

## SIMS Position paper for PAMPAS

### Background

Third-generation (3G) wireless technologies offer a launching pad for ideas such as wireless web, email (SMS, MMS), and other services, along with improvements to the core of the second-generation wireless (2G) technologies. Other technologies and services such as I-Mode, EDGE (*Enhanced Data Rates for GSM Evolution*), WCDMA (*Wideband CDMA*), GPRS etc. have been emerged supported by various vendors. The usual forces to get bigger, better, faster and more secure services will drive technology past the current status of 3G to 4G technologies. The fourth-generation wireless (4G) technology implements designs that will take the wireless telecommunication industry beyond 2010. The infrastructure of the 4G will function on top of the current existing CDMA (*Code Division Multiple Access*), GSM and TDMA (*Time Division Multiple Access*). It extends the 3G capabilities, thus the transmission must be based entirely on packet-switched network technology with higher bandwidths for multimedia services and it must also provide advanced network security. These technical opportunities strengthen the user mobility and encourage the deployment of the mobile technologies for the development of various (mobile) applications providing information, orientation (routing) and other helpful services.

Therefore, mobile users will take advantage of multi-interface (e.g. WLAN, Bluetooth, UMTS) PDAs and SmartPhones, participating in countless Ad-Hoc networks and using push services for orientation and information. Thus the user (and his device) is frequently switching networks, confronting him with interchanging security threats in a fast order. Coming home from a longer business trip and finally re-entering the home/corporate (W)LAN environment doesn't mean the user is secure – in contradiction to the feeling of entering a safe harbour, one must regard the homecoming device as a considerable security threat itself being a potential carrier of malicious code or trojans. Such threats dwarf the user acceptance which is necessary for the success of this technology. The fundamental factors to gain and improve the user acceptance are e.g. transparent services and security aspects. The very nature of most wireless communications makes security a significant factor that must be understood and addressed for wireless communication to achieve its vast potential.

### Scenario

Imagine an unsecured PDA roaming dozens of networks, freely interchanging data (such as vcards or documents), sharing resources (Ad-Hoc networks) and additionally having location based information pushed to the device wherever applicable. The repeated change of participation of mobile users in un-trusted networks is a challenge for both the direct security and integrity of the mobile device (attacks launched directly against it, like DoS depletion, misuse of the air interfaces, stealing of computational resources etc.) and the security of the home LAN (insertion of Trojans, malicious code and viruses behind the firewall and anti-virus gateway). With the increase of information that is sent to the device, the probability of malicious content being inserted also grows.

Another example for serious threats that already emerge in today's GSM/GPRS networks, is the usage of JAVA enabled phones and the problems arising from the data transfer when downloading JAVA content over the air. The JAVA environment on mobile or embedded devices, utilizing MIDP, kJAVA or proprietary subsets of the above, makes powerful applications, applets and games available to user. In Europe, this technology still evolves but in Japan a vast selection of services is available, supported mainly by I-mode, NTT DoCoMo's "mobile Internet", now being introduced to the German market by the carrier eplus. Recent papers discuss the security of java-enabled phones and first loopholes have been identified - and exploited by virus-like alterations of code. These problems, now being a mere annoyance due to their little impact on usage, can and will evolve, when devices become more powerful, networks offer higher bandwidth and applications get higher privileges. But devices will still not be capable to provide scan-engines like the ones offered for desktop machines!

Thus, the need for server-based or network-based solutions is evident and research has to be conducted to improve the security of both networks and end-user devices.

Besides the security regarding the device itself and its associated home LAN, issues of privacy vs. authentication have to be taken into account. On the one hand, providers for premium services need to be able to identify their customers for billing purposes or provision of tailor-made applications and services. On the other hand, user preference profiling and location tracing/tracking bring up privacy issues of considerable importance. Some ideas regarding the use of multiple pseudonyms have been introduced theoretically circumventing the above mentioned problems but introducing new ones with regard to multi-identity management and billing.

When considering technical solutions for the above introduced set of issues, the user himself has to be integrated in each concept right from the start. Security for applications, services and devices is mandatory, but the user and his behaviour will once again be the weakest point. Therefore, easy-to-use mechanism for extra authorization, change of pseudonyms etc. have to be implemented, allowing the user to adapt to the more complex environment of multi-service (multi-)wireless networks.

### Challenge

A major challenge for user e.g. SMEs (small and medium enterprises) and vendors of the information and communication technology is to implement security in a way that meets business needs cost-effectively, both in the short term and as the enterprise needs to expand. In order to meet this challenge, the improvement of the existing methods of identifying and analysing threats and security risks, and of specifying, designing and implementing security policies.

As a research group for the Advancement of Applied Research our view is to use applicable scenarios to investigate various aspects related to heterogeneity in the wireless access networks (also beyond 3G) from the security perspective. With regard to the existing variety of wireless devices based on different standards the question of what will be the appropriate trend in the future should be investigated. The focus of future research efforts should be to study following core topics in wireless communications:

- Security in Mobile Systems dealing with Secure mobile devices
- Secure mobile access technologies
- Secure operating systems
- Secure location, time and person related services (Location Based Services)
- Privacy issues

### Illustration of the point of view

The trust today's users have in their mobile communication equipment based on 2G or 2.5G technology is the foundation for the intense usage and broad acceptance of these services. Based on the requirements for 2G wireless networks and services, ingenious, and at the same time simple, security mechanism have been specified, designed and implemented. Even more specifications have been agreed upon, yet awaiting implementation helping to safeguard this security. The priority for future research in the area of wireless network security should be, to find and analyse the requirements that the new applications and services will generate. This should comprise a detailed review of the requirements of 2 and 2.5G networks as well as other wireless technologies such as e.g. WLAN, Hiperlan /2, Bluetooth. Taking these technologies and their problem sets into account is a necessity due to the convergence of voice and data networks and the high bandwidth future wireless network are expected to offer. Hence upcoming wireless technology will include many services that are yet limited to proprietary solutions (e.g. mobile banking ), thus all former proprietary problems have to be dealt with in the new systems. The next question to be worked upon, will be how to meet these requirements with means of existing, specified and/or not yet implemented mechanisms and protocols. If no sufficient solution can be found, new protocols or mechanism must be designed and implemented.

To reach the same level of trust that existing 2.5G technologies experience, thoroughly designed and flawlessly implemented applications must be launched in the upcoming multi-service networks. This can only be done by following strict security guidelines right from the start. To give service-providers and developers a framework to work with, security mechanism must be woven into the protocols supporting the applications, thus enabling the programmers to rely on them from the first line of code and still offering easy-to-use services to customers.

By analysis of the requirements and early integration of security mechanism into the underlying protocols and development frameworks, the groundwork for standardization is made. Carriers, service-providers and manufacturers must therefore cooperate closely, thus enabling the standards acceptance and producing a market driving force. Our working groups are eager to participate actively in the proposed research and standardization work.

Dr.-Ing. Kpatcha Bayarou, Dipl.-Ing. oec. Sebastian Rohr  
[bayarou|rohr]@sit.fraunhofer.de  
++49 6151 869 [274|279]  
Rheinstraße 75  
64295 Darmstadt