Cryptanalysis of Two Provably Secure Cross-Realm C2C-PAKE Protocols

Raphael C.-W. Phan[1] and Bok-Min Goi[2,⋆]

[1] Information Security Research (iSECURES) Lab,
Swinburne University of Technology (Sarawak Campus), 93576 Kuching, Malaysia
rphan@swinburne.edu.my
[2] Centre for Cryptography & Information Security (CCIS), Faculty of Engineering,
Multimedia University, 63100 Cyberjaya, Malaysia
bmgoi@mmu.edu.my

Abstract. Password-Authenticated Key Exchange (PAKE) protocols allow parties to share secret keys in an authentic manner based on an easily memorizable password. Byun *et al.* first proposed a cross realm client-to-client (C2C) PAKE for clients of different realms (with different trusted servers) to establish a key. Subsequent work includes some attacks and a few other variants either to resist existing attacks or to improve the efficiency. However, all these variants were designed with heuristic security analysis despite that well founded provable security models already exist for PAKEs, e.g. the Bellare-Pointcheval-Rogaway model. Recently, the first provably secure cross-realm C2C-PAKE protocols were independently proposed by Byun *et al.* and Yin-Bao, respectively; i.e. security is proven rigorously within a formally defined security model and based on the hardness of some computationally intractable assumptions. In this paper, we show that both protocols fall to undetectable online dictionary attacks by any adversary. Further we show that malicious servers can launch successful man-in-the-middle attacks on the variant by Byun *et al.*, while the Yin-Bao variant inherits a weakness against unknown key-share attacks. Designing provably secure protocols is indeed the right approach, but our results show that such proofs should be interpreted with care.

Keywords: Password-authenticated key exchange, cross realm, client-to-client, cryptanalysis, provable security, security model.

1 Introduction

A 2-party password-based authenticated key exchange (PAKE) protocol establishes a shared secret key between two parties. Authentication of parties is based on knowledge of a shared low-entropy password. The first known PAKE is due to Bellovin and Merritt [9]. This concept has also been extended to 3 parties, e.g. two clients and a trusted server or key distribution center (KDC).

⋆ The second author acknowledges the Malaysia IRPA grant (04-99-01-00003-EAR).

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 104–117, 2006.

Formal security models. The formal security model for 2-party PAKE protocols was proposed by Bellare *et al.* [8] so called the Bellare-Pointcheval-Rogaway (BPR2000) model, building on work by Bellare and Rogaway in [6,7]. Later, Abdalla *et al.* [2] extended this model to the 3-party case.

One informal approach to designing security protocols is to list all known attacks and argue why a protocol resists them. This list is clearly not exhaustive, and sometimes fails to catch specific types of attacks. The main problem is that this heuristic approach assumes the particular behaviour of the adversary, i.e. he is assumed to attack in some way. History [8,21] has shown that this is not the right approach, because intuitively an adversary behaves in any way he prefers as long as he can break the system. Thus it is often that such a protocol is broken and a minor fix proposed, etc. This cycle continues resulting in many slightly different protocol variants because breaks and subsequent fixes are heuristically done. There are many such instances but to be concise we only cite here a few recent ones: [10,22,23,29].

In contrast the approach based on formal security models does not assume on any specific attack method an adversary may use. Instead a communication model is defined that describes how parties within the protocol, as well as an adversary, communicate with each other, and what sort of information formalized via the notion of oracle queries, is available to or may be under the control of the adversary. Then, security properties of a protocol are defined as one or more games each intended to capture a security property, played by the adversary within the pre-defined communication model. A protocol is secure with respect to the defined security properties if the adversary's advantage in winning the game(s) is negligible, and further that the task of an adversary winning is reduced to computationally intractable assumption(s). This approach is also known as provable security [26]. Once proven secure, a protocol is guaranteed to resist attacks by any adversary who works within the communication model regardless of what specific attacks are mounted, as long as the assumptions remain intractable.

However, defining an appropriate model is not a trivial task, because not including some types of queries e.g. the Corrupt query [14,15], or improperly defining the adversarial game [8] may result in a security proof that fails to capture valid attacks (see [8,14,15] for more details).

PAKEs for cross realms. It is sometimes desirable that client parties from different environments (realms) be able to establish shared secret keys. Byun *et al.* [10] proposed a PAKE protocol that allows to achieve this, by using the KDCs in the different realms as the go-between, i.e. to perform translation of encrypted or blinded secrets in one realm to the other under passwords shared between the KDCs. Such protocols are more popularly known as *cross-realm* C2C-PAKE protocols. For ease of notation, we will simply call these C2C-PAKEs for the rest of this paper.

Considering this cross realm setting, several additional security issues arise that would otherwise not be relevant in a single realm setting, e.g. protecting secrets of the client in one realm from a malicious server [13] or a malicious