Fraud Prevention and User Privacy in Mobile Computing
(extended summary)

Yuliang Zheng

The Peninsula School of Computing and Information Technology
Monash University
McMahons Road, Frankston
Melbourne, VIC 3199, Australia
Email: yzheng@fcit.monash.edu.au
Phone: 03 9904 4196, Fax: 03 9904 4124

February 1996

1 Security Issues in Wireless Networks

Recent years have seen an explosive interest in wireless (information) networks that support the mobility of subscribers (and/or terminals). These networks serve as a foundation of future universal, mobile and ubiquitous personal communications systems.

Emerging wireless networks share many common characteristics with traditional wire-line networks such as public switched telephone/data networks, and hence many security issues with wire-line networks also apply to the wireless environment. Nevertheless, the mobility of subscribers, the transmission of signals through open-air and the requirement of low power consumption by a mobile equipment give a wireless network a large number of features distinctively different from those seen in a wire-line network. Especially, security and privacy becomes more eminent with wireless networks. For this reason, in this paper we will be primarily concerned with security issues related to or caused by the mobility of subscribers/terminals, open-air transmission of signals and low power supply of a mobile equipment.

When examining the security in a wireless network, a large number of issues have to be considered. Some of the issues are addressed in the following.

1. identification of a mobile unit.
2. anonymity of a mobile unit/user (protection of identity)

3. authentication of a base station.

4. security of information flowing between a mobile unit and a base station.

5. prevention of attacks by an insider from a base station.

6. hand-over of authentication information.

7. the communication cost of establishing a session key between a mobile unit and a base station, which includes the total number and length of messages to be exchanged.

8. the cost of communications between a foreign domain where a mobile unit is located at the mobile unit's home domain, as well as security requirement on the communication links between the two domains.

9. the computational complexity of achieving authenticity and security.

10. the computational requirement to a mobile unit that is in general much less powerful than a base station.

Some issues contract one another. For instance, to prevent the abuse of mobile network resources by a fraudulent user, a network relies on the identification/authentication of a mobile unit, which generally requires the user to reveal his or her identity. On the other hand, however, a user who wishes to be anonymous may be not willing to reveal his or her identity to a foreign cell. Two recent surveys [4, 13] discuss in details many issues in mobile networks, especially those related to security and privacy.

2 Previous Proposals

A concise summary of the authentication and security protocol employed by the global system for mobile telecommunication or GSM [10] can be found in [4]. A description of the proposed security and privacy mechanism used in the cellular digital packet data (CDPD) in USA is provided in [6], where potential threats and attacks to the mechanism, together with possible solutions, are also discussed. Other notable works include [3], [2], [8], and more recently, [7], [1] and [11]. In the full version of this paper, an outline of each of these protocols, together with a comprehensive comparison of various aspects of these protocols, will be described.

2.1 Problems with Beller-Chang-Yacobi Protocol

Among the protocols discussed above, the one presented in [3] which is the primary focus of this paper deserves special attention, as it represents one of the earliest solutions based on a combination of both private-key and public-key encryption algorithms. This protocol is called MSR+DH protocol. It is based on two hard problems: factorisation and discrete logarithm over a finite field.

Beller-Chang-Yacobi's protocol consists of three moves (or steps) of information. The third move is somewhat imprecisely defined: it requires a mobile unit and a base station to "exchange a know message" using a new session correctly established.

This imprecisely defined move of information could introduce potential difficulties: imagine a a mobile user roams into a friend cell whose base station does not share any "know message" with the mobile unit. With this problem in mind, let us further look at whether it is possible to eliminate this move.

As the protocol is based on public-key cryptography, any user, whether he is legitimate or illegitimate, can get the public key, as well as its certificate, of a mobile user, impersonate the mobile user and pass the second move of the protocol. Therefore, the third move in the protocol can not be omitted in order for the base station and the mobile user to confirm the consistency of their keys.

3 A New Proposal

This section proposes an authentication and security protocol based on public key cryptography. This protocol is remarkably simple: it consists of only 1.5 moves.

In this extended summary, we assume that the reader is familiar with the concept of encryption algorithms, including public-key and private-key encryption systems. An introduction to the concept will be provided in the full version of the paper.

3.1 Authentication Centre

As in many security solutions, we assume that a mobile network involves a *authentication centre* which provides public key certification services. (see for instance [5] for discussions on certification services.) In particular, each participant of the network, including mobile users and base stations, it provides a certificate for the participant's public key.

We assume that the authentication centre employs Schnorr's digital signature [12] or the closely related Digital Signature Standard [9]. Both signature schemes are based on discrete logarithm over a finite field.

3.2 Making Use of a Broadcasting Channel

Typically a mobile network uses a broadcast channel to continuously propagate from a base station to a mobile unit control information such as synchronisation parameters, available services, base station ID etc. The authentication protocol to be proposed in the following, uses part of the capacity of the broadcasting channel to propagate the base station's public key and associated certificate. To be more specific, the base station will regularly propagate its public key and the associated certificate.

To keep itself abreast of the various types of network information such as synchronisation data, types of services, and the public key and certificate of a base station, a mobile unit continuously monitors the broadcasting channel. In doing so, it will be able to authenticate the base station "at the background". For this reason, we say that that it contributes 0.5 move to the protocol.

3.3 Key Distribution and Authentication of a Mobile User

Assume that p is a large prime and g is a generator for the multiplicative group $GF(p)^*$ of the finite field $GF(p)$. Both p and g are public.

As discussed above a mobile unit can authenticate a base station "at the background". Now we assume that a mobile unit is in the cell covered by a particular base station, and that the mobile unit has successfully authenticated the base station, and wishes to initiate a communications session. The mobile unit chooses a random number $x \in [1, p-1]$ and a random session key $K \in \sum^n$, then sends the following to the base station:

$$(c_1, c_2)$$

where

$$c_1 = g^x \bmod p$$

and

$$c_2 = PRNG(y_B^x \bmod p) \oplus [K, T, y_M, Cert_M, HASH(K, T, y_M, Cert_M, y_B^{x_M+x} \bmod p)].$$

where x_M is the secret key, y_M is the public key and $Cert_M$ is the certificate of the mobile unit, while y_B is the public key of the base station, T is the current time stamp taken from the base station's broadcasting channel, PRNG is a pseudorandom number generator and HASH is a one-way hashing function. (We assume that $Cert_M$ contains information on the identity of the mobile user).

Note that the involvement of T, the current time stamp taken from the base station's broadcasting channel, is to ensure the freshness of the message. Also note that the main ideas behind the formation (c_1, c_2) are from [14], where three practical public key cryptosystems are designed to resist against chosen ciphertext attacks.

Upon receiving (c_1, c_2), the base station calculates $PRNG(c_1^{x_B} \bmod p) \oplus c_2$, and splits the result into five parts K^*, T^*, y_M^*, $Cert_M^*$ and tag^*. It then verifies y_M^* with the help of $Cert_M^*$ and also checks the freshness of T. The base station aborts the process if either y_M^* is invalid or T^* is obsolete. Otherwise, if both y_M^* and T^* are OK, the base station then performs the hashing operation $HASH(K^*, T^*, y_M^*, Cert_M^*, (y_M^* c_1)^{x_B} \bmod p)$. The base station is convinced of the identity of the mobile unit and accepts K^* as the common key shared with the mobile unit if and only if tag^* matches the output of the hash function.

Once a shared session key K is established between the mobile unit and the base station, they can use a private-key cryptosystem such as DES to encrypt data using K.

A few remarks follow:

1. Due to the participation of the mobile unit's secret key x_M in the creation of (c_1, c_2), the chance for an attacker who are even ware of y_M and $Cert_M$ to make a legal ciphertext is negligible small. Hence successful completion of

the protocol guarantees that $K^* = K$, namely the mobile unit and the base station have an identical shared key, with a probability extremely close to 1. Consequently, unlike Beller-Chang-Yacobi's protocol, there is no need to confirm the consistency of the keys through the exchange of a known message.

2. The proposed new protocol consists of 1.5 moves of information: 0.5 move for the authentication of a base station, and a single move for the authentication of a mobile unit together with the establishment of a session key.

3. The protocol provides anonymity of the mobile unit with respect to an onlooker: as all messages exchanged between a mobile unit and a base station, including the identity of the mobile unit which can be part of his certificate $Cert_M$, are transported in their encrypted form, an outsider or onlooker cannot figure out which mobile unit/user is talking to the base station.

4. The protocol prevents the impersonation of a mobile unit by a fraudulent base station: the messages sent from a mobile unit to a base station contains enough information for the base station to authenticate the mobile unit, but not enough for a fraudulent base station to masquerade the mobile unit. In fact the only entity who can create a correct pair of (c_1, c_2) is the mobile unit who knows his secrete key x_M.

In the full paper, a detailed analysis of the proposed new protocol is provided, covering time complexity of the protocol, strategies for pre-computation by a mobile unit, roaming, the procedure for a visited base station to contact the "home network" of a mobile unit and other issues.

References

[1] N. Asokan. Anonymity in a mobile computing environment. In *Proceedings of 1994 IEEE Workshop on Mobile Computing Systems and Applications*, 1994.

[2] Ashar Aziz and Whitfield Diffie. Privacy and authentication for wireless local area networks. *IEEE Personal Communications*, 1(1):25–31, 1994.

[3] Michael J. Beller, Li-Fung Chang, and Yacov Yacobi. Privacy and authentication on a portable communications system. *IEEE Journal on Selected Areas in Communications*, 11(6):821–829, 1993.

[4] Daniel Brown. Techniques for privacy and authentication in personal communications systems. *IEEE Personal Communications*, 2(4):6–10, 1995.

[5] Santosh Chokhani. Toward a national public key infrastructure. *IEEE Communications Magazine*, pages 70–74, September 1994.

[6] Yair Frankel, Amir Herzberg, Paul A. Karger, Hugo Krawczyk, C. Kunzinger, and Moti Yung. Security issues in a CDPD wireless network. *IEEE Personal Communications*, 2(4):16–27, 1995.

[7] Amir Herzberg, Hugo Krawczyk, and Gene Tsudik. On traveling *incognito.* In *Proceedings of 1994 IEEE Workshop on Mobile Computing Systems and Applications*, 1994.

[8] Refik Molva, Didier Samfat, and Gene Tsudik. Authentication of mobile users. *IEEE Network*, 1994.

[9] National Institute of Standards and Technology. Digital signature standard (DSS). Federal Information Processing Standards Publication FIPS PUB 186, U.S. Department of Commerce, May 1994.

[10] Moe Rahnema. Overview of the GSM system and protocol architecture. *IEEE Communications Magazine*, pages 92–100, April 1993.

[11] Didier Samfat, Refik Molva, and N. Asokan. Untraceability in mobile networks. In *Proceedings of MobiCom'95*, 1995.

[12] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[13] J. Wilkes. Privacy and authentication needs of PCS. *IEEE Personal Communications*, 2(4):11–15, 1995.

[14] Yuliang Zheng and Jennifer Seberry. Immunizing public key cryptosystems against chosen ciphertext attacks. *IEEE Journal on Selected Areas in Communications*, 11(5):715–724, June 1993.