Comments on an Optimized Protocol for Mobile Network Authentication and Security [*]

Keith M. Martin[a] *keith.martin@esat.kuleuven.ac.be*

Chris J. Mitchell[b] *C.Mitchell@rhbnc.ac.uk*

[a]Katholieke Universiteit Leuven, ESAT-COSIC, Kardinaal Mercierlaan 94, B-3001, Heverlee, Belgium
[b]Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K.

The level of network authentication and security offered by a protocol proposed in [3] is considered.

In [3] a protocol was described for providing "mutual authentication" and "key distribution" between a mobile user and a base station by means of the exchange of public key certificates. The protocol was specifically designed with the power consumption restrictions of the mobile device in mind. The authors explicitly requested interested parties to comment on the proposed protocol, and we thus provide some remarks on the authentication and security goals achieved by this particular protocol.

Setting aside the precise certificate design, the "mutual authentication and key distribution protocol" of [3] involves a very simple exchange of public key certificates. The base station accompanies its certificate with $y_m^{-x_b}K$, where y_m is the public key of the mobile user (extracted from the certificate of the mobile user), x_b is the secret key of the base station, and K is the session key (randomly generated by the base station).

We have a number of concerns, regarding both the degree of "mutual authentication" and the level of security that this process achieves. We start by considering what "authentication" it achieves.

1. *Mutual entity authentication* [2] provides assurance to both entities of the identity of the other entity involved in the protocol. This is clearly not offered by the protocol in [3] since an attacker can easily intercept a certificate and replay it on a later occasion (this attack is noted in [3] but appears not to be of concern). This problem arises because no time-varying information is used during the protocol.

2. *Key authentication* [2], sometimes called *implicit key authentication*, provides assurance that no entity other than a specifically identified entity can gain access to the key. In the protocol in [3] key authentication is provided from the base station to the mobile user, since only a possessor of x_m should be able to "decrypt" the key. There is no key authentication from the mobile user to the base station however, since the mobile user has to trust that the base station has generated the key on its own and by a suitable technique.

3. Moreover, the protocol does not provide *explicit key authentication* [2], in either direction. Although an attacker active on the user-to-base station interface should not be able to obtain access to the session key K, there is certainly nothing to stop them interfering with the transmitted key and sending on noise to the mobile user. There is no mechanism for enabling the mobile user to check that the computed key K is indeed correct.

4. Most worryingly, compromise of just one session key K leads to effective compromise of the secret key of the base station x_b. Although an attacker cannot obtain x_b, knowledge of a prior session key K' allows $y_m^{-x_b}$ to be obtained (assuming the attacker has been monitoring activity on the user-to-base station interface). The attacker can now act with impunity against the mobile user in the role of the base station in this protocol.

We conclude that the achievements of the protocol proposed in [3] seem rather limited with regards to network authentication and security. In particular we note that although the precise authentication and security goals of the protocol are not identified in [3], the achieved authentication and security goals do not strike us as strong enough for application in a real mobile network environment.

References

[1] W. Diffie and M. Hellman. New directions in cryptography. IEEE Trans. Info. Theory, 22:644–654, 1976.

[2] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 1996.

[3] X. Yi, E. Okamoto and K.Y. Lam. An optimized protocol for mobile network authentication and security. Mobile Computing and Communications Review, 2(3):37–39, 1998.

[*] This work was supported by the European Commission under ACTS project AC095 (ASPeCT).