Separable Identity-Based Deniable Authentication: Cryptographic Primitive for Fighting Phishing*

Willy Susilo** and Yi Mu

Centre for Information Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia
{wsusilo, ymu}@uow.edu.au

Abstract. Phishing emails are one of today's most common and costly forms of digital identity theft. They are now very convincing that even experts cannot tell what is and is not genuine. In a phishing attack, victims are lured by an official looking email to a fraudulent website that appears to be that of a legitimate service provider. Such attacks can be mitigated with digitally-signed emails. Unfortunately, traditional digital signatures will destroy the traditional repudiability of email and they also require the unrelialistic adoption of a Public Key Infrastructure. To overcome this problem, we introduce a new cryptographic primitive called *separable identity-based deniable authentication*. Firstly, we present a generic construction of such a scheme, and proceed with an efficient construction based on bilinear pairing, which is an instantiation of our generic construction. This construction is an affirmative answer to the open question proposed by Adida, Hohenberger and Rivest [AHR05+].

Keywords: phishing, email, repudiable, separable, ID-based, deniable, authentication.

1 Introduction

Phishing attacks are the act of sending an e-mail to a user falsely claiming to be an established genuine enterprise in an attempt to lure the user to a fraudulent website so that the user will surrender his/her private information. Over the past year, phishing attacks were launched pretending to be known services, such as AOL, eBay and many bank institutions, with an estimated cost of identity theft to these companies and their consumers surpassing $ 10 billion dollars [APWG+]. The consequences of phishing attacks are devastating to email as a communication medium. Banking institutions have been reduced to recommending that their users not selecting on links in emails [AHR05]. The

* This work is partially supported by ARC Linkage Project Grant LP0667899.
** This work is partially supported by ARC Discovery Grant DP0663306.

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 68–80, 2006.

very openness that originally made email easy to use is now threatening to make the medium completely unusable.

Defenses against phishing attacks exist, but none of them is satisfactory. For instance, the Anti-Phishing Working Group suggests to authenticate all emails using standard digital signatures like PGP or S/MIME [APWG]. We note that this simple solution will *not* solve the problem entirely since its adoption is unlikely due to the need of a widespread public key infrastructure (PKI) and the non-repudiability of digital signatures that will *destroy* the property of traditional email (i.e. deniability). We aim to find an alternative to the traditional digital signature solution *without* losing the inherent properties of the email. Email is currently repudiable. The use of traditional digital signatures will harm this property and strip email users of their privacy, since emails might become legally binding.

Adida, Hohenberger and Rivest suggested a notion of separable identity-based ring signature (SIBR) to fight phishing attacks [AHR05$^+$]. In their construction, they incorporate a ring signature scheme (eg. [AOS02, ZK02]) to construct a SIBR. Their solution is acceptable since it retains the email property together with not relying on a PKI infrastructure. Nonetheless, their construction depends on the existence of a ring signature scheme. Additionally, they also pointed out that an identity-based deniable signatures could be one of the possible solutions to solve phishing attacks, but there is *no* known construction available [AHR05$^+$], and the construction has been posed as an open problem.

Our Contribution

In this paper, we answer the question proposed in [AHR05$^+$] affirmatively, by presenting a generic construction of separable identity-based deniable signature. The term *separable* in this context refers to cross domains between the two parties, namely the sender and the receiver. We cannot expect both sender and receiver to use an agreed public parameter as this will become unrealistic. The notion of separability makes our new notion practical, since users select a *master* of their choice and cryptographic schemes operate across various masters. In the context of email, a user's master will simply be her email domain, for example Alice with email address `alice@earth.com`, will derive her public key from the Private Key Generator (PKG) at `earth.com`. In our new notion, we retain the property of traditional email system, namely *sender repudiability* based on *recipient forgeability*. Intuitively, a user Alice can send an email to Bob with a separable ID-based deniable signature attached to it, so that Bob will believe that the email is indeed from Alice, but Bob cannot convince anyone else about the fact that Alice was the real signer.

1.1 Related Work

In [RST01], the notion of *ring signatures* was formalized and an efficient scheme based on RSA was proposed. A ring signature scheme allows a signer who knows at least one piece of secret information (or trapdoor information) to produce a sequence of n random permutations and form them into a ring. This signature