New WAKE Key Recovery Protocol on M-commerce

Yong-ho Lee[1], Im-yeong Lee[2], and Hyung-woo Lee[3]

[1]S/W Quality Evaluation Center, Telecommunications Technology Association, Korea
abysskey@tta.or.kr
[2]Division of Information Technology Engineering, Soonchunhyang University, Korea
imylee@sch.ac.kr
[3]Dept. of Software, Hanshin University, Korea
hwlee@hanshin.ac.kr

Abstract. The ASPeCT project first tried to support the key recovery in wireless authentication and key establishment protocol Since then, a variety of protocols have been proposed. In this thesis, problems of conventional protocols are analyzed and new protocol is suggested to solve those problems.

Keywords: M-Commerce, Authentication, Key Establishment, Key Recovery

1 Introduction

The WAKE(Wireless Authentication and Key Establishment) Key Recovery protocol, which added the key recovery function to the WAKE protocol, was started by ASPeCT and is now in use for various security scenarios. In this thesis, methodologies introduced in existing researches are analyzed, the requirements of the WAKE Key Recovery protocol are derived based on the analysis, and finally, a new protocol is proposed to address the requirements.

Here, the three studies proposed so far are explained. First study, R-M WAKE Key Recovery protocol[1], proposed by Rantos and Mitchell in 1999 is hereby introduced. This is not satisfies requirements that Masquerade Attack Prevention, Public Verification of Key Recovery, Domain Extension, and Illegal Key Recovery Prevention. Second study, N-P-B-E WAKE Key Recovery protocol[2], proposed to solve problems as Masquerade Attack Prevention and Public Verification of Key Recovery of first study. Third study, K-L WAKE Key Recovery protocol[3], proposed to solve problems as Domain Extension of second study. But all conventional study is not satisfies Illegal Key Recovery Prevention.

2 Contribution

In this chapter, we propose a new wireless authentication and key establishment protocol supporting key recovery. The proposed method solves the problems of the existing wireless authentication and key establishment protocol and promotes efficiency and security, while supporting the key recovery function with a minimum level of overhead. This is consists of a total of three stages: initialization, wireless authentication and key establishment, and a key recovery stage in case of an emergency. New protocol has distinguishing mark about conventional protocols.

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 279–280, 2003.

In this proposed protocol, masquerade attack is not possible, unless all information on the user possessed by the key recovery agency and the escrow agency is disclosed. Masquerade attack is possible only when all secret information on the user, divided among the key recovery agency and the escrow agency and possessed by each other, is disclosed.

The existing protocols implement all public verification and key recovery functions by generating and using key recovery information. The new protocol is constructed, however, so that the process for public verification of key recovery is implemented separately. A unique feature of this is that to implement public verification of key recovery, it utilizes all the information that the key recovery agency, the escrow agency, and the user make public individually.

This proposed protocol assumes two users belonging to the same domain. When a domain is extended into multiple domains, additional information is used to solve any problem.

In this proposed protocol, each of two key recovery informations is put in escrow by the key recovery agency and the escrow agency. Illegal key recovery is thus prevented, unless the two agencies illegally confer with each other. To prevent this occurrence, a number of escrow agencies may be considered. The key recovery information is divided into two in this thesis in order to emphasize the different roles of the key recovery agency and the escrow agency.

Table 1. Compare among protocols

	R-M protocol	N-P-B-E protocol	K-L protocol	Proposal protocol
Public Verification of Key Recovery	**X**	O	O	**O**
Masquerade Attack Prevention	**X**	O	O	**O**
Domain Extension	**X**	**X**	O	**O**
Illegal Key Recovery Prevention	**X**	**X**	**X**	**O**

3 Conclusion

In this thesis, we consider that problems and requirement of WAKE Key Recovery protocol. The proposed protocol is proven to be much better in security and efficiency than existing protocols.

References

[1] K. Rantos and C. Mitchell, Key Recovery in ASPeCT Authentication and Initialization of Payment protocol, ACTS Mobile Summit, 1999

[2] J. Nieto, D. Park, C. Boyd, and E. Dawson, Key Recovery in Third Generation Wireless Communication System, PKC2000, Springer-Verlag, pp.223–237, 2000

[3] ChongHee Kim and PilJoong Lee, New Key Recovery in WAKE Protocol, PKC2001, Springer-Verlag, pp.325–338, 2001