Journal of Information Security and Applications 36 (2017) 127–134

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Randomized authentication primitive problem in key exchange with strong security

Zheng Yang[*], Chao Liu, Wanping Liu, Song Luo

School of Computer Science and Engineering, Chongqing University of Technology, 400054 Chongqing, China

ARTICLE INFO

Article history:

Keywords:
Authenticated key exchange
Security model
Partnership
Key compromise impersonation

ABSTRACT

Security proofs are invaluable formal criteria in assuring practitioners on the security properties of protocols. However, one could obtain various security results while proving the considered protocol in different security models. We notice that there are some security proof problems caused by randomized authentication primitives (RAP) in the recent authenticated key exchange (AKE) protocols. Those RAP problems would simply invalidate the security result of such protocols in the corresponding security models. Unfortunately, we figure out that some previous AKE protocols overlooked the RAP problem in their security analysis. We also introduce general solution ideas and concrete examples to avoid RAP problem.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Authenticated key exchange (AKE) protocols are among the most important building blocks of secure network protocols. An AKE protocol without security proof might be susceptible to active attacks. The essential part of security proof is a security reduction that makes use of the adversary breaking the security goals of considered protocol in certain security model, to solve some computational problem believed to be hard. The first formal security model for AKE was introduced by Bellare and Rogaway [3]. In this model an adversary takes full control the communication among parties with the security goal of distinguishing a target session key from a random value, where the chosen ephemeral key attacks and known session key attacks are also formulated. Since then, there are continuing trends to figure out new useful security properties and model them. In 1995, Bellare and Rogaway [4] introduced a new model which covers the strong adaptive corruption that allows the adversary to learn the long-term secret keys of parties. The CK model [9] was latter introduced to particularly formulate the leakage of secret session state. The recent eCK model [15] captures almost all security attributes identified so far in a single model that especially include the resistance to key compromise impersonation (KCI) attacks, chosen identity and long-term public key attacks, and weak perfect forward secrecy attacks (wPFS). In 2012, this model was further developed by Cremers et al. who proposed the eCK-PFS model [10] to capture the perfect forward secrecy (PFS) for two message protocols (this obliviously strengthened the eCK model).

1.1. Partnership

One important element of AKE security model is the definition of partnership of sessions. Sometimes it is referred to as matching sessions in literatures, which aims to capture the situation when two sessions are engaged in the same online communication. The notion of partnership plays a fundamental role in the AKE security model, which is normally used to formulate the 'behavior' of adversary in the security experiment. Namely, some adversary queries (such as Corrupt or RevealKey query) that can be performed to the test session must be formulated in the security definition according to the notion of partnership. Meanwhile the partnership is usually determined by the information of a session that may include identities of session participants and their roles, and session identifier. The most widely used approach to define the partnership is based on the communication transcript of a session (which is referred to as CT approach). The seminal work of CT approach is introduced by Bellare and Rogaway [3], in which a session is identified via *conversation* which is a concatenation of messages orderly sent and received by a party. Similar partnership notions based on CT (which may referred as *matching sessions*) were popular in literatures [14,17–20,22]. One noticeable advantage of the CT approach is the generality which is defined independent of any specific protocol. Nevertheless, in some models the partnership notion is alternatively defined relying on some form of session identifier (SID), e.g., the CK model [9] or the model proposed by Bellare, Pointcheval and Rogaway [2] (which is referred to as BPR model). As criticized by Bellare, Pointcheval and Rogaway [2, Remark 1], that the use of CT approach [3] may bring in ultimately irrelevant syntactic element. Our upcoming new result may support their

[*] Corresponding Author.
E-mail addresses: zheng.yang@rub.de, youngzheng@hotmail.com (Z. Yang).

http://dx.doi.org/10.1016/j.jisa.2017.09.001
2214-2126/© 2017 Elsevier Ltd. All rights reserved.

argument to some extent. However, SID in these models is not specified (in fact it is protocol-dependent or externally provided) but is required to be some unique string. In this sense, a protocol-specific session identifier definition might be inferior to a general definition (like the CT approach). Not only is it inconvenient for the reader to get used to specific SID each time when (s)he analyzes a new AKE scheme, but it also makes schemes harder to compare. Is there any new general way to define the session identifier?

1.2. Motivating problems

With the development of AKE security models, more and more adversary queries are introduced (like the Corrupt and EphemeralKeyReveal[1]) to capture various active attacks, such as KCI attacks [13]. However, we noticed the increased adversary power may also bring some easily neglected problems in the security models for analyzing a certain class of AKE protocols involving *randomized authentication primitives (RAP)* (such as digital signature or message authentication code). However, the randomized authentication primitives have been mainstream not only in the theoretical research fields but also in real world applications. Therefore the problem caused by RAP needs our great attention. Note that an AKE protocol might normally make use of some RAP to generate messages (say signature) during key exchange procedure. In particular, we notice that the security proof of such protocol (using RAP) might trivially become invalid in the model with partnership that is defined based on full communication transcript. We will elaborate on the RAP problem in Section 4. We here first briefly describe the general idea of RAP problem. Consider the following situation (for instance) that a protocol Π involves the randomized signature which is used to sign the outgoing ephemeral key (see the generic compiler in Section 4). We address that, for example, there might exist RAP problem when proving such kind of protocol in a strong indistinguishability-based security model (e.g., such as eCK-PFS [10]) where the KCI is modeled and the partnership is defined via full communication transcript. Namely, in such model we have the following facts: (i) the corruption of the test session is allowed (in order to model the KCI attacks); (ii) two partnered sessions must have the same communication transcript; (iii) the goal of adversary is to distinguish the session key of the test session from a random value. The main idea of RAP problem is that, based on those facts, the adversary may result in two sessions (represented by oracle π) accepting the same session key (or keying material) without matching sessions (nor partnered). More specifically, the attacker against Π can easily break its indistinguishability in the above assumed security model (wherein it is proved) as follows: (i) $\mathcal{M}$ honestly relays messages exchanged between sessions $\pi^{s^*}_{\mathsf{ID}_1}$ and $\pi^{t}_{\mathsf{ID}_2}$ except for the signature σ_{ID_1}, (ii) $\mathcal{M}$ drops the σ_{ID_1} and computes another signature $\sigma_{\mathsf{ID}_1}{}'$ on the same messages as σ_{ID_1} (using the long-term secret of ID_1 obtained from a Corrupt query), and sends $\sigma_{\mathsf{ID}_1}{}'$ to $\pi^{t}_{\mathsf{ID}_2}$. Eventually, those two oracles would generate the same session key but they have no matching sessions. Since the signature $\sigma_{\mathsf{ID}_1}{}'$ received by $\pi^{t}_{\mathsf{ID}_2}$ is not sent by ID_1. Then $\mathcal{M}$ can reveal the session key (or ephemeral key) of session $\pi^{t}_{\mathsf{ID}_2}$ to win the security experiment. We highlight that the similar problem may also caused by EphemeralKeyReveal query (which could help adversary to learn some important keying material for session key generation). Somewhat frustratingly, the RAP problem was still ignored by the most recently work [1]. Namely, the above 'attack' approach can simply invalidate their security result. We believe that attentions should be taken by researchers to somehow circumvent the RAP problem in the corresponding security argument. Otherwise such result (with RAP problem) would be somewhat awkward.

However, is the above attack realistic? The answer is obliviously negative. Since after obtaining the victim ID_1's long-term signing key, of course the adversary can sign anything of her own choice on behalf of ID_1. Although this attack is a result due to the compromise of long-term key, it is not truly consistent with the idea of KCI attack. Because the attacker cannot impersonate the party ID_2 to party ID_1 by using the compromised long-term key of ID_1. This attack just breaks the definition of matching sessions (relying on CT) via exploiting the result from previous attack (i.e., Corrupt query), nor the security problem of the considered protocols. In other word, while we strengthen the security model (relying on CT) to encompass some strong active attacks via giving the adversary additional power to obtain critical information of the test session, it may also inadvertently introduce some 'trivial' unrealistic attacks. It is not hard to see that if we forbid the Corrupt query to the owner of the test session, then the above unrealistic attack does not exist anymore, due to the security of signature schemes. But such model would also fail to provide security argument for AKE regarding the resilience of corresponding active attacks. Therefore the open question left is how to correctly formalize the partnership for a security model in presence of strong adversary which is given access to queries like Corrupt and EphemeralKeyReveal.

1.3. Contributions

We identify new problems when defining security via different partnership definitions in strong security models. Specifically, we present a new theoretical attack that may be applied to AKE protocols which are constructed with randomized cryptographic primitive and are proved in a strong model (formulated KCI attacks or leakage of secret ephemeral keys) where the partnership is defined involving the message generated by underlying randomized cryptographic primitive. We particularly raise attentions to take care of the partnership definition when choosing specific strong model for proving considered protocol (where the partnership is normally used to define freshness of the test session). As a concrete example, we point out that the signature based compiler [10] may be subject to RAP problem in the simplified eCK-PFS model without EphemeralKeyReveal query (denoted as seCK-PFS, for short). We take the work [10] as example, because the authors claims in [10, Remark 1] that their compiler can be secure in the seCK-PFS model with randomized signature scheme. However, the RAP problem does not really break the protocol in any practically harmful way but would invalidate the security proof in the corresponding model. In addition, we somehow generalize the idea of the concrete RAP problem. Such generalized RAP problem can be applied to several protocols, which previously have been believed to be provably secure in the security models (where those protocols were proved respectively).

In addition, several solutions on how to avoid the RAP problem are also given, that might be not only useful for these existing problematic protocols to retain provable security but also good guideline for designing new protocols. One could utilize deterministic scheme as alternative, or define the partnership without the messages generated by randomized cryptographic primitive. In particular, we hereby propose a new general partnership formalism independently of the protocol messages. Besides the restrictions on roles and identities of session participants, the new partnership notion is mainly defined based on session keys. This idea is inspired by the partnership of BPR model. Roughly speaking, the BPR partnership notion states that: two sessions are partnered if both oracles accept holding the same session key, session identifier (SID) and identities of participants (with distinct roles). The session identifier SID is not specified in the BPR model but require

[1] The EphemeralKeyReveal query [10] would return the ephemeral secret key (e.g., the randomness generated by each session) to the adversary.

Download English Version:

https://daneshyari.com/en/article/4955742

Download Persian Version:

https://daneshyari.com/article/4955742

Daneshyari.com