Willy Susilo
Joseph K. Liu
Yi Mu (Eds.)

LNCS 4784

Provable Security

First International Conference, ProvSec 2007
Wollongong, Australia, November 2007
Proceedings

Springer

Willy Susilo Joseph K. Liu
Yi Mu (Eds.)

Provable Security

First International Conference, ProvSec 2007
Wollongong, Australia, November 1-2, 2007
Proceedings

Springer

Volume Editors

Willy Susilo
University of Wollongong
School of Computer Science and Software Engineering
Wollongong NSW 2522, Australia
E-mail: wsusilo@uow.edu.au

Joseph K. Liu
Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613, Singapore
E-mail: ksliu@i2r.a-star.edu.sg

Yi Mu
University of Wollongong
School of Computer Science and Software Engineering
Wollongong NSW 2522, Australia
E-mail: ymu@uow.edu.au

Library of Congress Control Number: 2007937100

CR Subject Classification (1998): D.4.6, E.3, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-75669-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75669-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12172443 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4784

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4784: W. Susilo, J.K. Liu, Y. Mu (Eds.), Provable Security. X, 237 pages. 2007.

Vol. 4779: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.), Information Security . XIII, 437 pages. 2007.

Vol. 4752: A. Miyaji, H. Kikuchi, K. Rannenberg (Eds.), Advances in Information and Computer Security. XIII, 460 pages. 2007.

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B. M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4356: E. Biham, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

Preface

The First International Conference on Provable Security 2007 (ProvSec 2007) was held in Wollongong, Australia, November 1–2, 2007. The conference was sponsored by iCORE Information Security Laboratory and RNSA (Research Network for a Secure Australia). We are grateful to these organizations for their support of the conference.

The conference proceedings, representing both full papers and short papers, were published in time for the conference in this volume of Lecture Notes in Computer Science series by Springer. This year the program committee invited an international keynote speaker: Colin Boyd from Queensland University of Technology, Australia. Prof. Boyd's talk addressed the topic of "On One-Pass Key Establishment".

The Program Committee received 51 submissions. Ten submissions were selected for full paper presentation and seven were selected for short paper presentation. The reviewing process was run using the iChair software, written by Thomas Baignères and Matthieu Finiasz (EPFL, Switzerland). It took seven weeks; each paper was carefully evaluated by at least three members of the Program Committee. We appreciate the hard work of the members of the Program Committee and the external referees, who gave many hours of their valuable time.

We would like to thank all the people involved in organizing this conference. In particular we would like to thank the General Chair Yi Mu, the Organizing Committee Man Ho Au and Xinyi Huang and the Webmaster, Lan Zhou, for their time and efforts.

Finally, we would like to thank all authors for submitting interesting new research papers to ProvSec, providing us with an embarrassment of riches out of which we could only accept a total of 17 contributed papers, even though many more would have been worth publishing.

November 2007

Willy Susilo
Joseph K. Liu

First International Conference on Provable Security 2007 (ProvSec 2007)

General Chair

Yi Mu	University of Wollongong, Australia

Program Chairs

Willy Susilo	University of Wollongong, Australia
Joseph K. Liu	Institute for Infocomm Research, Singapore

Program Committee

Joonsang Baek	Institute for Infocomm Research, Singapore
Feng Bao	Institute for Infocomm Research, Singapore
Emmanuel Bresson	CELAR, France
Xavier Boyen	Voltage Inc., Palo Alto, USA
Liqun Chen	Hewlett-Packard Laboratories, UK
Kim-Kwang Raymond Choo	Australian Institute of Criminology, Australia
Sherman S.M. Chow	New York University, USA
Nelly Fazio	IBM Almaden Research Centre, USA
Dengguo Feng	Chinese Academy of Sciences, China
David Galindo	University of Nijmegen, Netherlands
Craig Gentry	Stanford University, USA
Swee-Huay Heng	Multimedia University, Malaysia
Marc Joye	Thomson R&D, France
Eike Kiltz	CWI, Netherlands
Kwangjo Kim	ICU, Korea
Fabien Laguillaumie	University of Caen, France
Benoit Libert	UCL, Belgium
Javier Lopez	University of Malaga, Spain
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Chanathip Namprempre	Thammasat University, Thailand
Miyako Ohkubo	Information-Technology Promotion Agency, Japan
Tatsuaki Okamoto	NTT Labs, Japan
Juanma Gonzalez Nieto	Queensland University of Technology, Australia
Duong Hieu Phan	France Telecom R&D and University of Paris 8, France

Raphael C.W. Phan	EPFL, Switzerland
Josef Pieprzyk	Macquarie University, Australia
Pascal Paillier	Gemplus, Security Technology Department, France
David Pointcheval	CNRS and ENS, France
Jean-Jacques Quisquater	UCL CryptoGroup, Belgium
Rei Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Alice Silverberg	U.C. Irvine, USA
Martijn Stam	EPFL, Switzerland
Ron Steinfeld	Macquarie University, Australia
Tsuyoshi Takagi	Future University-Hakodate, Japan
Damien Vergnaud	b-it, Computer Security Group (Bonn), Germany
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan S. Wong	City University of Hong Kong, Hong Kong
Fangguo Zhang	Sun Yat-sen University, China

Organizing Committee

Man Ho Au	University of Wollongong, Australia
Xinyi Huang	University of Wollongong, Australia
Lan Zhou	University of Wollongong, Australia

External Referees

Masayuki Abe
Mohamad Yusoff Alias
Patrick Amon
Vivien Dubois
Georg J. Fuchsbauer
Emeline Hufschmitt
Sozo Inoue
Marcelo Kaihara
Tadayoshi Kohno
Shinichiro Matsuo
Yoichi Omori
Olivier Pereira
Masaaki Shirase
Masakazu Soshi
Francois-Xavier Standaert
Xiaojian Tian
Elvis Tombini
Bogdan Warinschi
Yuji Watanabe
Go Yamamoto
Guomin Yang
Wei-Chuen Yau

Table of Contents

Authentication

Asymmetric Encryption

Signature

Protocol and Proving Technique

Authentication and Symmetric Encryption (Short Papers)

Signature (Short Papers)

Asymmetric Encryption (Short Papers)

Stronger Security of Authenticated Key Exchange

Brian LaMacchia[1], Kristin Lauter[2], and Anton Mityagin[3]

[1] Microsoft Corporation, 1 Microsoft Way, Redmond, WA
bal@microsoft.com
[2] Microsoft Research, 1 Microsoft Way, Redmond, WA
klauter@microsoft.com
[3] Microsoft Live Labs, 1 Microsoft Way, Redmond, WA
mityagin@microsoft.com

Abstract. Recent work by Krawczyk [12] and Menezes [16] has highlighted the importance of understanding well the guarantees and limitations of formal security models when using them to prove the security of protocols. In this paper we focus on security models for authenticated key exchange (AKE) protocols. We observe that there are several classes of attacks on AKE protocols that lie outside the scope of the Canetti-Krawczyk model. Some of these additional attacks have already been considered by Krawczyk [12]. In an attempt to bring these attacks within the scope of the security model we extend the Canetti-Krawczyk model for AKE security by providing significantly greater powers to the adversary. Our contribution is a more compact, integrated, and comprehensive formulation of the security model. We then introduce a new AKE protocol called NAXOS and prove that it is secure against these stronger adversaries.

1 Introduction

In this paper we extend the Canetti-Krawczyk [11,12] security model for authenticated key exchange (AKE) to capture attacks resulting from leakage of ephemeral and long-term secret keys. Our security model for authenticated key exchange is defined in the spirit of Bellare and Rogaway [3] and Canetti and Krawczyk [11] by an experiment in which the adversary is given many corruption powers for various key exchange sessions and must solve a challenge on a test session. We extend adversarial capabilities to the following extent: the only corruption powers we do not give an adversary in the experiment are those that would trivially break an AKE protocol. We also define a new AKE protocol which is secure in our new model.

More specifically, in an authenticated key exchange protocol, two parties exchange information and compute a secret key as a function of at least four pieces of secret information: their own long-term (static) and ephemeral secret keys and the other party's long-term and ephemeral secret keys. Of the four pieces of

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 1–16, 2007.

information, we allow an adversary to *reveal*[1] any subset of the four which does not contain both the long-term and ephemeral secrets of one of the parties. To explain this more precisely, we divide AKE test sessions (sessions which are subject to attack by an adversary) into two types. In sessions of the first type ("passive" sessions), the adversary does not cancel or modify communications between the two parties. In sessions of the second type ("active" sessions), the adversary may forge the communication of the second party. Another way to phrase the distinction, as done by Krawczyk in the analysis of the HMQV protocol [12], is whether the adversary actively intervenes in the key exchange session or is a passive eavesdropper.

In addition to distinguishing between passive and active sessions, we identify which pieces of secret information the adversary can reveal without being able to trivially break the AKE protocol (compute the session key for any AKE protocol). In both types of sessions, if an adversary can reveal the long-term and the ephemeral secret keys of one of the parties in the session, then the adversary can trivially compute a session key as it has all the secret information of one of the legitimate parties in the session.

For passive sessions, an adversary may reveal both ephemeral secret keys, both long-term secret keys, or one of each from the two different parties without trivially breaking the protocol. Thus security in our model implies weak Perfect Forward Secrecy, defined by Krawczyk to be security against revelation of long-term secret keys after the session is completed (without active adversarial intervention in the session establishment).

For active sessions, the adversary may forge communications from one of the parties. Thus, if the adversary can also reveal the long-term secret key of that same party, then the adversary can trivially compute the session key. The same argument was used by Krawczyk to show that no 2-round AKE protocol can achieve full perfect forward secrecy (PFS). Still, an adversary can reveal a long-term secret key or ephemeral secret key of the other party without trivially breaking the session. So for another example, our extension to the Canetti-Krawczyk model also implies security against Key Compromise Impersonation (KCI) attacks, where the adversary first reveals a long-term secret of a party and then impersonates others to this party.

Considering attacks involving both types of sessions, it is natural to define a single security model which captures all of them. In our model, in passive test sessions we allow the adversary to reveal any subset of the four pieces of secret information which does not contain both the long-term and ephemeral secrets of one of the parties. In active test sessions, we allow the adversary to reveal only the long-term secret or the ephemeral secret key of the party which is executing the test session. In our security experiment, a test session is still considered *clean* even if the adversary has revealed any of the allowable combinations of secret keys of the two parties.

[1] We say that an adversary "reveals" a piece of secret information when that adversary chooses to learn the value of that information by performing the corresponding key reveal query as defined in Section 3.2.

Security in this extended Canetti-Krawczyk model also implies security against a number of other attacks not covered by the Canetti-Krawczyk model (see Section 2.2). In a sense, our model is just an extension of an instance of the Canetti-Krawczyk model, since we define the session state of a party to be the ephemeral secret key. On the other hand, *some* instance of the Canetti-Krawczyk model must be chosen when considering the security of any protocol, since the definition of the session-state reveal query must be specified, and our model is stronger than a model which does not include the ephemeral secret key as part of the session state for the session state reveal query. In addition, the Canetti-Krawczyk model does not allow the adversary to attack sessions against which a session state reveal query has been made. They consider such sessions broken, while our definition covers the security of these partially corrupted sessions. Krawczyk does extend the model in [12], but still some attacks are not covered because those sessions are not considered clean. Our model extends the notion of a clean session further, giving the adversary more power to reveal long-term and ephemeral secret keys. Our motivation to include revelations of ephemeral secret keys in the model comes from "practical" (i.e. engineering) considerations and scenarios such as active adversarial attacks or compromise of the random number generator (RNG) used by one of the parties.

We stress that our extension of the security model allows the adversary to register arbitrary public keys for adversary-controlled parties without any checks such as proof-of-possession done by the certificate authority. In contrast, some of the protocols in the literature [13,14] were proved secure assuming that the key registration is done honestly. Namely, that initially a trusted party generates keys for all, even adversary-controlled parties.

Finally, we present a new AKE protocol, called NAXOS, which provably meets our definition of AKE security. We prove the security of NAXOS under the standard Gap Diffie-Hellman assumption. We also improve the concrete security of NAXOS under the related Pairing Diffie-Hellman assumption. A version of the NAXOS protocol with key confirmation is also possible.

In Figure 1 we compare the efficiency and security of NAXOS with four other recent authenticated key exchange protocols: HMQV, KEA+ [15], protocol $\mathcal{TS}3$ by Jeong, Katz and Lee [13] and Kudla-Paterson [14][2]. The second column in the table, "Efficiency," lists the relative efficiency of the protocol as measured by the number of exponentiations executed by one party. (Communication costs in all of these protocols, except for Jeong-Katz-Lee, is the same as in the original Diffie-Hellman protocol.) Column 3, "Key Registration," specifies whether adversary-controlled parties can register arbitrary public keys or if honest key-registration is assumed. The fourth column, labeled "Ephemeral," indicates whether an adversary is allowed to reveal ephemeral secret information of the parties. Column 5 lists

[2] Kudla and Paterson [14] define partnership via matching session identifiers (computed by the parties), although for their protocol this appears to be equivalent to matching conversations.

Protocol	Effic.	Key Reg.	Ephemeral	Security	Assumptions
NAXOS	4	Arbitrary	yes	Extended CK	GDH (or PDH) + RO
HMQV	2.5	Arbitrary	yes	CK + wPFS + KCI	GDH + KEA1 + RO
KEA+	3	Arbitrary	yes	CK + wPFS + KCI	GDH (or PDH) + RO
Jeong-Katz-Lee	3	Honest	no	BR + wPFS	DDH + secure MACs
Kudla-Paterson	3	Honest	no	BR + KCI	GDH + RO

Fig. 1. Comparison of recent AKE protocols

the security model for each protocol[3]. Finally, the sixth column ("Assumptions") lists the security assumptions upon which each protocol depends[4]. We refer the reader to Chapter 7 of [6] for a good overview of Diffie-Hellman assumptions.

We begin with a brief review in Section 2 of the Canetti-Krawczyk security model and discuss some attacks not covered by their definition in Section 2.2. We introduce our extension of the Canetti-Krawczyk security model in Section 3. In Section 4 we describe the NAXOS protocol and prove its security in the extended model.

2 Previous Models

2.1 Overview of the Canetti-Krawczyk Model

The Canetti-Krawczyk security model is among a family of security models for authenticated key exchange that includes those of Bellare and Rogaway [3,5] and Bellare, Pointcheval and Rogaway [2]. We refer the reader to Choo et al. [9] for a concise summary of the differences among these various models. We give a high-level overview of the Canetti-Krawczyk model and introduce some notation which will be useful later in the paper. We remark that the model we describe differs from the original definition in that we use session identifiers defined via matching conversations. The same definition was used by Krawczyk when analyzing the security of the HMQV protocol [12] and it is now a commonly used variant of the Canetti-Krawczyk model.

The AKE security experiment involves multiple honest parties and an adversary $\mathcal{M}$ connected via an unauthenticated network. The adversary selects parties to execute key-exchange sessions and selects an order in which the sessions will be executed. Actions the adversary is allowed to perform include taking full

[3] CK denotes Canetti-Krawczyk security without perfect forward secrecy, assuming that partnership is defined via matching conversations. BR denotes the Bellare-Rogaway model [3], which appears to be equivalent to the Canetti-Krawczyk model with no ephemeral reveals allowed and key-registration done honestly [9]. KCI denotes security against key-compromise impersonation. wPFS denotes weak perfect forward secrecy. Extended CK denotes our extension of the Canetti-Krawczyk model.

[4] RO – random oracle model [4], DDH – Decisional Diffie-Hellman, GDH – Gap Diffie-Hellman [17], PDH – Pairing Diffie-Hellman [15] and KEA1 – knowledge of exponent assumption [1].

control of any party (a Corrupt query), revealing the session key of any session (a Reveal query), or revealing session-specific secret information of any session (a Session-State Reveal query).

We stress that an AKE session is executed by a single party: since all communication is controlled by an adversary, a party executing a session cannot know for sure with whom it is communicating. The party executing the session is called the *owner* of the session and the other party is called the *peer*. The *matching session* to an AKE session (by the owner with the peer) is the corresponding AKE session which is supposed to be executed by the peer with the owner. The matching session might not exist if the communications were modified by the adversary. The *session identifier* of an AKE session consists of the parties' identities concatenated with messages they exchanged in the session[5]. In [12], a completed session is definied to be "clean" if the session as well as its matching session (if it exists) is not corrupted (neither session key nor session state were revealed by $\mathcal{M}$) and if none of the participating parties were corrupted.

At some point in the experiment, the adversary is allowed to make one Test query: it can select any clean completed session (called the *test session*) and it is given a challenge which consists either of the session key for that session or a randomly selected string. The adversary's goal is to guess correctly which of the cases was selected.

Additionally, the Canetti-Krawczyk [11] definition has an optional perfect forward secrecy (PFS) requirement. In the variant of Canetti-Krawczyk security with PFS, the adversary is allowed to corrupt a participant of the test session (either owner or peer) after the test session is completed. As noted by Krawczyk [12], the PFS requirement is not relevant for 2-round AKE protocols since no 2-round protocol can achieve PFS. Krawczyk introduced the notion of *weak perfect forward secrecy* (wPFS) which can be achieved by 2-round protocols and which he demonstrated is achieved by HMQV [12]. Weak PFS guarantees perfect forward secrecy only for those AKE sessions where the adversary didn't modify communications between the parties. (Using the above terminology, the matching session exists for the test session and both test and matching sessions are clean.)

2.2 Attacks Not Covered by the Existing Definitions

We point out several attacks which are not captured by the previous definitions and explain which components of the Canetti-Krawczyk model prohibit these attacks from being considered. First, we observe that although the adversary is allowed to reveal the session state of the parties, he is not allowed to make Session-State Reveal queries against the session he wants to attack (the test session). That is, existing security models do not provide any security guarantees for a session if the ephemeral secret key of either party has been leaked. While Krawczyk ([12]) extends the Canetti-Krawczyk model by making a definition of clean session that allows him to consider resistance to Key Compromise

[5] We remark that for protocols, where participants do not have full view of the messages exchanged (for example, see [10]), it might not be possible to define such session identifiers.

Impersonation (KCI) attacks and achieve weak Perfect Forward Secrecy (wPFS), this extension still does not include attacks such as revelation of both ephemeral secret keys or both long-term secret keys. Krawczyk does consider resistance to revelation of both ephemeral secret keys separately, and proves HMQV secure against this attack under the stronger assumptions of GDH and KEA1.

Second, when the adversary corrupts an honest party, he takes full control over this party and reveals all its secret information. This definition of the Corrupt query does not allow attacks where the adversary reveals a long-term secret key of some party prior to the time when that party executes the test session. Here we summarize some attacks which are not allowed by the Canetti-Krawczyk model but are permitted under our new definition:

- Key-compromise impersonation (KCI) attack [7,12]: the adversary reveals a long-term secret key of a party and then impersonates others to this party.
- An adversary reveals the ephemeral secret key of a party and impersonates others to this party.
- Two honest parties execute matching sessions, and the adversary reveals the ephemeral secret keys of both of the parties and tries to learn the session key.
- Two honest parties execute matching sessions. The adversary reveals the ephemeral secret key of one party, the long-term secret key of the other party and tries to learn the session key
- Two honest parties execute matching sessions. The adversary reveals the long-term keys of both of the parties prior to the execution of the session and tries to learn the session key.

3 Definitions

3.1 Motivation for Our Security Definition

We modify the Canetti-Krawczyk model in the definition of adversarial power and in the notion of cleanness of the test session. Specifically, we replace the Session-State Reveal query with an "Ephemeral Key Reveal" query which reveals the ephemeral secret key of the party. Additionally, we give the adversary the power to reveal a long-term secret key, by making a Long-Term Key Reveal query, without corrupting the party. We remove the Corrupt query as it is no longer necessary: the adversary can achieve the same result as the Corrupt query by revealing all the secret information of the party through Long-Term Key Reveal, Ephemeral Key Reveal and Reveal queries and by computing everything on behalf of that party. We also modify the definition of a "clean session" by allowing the adversary to reveal the maximum possible amount of data. We disallow only those corruptions which allow the adversary to trivially break any AKE protocol.

We classify the test sessions as either "passive" or "active" depending on whether the adversary is able to cancel or modify the information sent between two honest participants. Formally, passive sessions are those where the matching