SPADE : un protocole délimiteur de distance anonyme et résistant à la fraude terroriste

Xavier Bultel, Sébastien Gambs, David Gérault, Pascal Lafourcade, Cristina Onete, Jean-Marc Robert

SPADE : un protocole délimiteur de distance anonyme et résistant à la fraude terroriste ‡

Xavier Bultel[1], Sébastien Gambs [2], David Gérault [1], Pascal Lafourcade [1], Cristina Onete [3] et Jean-Marc Robert [4]

[1]*LIMOS, University Clermont Auvergne, France,* [2]*UQAM, Montréal,* [3]*INSA/IRISA Rennes* [4]*, ÉTS, Montréal*

Les communications sans contact sont omniprésentes dans notre quotidien, allant des badges de contrôle d'accès au passeport électronique. Ces systèmes sont sensibles aux *attaques par relais*, dans lesquelles un adversaire transfère simplement les messages entre le prouveur et le vérifieur pour usurper l'identité du prouveur. Les protocoles délimiteurs de distance (*distance-bounding*) ont été introduits pour contrer ces attaques en assurant une borne sur la distance entre le prouveur et le vérifieur grâce à la mesure du temps des communications. Par la suite de nombreux travaux ont amélioré la sécurité de ces protocoles, mais ont aussi cherché à assurer le respect de la vie privée face à des adversaires actifs et également face à des vérifieurs malicieux.

En particulier, une menace difficile à prévenir est la *fraude terroriste*, où un prouveur lointain coopère avec un complice proche pour tromper le vérifieur. La contre-mesure usuelle pour cette menace est de rendre impossible l'action du complice sans l'aide du prouveur lointain, à moins que le prouveur ne lui donne suffisament d'information pour qu'il retrouve sa clef privée et puisse ainsi toujours se faire passer pour le prouveur.

Dans cet article, nous proposons une *nouvelle approche* où le prouveur ne révèle pas sa clef privée mais utilise une clef de session avec une signature de groupe, la rendant ainsi utilisable plusieurs fois. Ceci permet à un adversaire d'usurper l'identité du prouveur sans même connaître sa clef de signature. Grâce à cette approche nous proposons SPADE le premier protocole de délimiteur de distance qui est anonyme, révocable et formellement prouvé sûr.

Mots-clefs : Protocole délimiteur de distance (Distance Bounding), Sécurité, résitance à la fraude terroriste.

1 Introduction

With the accelerating convergence of our digital identities on our ubiquitous *smartphones*, developing secure authentication protocols is more important than ever. As an example, a virtual wallet including various personal credentials can be used for everyday life applications such as public transport, logistics and contactless-payment systems. Another crucial notion is to protect the privacy of the users against external eavesdroppers and legitimate entities. The canonical application for this concept is the contactless pass used for accessing public transport systems. In this context, privacy is a fundamental property in order for users to trust the system deployed.

Authentication protocols are among the most fundamental cryptographic primitives of the digital world. They enable an entity, called a *verifier*, to check the legitimacy of users (called *provers*) before giving access to a resource. The provers are assumed to possess cryptographic devices storing their secret credentials. To be secure, an authentication protocol must guarantee that a legitimate prover is always authenticated, while all illegitimate ones should be rejected by the verifier. Authentication protocols are often prone to *relay attacks* [2], in which an adversary relays to the verifier the responses of a legitimate prover. This attack bypasses standard countermeasures such as encryption or digital signatures.

Distance bounding (DB) was introduced by Brands and Chaum [3] to thwart relay attacks by allowing the verifier to estimate an upper bound on the distance between him and the prover using several *time-critical*

†Ce travail est partiellement financé par la Chaire de confiance numérique de la foncdation de l'Université d'Auvergne, par le "NSERC Discovery and Accelerator Supplement grants", et par l'union européene via le fond FEDER.

‡Ce papier est une version courte d'un papier présenté à Wisec2016.

challenge-response rounds. Assuming that trust requires physical proximity, if a prover is *outside* the close vicinity of the verifier, he should be rejected. Thus, in DB protocols, verifiers are equipped with a clock, and they measure the time between sending a challenge and receiving the corresponding response from the prover. Once the different *Round Trip Times* (RTTs) for all challenge-response rounds are measured, the verifier compares these values to a pre-existing bound t_{max} and accepts the prover if and only if : (a) the responses are correct and (b) all RTT values are below the threshold t_{max}.

To be secure, a DB protocol must resist at least to : (1) *Mafia fraud* (MF), (2) *Distance fraud* (DF) and (3) *Impersonation fraud* (IF). MF resistance requires that no illegitimate *Man-in-the-Middle* (MiM) adversary can authenticate to the verifier, even in the presence of a legitimate prover with whom he can interact. DF resistance demands that no legitimate but malicious prover, located outside the verifier's trusted vicinity, should be able to authenticate.

Finally, the IF resistance adresses the simple situation in which the malicious adversary tries to fool the verifier without any help. Another important threat against DB protocols is the *Terrorist Fraud* (TF), in which a malicious yet legitimate prover helps a cooperative MiM accomplice to authenticate. However, one of the assumptions is that the prover wants to retain control of his secret credentials. Thus, he is willing to help his accomplice, but without giving him a better chance to authenticate in latter attempts. In this context, the usual countermeasure against TF is to force the prover to leak parts of his long-term key if he wants to give his accomplice a fair chance to succeed.

Since DB protocols were defined for RFID tags and readers, they use shared symmetric keys between provers and the verifier. However, the seminal DB protocol of Brands and Chaum [3] was based on public-key cryptography. Improvements in RFID architectures as well as the emergence of NFC smartphones have motivated recent research in DB to consider public-key cryptography [7, 6, 9].

A recent concern in DB protocols is *privacy*. One of the first schemes to address this concept is the Swiss-Knife protocol [8]. However, its guarantee holds only if secret keys can never be leaked, and only with respect to an external eavesdropper but not against a legitimate verifier. However, no precise definition of this property is given and no formalized proof exists in the literature.

Introducing privacy with respect to the verifier raises the question of the revocability of a prover by the registration authority. Hence, before the authentication succeeds, the verifier should check whether this prover has been revoked. Indeed, if this property is not taken into account, the corruption of a prover makes the whole system vulnerable, as there is no way to distinguish whether a prover uses stolen credentials or legitimate ones. Our protocol provides anonymity with a revocation mechanism.

A typical scenario for our secure and anonymous DB protocol can be described as follows. In a public transport system, users relying on their NFC-enabled phones may have access to buses or subway stations if they can properly authenticate. However, users must protect their identity with respect to legitimate verifiers trying to profile them. In such a context, a TF attack is simply a user ready to lend illegally his monthly pass to someone for a single trip while he is not using it. However, this user would not accept that his accomplice can impersonate him later at will to avoid being caught (if the same nonce N_p is used successfully numerous times). Thus, the presence of a backdoor in the verifiers can play an important role to deter such frauds. In an in-depth security approach, tamper-proof protection is not sufficient in this case. Indeed, it may protect the long term private key, but it would be useless to protect the two strings used in the time-critical phase implemented directly in the network access card for efficiency. The prover should answer the challenges as fast as possible, or otherwise the verifier can estimate that the prover is further than he really is. These strings are critical for the TF attacks and can therefore be easily obtained.

2 Our protocol : SPADE

We propose SPADE (for *Secure Prover Anonymous Distance-bounding Exchange*), the first protocol to achieve prover-anonymity with respect to the strongest possible adversaries, provable TF resistance, and revocability of corrupted provers. The protocol description is given in Figure 1, detailled explanations are given in our paper published at WISEC'16 [4].

For ensuring anonymity, our construction relies on the concept of group signatures [1], which enables a member of a group to sign anonymously on behalf of the group. New members can dynamically join the

Prover P		**Verifier** V
$\mathsf{pk}_V, \mathsf{ssk}_P$		$\mathsf{sk}_V, \mathsf{gpk}$
	Initialisation	
$N_P \xleftarrow{\$} \{0,1\}^n, \sigma = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$		$N_V \xleftarrow{\$} \{0,1\}^n, m \xleftarrow{\$} \{0,1\}^n$
$e = \mathsf{E.enc}_{\mathsf{pk}_V}(N_P, \sigma)$	$\xrightarrow{e}$	$(N_P, \sigma) = \mathsf{E.dec}_{\mathsf{sk}_V}(e)$
$a = PRF_{N_P}(N_V)$	$\xleftarrow{m, N_V}$	if $\mathsf{G.ver}_{\mathsf{gpk}}(\sigma, N_P, \mathsf{RL}) = 0$ then abort
	Distance Bounding for $i = 1$ to n	
		$c_i \xleftarrow{\$} \{0,1\}$
$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{Pi} \oplus m_i & \text{if } c_i = 1 \end{cases}$	$\xleftarrow{c_i}$	**Start clock**
	$\xrightarrow{r_i}$	**Stop clock**
		Check timers Δt_i
	Verification	
$C = c_1 \|\| \ldots \|\| c_n$ and $R = r_1 \|\| \ldots \|\| r_n$		$C = c_1 \|\| \ldots \|\| c_n$ and $R = r_1 \|\| \ldots \|\| r_n$
$\mathcal{T} = PRF_{N_P}(N_V \|\| m \|\| C \|\| R)$	$\xrightarrow{\mathcal{T}}$	Check that $\mathcal{T} \stackrel{?}{=} PRF_{N_P}(N_V \|\| m \|\| C \|\| R)$
		If $\#\{i : r_i$ and Δt_i correct$\} = n$
	$\xleftarrow{Out_V}$	then $Out_V = 1$ else $Out_V = 0$

FIGURE 1: SPADE our anonymous TF resistant protocol that uses a public key encryption $E = (\mathsf{E.enc}_{\mathsf{pk}_V}(m), \mathsf{E.dec}_{\mathsf{sk}_V}(c))$, a pseudo-random-function set PRF and a revocable group signature $G = (\mathsf{G.sig}_{\mathsf{ssk}_P}(m), \mathsf{G.ver}_{\mathsf{gpk}}(\sigma, m, \mathsf{RL}))$, where $a||b$ is the concatenation of a and b; $x \xleftarrow{\$} U$ is random value uniformly chosen in U and $x \oplus y$ denotes the exclusive-or.

group or be revoked. This is managed by a central registration authority, which has to be involved in any signature verification. In case of dispute, a trusted authority can retrieve the identity of a signer.

In addition to privacy, our main contribution is to ensure TF resistance. Most TF-resistant DB protocols achieve this property by binding the responses of the time-critical phases to a long-term secret key. This forces the provers to reveal to their MiM accomplices some bits of their secret key to authenticate, thus allowing their accomplice to impersonate a prover in latter runs of the protocol. Our approach represents a radical change in the sense that it is based on a session key, chosen by a legitimate prover and signed with his group signature key, before being encrypted. To prevent replay attacks, the responses to the time-critical phases depend on a verifier-specific nonce. However, given a value that is reasonably close to the prover's session key, the adversary can replay the prover's signature to be authenticated on his behalf. The presence of a *backdoor*, which can be used to retrieve the information needed to impersonate a prover, should deter any prover to help potential accomplices. This was originally suggested by Fischlin and Onete [5].

Novel Approach In contrast to most protocols in the literature, our DB protocol does not rely on a long-term shared secret between a prover and the verifier, but on a session key NP exchanged anonymously. Long-term shared secrets constitute a serious burden to overcome to provide anonymity for the prover as these secrets can be easily used to link different sessions of a user. The radical shift that we propose is our main contribution. Hence, SPADE is built in such a way that an adversary can replay a session key if he gets access to it (e.g., during a TF). To ensure that provers protect their session keys, we introduce a stateless backdoor in the verifier, allowing an adversary to recover the complete session key NP provided that he knows enough bits about it (Figure 2). This sets a trade-off between the malicious prover and any potential accomplice. Indeed, providing too much information to an accomplice, he may eventually impersonate the prover, which is not desirable. At the other end of the spectrum, by not giving him enough information, he may not be helpful to the prover. This new approach for proving the TF resistance makes SPADE the first secure provable revocable and anonymous DB protocol.

Prover P, $\mathsf{pk}_v, \mathsf{ssk}_p$		**Verifier** V, $\mathsf{sk}_v, \mathsf{gpk}$
	Initial message	
	$\xrightarrow{b}$	
if $b = 0$, run the protocol normally		
else		$(N_P, \sigma) = \mathsf{E.dec}_{\mathsf{sk}_v}(e)$
	$\xrightarrow{e, N'_P}$	if $\mathsf{G.ver}_{\mathsf{gpk}}(\sigma, N_P, \mathsf{RL}) = 1$ and $d_H(N_P, N'_P) \leq t$
	$\xleftarrow{ret}$	then $ret = N_P$ else $ret = 0$

FIGURE 2: The backdoor mechanism. If the initial message is $b = 0$, the protocol is run normally. Otherwise, the verifier simply waits to receive a value e that he parses as (N_P, σ) and a string N'_P. If N_P and N'_P are close enough (the Haming ditance $d_H(N_P, N'_P)$ is smaller or equal than t, he returns N_P.

3 Conclusion

Considering the widespread development of contactless technologies, we believe that it is crucial to develop provably secure DB protocols, which address privacy issues to limit the ability of tracking users. In this paper, we have proposed SPADE, a provably TF-resistant prover-anonymous DB protocol, which uses group signatures to hide the prover's identity, even against a potentially malicious verifier. While our construction is prover anonymous and provably resistant to all known attacks against DB protocols (DF, MF, TF, IF), the backdoor introduced to obtain the TF-resistance lowers the resistance of the protocol to other threats. This is a frequent problem when designing provably TF-resistant protocols. In addition to building the first protocol ensuring these properties, we have introduced a promising new approach to ensure TF resistance. In essence, the information leaked to an accomplice during a TF is no longer a long-term secret key but rather a temporary session key. Such a session key can then be used by the accomplice to authenticate. This novel approach opens the door for further research on terrorist fraud resistance.

Références

[1] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures : Formal definitions, simplified requirements, and a construction based on general assumptions. In *Advances in Cryptology – EUROCRYPT 2003*, pages 614–629. Springer, 2003.

[2] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J.-J. Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3) :175–183, 1991.

[3] S. Brands and D. Chaum. Distance-bounding protocols. In *Proc. of Advances in Cryptology – EUROCRYPT'93*, volume 765 of *LNCS*, pages 344–359. Springer-Verlag, 1993.

[4] X. Bultel, S. Gambs, D. Gerault, P. Lafourcade, C. Onete, and J. Robert. A prover-anonymous and terrorist-fraud resistant distance-bounding protocol. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WISEC 2016*, pages 121–133. ACM, 2016.

[5] M. Fischlin and C. Onete. Terrorism in distance bounding : Modeling terrorist fraud resistance. In *Proceedings of ACNS 2013*, volume 7954 of *LNCS*, pages 414–431. Springer Verlag, 2013.

[6] S. Gambs, C. Onete, and J.-M. Robert. Prover anonymous and deniable distance-bounding authentication. In *Proceedings of AsiaCCS 2014*, pages 501–506. ACM Press, 2014.

[7] J. Hermans, R. Peeters, and C. Onete. Efficient, secure, private distance bounding without key updates. In *Proceedings of WiSec 2013*, pages 207–218. ACM Press, 2013.

[8] C. H. Kim, G. Avoine, F. Koeune, F. Standaert, and O. Pereira. The swiss-knife RFID distance bounding protocol. In *Information Security and Cryptology (ICISC) 2008*, LNCS, pages 98–115. Springer, 2008.

[9] S. Vaudenay. Proof of proximity of knowledge. Cryptology ePrint Archive, Report 2014/695, 2014. http ://eprint.iacr.org/2014/695.pdf.