Knowledge-Based Systems 59 (2014) 149–158

Contents lists available at ScienceDirect

Knowledge-Based Systems

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

On securing online registration protocols: Formal verification of a new proposal

Jesus Diaz *, David Arroyo, Francisco B. Rodriguez

Grupo de Neurocomputación Biológica, Departamento de Ingeniería Informática, Escuela Politécnica Superior, Universidad Autónoma de Madrid, Spain

ARTICLE INFO

Article history:
Received 27 May 2013
Received in revised form 2 December 2013
Accepted 14 January 2014
Available online 5 February 2014

Keywords:
Protocol security
Automated verification
EBIA
Security-by-design
Digital identity

ABSTRACT

The deployment of Internet based applications calls for adequate users management procedures, being online registration a critical element. In this respect, Email Based Identification and Authentication (EBIA) is an outstanding technique due to its usability. However, it does not handle properly some major issues which make it unsuitable for systems where security is of concern. In this work we modify EBIA to propose a protocol for users registration. Moreover, we assess the security properties of the protocol using the automatic protocol verifier ProVerif. Finally, we show that the modifications applied to EBIA are necessary to ensure security since, if they are removed, attacks on the protocol are enabled. Our proposal keeps the high usability features of EBIA, while reaching a reasonable security level for many applications. Additionally, it only requires minor modifications to current Internet infrastructures.

1. Introduction

Creating usable systems is certainly a subject of critical importance for Internet applications aiming to reach a high acceptance among its users. However, combining usability with security is normally a source of difficulties. In the area of online registration, which comprises a critical component of Internet based systems, Email Based Identification and Authentication (EBIA) is almost certainly one of the techniques that stands out among the set of alternatives [1]. EBIA uses email addresses as identifiers, and as authenticators the fact of accessing to URLs contained within email messages sent to those addresses. Its main advantages are usability and ease of deployment, while its major drawback is security [2].

In the registration process of EBIA-based systems (shown in Fig. 1) it is assumed that only the owner of the email account can access the activation link sent within registration email messages. However, this has a well-known security problem [2], for emails are typically sent over an insecure channel (with no encryption whatsoever). In this matter it should be noticed that the SSL/TLS connection between user and email server does not suffice to avoid eavesdropping unless emails are encrypted, since the rest of the path followed by the email is not always encrypted. As a result, a passive attacker might wait until her victim initiates registration, and then access the activation link by eavesdropping the email, possibly setting a new password or something similar (this sequence is shown following the initial step 1a in Fig. 2). Alternatively, an active attacker might try to register herself using an email account that she does not own, since she does not need access to the email account in order to read the email message contents, as shown in the path initiated with step 1b in Fig. 2. Therefore, the actual flaw of EBIA is to assume that accessing the link sent within the registration emails is equivalent to a proof of ownership of the associated email account.

Our proposal is to convert EBIA's authenticating action (i.e., accessing the registration link) into an explicit acknowledgment message sent by a trusted entity. In fact, the protocol structure provides an ideal candidate for this role, namely, the email provider. More specifically, the Mail Servers that are accessed securely (it is a common practice nowadays to protect accesses to Mail Servers with SSL/TLS) by the email account owners to fetch the email messages in their in-boxes. By providing the Mail Servers with digital identities trusted by the registration server, those servers can send authenticated acknowledgment messages after receiving an instruction from the user.

The rest of the paper is organized as follows. In Section 2 we analyze several alternatives/extensions to EBIA toward solving the above explained security drawbacks. Based on the insight gained from this analysis, we present an EBIA-based registration system in Section 3. The security of this scheme is evaluated in Section 4 by using the automated protocol verifier ProVerif [3]. In Section 5 the security assessment is complemented by discussing the minimality of the protocol, i.e., by underlining the needs of each component of the protocol and pinpointing the subsequent attacks

* Corresponding author.
E-mail address: j.diaz@uam.es (J. Diaz).

http://dx.doi.org/10.1016/j.knosys.2014.01.011
0950-7051/

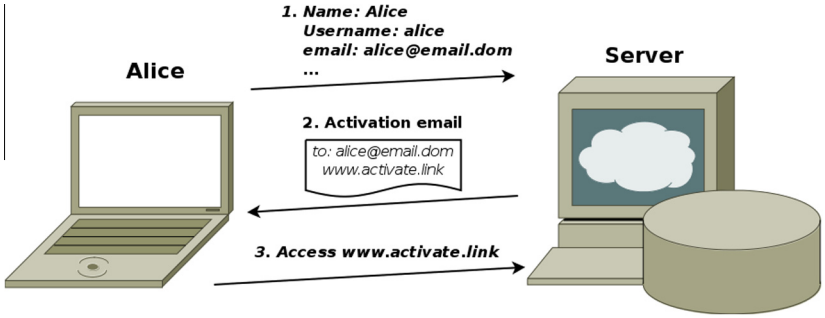

Fig. 1. Behavior of EBIA systems. (1) The user sends the request with her data. (2) The server validates the data and sends back an activation link via email. (3) The user accesses the activation link.

enabled in case of either omitting some of them or changing the interrelationship order. We continue in Section 6 with an analysis of the additional costs, trust relationships, modifications over the existing infrastructures and usability. Finally, the article ends with the conclusion in Section 7.

2. A brief security analysis of EBIA-based registration protocols

Several alternatives have been proposed to solve or reduce the impact of EBIA's security limitations, typically by incorporating some kind of multifactor and/or multichannel method [4]. In [5], an authentication protocol is proposed intended to provide single use authenticators through a multichannel technique, with the aim of reducing the effect of possible attacks. The security of the scheme is claimed to improve the performance of EBIA by adding a token sent via SSL ("SSL token") in the same session established by the registering user during the authentication request. Besides sending this token via SSL, an extra token is sent unencrypted via email. The related digital identity is only generated if the user sends back to the server both tokens. The intuition behind this approach is that, by using SSL, only the user who started the authentication request receives the "SSL token". Thus, if this user also proves knowledge of the token sent via email, it is assumed that the user who started the session is the owner of the email account. However, even with SSL in use, this approach is vulnerable to the attack on EBIA illustrated in Fig. 2 (attack initiated with step 1b). Although it is an attack that assumes that the attacker takes an active role (i.e., it is not limited to just observing the communications), its security is not higher than that of classic EBIA. In detail, an active attacker starting the registration process would just have to eavesdrop the activation email to obtain a legitimate identity. For the sake of clarity, we have implemented a ProVerif model of this protocol to show the mentioned attack by executing the code available from [6]. This shortcoming is addressed in [5] by combining several email accounts. In this new setup, the challenge for an attacker is more complicated, since she has to break into several Mail Servers. Nevertheless, this also erodes the scheme's usability as users have to manage more than one email address, and thus they can be reluctant to adopt this alternative. As a result, a third possible implementation is proposed in [5] consisting first of the encryption of the email using a key sent jointly with the SSL token, and secondly by routing the resulting message via an anonymizing network. Therefore, even though the attacker can start the SSL session and get the SSL token plus the key used to encrypt the email, allegedly she cannot gain possession of the email because it is sent via an anonymizing network. However, if the

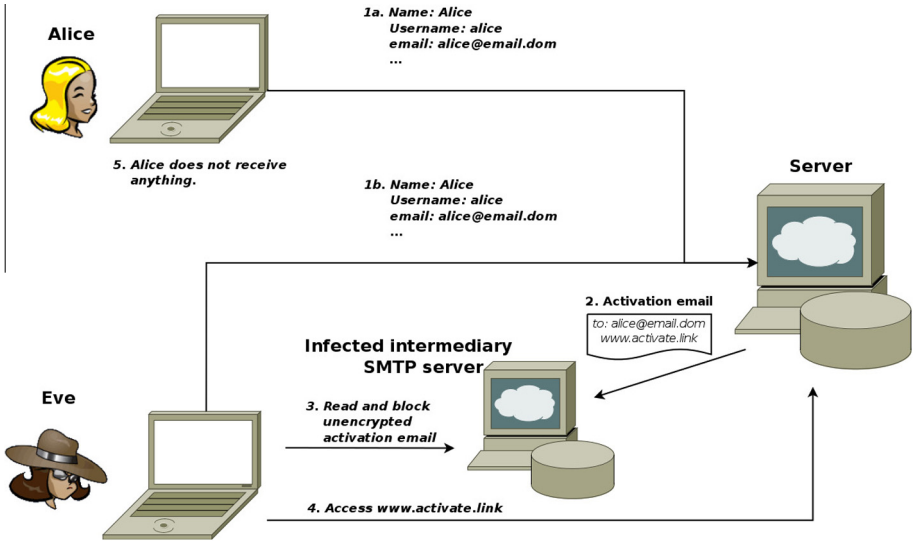

Fig. 2. Attacks to EBIA systems. The attack initiated with step 1a depicts a possible attack by passive adversaries. The attack initiated with step 1b depicts a possible attack by active adversaries. Steps 2–5 are the same for both attacks. (1a) Alice requests registration to the Web Server. (1b) Eve starts registration on behalf of Alice. (2) The server sends the activation email to Alice, containing the activation link, which passes through an infected intermediary server under Eve's control. (3) Eve intercepts and blocks the activation email. (4) Eve activates the account in Alice's behalf. (5) Alice will probably just think that an error occurred.