Some Weaknesses of "Weaknesses of Undeniable Signatures"

David Chaum

CWI (Centre for Mathematics and Computer Science)
Kruislaan 413 1098 SJ Amsterdam

ABSTRACT: The weaknesses that are the subject of [DY 91] have already been addressed in the published literature [C 90 & CvA 89]. The main class of these weaknesses consists of ways of cheating undeniable signatures; but these ways are shown here to themselves be "weak." Specifically, a cheater using them can double-cross the other cheaters, to the extent that the original ways of cheating are rendered useless. The remaining cited weaknesses are re-statements of, or variations on, some previously observed blinding techniques [CvA 89]. These techniques allow advantages in some applications when desired, but are also easily excluded when not desired.

Introduction

The paper [DY 91] proposes two classes of "weaknesses" of undeniable signatures. It presents a main class in Section 3, which includes two "attack" protocols, and a minor class in Section 4, which comprises three more such protocols. Here, the discussion is similarly organized into two sections whose titles include those of the original.

On "Verification by multiple unknown verifiers is possible"

This first and main weakness class relates to the desirable property of undeniable signatures that requires cooperation of the signer for each verification of a signature. Thus, for example, the only way to be convinced that the signature on a piece of software is valid should be to pay for the software and then verify the signature by conducting a protocol with its author. The weakness perceived by [DY 91] takes the form of two specific attack protocols that are claimed to allow multiple cooperating cheating parties to be convinced while the software author

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 554-556, 1991.

believes he is convincing only a single paying customer. (This would of course still not allow any after-the-fact cheating or victimization of non-cheating customers.)

It has already been pointed out by [C 90] that such attacks can exist, and it was also claimed there that they could be prevented by special techniques for a very broad class of protocols, including known undeniable signature protocols (see [C 91] for details of how this is achieved). But none of these techniques are needed to prevent the attacks of [DY 91]; in fact, no preventive measures are needed at all. The two attack protocols simply have the feature that a cheating verifier can compute messages from exactly the same distribution as those issued by the genuine signer. This allows a cheater to double-cross all other cheaters into believing that the signer is participating. The double-crossing cheater can even convince the other cheaters that arbitrary values are valid signatures on chosen messages.

To see this, observe that knowing how the first message in the protocol is formed, i.e., knowing a and b, allows one to generate acceptable responses—even when $z \neq m^x$. Thus, in the first attack, which is just a set of cheaters who do a coin-flipping protocol to determine their challenge to the signer, any cheater can create false responses that are apparently valid responses from the signer. The second attack is a chain of "challenge and response blinding" [CvA 89] cheaters stretching from an honest customer to the signer. In this attack, the cheater nearest the customer can simply put the customer in communication with the signer and cheat all the other cheaters into believing a false signature. More generally, any chain segment is similarly cheated by those who control both its ends.

On "Vulnerability to on-line multiplicative attacks"

The second of the three attacks in this minor class seems to be simply a re-statement of the well-known basic blind signature protocol described in the context of undeniable signatures by [CvA 89]. It involves a set of valid messages, each of which the signer is willing to sign, but without knowing which one is being signed. An example use for this is where each valid signed message is the equivalent of an electronic coin [C 85]. The bank does not care which of the equivalent denomination coins it signs, so long as it can deduct the coin value from the recipient's account. If the signer does not wish to issue blind signatures, and hence wishes to prevent the attack, then the signer simply issues signatures only on valid messages.

The first and third attacks involve a cheater who interposes herself in the communication between the signer and a victimized receiver of a signature. These

protocols are superfluous, since the same effect can always be achieved without interacting with the signer. To see this, notice that the assertion made at the end of Section 2 in [DY 91], that signatures on random messages cannot be forged (sometimes referred to as "existential forgery"), is incorrect: anyone can simply raise the public generator g and the public key g^x to the same random power r to obtain each message g^r and its corresponding signature g^{rx}. Of course such ease of obtaining signatures on random messages in no way compromises the security of systems that make a distinction between messages and valid messages, which distinction is a well-known component of blind signature systems.

These first and third attacks also suffer from an additional problem, similar to that of the second attack of this class. They both expect a receiver who is following protocol to accept a signature on a random message (i.e., an invalid message), which of course no receiver need do. Furthermore, the first attack also involves blinding of the challenge and response, as detailed in [CvA 89], which, while possibly useful in some applications, is easily thwarted in other applications by the signer confirming signatures only on valid messages.

Conclusion

No significant weakness of undeniable signatures is contained in [DY 91].

References

[C 85] Chaum, David "Security without identification: Transaction systems to make big brother obsolete," Communications of the ACM, October 1985, pp. 1030–1044.

[C 90] Chaum, David "Zero-knowledge undeniable signatures," Advances in Cryptology—Eurocrypt '90, Springer-Verlag, pp. 458–464.

[C 91] Chaum, David "Provers *can* limit the number of verifiers," pre-print available from the author.

[CvA 89] Chaum, David and Hans van Antwerpen, "Undeniable signatures," Advances in Cryptology—CRYPTO '89, Springer-Verlag, 1991, pp. 212–216.

[DY 91] Desmedt, Yvo and Moti Yung "Weaknesses of undeniable signature schemes," Pre-Proceedings of Eurocrypt '91.