

## Security Challenges in the future mobile Internet<sup>1</sup>

Bernd Lamparter, Dirk Westhoff  
NEC Europe Ltd., Adenauerplatz 6, D-69115 Heidelberg  
{bernd.lamparter,dirk.westhoff}@ccrle.nec.d

*Abstract* -The last decade showed a trend from the closed telephone network provided by a few operators towards open networks provided by many companies. With ad hoc networks, we even see a trend towards networks without any ownership by ISPs or other commercial providers and without any centralized infrastructure. Furthermore, the technologies to access these networks are developing rapidly and will be very heterogeneous. In the upcoming personal area networks (PAN), people will wear a couple of devices around themselves and install them in a self-configurable manner in the personal LAN of their flats. Research in the area of security for (1) privacy, (2) authentication, (3) accounting and billing, (4) availability, and (5) reliability is to be conducted to make mobile communication trustworthy and successful. The key objectives are to analyse the security problems, to develop appropriate secure solutions related to all layers, to implement sample prototype solutions and finally to stimulate the standardization process. To make this integrated secure system approach a reality in the future secure Internet, at least the following problems have to be solved, and protocols as well as data formats have to be standardized.

### 1. Protecting Data for Privacy and weaving Trust into Data:

These new technological possibilities raise new security issues not only at all network layers, but also for access rights for data on the individual devices. Let us consider an example: Assume you have a medical chip storing all your medical data with you. In case of an accident you would like everybody helping you to survive to have access to this data. But you do not want this transparency every day or to everybody in non-emergency situations. Additionally, you would not like everybody to be able to eavesdrop on the communication between the medical device and the hospital. Obviously, even the hospital may not be trustworthy. Other examples of data and devices to be secured are digital cameras or pace makers. To implement such concepts in an infrastructure less environment, distributed certification authorities to establish some sort of trust and to support reliability for the logic certification authority have to be analysed. Related to the described pervasive computing scenario, new privacy and data concealment concepts for different subgroups need to be proposed: Subgroups of a pervasive computing system may be a) entities belonging to the same subscriber, b) entities belonging to the same social context, i.e. devices of two or more subscribers who have some previous relationship and want to communicate now, and c) totally unknown subscribers that neither know each other nor share the same administrative domain.

Currently, a lot of information can be found in the Internet. Much of this must be considered as garbage, but certainly there is also a lot of valuable information from companies, research institutes or governmental organizations. The problem is that it is hard for the user to know which information he can trust even when he knows an institution as trustworthy, since the information (or the website) might be forged. The same problem applies for internal information, e.g. name services (DNS) or routing information (especially in ad hoc networks). Some sort of digital signatures could solve this problem, but current algorithms are a challenge for devices with weak processors. Also, after a change of the media, digital signatures are no longer visible, e.g. printed web documents or an mp3 file after it is copied to an analog medium. Furthermore, we have to face the problem of different life times of keys and information bearers. Whereas the key lifetime is limited, the lifetime of the information bearer might be unlimited.

### 2. Integration with wired networks:

When new types of networks, such as ad hoc networks, are integrated as a kind of stub network to traditional fixed networks with infrastructure, two very different types of networks come together. Whereas we have pre-established services for fixed networks, we see the on-demand paradigm for ad hoc networks. This applies to all services including routing, and creates new challenges for security aspects because there are no central instances that all devices trust. Routing itself is a service that has to be secured against misuse and intrusion.

Currently, many security protocols are known and standardized, e.g. IPsec or SSL/TLS, and some layer 2 protocols like 802.11 and Bluetooth include security protocols. They are either used for end-to-end or hop-by-hop encryption. Without some pre-established security associations especially over wireless and dynamic connections, building low-cost secure channels is still a challenge. It is still not clear how to handle a public key infrastructure in a very large scale with many dynamic communication channels. Rapid changes of the network topology make the job even harder. It is also unclear how security mechanisms for communication like IPsec cooperate with mobile IP and firewalls.

New security challenges appear in this dynamic mobile connected world. Today, operators of mobile phone systems are able to localize their customers. It is predicted that there will even be applications that make use of this knowledge, i.e. they are location aware. But how can a user define to whom he wants to disclose this information? He might even want to exclude the operator from the knowledge of his location. But still he wants to be reachable. This is one example of context-aware applications. There will be other applications making use of personal data to improve their value for users, e.g. travel habits. It is unknown how this data can be protected against misuse.

---

<sup>1</sup> This work is substantiated in the SecMad EoI.

New Internet protocols tend to create new security problems. Web services allow transferring data via HTTP in a very flexible way, but current firewall software has no chance to filter out sensitive transmissions. We assume, that new applications or protocols have to be developed with security in mind from the beginning. The deployment and integration of standardized protocols like IETF's IPsec on top of a reference architecture supporting mobility may result in an insecure and heavy-weight solution.

### **3. Cryptographic Algorithms in Constraint Environments:**

Modern security protocols require both public-key and symmetric algorithms. The former ones are notoriously computationally intensive, since they are based on arithmetic with very long numbers (typically between 160-2048 bits). However, symmetric algorithms can also be difficult to implement if there are resource restrictions (e.g., chip area or code size). Whereas these problems have been widely overcome in traditional networks (security in the Internet, LAN, etc.) due to the increasing computation capabilities of PCs and workstations, efficient cryptographic algorithms in low-power environments as they are often found in ad hoc networks remain unsolved at present. The corresponding network nodes often have limited chip area, power consumption, processing power, and code size. Many limitations are inherent to ad hoc nodes since they are (i) often wireless and (ii) pervasive which often implies small form factors and cost constraints. It will be of crucial importance for the success of next generation networks to find solutions to the following problems: (1) development of new, highly efficient hardware and software implementation techniques for existing public-key algorithms which are suited for heavily constrained platforms (a factor 10 better than current methods), (2) development of new and/or tailoring of existing public-key and symmetric algorithms for constrained environments (e.g., algorithms that are optimised for 8 bit microcontrollers), (3) development of a security/cost metric which allows to finely tune implementations to a given platform, and which enables security/performance trade-offs.

### **4. Security Protocols in Ad-hoc Networks:**

Security in ad hoc networks is difficult to achieve. Due to its decentralized character, security issues for ad hoc networks are very different from those for traditional networks. Limited physical protection of the nodes and the communication channel, mobility of the nodes, and thus a dynamically changing topology, as well as the absence of any central service or central management induce security problems. The main goals of a security protocol are to provide availability and to ensure communication security. Only a few security protocols have been proposed for ad hoc networks so far. They range from a distributed PKI, distributed webs of trust, direct trust relationships to securing the routing mechanism itself. Especially in civilian ad hoc networks, nodes have no incentive to forward foreign traffic. However, none of the proposed protocols seem to be sufficiently evolved for deployment. The following problems have to be solved in order to apply next generation networks in practice: (1) How much security do we need for various applications in ad-hoc networks? (2) What are the essential threats in an ad hoc network? (3) Which solutions were already proposed, and how suitable are they for which applications? (4) Development of (key distribution) protocols for ad hoc networks.

### **5. Charging and Billing:**

Currently it is totally unclear what business models will fit future open, heterogeneous and packet-oriented networks that may need to integrate wireless multi-hop scenarios. We envision that, in such an environment, both, the role of subscriber and network-provider, as well as the role of subscriber and content-provider, may melt into one another. Although it is not predictable which business models will gain acceptance, we have to prepare the technical and security related support.

It is assumed that more and more Internet services will not be free of charge any longer. There will be many possible ways for a user to pay, but by far the simplest solution would be combining this with the charging of the Internet access. Users will get only one bill from their home provider for all kinds of services used via the Internet and independent of the network they have used. This kind of charging has to be implemented in a secure, scalable and highly available way. Civilian ad hoc networks are challenging because devices of other people are used to forward packets. The question is how they could be motivated to let their devices participate in building an ad hoc network. Business models, which are attractive for all three (the individual giving away battery power, the operator providing the Internet service, and the user), have to be developed, so that they can be deployed with the necessary level of security.

### **6. Social and legal problems:**

The use of security mechanisms has a price, which might be monetary or in terms of usability or functionality. If it is too complicated to use security mechanisms, people invent tricks, like writing passwords into their address book under "s" like secret. Many people are just frustrated because of the amount of passwords and PINs they have to remember. Simple, integrated, but still secure solutions are necessary, e.g. biometric procedures. This only authenticates a user, but the problem of authorization still remains, because people belong to many groups each with special access rights. After the development of a technical solution for a security problem, we face two further problems: Does it match the social behaviour of the potential users, and is the usage legal in the international world we have today. People tend to be suspicious about sending their credit card number over the Internet, but pay with the very same card in foreign countries in every shop. Some countries allow strong encryption; in other countries people have to stick to weak keys.