

Position paper PAMPAS workshop

Security and Privacy issues in Next Generation Mobile Networks and Services

Jan Huizenga, Thijs Veugen, Hans van Vliet
huizenga@fel.tno.nl, veugen@fel.tno.nl, p.j.vanvliet@fel.tno.nl
Tel. +31 70 374 03 08 // +31 6 20 43 15 47
www.tno.nl/instit/fel
TNO Physics and Electronics Laboratory
PO Box 96864, 2509 JG The Hague, The Netherlands

Introduction

In this paper some of the main security and privacy issues towards the next generation Internet are highlighted as well as some promising solution areas. Firstly the problems are analysed from the application and technological perspective. Secondly a view is given on the perspective of socio-ethical, economic and legal/regulatory perspective for the users in the European Information Society.

Application and Technological viewpoint: “Critical mobile infrastructure improvement”

The network infrastructure is expected to grow rapidly, with increasing bandwidth and more and more different technologies being used. In particular the wireless part of the network will change the infrastructure significantly. The future access infrastructure will consist of a combination of different types of networks, like mobile cellular networks (e.g. UMTS), wireless local area networks (e.g. IEEE 802.11) and wireless personal area networks (e.g. Bluetooth). These different classes of networks have been designed for different types of use. For (public) mobile cellular networks the user needs a terminal to access the cellular network, all the problems related to security, privacy, routing, availability are managed by the provider. For (private) local wireless networks security is a matter of the user, not only in the meaning that she has to choose the right implementation (e.g. the correct number of encryption bits for WEP), but the user is also responsible for the configuration.

The number of users and devices connected to the network and the type of services offered will increase. Advanced mobile services will be enabled by service platforms that provide open interfaces between applications and mobile networks. Furthermore, the future will bring users, which will be able to connect to different (wireless) networks in an ad hoc and transparent manner with different devices and using different types of services. This results in three different concepts of mobility: (1) mobility of users, (2) mobility of devices, and (3) mobility of software (agents). We foresee a complete integration of the different types of networks. Access to similar mobile services will be possible using different types of networks. For this, an entirely new approach to security is needed.

It is essential to understand the potential weaknesses and vulnerabilities in the critical mobile infrastructure, which consists of different types of access networks and service platforms on top of these and which is characterised by the keywords: large, distributed, heterogeneous, ad hoc, and mobile. This understanding can be achieved by both modelling and analysing (properties of) the mobile infrastructure as well as via a theoretical and practical vulnerability-analysis of the new technologies and interdependencies.

An important role can also be fulfilled by offering users transparency of the quality of networks, services, and security, offered by different access, service and application providers. This will help users to compare different providers and products and can hence provide a market-mechanism to improve performance and security of networks. The objective is to (1) define, standardise and implement metrics for quality of performance, integrity, and confidentiality (2) increase the research, development, and usage of measurement tools, such as such as Privacy Enhancing Technologies, Mobile PKI and Intrusion Detection Systems (IDS).

User and information society viewpoint; “Privacy and security issues”

An essential element of the information society is the collection, processing and distribution of information on a large scale. Users are ‘always on-line’ and numerous new information services and products are developed, enabling new ways of doing business and of communication within our society. As a result the amount of personal and business information available and used on-line is and will remain increasing coming years. More and more of the on-line products and services are not restricted to a physical location



and even offer location-based added value. Customised services ‘Wireless communications’, ‘Seamless access’, ‘Context and Location-aware services’ and ‘Ambient intelligence’ are the keywords for the future.

For the civilians there is a growing information privacy threat and for business users there is a comparable threat to sensitive business data. Privacy Enhancing Technologies (PET) are a promising solution to be researched and implemented to reduce the privacy (-related) problems. Unfortunately, market drivers for Privacy Enhancing Technologies are still insufficient and community and governmental/legal support is therefore at this point still essential.

Privacy Enhancing Technologies should be an integral part of the information society infrastructure. Both content and intelligent analysis (data mining, user profiles) of this content is increasing in the network. These processes need to be analysed for privacy vulnerabilities, and generic solutions for privacy incorporation and disclosure control are to be developed. A particular objective should be to have measures compliant with EU-directives. Related to privacy measures are issues around trust, authentication, and identity management. Security and privacy solutions should be easy-to-use for end-users, preferably transparent, or offered as a managed service.

Closely related to security and privacy is the issue of mobile communications crime and fraud. There are a couple of important issues in this area to be solved, including efficient international co-operation and harmonised legal systems. But also the more technical R&D issues in the area of digital forensics, law-enforcement access to data, and tracing of delinquents using mobile devices. An important challenge is to develop the required tools for law-enforcement, while preserving the privacy of the citizens.

New directions of research

Security must be a shared layer in the whole architecture. This approach is clearly different from what has happened in the mobile communication networks for all generations up to the third. In a basically single provider/single medium approach (as in mobile networks today), security and privacy of the users can be protected by enforcing strict policies on the network infrastructure. Clearly this approach is unfeasible when applied to a multiple provider (maybe no provider)/multiple network/multiple media device.

The new devices will be directly connected to several wireless communication networks both local and wide area. Today the user can trust nation-wide mobile network providers. Tomorrow with a beyond 3G device she will have to deal with several untrusted attempts of communication, the most of them are related to useful, interesting and well behaved services but she will have to face also to some malicious hacking attacks.

Concepts like trusted domains, hierarchy of trusted networks, degree of trusting, limited trusting in time and space must be included in the security model

The main security and privacy issues towards the next generation mobile networks and services can be summarised as follows:

- Generic, network and application independent security, trust and privacy mechanisms.
- “Critical mobile infrastructure improvement”
- Metrics for measuring quality of performance, integrity and confidentiality.
- Wireless Public Key Infrastructure.
- Privacy Enhancing Technology for mobile code, devices, users and databases.
- Mobile Identity Management, EC-Passport
- “Mobile CERT”
- Business modelling of security and privacy features (licensing, legal control)
- Human Computer Interfaces for security, safety and privacy in mobile applications (cars, transport, industry, gaming)
- EC-Evaluation method for mobile devices and applications
- Privacy Incorporated Mobile Software Agent

These can be topics of integrated projects (IP) possibly combined with networks of excellence (NoE) on critical (mobile) infrastructure.



TNO

TNO, the Netherlands Organisation for Applied Scientific Research, is a large contract research organisation. TNO's mission is to apply technological knowledge with the aim of strengthening the innovative power of industry and government.

TNO has a staff of about 5.100 highly educated and driven professionals. The organisation has 14 institutes. The TNO-FEL institute (TNO Physics and Electronics Laboratory) has a staff of more than 550 professionals. TNO-FEL is the largest independent ICT-lab in the Netherlands.

In the areas of electronic commerce, telecommunication networks, mobile networks and services, knowledge and information management, information security systems, privacy and usability, TNO-FEL contributes towards solving issues that emanate from the emergence of an information society: the investment, living and social climates; the competitiveness of businesses that use ICT services; and the expansion and growth of the ICT cluster.

Related Projects

1. PISA

The Privacy Incorporated Software Agent project (PISA, www.pet-pisa.nl) is a three-year collaborative European Union Fifth Framework project involving the development of Privacy Enhancing Technologies for the next generation of agent-based e-business applications. The project commenced in January 2001, and includes partners in the Netherlands, Belgium, Italy and Canada.

2. RAPID

The RAPID project (www.ra-pid.org) will develop a strategic roadmap for applied research in the area of privacy and identity management (PIM). RAPID will build a robust forum of leading experts and stakeholders and provide a platform in which these stakeholders can develop a detailed technology roadmap for R&D activities in FP6. The experts are drawn from industry, academic research institutions and civil rights organisations and cover the domains of privacy enhancing technologies, privacy law, socio-economic aspects of privacy and privacy security issues. In order to meet the FP6 'deadline', RAPID has set itself the goal to complete its work plan in 12 months.

3. GigaMobile

The GigaMobile project, with participants from Dutch knowledge institutes, is a project in the scope of GigaPort (www.gigaport.nl), the national Netherlands programme on next generation Internet infrastructure and applications. The project focuses on enabling technologies for customised mobile services based on user preferences, location and network and terminal QoS. Solutions for privacy and security issues related to user information, like user profiles, are studied within the project.

4. ACIP

The goal of ACIP (www.eu-acip.de) is to determine how protection of critical infrastructures can be analysed and assessed by modelling and simulation. The aim of ACIP is to provide a roadmap for the development and application of modelling and simulation, gaming and other methodologies and tools.

Representative

Jan Huizenga.

In 1998 Jan has been engaged as a principal research scientist with the Telecommunications and Security Group at the TNO Physics and Electronics Laboratory (The Hague, The Netherlands). Currently he is involved in research for security-studies and development of new techniques for e-commerce, mobile commerce, Internet/Intranet, privacy and multilevel security. He was project leader of the KWINT-project (Vulnerability of the Dutch Internet). He is project co-ordinator for the EC PISA-project (Privacy Incorporated Software Agent, IST 2000-26038), contributes in the PET-study for the Dutch Ministry of the Interior and is member of the EC-RAPID-project, to develop a roadmap for Privacy and Identity Research in the FP6.

