Revisiting Lee, Kim, & Yoo Authenticated Key Agreement Protocol

Kim-Kwang Raymond Choo

Information Security Institute, Queensland University of Technology
GPO Box 2434, Brisbane, QLD 4001, Australia (Email: k.choo@qut.edu.au)

(Received Aug. 9, 2005; revised and accepted Sep. 12, 2005)

Abstract

In recent issue of Journal of Applied Mathematics and Computation (2005), Lee, Kim, & Yoo revealed an attack on Hsu, Wu, & Wu (2003) authenticated key agreement protocol, and then presented an improved protocol. However, Lee, Kim, & Yoo (2005) present only heuristic argument with no formal proof of security. In this work, we revealed previously unpublished flaw in the protocol. We may speculate that such errors could have been found by protocol designers if proofs of security were to be constructed, and hope this work will encourage future protocol designers to provide proofs of security. We conclude with a countermeasure due to Choo, Boyd, & Hitchcock (2005).

Keywords: Key agreement protocols, provable security, password-based protocols

1 Introduction

With the velocity of technological advances in today's globalising electronic commerce landscape, cryptographic protocols are the *sine qua non* of many diverse secure electronic commerce applications. Although technology advances have brought us many conveniences and benefits, they have also resulted in the erosion of many assumptions about the design of cryptographic protocols, which began in the 1970s. As a result, the environment for cryptographic protocols has changed drastically over the years. One thing that does not change with time is that the design of cryptographic protocols is still notoriously hard. The difficulties associated in obtaining a high level of assurance in the security of almost any new or even existing protocols are well illustrated with examples of errors found in many such protocols years after they were published [1, 2, 3, 4, 10, 18, 19, 20, 22, 23, 26, 28, 37, 38, 40, 41, 42, 43, 44].

The many flaws discovered in published protocols for key establishment and authentication over many years, have promoted the use of formal models (i.e., the computer security approach [27, 34, 35]) and rigorous security proofs (i.e., the computational complexity approach [5, 6, 7, 8, 9, 12, 13, 14, 15, 39]). The computer security approach concentrates on designing tools to formally verify the security of cryptographic protocols while the computational complexity approach concentrates on designing provably secure protocols.

1.1 Computer Security Approach

Emphasis in the computer security approach is placed on automated machine specification and analysis (e.g., model checking and theorem proving). The Dolev & Yao [25] adversarial model is the de-facto model used in formal specifications, where cryptographic operations are often used in a "black box" fashion ignoring the various cryptographic properties, resulting in possible loss of partial information. One of the main obstacles in this automated approach is the undecidability and intractability problems since the adversary can have an exponentially large set of possible actions (or combinations) which result in a state explosion [16]. Furthermore, protocols proven secure in such a manner could possibly be flawed (i.e., giving a false positive result – analogous to a Type II error in hypothesis testing). From a real world practicality perspective, it is debatable whether proofs of security in this manner carry significant weight in the real world, due to their idealistic model. However, the computer security approach should be credited for proving insecurities in protocols (i.e., finding both known and previously unknown flaws in protocols).

1.2 Computational Complexity Approach

On the other hand, the computational complexity approach adopts a deductive reasoning process (i.e., the logical process of deriving a conclusion from a known premise) whereby the emphasis is placed on a proven reduction from the problem of breaking the protocol to another problem believed to be hard. Since the initiative

$A\ (Pwd_{AB}, Q, Q^{-1})$		$B\ (Pwd_{AB}, Q, Q^{-1})$
$a \in_R \mathbb{Z}_q$		$b \in_R \mathbb{Z}_q$
$X_1 = g^{aQ} \oplus Q\ mod\ n$	$\xrightarrow{X_1}$	$Y_1 = g^{bQ} \oplus Q\ mod\ n$
$SK_A = (Y_1 \oplus Q)^{aQ^{-1}} = g^{ab}\ mod\ n$	$\xleftarrow{Y_1}$	$SK_B = (X_1 \oplus Q)^{bQ^{-1}} = g^{ab}\ mod\ n$
	$SK_A = g^{ab}\ mod\ n = SK_B$	

Figure 1: Lee, Kim, & Yoo (2005) authenticated key agreement protocol

of Bellare & Rogaway [6] who provided the first treatment of computational complexity to cryptographic protocol analysis, more than 100 protocols with accompanying computational proofs of security have been proposed in the literature [17]. Although these proofs provide a strong assurance for arguing about the security properties of the protocols, it is often difficult to obtain correct computational proofs of security. Furthermore, such proofs usually entail lengthy and complicated mathematical proofs, which are daunting to most reader as suggested by Koblitz & Menezes [29, 30]. A supporting example is the well-known example of OAEP mode for public key encryption [40]. Despite its popularity and inclusion in the SET electronic payment standard of MasterCard and Visa, a problem was found (and subsequently fixed in the case of RSA) years later. Difficulties in obtaining correct computational proofs of protocol security are evidenced by the breaking of provable-secure protocols after they were published. Despite these setbacks, proofs are invaluable tools for arguing about security and certainly are one very important tool in getting protocols right [18].

1.3 Case Study

In this work, we advocate the importance of proofs of protocol security and the proposal of any protocol should provide a rigorous proof of security as we argue that protocols without any computational proofs of security leads one to question the level of trust in the correctness in such protocols. We use the authenticated key agreement protocol of Lee, Kim, & Yoo [33] as a case study. We then demonstrated previously unknown flaw in the protocol.

1.4 Organization of Paper

The remainder of this paper is structured as follows: Section 2 describe the key agreement protocol of Lee, Kim, & Yoo [33] that will be used as case study. A previously unpublished attack on this protocol is revealed and a countermeasure is presented. Section 3 presents the conclusions.

2 Lee, Kim, & Yoo (2005) Authenticated Key Agreement Protocol

Figure 1 describes the key agreement protocol of Lee, Kim, & Yoo [33]. There are two communicating principals in the protocol, namely A and B. Both A and B are assumed to share a secret password, Pwd_{AB}, and integers, $Q\ mod\ n$ and $Q^{-1}\ mod\ n$, are computed in some predetermined manner from Pwd_{AB}. The system parameters are n and g, where n is a large prime and g is a generator of order $n-1$ of $GF(n)$. In the protocol, the notation $a \in_R \mathbb{Z}_q$ denotes that a is randomly drawn from $\mathbb{Z}_q$.

At the end of the protocol execution, both A and B will share a common secret session key, $SK_A = g^{ab}\ mod\ n = SK_B$.

2.1 A Reflection Attack

Figure 2 describes the execution of Lee, Kim, & Yoo (2005) authenticated key agreement protocol in the presence of a malicious adversary, $\mathcal{A}$. Let $\mathcal{A}_U$ denotes the adversary impersonating some user, U.

At the end of the protocol execution shown in Figure 2, A has accepted two session keys, SK_A and $SK_{A(S2)}$, which A believes that both keys are shared with B in different sessions, as explained below:

- SK_A is being used in the session where A is the initiator and
- $SK_{A(S2)}$ is being used in the session (S2) where A is the responder.

We observe that both session keys accepted by A, SK_A and $SK_{A(S2)}$, are of the same value, as shown below:

$$\begin{aligned} SK_A &= (X_1 \oplus Q)^{a_{S2} Q^{-1}} \\ &= g^{a a_{S2}}\ mod\ n \\ SK_{A(S2)} &= (X_2 \oplus Q)^{aQ^{-1}} \\ &= g^{a a_{S2}}\ mod\ n \\ &= SK_A. \end{aligned}$$

A		$\mathcal{A}_B$
$a \in_R \mathbb{Z}_q$	$\xrightarrow{X_1 = g^{aQ} \oplus Q \; mod \; n}$	Intercept message meant for B
$a_{S2} \in_R \mathbb{Z}_q$	$\xleftarrow{S2 : X_1}$	Reflect message back to A and start concurrent session
	$\xrightarrow{S2 : X_2 = g^{a_{S2}Q} \oplus Q \; mod \; n}$	Intercept message meant for B
	$\xleftarrow{X_2}$	Reflect message back to A
$SK_A = (X_1 \oplus Q)^{a_{S2}Q^{-1}}$		
$SK_{A(S2)} = (X_2 \oplus Q)^{aQ^{-1}}$		

Figure 2: Execution of Lee, Kim, & Yoo (2005) authenticated key agreement protocol in the presence of a malicious adversary

However, B is unaware of any of these sessions, and the adversary, $\mathcal{A}$, is able to trivially expose any of this key to obtain the other fresh session key. Such an attack is known as a *reflection attack* and is realistic in the real world, as some party might want to establish a secure channel with itself (e.g., a mobile user that communicates to its desktop computer, while both the mobile device and the desktop have the same identity in the form of the same digital certificate) as described by Krawczyk [32].

The countermeasures are well studied and we may adopt the same approach by Choo, Boyd, & Hitchcock [21], who suggest that

- Including the identities of the participants and their roles in the key derivation function provides resilience against unknown key share attacks [11, Chapter 5.1.2] and reflection attacks [31], and
- Including the transcripts in the key derivation function provides freshness and data origin authentication.

Hence, we propose to include the sender's and responder's identities and transcripts, $\mathcal{T}_U$ (i.e., concatenation of all messages sent and received), in the key derivation function, which will (effectively) bind the session key to all messages sent and received by both A and B, as shown below:

$$\begin{aligned} SK_{A(Fixed)} &= \mathcal{H}(A||B||\mathcal{T}_A||(Y_1 \oplus Q)^{aQ^{-1}}) \\ SK_{B(Fixed)} &= \mathcal{H}(A||B||\mathcal{T}_B||(X_1 \oplus Q)^{bQ^{-1}}) \\ &= SK_{A(Fixed)}, \end{aligned}$$

where $\mathcal{H}$ denotes a secure hash function [24, 36] and $||$ denotes the concatenation of messages.

Intuitively, the reflection attack outlined in Figure 2 is no longer valid, since

$$\begin{aligned} SK_{A(Fixed)} &= \mathcal{H}(A||B||\mathcal{T}_A||((X_1 \oplus Q)^{a_{S2}Q^{-1}})) \\ &= \mathcal{H}(A||B||\mathcal{T}_A||(g^{aa_{S2}} \; mod \; n)) \\ SK_{A(S2)(Fixed)} &= \mathcal{H}(B||A||\mathcal{T}_B||((X_2 \oplus Q)^{aQ^{-1}})) \\ &= \mathcal{H}(B||A||\mathcal{T}_B||(g^{aa_{S2}} \; mod \; n)) \\ &\neq SK_{A(Fixed)}. \end{aligned}$$

3 Conclusion

Through a detailed study of the authenticated key agreement protocol of Lee, Kim, & Yoo [33], we demonstrated previously unpublished flaw in the protocol where the latter does not have accompanying proof of security. Proofs are invaluable for arguing about security and certainly are one very important tool in getting protocols right [18]. Without proofs of security, protocol implementers cannot be assured about the security properties of protocols. Flaws in protocols discovered after they were published or implemented certainly will have a damaging effect on the trustworthiness and the credibility of key establishment protocols in the real world. As a result of this work, we would recommend that protocol designers provide proofs of security for their protocols, in order to assure protocol implementers about the security properties of protocols.

Acknowledgements

This work was partially funded by the Australian Research Council Discovery Project Grant DP0345775.

References

[1] F. Bao, "Security analysis of a password authenticated key exchange protocol," in *6th Information Security Conference - ISC 2003*, LNCS 2851, pp. 208–217, Springer-Verlag, 2003.

[2] F. Bao, "Colluding attacks to a payment protocol and two signature exchange schemes," in *Advances in Cryptology - Asiacrypt 2004*, LNCS 3329, pp. 417–429, Springer-Verlag, 2004.

[3] D. A. Basin, S. Mödersheim, and L. Viganó, *An On-the-fly Model-checker for Security Protocol Analysis*, Technical Report 404, Information Security Group, ETH Zentrum, 2003.

[4] D. A. Basin, S. Mödersheim, and L. Viganó, "An on-the-fly model-checker for security protocol analysis," in *8th European Symposium on Research in*

Computer Security - ESORICS 2003, LNCS 2808, pp. 253–270, Springer-Verlag, 2003.

[5] M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols," in *30th ACM Symposium on the Theory of Computing - STOC 1998*, pp. 419–428, ACM Press, 1998.

[6] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Advances in Cryptology - Crypto 1993*, LNCS 773, pp. 110–125, Springer-Verlag, 1993.

[7] M. Bellare and P. Rogaway, "Provably secure session key distribution: The three party case," in *27th ACM Symposium on the Theory of Computing - STOC 1995*, pp. 57–66, ACM Press, 1995.

[8] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *6th IMA International Conference on Cryptography and Coding*, LNCS 1355, pp. 30–45, Springer-Verlag, 1997.

[9] S. Blake-Wilson and A. Menezes, "Security proofs for entity authentication and authenticated key transport protocols employing asymmetric techniques," in *Security Protocols Workshop*, LNCS 1361, pp. 137–158, Springer-Verlag, 1997.

[10] D. Bleichenbacher, "Breaking a cryptographic protocol with pseudoprimes," in *Public Key Cryptography - PKC 2005*, LNCS 3386, pp. 9–15, Springer-Verlag, 2005.

[11] C. Boyd and A. Mathuria, *Protocols for Authentication and Key Establishment*, Springer-Verlag, June 2003.

[12] R. Canetti, *Universally Composable Security: A New Paradigm for Cryptographic Protocols*, Cryptology ePrint Archive, Report 2000/067, 2000. `http://eprint.iacr.org/2000/067/`.

[13] R. Canetti and M. Fischlin, "Universally composable commitments," in *Advances in Cryptology – Crypto 2001*, LNCS 2139, pp. 19–40, Springer-Verlag, 2001.

[14] R. Canetti, S. Halevi, J. Katz, Y. Lindell, and P. MacKenzie, "Universally composable password-based key exchange (extended version available from `http://eprint.iacr.org/2005/196`)," in *Advances in Cryptology - Eurocrypt 2005*, LNCS 3494, pp. 404–421, Springer-Verlag, 2005.

[15] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels (extended version available from `http://eprint.iacr.org/2001/040/`)," in *Advances in Cryptology - Eurocrypt 2001*, LNCS 2045, pp. 453–474, Springer-Verlag, 2001.

[16] I. Cervesato, N. Durgin, P. D. Lincoln, J. C. Mitchell, and A. Scedrov, "A meta-notation for protocol analysis," in *12th Computer Security Foundations Workshop - CSFW 1999*, pp. 55–71. IEEE Computer Society Press, 1999.

[17] K.-K. R. Choo, "The provably-secure key establishment and mutual authentication protocols lounge, `http://sky.fit.qut.edu.au/~choo/lounge.html`,", 2005.

[18] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "Errors in computational complexity proofs for protocols (available from `http://sky.fit.qut.edu.au/~choo/publication.html`)," in *(Accepted to appear in) Advances in Cryptology - Asiacrypt 2005*, Lecture Notes in Computer Science, Springer-Verlag, 2005.

[19] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "Examining indistinguishability-based proof models for key establishment protocols (extended version available from `http://eprint.iacr.org/2005/270`)," in *(Accepted to appear in) Advances in Cryptology - Asiacrypt 2005*, Lecture Notes in Computer Science, Springer-Verlag, 2005.

[20] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "The importance of proofs of security for key establishment protocols: Formal analysis of jan–chen, yang–shen–shieh, kim–huh–hwang–lee, lin–sun–hwang, & yeh–sun protocols (extended version available from `http://eprints.qut.edu.au/perl/user_eprints?userid=51`)," *(To appear in) Journal of Computer Communications - Special Issue of Internet Communications Security*, 2005.

[21] K.-K. R. Choo, C. Boyd, and Y. Hitchcock, "On session key construction in provably secure protocols," in *1st International Conference on Cryptology in Malaysia - Mycrypt 2005*, LNCS 3715, pp. 116–131, Springer-Verlag, 2005.

[22] K.-K. R. Choo, C. Boyd, Y. Hitchcock, and G. Maitland, "On session identifiers in provably secure protocols: The bellare-rogaway three-party key distribution protocol revisited (extended version available from `http://eprint.iacr.org/2004/345`)," in *4th Conference on Security in Communication Networks - SCN 2004*, LNCS 3352, pp. 352–367, Springer-Verlag, 2004.

[23] K.-K. R. Choo and Y. Hitchcock, "Security requirements for key establishment proof models: Revisiting bellare–rogaway and jeong–katz–lee protocols (extended version available from `http://sky.fit.qut.edu.au/~choo/publication.html`)," in *10th Australasian Conference on Information Security and Privacy - ACISP 2005*, LNCS 3574, pp. 429–442, Springer-Verlag, 2005.

[24] I. Damgård, "A design principle for hash functions," in *Advances in Cryptology - Crypto 1989*, LNCS 435, pp. 416–427, Springer-Verlag, 1989.

[25] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transaction of Information Technology*, vol. 29, no. 2, pp. 198–208, 1983.

[26] B. Donovan, P. Norris, and G. Lowe, "Analyzing a library of security protocols using Casper and FDR," in *Workshop on Formal Methods and Security Protocols*, 1999.

[27] C. J. Fidge, *A Survey of Verification Techniques for Security Protocols*, Technical Report 01-22, Software Verification Research Centre, The University of Queensland, Brisbane, 2001.

[28] B. S. Kaliski, "An unknown key-share attack on the mqv key agreement protocol," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 275–288, 2001.

[29] N. Koblitz and A. Menezes, "Another look at "provable security",". Cryptology ePrint Archive, Report 2004/152, 2004. `http://eprint.iacr.org/2004/152/`.

[30] N. Koblitz and A. Menezes, *Another Look at "Provable Security"*, Technical Report CORR 2004-20, Centre for Applied Cryptographic Research, University of Waterloo, Canada, 2004.

[31] H. Krawczyk, "Sigma: The 'sign-and-mac' approach to authenticated diffie-hellman and its use in the ike-protocols," in *Advances in Cryptology - Crypto 2003*, LNCS 2729, pp. 400–425, Springer-Verlag, 2003.

[32] H. Krawczyk, "Hmqv: A high-performance secure diffie-hellman protocol (extended version available from `http://eprint.iacr.org/2005/176/`)," in *Advances in Cryptology - Crypto 2005*, LNCS 3621, pp. 546–566, Springer-Verlag, 2005.

[33] S.-W. Lee, H.-S. Kim, and K.-Y. Yoo, "Improvement of lee and lee's authenticated key agreement scheme," *Journal of Applied Mathematics and Computation*, vol. 162, pp. 1049–1053, 2005.

[34] C. Meadows, "Open issues in formal methods for cryptographic protocol analysis," in *DARPA Information Survivability Conference and Exposition*, vol. 2052, pp. 237–250, IEEE Computer Society Press, 2000.

[35] C. Meadows, "Formal methods for cryptographic protocol analysis: Emerging issues and trends," *IEEE Journal on Selected Area in Communications*, vol. 21, no. 1, pp. 44–54, 2003.

[36] R. Merkle, "One way hash functions and DES," in *Advances in Cryptology - Crypto 1989*, LNCS 435, pp. 428–446, Springer-Verlag, 1989.

[37] J. Nam, S. Kim, and D. Won, "Attacks on bresson-chevassut-essiari-pointcheval's group key agreement scheme," Cryptology ePrint Archive, Report 2004/251, 2004. `http://eprint.iacr.org/2004/251/`.

[38] K. Shim, "Cryptanalysis of mutual authentication and key exchange for low power wireless communications," *IEEE Communications Letters*, vol. 7, no. 5, pp. 248–250, 2003.

[39] V. Shoup, *On Formal Models for Secure Key Exchange (version 4)*, Technical Report RZ 3120 (#93166), IBM Research, Zurich, 1999.

[40] V. Shoup, "Oaep reconsidered," in *Advances in Cryptology - Crypto 2001*, LNCS 2139, pp. 239–259, Springer-Verlag, 2001.

[41] Z. Wan and S. Wang, "Cryptanalysis of two password-authenticated key exchange protocols," in *9th Australasian Conference on Information Security and Privacy - ACISP 2004*, LNCS 3108, pp. 164–175, Springer-Verlag, 2004.

[42] J. M. Wing, "A symbiotic relationship between formal methods and security," in *Workshops on Computer Security, Fault Tolerance, and Software Assurance: From Needs to Solution*, IEEE Computer Press, 1998.

[43] D. S. Wong and A. H. Chan, "Efficient and mutually authenticated key exchange for low power computing devices," in *Advances in Cryptology - Asiacrypt 2001*, LNCS 2248, pp. 172–289, Springer-Verlag, 2001.

[44] M. Zhang, "Breaking an improved password authenticated key exchange protocol for imbalanced wireless networks," *IEEE Communications Letters*, vol. 9, no. 3, pp. 276–278, 2005.

Kim-Kwang Raymond Choo received his BSc Maths, BAppSci (Hons) Industrial & Applied Maths, and Master of Information Technology degrees in Dec 2000, Dec 2002, and May 2002 respectively. He is currently a full-time Ph.D. candidate with Information Security Institute, Queensland University of Technology, Australia; and a part-time MBA student with the University of Queensland, Australia. His research interests include formal specification and analysis of key establishment protocols, and provably-secure protocols. He is a member of IEEE Computer Society and Formal Methods Europe, and a Computer Graduate Member of the Society for Industrial & Applied Maths (SIAM).