

Position Paper for the PAMPAS '02 Workshop on Requirements for Mobile Privacy & Security

Michael Schmidt

Institute for Data Communications Systems, University of Siegen,
Hoelderlinstrasse 3, 57068 Siegen,
Germany

Abstract-The foreseeable popularity of mobile communication devices raises novel concerns in the areas of security and privacy. Especially Personal Area Networks (based on ad-hoc networking technology) demand for increased research on ways to avoid so-called location tracking attacks, where an attacker attempts to create profiles of his victim that allow the attacker to track down when his victim was present in certain (monitored) locations. The use of pseudonyms is one possible way to tackle this problem. Pseudonyms, however, introduce new problems in the areas of both technical implementation and legal use.

I. INTRODUCTION

Ad-hoc networking describes the formation of radio networks in a more or less random fashion, i.e., ad-hoc radio devices arbitrarily join and shape a network without any ahead planning and administrative overhead. Together with the growing popularity of ad-hoc technologies like Bluetooth (BT), the term “Personal Area Network” (PAN) has been created to describe an ad-hoc network that comprises of radio devices which reside (more or less) within the personal reach of a device user. Fig. 1 shows a scenario with a roving wireless PDA user who establishes a PAN whenever

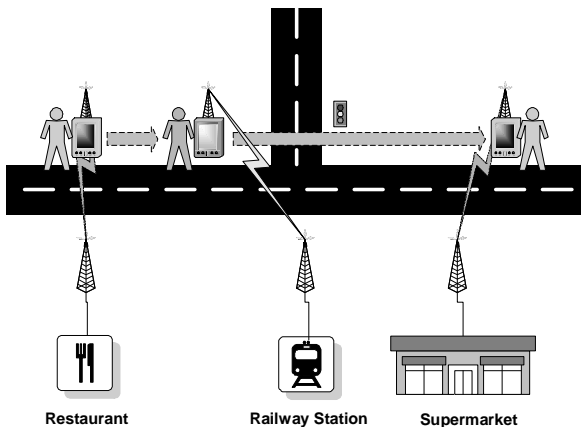


Fig. 1. Subscriptionless mobile networking

he (i.e., his device) comes into radio reach of one of the other (here stationary) radio devices. With BT, for example, a PAN can be established as soon as two devices fall short of a distance of about 10 m. In [1], this scenario is called “Subscriptionless Mobile Networking” (SMN).

PAN nodes use a variety of identities, e.g. a user or node identity on the application or service level, an IP address on the network layer, and finally a device address (MAC address) on the link layer. Whereas the user/node ID often is variable, the IP address tends to be fixed or at least repeating frequently. The device address is fixed in most existing technologies. These addresses may be seen as identities that belong to a device and/or its owner (user). Whereas the fact that fixed identities are used is considered a technical and organisational advantage in fixed networks, it means a privacy problem in PANs. In detail, fixed identities become a problem whenever the device exposes them automatically without explicit user approval. An attacker who is able to deploy a certain amount of spy devices in an area or at spots of interest is able to collect information of location and time of presence of victim devices at known locations. Therefore, the spy devices page or contact victim devices and prompt them to emit their identities. Subsequently, the location – time data records are collected in a database, so they can subsequently be processed and converted to location traces of individual identities. [2] outlines that this is a concrete problem with BT, which uses fixed MAC addresses and exposes them regularly without explicit user approval. It is also shown that there exist ways to correlate the device ID with the corresponding user subsequently.

II. TECHNOLOGY REQUIREMENTS/QUESTIONS

SMN [1] outlines a concept of variable identities (pseudonyms) that are used on all layers (application/service, network and link layer) whenever this is feasible. In detail, pseudonyms can be used in communication sessions whenever there are no high legal requirements on the communica-

tion session, i.e. no or only low-value payments are involved. Therefore, SMN imitates “local market” sales communications, where the communication partners are not necessarily interested in knowing the true names of each other. In fact, in such electronic face-to-face scenarios it is only necessary to assure that the partner identity shown on the communication device corresponds the person one faces.

The use of variable device addresses, however, is problematic. Currently only Hiperlan/2 supports the use of variable device addresses. Unfortunately, Hiperlan/2 is quite academic, and no devices exist so far in the market. For SMN, BT devices are used whose device addresses have been made variable in a proprietary way. This works satisfactorily in closed, academic “SMN scenarios” where no regular Bluetooth devices interfere. In the real world, address collisions with Bluetooth devices with regular (IEEE-assigned) addresses may occur. Also, in scenarios where SMN devices participate in networks with fixed network adapters with regular device addresses address collisions may occur. To conclude, privacy through pseudonyms is a requirement, and research is necessary in the areas of variable device address assignment with automatic collision avoidance and conformance with existing network device address spaces and standards.

Another problem with the use of short-term pseudonyms in SMN is secure authentication. Since typically no Public Key Infrastructure shall be used, there is no secure binding between pseudonym and its public key unless additional certification information is exchanged out-of-band to verify the authenticity of the exchanged public keys. This issue is comparable with the use of PGP, where the authenticity of an exchanged public key is verified via out-of-band exchange of public key fingerprints (a hex representation of the hashed public key). Since a fingerprint typically consists of 40 or more digits, its use is unpopular and error-prone. Fortunately, there is an alternative to using fingerprints: The Déjà Vu project [3] shows how hash values can be presented graphically through fractals. In SMN, they could be shown on the PDA display. This kind of presentation is much user-friendlier and easier to perceive and memorise for humans. Unfortunately, the cryptographic strength of this approach

has not been investigated very deeply. To formulate it as a requirement, user-friendliness in privacy-preserving authentication is requested. Further research is necessary.

III. LEGAL AND REGULATORY REQUIREMENTS/QUESTIONS

Due to the current legislation (Germany and EU), non-disclosure of one’s real identity (i.e., the use of pseudonyms) is legal in electronic communication scenarios with ad-hoc and/or PAN networks. As soon as a connection to an ISP is established, previous registration of a user with the ISP is required, though. It is currently unclear which legislation applies if the Internet is accessed via an SMN device (via gateway) while using a pseudonym only. One of the basic ideas of SMN is the avoidance of subscription procedures whenever possible (hence the name “Subscriptionless Mobile Networking”).

The requirement here is clarification about the use of pseudonyms and/or registration-less service access in hybrid network architectures with both ad-hoc radio and fixed components.

REFERENCES

- [1] Michael Schmidt, “Subscriptionless Mobile Networking: Anonymity and Privacy Aspects”, presented at the IEEE WCNC 2002, www.nue.et-inf.uni-siegen.de/~schmidt/english/literat.html
- [2] Markus Jakobsson and Susanne Wetzels, “Security weaknesses in Bluetooth,” Lucent Technologies – Bell Labs Information Sciences Research Center, Murray Hill, NJ 07974, USA, 2000,
- [3] A. Perrig, D. Song, “Hash Visualization: a New Technique to improve Real-World Security,” Computer Science Department, Carnegie Mellon University, Pittsburgh, 1999