Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER Electronic Notes in Theoretical Computer Science 121 (2005) 47–63

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Analysing Password Protocol Security Against Off-line Dictionary Attacks

Ricardo Corin[1]

Faculty of Computer Science, University of Twente, The Netherlands

Jeroen Doumen[2]

Faculty of Computer Science, University of Twente, The Netherlands

Sandro Etalle[3]

Faculty of Computer Science, University of Twente, The Netherlands
CWI, Center for Mathematics and Computer Science Amsterdam

Abstract

We study the security of password protocols against off-line dictionary attacks. In addition to the standard adversary abilities, we also consider further cryptographic advantages given to the adversary when considering the password protocol being instantiated with particular encryption schemes. We work with the applied pi calculus of Abadi and Fournet, in which we present novel equational theories to model the (new) adversary abilities.These new abilities are crucial in the analysis of our case studies, the *Encrypted Password Transmission* (EPT) protocol of Halevi and Krawczyk, and the well-known *Encrypted Key Exchange* (EKE) of Bellovin and Merritt. In the latter, we find an attack that arises when considering the ability of distinguishing ciphertexts from random noise. We propose a modification to EKE that prevents this attack.

Keywords: Password protocols, dictionary attacks, verification, pi calculus.

[1] Email: corin@cs.utwente.nl

[2] Email: doumen@cs.utwente.nl

[3] Email: etalle@cs.utwente.nl

1571-0661/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.entcs.2004.10.007

1 Introduction

Due to the low entropy available in user-chosen passwords, password protocols are usually subject to *off-line dictionary attacks*. The attack is mounted by a passive adversary who eavesdrops protocol messages and then goes off-line to perform the password search.

Recently, there have been some attempts to deal with the formal verification of password protocols that are subject to off-line dictionary attacks [13,7,8]. These approaches are based on the usual Dolev-Yao adversary, and assume *ideal* or *perfect* encryption: ciphertexts do not leak *any* information to an adversary that does not have the correct key.

Unfortunately, assuming ideal encryption to analyse password protocols is not realistic, since most practical encryption schemes are far from this ideal. In practice, password protocols are designed to be secure when instantiated with a particular encryption scheme, which makes the security against dictionary attacks dependent on the chosen cryptosystem. Typically, the security of an encryption scheme is characterized by certain properties that the ciphertexts satisfy. For instance, an encryption scheme is said to be *repetition concealing* [2] if an adversary cannot detect two instances of the same message encrypted with the same key (to achieve this, probabilistic [10] or stateful encryption is needed). Similarly, an encryption scheme is *which-key concealing* if an adversary cannot deduce if two messages are encrypted under the same key [2]. Besides these general properties, usually each particular cryptosystem has its own subtleties that can also provide useful information to an adversary. For example, a public key in RSA consisting of a pair (n, e) can be distinguished from a random string because e is odd and n contains no small prime factors. As discussed by Mellovin and Merritt [3], this simple fact allows a dictionary attack over EKE when instantiated with RSA.

In this paper, we study password protocols using the applied pi calculus [1]. Our contribution is twofold: First, we show how to analyse, in a precise formal framework, the security of password protocols when they are instantiated with particular encryption schemes, which may or may not satisfy specific properties. We model (most of) these properties by extending the equational theory of the applied pi calculus. In particular, we show how to model encryption schemes which are repetition and which-key revealing, and also encryption schemes that allow an adversary to distinguish ciphertexts and public keys from random noise. Second, we study, as illustrating examples, two well-known protocols: the EPT protocol of Halevi and Krawczyk [11], and the already mentioned EKE protocol [3]. For EPT, we show that security against dictionary attacks is achieved when encryption is repetition concealing. For the EKE protocol we show that security can be established if encryption is