Information Sciences 363 (2016) 1–7

Contents lists available at ScienceDirect

Information Sciences

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

Pitfalls in a server-aided authenticated group key establishment

María Isabel González Vasco[a,*], Angel L. Pérez del Pozo[a], Adriana Suárez Corona[b]

[a] *Área de Matemática Aplicada, MACIMTE, Universidad Rey Juan Carlos, C/ Tulipán s/n. Móstoles, 28933, Madrid, Spain*
[b] *Research Institute of Applied Sciences in Cybersecurity, RIASC, Departamento de Matemáticas, Universidad de León Campus de Vegazana, s/n, León 24071, Spain*

ARTICLE INFO

Article history:
Received 29 May 2015
Revised 13 January 2016
Accepted 8 May 2016
Available online 12 May 2016

Keywords:
Provable secure group key agreement
Certificateless signatures
Cryptanalysis
Server-aided key exchange

ABSTRACT

In this paper, we present a cryptanalysis of a recently proposed server-aided group key agreement scheme by Sun et al. This proposal is designed for mobile environments, in which a group of users aim at establishing a common secret key with the help of a semi-trusted server. At this, authentication is achieved using certificateless public key cryptography. We evidence that the scheme does not achieve forward secrecy, is vulnerable to a known session attack (that can, for instance, be mounted by a semi-honest server) and is not (as claimed by the authors) contributory. Further security hardships in more restricted models (i.e. in which stronger corruptions are allowed) are also discussed.

1. Introduction

In this paper, we analyze a recent proposal by Sun et al. [10] of a server-aided group key agreement protocol for mobile environments, and evidence several security problems in it. Secure communication over an untrusted channel is one of the most fundamental problems in cryptography. In order to attain privacy on an insecure network, key agreement protocols allow a designated group of parties to come up with a common secret key, which can later be used for securing their communications by means of symmetric encryption and message authentication schemes. The way users authenticate themselves as legitimate members of the group varies depending on the storage and computation resources of all participants, as well as on the available (trusted) set-up information. Often, only low entropy secrets (passwords) are used to this aim; it can be the case that all group members share a common password, or that participants share two-by-two passwords for mutual authentication. If no strict computation/storage restrictions are in place, public key signature schemes are the default choice; yet this is not the case in many application scenarios, where, for instance, mobile devices may be involved.

Server-aided group key exchange has been introduced in order to leverage strict computation/storage limitations of users. At this, a server (which can be fully trusted or not) helps essentially in two different ways: as an authentication center (so that, for instance, users share just one password with the server instead of a password with every group member) and as a computational resource (for schemes in which all on-line computational burden is shifted to the server)[1]. The scheme

[*] Corresponding author.
E-mail addresses: mariaisabel.vasco@urjc.es, mariaisabel.vasco@urjc.es (M.I. González Vasco), angel.perez@urjc.es (A.L. Pérez del Pozo), asuac@unileon.es (A. Suárez Corona).

[1] We refer to [1] and [6] as nice illustrative examples of these two flavours of server-aided group key exchange.

http://dx.doi.org/10.1016/j.ins.2016.05.004
0020-0255/© 2016 Elsevier Inc. All rights reserved.

proposed by Sun et al. in [10] fits in the first scenario, as it presents a group key agreement protocol in which a (semi-trusted) server helps a group of users, authenticating themselves via certificateless signatures, to agree upon a common secret key. The on-line computation load of users is comparable to that of the server, yet obviously the number of signatures they have to verify is only one (the server's) and is thus independent of the group's size. As additional features, the scheme is claimed to be particularly suitable for mobile environments, and to provide key privacy with respect to the server.

Contributions: We evidence, giving concrete attacks, that the protocol proposed in [10] presents severe security flaws. After briefly recalling the construction of Sun et al. in Section 2, we provide in Section 3 a sound security model for the considered scenario by adapting standard security models for group key exchange (see, for instance [3–5]). This suffices to formalize our attacks in Section 4, and in turn refute all theorems contained in Section 5 of [10]. Furthermore, in Section 5 we describe additional attacks that can be carried over when either group members or the server behave maliciously. Note that the authors of [10] only consider honest but curious servers, yet malicious participants are not explicitly excluded in their discussion.

2. The scheme of Sun et al.

We briefly describe here the scheme proposed in [10], which is in turn schematized in Fig. 1.

Initialization. A key generation procedure is first executed with the aid of a trusted Key Generation Center (KGC), following the usual steps in certificateless public key cryptography (see [2]). This procedure will allow users to authenticate using Tso's certificateless signature scheme from [11]:

Let G_1 be an additive cyclic group and G_2 a multiplicative cyclic group, both of prime order q. Let $e : G_1 \times G_1 \longrightarrow G_2$ be a bilinear map, and consider two hash functions H_0 and H_1 ranging in G_1 and $\mathbb{Z}_q^*$ respectively. The KGC chooses a generator $P \in G_1$ and a master secret key $s \in \mathbb{Z}_q^*$. Further, it computes $P_{pub} = sP$ and publishes $params = \{G_1, G_2, e, P, P_{pub}, H_0, H_1\}$.

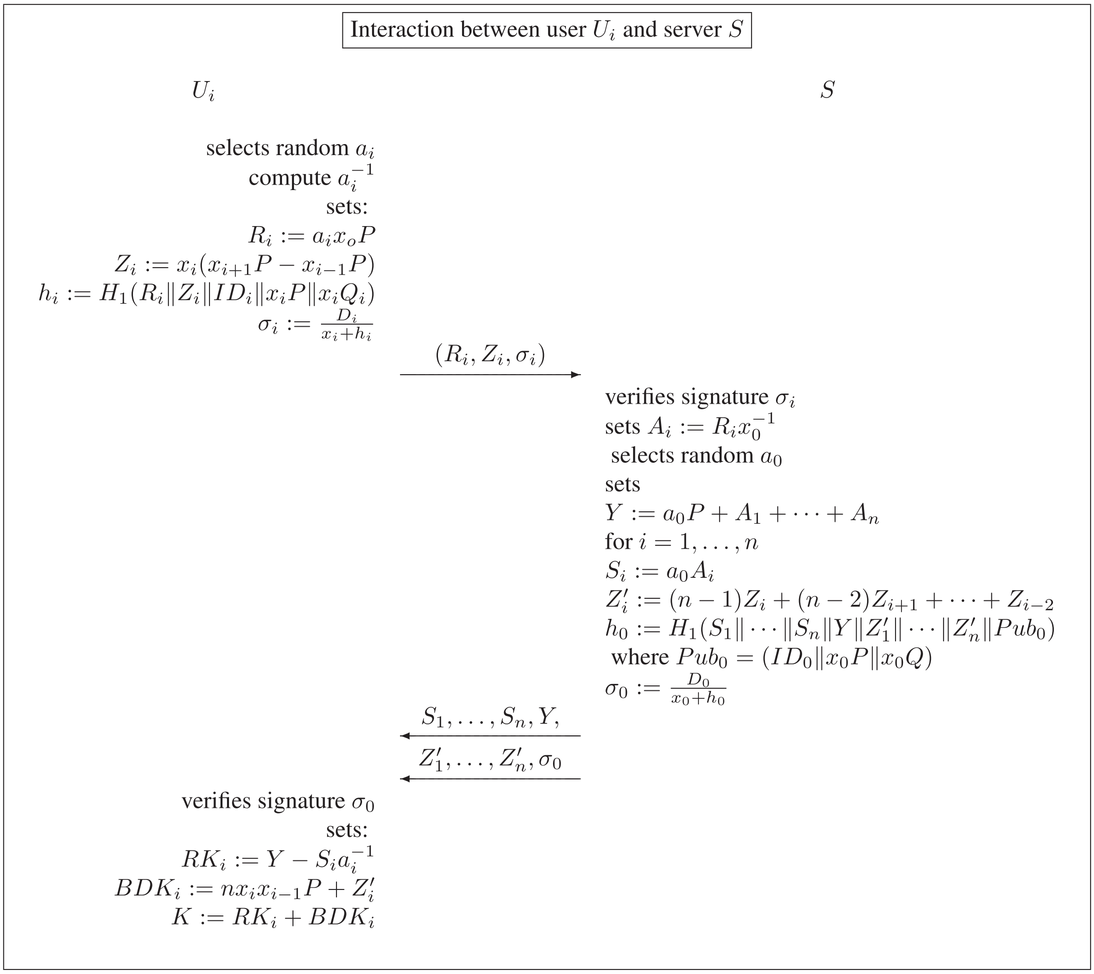
Interaction between user U_i and server S
U_i
S
selects random a_i
compute a_i^{-1}
sets:
$R_i := a_i x_o P$
$Z_i := x_i(x_{i+1}P - x_{i-1}P)$
$h_i := H_1(R_i \| Z_i \| ID_i \| x_i P \| x_i Q_i)$
$\sigma_i := \frac{D_i}{x_i + h_i}$
(R_i, Z_i, σ_i)
verifies signature σ_i
sets $A_i := R_i x_0^{-1}$
selects random a_0
sets
$Y := a_0 P + A_1 + \cdots + A_n$
for $i = 1, \ldots, n$
$S_i := a_0 A_i$
$Z_i' := (n-1)Z_i + (n-2)Z_{i+1} + \cdots + Z_{i-2}$
$h_0 := H_1(S_1 \| \cdots \| S_n \| Y \| Z_1' \| \cdots \| Z_n' \| Pub_0)$
where $Pub_0 = (ID_0 \| x_0 P \| x_0 Q)$
$\sigma_0 := \frac{D_0}{x_0 + h_0}$
$S_1, \ldots, S_n, Y,$
$Z_1', \ldots, Z_n', \sigma_0$
verifies signature σ_0
sets:
$RK_i := Y - S_i a_i^{-1}$
$BDK_i := n x_i x_{i-1} P + Z_i'$
$K := RK_i + BDK_i$

Fig. 1. Certificateless server-aided group key agreement of Sun et al.