedgrupper:</th></tr>
<tr><td><i>Generiske problemstillinger</i>
• Risikobildet, sårbarhet og samfunnets risikotoleranse
• Politikk, styring og reguleringer
• Kompleksitet og endring
• Teknologier i samspill med samfunn, organisasjon og mennesket
• Krisehåndtering og risikokommunikasjon
• Spesielle dilemmaer og verdikonflikter</td><td rowspan="2"><i>Eksempler på spesielle studieområder</i>
• Sårbarheten i kritisk infrastruktur
• Komplekse kriser og internasjonal koordinering
• Terrorisme
• Samfunnssikkerhet og svikt i sosiale sikkerhetsnett
• Organisert kriminalitet
• Naturkatastrofer og klimaendringer
• Menneskeskapte ulykker
• Internasjonale trusler mot folkehelsen</td></tr>
<tr><td><i>Metoder og modeller</i>
• Risiko- og sårbarhetsanalyser
• Trusselvurderinger
• Scenarioanalyser og simulering</td></tr>
</table>

Den grunnleggende kunnskap innen disiplinorienterte studier i matematikk, realfag, samfunnsfag og humaniora som sikkerhetsforskningen må bygge på, forventes ivaretatt utenfor dette programmet. Det samme gjelder for helt sektorspesifikke problemstillinger. Heller ikke *grunnleggende teknologiutvikling, medisinsk eller miljøforskning hører hjemme i programmet. Den mer generiske kunnskap som produseres i SAMRISK vil imidlertid kunne representere interessante koblinger for slike spesialiserte prosjekter. SAMRISK vil ikke gjøre spesialisert, anvendt sikkerhetsforskning innen transport, oljevirksomhet, IKT m.m. overflødig.*

2.3.4 The NFR VERDIKT Program

The VERDIKT program [NFR 2005] (Kjernekompetanse og Verdiskapning i IKT) (KnowHow and Value Creation in ICT) of the Norwegian Research Council (NFR) offers research funding on a competitive basis for ICT related projects in the period 2005-2014. VERDIKT articulates the following three specific themes related to information security: *Security*, *Privacy* and *Vulnerability* (Sikkerhet, Personvern og Sårbarhet). The general and high level formulation of security themes in VERDIKT gives NFR the freedom to define a wide range of specific calls related to information security under the program.

3 Proposed Information Security Research Priorities

Information security technologies and solutions are diverse and can be difficult to categorize in a concise way. For the purpose of this report, the research priorities have been grouped according to whether they relate to *fundamental information security* or *application oriented information security*. Fundamental information security, which consists of 11 specific topics, covers the design, and engineering of fundamental security building blocks. Application oriented information security, which also consists of 11 specific topics, covers security in services and applications. From a global perspective, some of the described topics have been research priorities for 30 years or more, whereas others are more recent. Information security is an ever changing landscape, and the research priorities articulated here represent a selection of important and timely topics.

The purpose of IT and information security solutions must be seen in the light of the societal goals they support. While the research challenges described below are described from the point of views of information security community, it should be noted that relevant security solutions must be integrated with other technologies and disciplines in order to be beneficial for society.

3.1 Research Priorities for Fundamental Information Security

Design and Engineering of Fundamental Security Building Blocks

Fundamental information security denotes security technology and mechanisms in the computing and communication platforms that support applications and services.

3.1.1 Baseline Security in Commodity Platforms

In the April 2008 issue of the Internet Security Threat Report [Symantec 2008], the Norwegian segment of the Internet was identified as the source of most attacks targeting computers and networks in Europe, and is ranked the 8th largest source of attacks worldwide. An explanation, which could be used as excuse for this sad situation, is the high penetration of broadband connections in Norway combined with the fact that attackers prefer using computers in high bandwidth networks to host their attacks. The real explanation is that the baseline security of commodity platforms is inadequate. It is simply unacceptable that malware and attackers routinely take over the control of computers and networks. The reasons for the low level of baseline security can be economical or political rather than technical, but it is still unacceptable. There is also the danger that commodity mobile platforms will become equally vulnerable to malware and attackers as commodity desktop computers, and it could be called a technological tragedy if that should happen.

The research challenge is to define the necessary technical, economical and political controls to improve the baseline security of commodity platforms to resist malware and sophisticated attackers. The challenge is to develop resistant hardware and software architectures that retain sufficient functionality to support legacy business models. In addition, regulation of mandatory security controls could be considered. To use an analogy, it was only through regulation that car manufacturers began equipping cars with safety belts for all seats. Finding adequate technical controls for computer security is one thing, and getting them universally installed and used is another.

3.1.2 Network Security

Network security can mean a variety of things. It is often used in the sense of communication security based on cryptography and security protocols. It can also denote network perimeter defense technologies such as Firewalls and IDS (Intrusion Detection Systems). Network security can also be used in the sense of securing the fundamental building blocks of large communication networks such as the DNS (Domain Name System) and routing mechanisms of the Internet, and the Signaling Systems of the PSTN (Public Switched Telephone Network).

Research Challenges include making Firewall and IDS technologies more intelligent and more efficient to be able to filter out subtle and stealth attacks and other malicious traffic in high bandwidth channels. The configuration of Firewalls is a major challenge, especially for normal users, but also for security exerts. Research must focus on making such technology more user friendly.

During the 1980s, ITU (International Telecommunications Union) developed an alternative Internet called OSI (Open Systems Interconnection) which never became widespread because of its relative complexity and the competition from the much simpler TCP/IP technology of the current Internet. A fundamental problem with the current Internet is that it ultimately is controlled by the US Department of Commerce. Proposals to let the ITU and the UN to take over the control of the Internet have been rejected by US Authorities. A compromise led to the establishment of the Internet Governance Forum (IGF) that meets once per year to debate fundamental issues such as global policing of the Internet to stop the increasing volume of malicious traffic, but so far no effective measures have been designed. Research is needed to evaluate the fundamental principles of the Internet. It is worth considering an alternative Internet under a different root governed by ITU and the UN with strict policing. Instead of relying on Firewalls to keep malicious traffic out, the network itself could be civilized so that it no longer carries large amounts of malicious traffic. An analogy would be the evolution from the Middle Ages where roads were unsafe and towns had to be protected by walls to the modern civilized societies where cities no longer need walls because the whole society is policed.

3.1.3 Trusted Systems

Security can in principle never be stronger than the weakest link. Operating high security application will therefore require trusted platforms. This means that each component of the system must have sufficiently strong security, thereby creating a chain of trust. The concept of trusted systems means a computing platform with applications that can support an uninterrupted chain of trust, thereby enabling high security applications.

Trusted systems must necessarily be rooted in trusted hardware integrated with software. The ability to have strictly controlled separation of processes is a fundamental requirement for trusted platforms. For practical reasons and to support certain business models it can be a requirement that applications with different levels of security execute on the same platform. The research challenge is to design formally verified security architectures that make this possible and practical, and to implement these architectures securely in hardware and software.

3.1.4 Secure Software Development Methodologies

Security must be an inherent property in both software and other technical systems. The greatest challenge is to weave in security throughout the complete software development lifecycle, from planning, requirements, design, implementation, testing, deployment, maintenance, and further development.

There are already several frameworks and methodologies available that intend to facilitate the creation of secure software, but the problem is that these are often cumbersome to use, and are thus only used by projects where security is an explicit requirement. Recent surveys have shown, however, that security errors in *ordinary* software (i.e. software that has not been considered particularly security sensitive, or does not contain security mechanisms) cause a large proportion of reported security incidents. It is therefore necessary to create lightweight methods that are suitable for use in *all* development projects.

To bridge the gap between software deployment and error patching, methods and tools for provisioning of security assurance in software are missing. Developing and using such tools would give many advantages:

- Software and protocols can be tested before their possible failures affect customers or society
- Verification tools reduce cost and turnaround time for assurance evaluation, e.g. according to the Common Criteria (ISO 15408) and related methods
- A formal analysis reveals documentation errors and security gaps in the security software implementation

Our national industry will have difficulty competing with countries like India or China in producing the *cheapest* software, but we could excel at producing the overall *most secure* software and thereby gain a competitive advantage.

3.1.5 Cryptography

Cryptography will always represent a fundamental security building block, and therefore deserves constant attention in the research community. This area covers standalone algorithms such as block and stream ciphers, hash functions and digital signature algorithms, as well as security protocols for authentication and other purposes. The suitability of cryptographic algorithms depends on the balance of performance and strength. The advances in processing power and analytical capabilities make it necessary to constantly evaluate the strength of these mechanisms and to develop new designs that maintain an adequate performance-strength balance.

A particular challenge is to combine cryptography with the concept of pervasive computing based on lightweight processing devices, e.g. powered by small batteries or by proximity radiation and magnetic induction. This will severely limit the available processing power, and thereby the ability to execute the processes required by current conventional cryptographic mechanisms. *Lightweight cryptography* refers to cryptographic algorithms and protocols designed to execute sufficiently fast with low processing power. Such mechanisms are essential for secure deployment of many emerging technologies, including RFID, sensor networks, and ad hoc mobile networks.

The research challenge in the area of lightweight crypto is to develop cryptographic mechanisms that can provide *sufficiently* strong security with *limited* processing power. It is likely that many different cryptographic techniques are needed to satisfy applications that may differ significantly in terms of available processing power and security requirements.

3.1.6 Security Usability

Humans represent the weakest link in the security chain of many prominent applications. Security systems must be viewed as socio-technical systems that depend on the human and social context in which they are embedded to function correctly. Security systems will only be able to provide the intended protection when people actually understand and are able to use them correctly. There is a very real difference between the degree by which systems can be considered theoretically secure (assuming they are correctly operated) and actually secure (acknowledging that often they will be operated incorrectly). In many cases, there is a trade-off between usability and theoretical security. It can be meaningful to reduce the level of theoretical security to improve the overall level of actual security. When implementing new security solutions or improving the usability of existing security applications, it is necessary to examine the underlying security technologies, and consider whether increased overall security can be achieved by replacing them by totally new security technologies that provide a better basis for good usability.

With the recognition that the human factor represents the weakest security link, research in security usability is growing in importance worldwide. In general, a security architecture that does not include the human factor must be considered incomplete. The challenge is to better understand the complex interplay between human cognitive capabilities and security mechanisms and procedures, and to define clear security usability principles that allow security architects to include the human factor in a consistent and systematic way. The goal must be to make it standard procedure to include the human factor as part of the vulnerability, threat and risk analysis as well as the security design itself. Of particular concern are people who traditionally have difficulties in adopting and using IT. These people will have even greater difficulty in understanding secure practice and will therefore be particularly vulnerable to attacks. In the face of the European and Norwegian initiatives for e-inclusion, security usability for all users is a urgent security research priority.

3.1.7 Information Risk Management

Security and risk need to be well understood to be well managed. It is therefore worrisome to recognize that it is difficult to assess security and risk in a consistent and reliable way. Input parameters to risk analysis are often characterized by considerable degrees of uncertainty. In such situations the outputs of a risk analysis will be equally subject to uncertainty. The degree of uncertainty is not traditionally included in risk analysis, and becomes even more abstract because potential risks usually do not materialize and therefore provide a weak basis for statistical analysis. In particular, the risk posed by privacy breaches - the loss of personal information - is not well understood in the medium- and long-term perspective.

This research challenge is to investigate role uncertainty plays in risk analysis and to extend existing risk analysis methodologies to allow explicit representation of uncertainty. A possible approach can be to assess the degree of uncertainty in the input parameters, and to determine how this uncertainty propagates through the analysis to the output conclusion. Being able to assess the uncertainty of estimated risks can be valuable for determining investment in risk mitigation, or for identifying areas where additional assessments are required. The collection of empiric evidence for evaluation of security and privacy risks, and the development of tools for risk modelling and risk analysis should be a research priority.

3.1.8 Digital Forensics

Digital forensics can be defined as the art of discovering, retrieval, preservation and presentation of information about computer crimes in such a way to make it admissible to the court. This seemingly simple definition stands in sharp contrast to the enormous difficulty security professionals and law enforcement agencies have in investigating the fast growing number of computer crimes and sabotage. Digital forensics is important for protecting against corporate espionage, white collar crime, child pornography, privacy violations and crimes in general, and is in fact a crucial factor for critical information infrastructure protection. Challenges for digital forensics include e.g. the large diversity of devices and systems, management of large volumes of evidence, the distributed nature of evidence, establishment of trust in audit trails, testing and validation of evidence, the use of anti-forensics practices by criminals and the lack of trained forensics professionals.

Digital forensics is still a relatively young discipline that has not received sufficient attention in academic and research communities. Research challenges include the establishment of accepted standardized principles for representation, collection and preservation of forensic evidence, inclusion of tracing and non-repudiation techniques in network architectures, and the establishment of training programs in our educational institutions to produce graduates who can become skilled forensics professionals.

3.1.9 CIIP: Critical Information Infrastructure Protection

Critical information infrastructure is the information infrastructure on which important functions of the government, the economy and society as a whole are dependent, and without which critical services would be disrupted or seriously affected. CIIP (Critical Information Infrastructure Protection) is the protection of this infrastructure. Telephone communication networks for example represents CII. While the traditional PSTN is relatively isolated and independent from other networks and even works in case of power failure, VoIP is totally integrated with the Internet and will suffer from the same vulnerabilities as other Internet applications.

The research challenge will be to identify the elements of the total information infrastructure which constitutes the critical parts, to assess their vulnerabilities, identify threats, conduct attack scenario analyses, assess relative risks and investigate potential security controls. For example, the reliability and Quality of Service (QoS) in VoIP, taking into account possible attacks, identity management, phone spamming, Denial of Service (DoS) attacks and emergency call management must be studied.

3.1.10 Privacy Enhancing Technologies in the Internet Age

The quote:*"You have zero privacy, get over it"* (Scott McNealy, CEO Sun Microsystems, 1999) reflects the failure of the IT industry and regulators to implement and enforce adequate privacy protection in the Internet age. During the period of enacting the first privacy legislations as e.g. articulated by the European Union's Directive of Data Protection (Directive 95/94/EC), the optimistic view was that it would be possible to enforce privacy protection through legislation and policing. Unfortunately, this legislation was based on the assumption that personal data would be stored in servers with relatively limited, and thereby controllable, exchange of data. On the Internet today, personal data is collected everywhere in the network, and enforcement of state privacy legislation has become almost impossible.

Ubiquitous computing, eHealth and "Web 2.0" are buzzwords which imply collection and transfer of enormous amounts of personal data over publicly accessible networks, such as the Internet and mobile data networks. It is of utmost importance that privacy aspects are considered in such environments.

The research challenge is to improve existing and develop totally new approaches to privacy protection that take into account the way people use the Internet. In the age of social communities, Web 2.0, and permanent mobile on-line connectivity, any aspects of people's life are shared on-line for an indefinite amount of time. Web services, service-oriented architectures and users that willingly provide their private life on-line call for new concepts in identity management, privacy management and policy enforcement.

Norway together with other European countries has been a pioneer in the development of privacy principles and legislation. To continue this tradition, research in new and innovative privacy enhancing technologies, their usage, and deployment policies should be seen as priority.

3.1.11 Biometric User Identification and Authentication

Biometric identification and authentication of persons can offer several advantages in terms of security strength and usability. In theory with such systems there is no need to remember passwords or carry security tokens, and it can even make the typing of logon Ids superfluous. However, it must be clear that biometric technology still is relatively immature and must be deployed with care. Depending on the technology used, biometric systems can produce false positives and negatives either as a result of malicious intent or by accident. Biometric systems can also cause safety and privacy risks when inappropriately implemented.

The research challenges are to improve the resistance of biometric capture devices with regard to faked biometric characteristics (gummy finger etc.), to improve the protection of stored biometric references both in terms of non-invertability to the original biometric sample and to allow diversification of biometric references stemming from one and the same source. The latter is essential to prevent linkability of biometric databases and to avoid profiling of data subjects. The third essential challenge is to improve the biometric performance and to minimize intrinsic errors of the biometric systems (false-positives and false-negatives) by means of continuous research on effective feature extraction and analysis of fused multibiometric information channels (multimodal and multisensorial).

3.2 Research Priorities for Application Oriented Information Security

Security in Services and Applications

Application oriented information security denotes security on service, application and semantic levels where underlying fundamental information security technologies and mechanisms are used as building blocks.

3.2.1 Identity Management

When making services and resources available through computer networks, there is often a need to know who the users are and to control what services they are entitled to use. In this context, identity management has two main parts, where the first consists of issuing users with credentials and unique identifiers during the initial registration phase, and the second consists of authenticating users and controlling their access to services and resources based on their identifiers and credentials during the service operation phase. A problem with many identity management systems is that they are designed to be cost effective from the perspective of the service providers (SP), which sometimes creates inconvenience and poor usability from the users' perspective. The traditional silo model consists of having a separate identity and corresponding credential for every service provider. This creates security vulnerabilities because users are unable to securely manage their many different identities and credentials. In addition to being SP centric, traditional identity management systems have largely ignored that it is often equally important for users to be able to identify service providers, as it is for service providers to authenticate users.

The Internet and mobile networks have developed relatively independently, with different technologies and different business models. For example, identity is weak on the Internet and relatively strong in mobile networks. This and many other differences are mainly due to the lack of billing and subscriber relationships on the Internet and the presence thereof in mobile networks. With the convergence between the two networks there is a potential for leveraging the relatively strong identity and security functionality to strengthen identity and security in Internet-based applications.

The research challenge is to develop architectures that preserve strong security and privacy while at the same time allowing scalability from the user perspective. Users must be able to manage all their identities and credentials efficiently and securely. This represents a global security challenge where Norwegian researcher organizations are well placed to make an impact.

3.2.2 Security of the Semantic Web

The Semantic Web means that Web content is described with metadata to allow efficient automated search, mapping and combination. Several industry initiatives are currently under way in the area of “Integrated Operations”, e.g. in the oil and gas industry, to deploy semantic web technologies on a large scale. Unfortunately, the state of the art in semantic web technology is plagued with unsolved security problems. The semantic web assumes that:

- Data/documents are electronically available and searchable
- Relations between data are described
- An information security regime that ensures confidentiality, integrity and availability of information exists

- Rights with respect to access to, and use of, data are respected/enforced
- The security level of combinations of documents/data is maintained, including internal and external relations
- No intentional or accidental semantic misrepresentation exists

Although there are many tools available for the various standards that relate to the semantic web, they are totally inadequate as a basis for making these assumptions with any degree of confidence. A significant body of knowledge (standards, manuals, process descriptions, etc.) must be indexed, tagged, and transferred to the semantic web. This will need to be done in each organisation, but also between organisations, and eventually interface with a global semantic web comparable with the WWW of today. The research challenge is to provide a security framework that makes this process robust and reliable.

3.2.3 Security in Convergent Mobile-Internet Environments

The Internet and mobile networks have developed relatively independently, with different technologies and different business models. For example, identity is relatively weak on the Internet and strong in mobile networks. This and many other differences are mainly due to the lack of billing and subscriber relationships on the Internet and the presence thereof in mobile networks. The vision of future mobile network technologies as discussed in “Beyond 3G” (B3G) architectures is based on heterogeneous networks and all-IP core. For the integration of heterogeneous networks it is essential to create an open environment where various network operators and service providers share the core infrastructure via open interfaces, and where end-user devices use open H/W and S/W platforms. The openness of B3G- systems poses greater security challenges than traditional closed environments (e.g. GSM) that have an inherent advantage of protection against security threats.

The research challenge for convergent mobile-Internet infrastructures is to design security architectures that can combine the best of the two worlds, and to prevent the spreading of malicious software and spam to the mobile world. This must include an overlay security architecture that seamlessly integrates the security of the various underlying networks. Such overlay security (and privacy enhancing) architectures should also take into consideration the connection of mobile phones to wireless sensor networks.

The security of the mobile devices itself represents an additional security challenge. Devices will have extended service capabilities and multiple-radio, which make them more vulnerable to malware. Over-the-air software installation, mobility and ever-changing environments could potentially make it harder to control the mobile phone as compared to commodity desktop computers.

3.2.4 Trust and Reputation Management

It is challenging to reliably assess the quality of resources or the reliability of entities in the online environment. This makes it difficult to make decisions about which resources can be relied upon and which entities it is safe to interact with. Trust and reputation systems are aimed at solving this problem, and have emerged as a key element for providing soft security, i.e. as collaborative method for moderating and civilising markets and communities on the Internet. In the case of reputation systems, the basic idea is to let parties rate each other, for example after the completion of a transaction, and use the aggregated ratings about a given party to derive its reputation score. In the case of trust systems, the basic idea is to analyze and combine paths and networks of trust relationships in order to derive measures of trustworthiness of specific nodes. Reputation scores and trust measures can assist other parties in deciding whether or not to transact with a given party in the future, and whether it is safe to depend on a given resource or entity. This represents an incentive for good behaviour and for offering reliable resources, which thereby tends to have a positive effect on the quality of online markets and communities.

The research challenges are:

- To find adequate online substitutes for the traditional cues to trust and reputation that we are used to in the physical world, and identify new information elements (specific to a particular online application) which are suitable for deriving measures of trust and reputation.
- To take advantage of IT and the Internet to create efficient and reliable systems for collecting that information, and for deriving measures of trust and reputation, in order to support decision making and to improve the quality of online markets.
- To make trust and reputation systems robust against strategic and malicious manipulation and attacks.

3.2.5 Digital Information Access Management

Access to information stored on a physical medium is naturally restricted by the ability to access the physical medium itself. This restriction is removed when the information is represented in digital form because the information can be cheaply and rapidly copied to a multitude of different physical media and transferred through any digital communication channel. The consequences are both promising and threatening.

On the one hand it can provide knowledge and information to billions of people who otherwise have limited access to information. One the other hand it threatens the traditional right to commercially exploit intellectual property because the traditional method of controlling the distribution of physical media becomes irrelevant. The industry’s reaction to this development in turn becomes a threat to the traditional fair use of intellectual property because it tends clamps down on the users’ ability to copy and playback legally purchased intellectual property such and music and film on different media. Another threatening consequence of efficient distribution and universal access to digital content is the difficulty of preventing the distribution of illegal information such as racist propaganda and child pornography.

Digital information can represent many different things, such as music, film, pictures, text and software. There are conflicting views on how distribution of and access to the various types of digital information should be managed. Research challenges are for example to find a combination of security mechanisms, practical policies, international regulations and innovative business models that can constitute an acceptable compromise and adequately satisfy stakeholders. Solutions must be adapted to relevant platforms and environments such as satellite TV, workstations connected to the Internet, mobile terminals connected to mobile networks and wireless Internet, or any combination of the above.

3.2.6 Security in MANETs and Sensor Networks

A MANET (Mobile Ad-hoc NETwork) is a collection of wireless mobile nodes dynamically forming a temporary network. A sensor network is an interconnected set of sensor nodes that can monitor and report various conditions at different locations. Combined, these two network concepts form a powerful paradigm with a multitude of applications in military and civilian contexts.

Security will be required whenever such networks carry sensitive information and where there are perceived threats.

MANETs can potentially play an important role in future military as well as in civil rescue operations. It is to be expected that ad hoc networks will carry sensitive traffic and that they can be subject to attacks, making it necessary to develop appropriate security solutions.

Nodes in MANETs and sensor networks are typically characterised by having limited processing and transmission capacity as well as limited power supply. These constraints together with the dynamic and ad-hoc nature of such networks require specially designed security solutions not normally used in traditional computer networks.

Security research challenges for MANETs and sensor networks include light-weight security mechanisms, distributed and dynamic authorization, authentication and access management, routing protocols based on collaborative trust and reputation management, and autonomous decision making based on authority and trust structures.

3.2.7 RFID Security

RFID (Radio-Frequency Identification) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader. Current RFID technology suffers from serious vulnerabilities, and can be attacked relatively easily in the presence of attacks. Security research challenges include:

- Protection controls to prevent direct attacks on sensor or RFID system components which potentially could undermine the business processes the sensor/RFID system was designed to enable.
- Access control mechanisms to prevent an adversary or competitor from gaining unauthorized access to sensor/RFID-generated information and use it to harm the interests of the organization implementing the sensor/RFID system.
- Policies and security controls for protecting privacy rights that may be compromised if a sensor/RFID system can be related to personally identifiable information. RFID tags represent a privacy risk because they enable tracking of those holding tagged items.
- Shielding controls to protect surrounding networks, systems, assets and people from RFID technology, and for protecting different RFID systems from each other.

3.2.8 Security of SCADA Networks

Modern economies and developed countries rely heavily on the correct functioning of their critical infrastructures. Energy, water, transports, telecommunications and public service infrastructures are absolutely essential to provide the grounds for thriving economic activities as well as to ensure a minimum degree of public well-being. Significant disruption of these functions can disable good governance, increase divisiveness and undermine the confidence of citizens in their government. Occasional events in the area of public transport and with energy production and distribution infrastructures have led to concerns about the security of these functions.

The increasing interdependency between critical infrastructures, their complexity and dimensions, and their distributed character all contribute to a significant security challenge. Historically, the complexity of the processes involved in critical infrastructures and industry have been tackled by SCADA[1] systems (Supervisory Control And Data Acquisition). These have become practically indivisible from the critical infrastructures and therefore constitute an unavoidable aspect in any critical infrastructure security consideration.

SCADA networks have traditionally had strong mechanisms to prevent/detect safety incidents, but insufficient mechanisms against network-based intrusions. The current interconnection of SCADA networks with other networks (including the open Internet) is making this an unacceptable risk.

Design of security mechanisms for SCADA networks requires careful consideration of requirements not found in general purpose computing. These are related to:

- The need to maintain availability as a first priority;
- The need to ensure robustness along with controlled and predictable service degradation and safety; and
- The need to honour real-time constraints.

3.2.9 eHealth Security

Well integrated eHealth solutions have the potential of radically improving efficiency and quality of health care. Health informatics is characterised by numerous security requirements that often have strongly contradictory goals. For example, patient privacy requirements put constraints on health care providers' access to patient data, whereas the concern for patients' health should give health care providers open and easy access to patient data.

On a high level, the research challenge for eHealth security is to define adequate and practical security policies for management of patient data and other eHealth related data, and then to develop adequate architectures for implementing and enforcing these policies.

3.2.10 Long-Term Preservation of Information

IT changes our notion of preservation of information. Traditional media allow the physical representation of information be touched and sensed directly, whereas digital information is immaterial and requires the help of a machine. This poses totally new challenges for the preservation of information in the digital age. Preservation of digital information is not so much about preservation of physical media, but more about specifying formats and establishing procedures for migrating information to new digital media in pace with the ageing of digital media and the technological development. This requires deep and continuous commitment with a perspective of thousands of years.

Research challenges for preservation of information include the investigation of formats, media and methods for storage and migration, the definition of criteria for selecting information, the determination of appropriate quality (e.g. resolution of images), the design of adequate methods for error correction, preservation of confidentiality and integrity through e.g. encryption and digital signatures, and the definition of access policies that span generations of users.

[1] Also known as ”Distributed Control Systems” – DCS

3.2.11 Security of e-Government

The concept of e-Government denotes the application of ICT in legislature, judiciary, or government administration, in order to improve internal efficiency, the delivery of public services, or processes of democratic governance. It is also aimed at enhancing social inclusion through online communication, online consultation between government representatives and their constituents, online political activity and discussions groups, and e-voting.

The success of e-Government programs will be judged on the public's trust in the technology used. A large-scale security breach on an e-Government system would undermine the citizens' trust and could undermine the political process. The robustness of e-Government relies on traditional security elements such as platform, software, communication and web security, but also includes privacy protection and trust management. A particular research challenge is to investigate whether e-voting systems can be made sufficiently reliable to be practical. There is a significant difference between e-voting at the polling booth and online e-voting, where only the former can be made relatively secure with current technology. There is a concern that internet elections could be the target of foreign governments or terrorist organizations attempting to disrupt elections. Another challenge with online e-voting is ensuring the person logging onto the web site is the person actually voting. Coupled with the need to identify the voter, the technology would also need to remove any authenticating details from the vote in order to keep the ballot secret. No security solutions currently exists that can reliably satisfy these strict requirements.

4 Outline of an Information Security Research Program

4.1 List of Information Security Research Challenges

Table 1 below lists the research challenges described in the previous sections. The list separates between fundamental and application oriented research challenges.

Fundamental Security Research challenges		**Application oriented research challenges**	
F1	Baseline Security in Commodity Platforms	A1	Identity Management
F2	Network Security	A2	Security of the Semantic Web
F3	Trusted Systems	A3	Security in Convergent Mobile-Internet Environments
F4	Secure Software Development Methodologies	A4	Trust and Reputation Management
F5	Cryptography	A5	Digital Information Access Management
F6	Security Usability	A6	Security in MANETs and Sensor Networks
F7	Information Risk Management	A7	RFID Security
F8	Digital Forensics	A8	Security of SCADA Networks
F9	CIIP: Critical Information Infrastructure Protection	A9	eHealth Security
F10	Privacy Enhancing Technologies in the Internet Age	A10	Long-Term Preservation of Information
F11	Biometric User Identification and Authentication	A11	Security of e-Government

Table 1. Research challenges in information security

Constant technology innovation and the changing threat environment make information security an ongoing process that always must address new challenges. The list must therefore be seen as representing as a snapshot of current challenges that NISNet members consider important and that therefore merit investment in research.

4.2 Multidisciplinary Research for High Level Societal Goals

IT security must be integrated with other disciplines in order to support high level societal goals. The integration can take place using security solutions as building blocks together with the necessary complementary elements from other disciplines such as law, business, sociology and politics. It is often advantageous to consider the integration at an early stage, i.e. already during the research phase, in order to achieve the best possible outcome with the largest possible impact.

We will consider a set of high level societal goals as an example where a multidisciplinary approach to information security research will be beneficial. The high level goals to be used as examples are: 1) *Quality Markets and Communities*, 2) *Safety for the Citizens,* and 3) *Inclusive Democracies*. These goals are briefly described below.

1. **Quality Markets and Communities**

   Markets and communities represent the life blood of human societies. Supporting the creation and continuity of high quality markets and communities contributes to welfare and stability in the society. e-Commerce marks a fundamental transformation of commerce through a spectacular increase in efficiency. It allows efficient provision of online services and it supports intelligent logistics for people, goods and utilities. People can for example work more efficiently wherever they are, at their workplace, at home or while travelling, thereby reducing the load on transport infrastructures which in turn reduces cost and improves living conditions. The internet also allows very efficient creation and organization of communities both locally and globally. In order to ensure a positive and sound evolution of e-markets and communities, IT and security must be integrated with disciplines such as business, law, sociology, regulation and politics.

2. **Safety for the Citizens**

   Safety for citizens means that citizens must be protected from threats such as acts of terrorism and (organized) crime, natural disasters and industrial accidents while respecting fundamental human rights including privacy. Information technology can both play an important role for ensuring safety e.g. by providing efficient means of prevention and intervention, but it also can represent a threat in the sense that the failure of IT systems can but citizens at risk either as a result of natural events of malicious intent. In order to ensure the safety of citizens, IT security must be combined with disciplines such as law, intelligence analysis, transport, engineering and natural resources management.

3. **Inclusive Democracies**

   Democracy and civilization are upheld by people, their institutional instruments and their technology. The efficiency of IT and computer networks should be used to strengthen democracy and civilization within nations, regionally and globally. Dissemination of information about political and governmental processes can for example provide more transparency for citizens with regard to local and national governments, and even regional and global political structures such as the EU and the UN. More direct involvement of citizens in the democratic processes is desirable and can be achieved though clever use of ICT. These elements provide a basis for political stability as well as for the prevention and timely resolution of conflict. The integrity of such ICT infrastructures will be crucial to obtain the citizens' trust. This can only be achieved through having thorough security requirements and through integrating security solutions with disciplines such as regulation, policy making and politics.

Fig.1 below illustrates the basic principle of how fundamental and application oriented security research can be combined with other disciplines to support the high level societal goals described above.

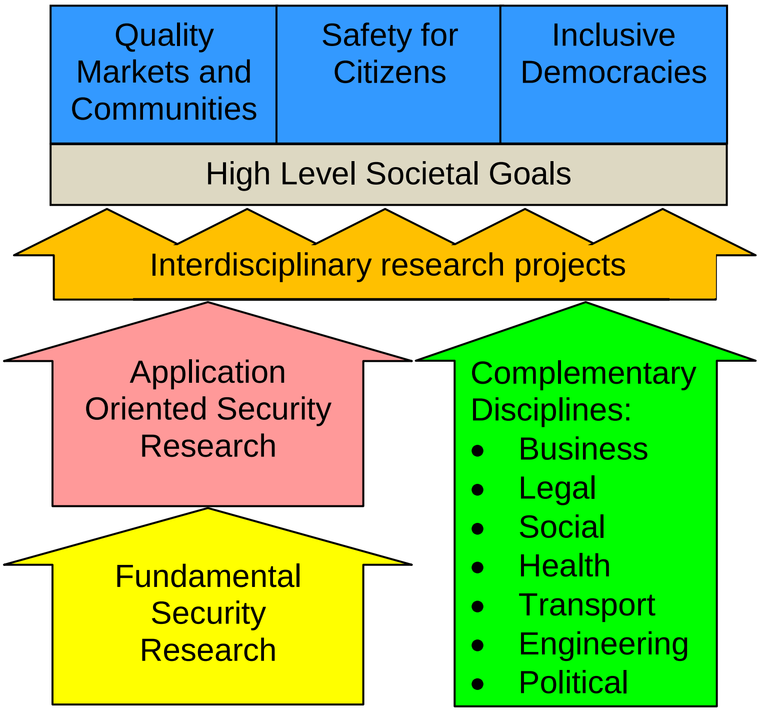
Quality Markets and Communities
Safety for Citizens
Inclusive Democracies
High Level Societal Goals
Interdisciplinary research projects
Application Oriented Security Research
Fundamental Security Research
Complementary Disciplines:
• Business
• Legal
• Social
• Health
• Transport
• Engineering
• Political

Figure 1. Interdisciplinary security research to support high societal goals

4.3 Estimated Research Outcome and Impact

Assuming that NOK 50 Millions in funding for security research can be provided over the next 4-5 years is it will be possible to complete 4-6 average size research projects. In terms of research staff, the mentioned level of funding will support around 15 PhD completions and 5 PostDoc positions over the funding period.

The outcomes will be knowledge and technologies that will provide crucial contributions towards high societal goals like the ones described above.

Multidisciplinary research will ensure that outcomes will have high relevance and be relatively easy to adapt and embed in real environments where information technology is only one of many aspects.

5 Summary and Recommendations

This document describes a relatively broad range of security research topics that have been grouped into fundamental security and application oriented security research challenges. Table 1 below summarises the described research challenged. The set of research topics is not meant to represent an exhaustive list, but reflects the view of the NISNet members regarding important and timely security challenges in the near to medium term.

The NISNet study group recommends that funding be provided for research projects that express innovative research visions and that articulate sound approaches to investigating and developing information security solutions. This includes interdisciplinary research as well as the integration of multiple types of information security technology to solve relevant problems. While a single research project with a limited budget necessarily will have a limited scope, it should always be seen in the light of high level societal goals. Constant technology innovation and the changing threat environment make information security an ongoing process that always requires new solutions. For that reason, it should be noted that information security research topics other than those directly described in this document can also have merit and be fundable. Project proposals should always be assessed by impartial experts who through their continuous engagement in the information security community stay constantly updated and informed about the changing information security landscape.

6 References

[CORDIS 2007] KOLOSSA, T.
http://cordis.europa.eu/fp7/ict/security/fp7_en.html. (accessed 13.04.08)

[FFI 2007] FRIDHEIM, H., AND HAGEN, J. Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer - sluttrapport, 2007. FFI-rapport 2007/01204, Forsvarets forskningsinstitutt/ Norwegian Defence Research Establishment (FFI).

[N.Gov. 2007] Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010.
http://www.regjeringen.no/Upload/FAD/Vedlegg/IKTpolitikk/fad%20lav.pdf. (accessed 13.04.08)

[NFR 2005]
http://www.forskningsradet.no/no/Utlysning/VERDIKT/1114506644055&visAktive=true

[Smith&Spafford 2004] SMITH, S. W., AND SPAFFORD, E. H. Grand challenges in information security: Process and output. IEEE Security and Privacy 2, 1 (2004), 69–71.

[Symantec 2008] Symantec Corporation. Internet Security Threat Report, April 2008.
http://www.symantec.com/business/theme.jsp?themeid=threatreport