Report

A distance hijacking attack on the CRCS distance bounding protocol

Author(s):
Cremers, Cas

Publication Date:
2011

Permanent Link:

https://doi.org/10.3929/ethz-a-006905056 →

A distance hijacking attack on the CRCS distance bounding protocol

ETH Zurich, Technical Report number 718

Department of Computer Science
Chair of Information Security

Cas Cremers

Version 1.1, February 25, 2011

Abstract

In [2], Rasmussen and Capkun present a practical distance verification mechanism and use it to construct the first practical distance bounding protocol. In this paper we show that the protocol is vulnerable to what we call a *distance hijacking attack*, in which a malicious prover Q can convince the verifier V that he is at the same distance as some honest prover P, even though Q is further from V than P, by inserting his own identity into a run of the distance bounding protocol between P and V.

1 Introduction

The CRCS protocol is presented by Rasmussen and Capkun in [2]. The core of the protocol is a novel mechanism for distance verification that requires no demodulation of the signal, thereby significantly reducing the processing time required of the prover. This effectively allows the distance verification phase to achieve an unprecedented precision, which is an enabling factor in making distance bounding practical. For details on this mechanism we refer the reader to the original paper.

Our focus here is the CRCS distance bounding protocol that is built around the previously mentioned distance verification mechanism. The protocol is based on the original distance bounding protocols by Brands and Chaum [1] and involves a PKI scheme. In particular, our focus will be on the (logical) interaction between the distance verification mechanism and the PKI-based authentication aspect of the CRCS protocol.

Overview. We present the logical structure of the CRCS protocol in Section 2. In Section 3 we present a type of attack that we call a *distance hijacking*

attack on the CRCS protocol, in which a malicious prover Q "hijacks" the session of a honest prover P. Let the distance between x and y be denoted as $dist(x, y)$. The attack effectively enables Q to make a verifier V believe that the distance between Q and V is equal to $dist(P, V)$. Finally, we conclude in Section 4.

2 The CRCS protocol

The CRCS protocol is presented by Rasmussen and Capkun in [2].

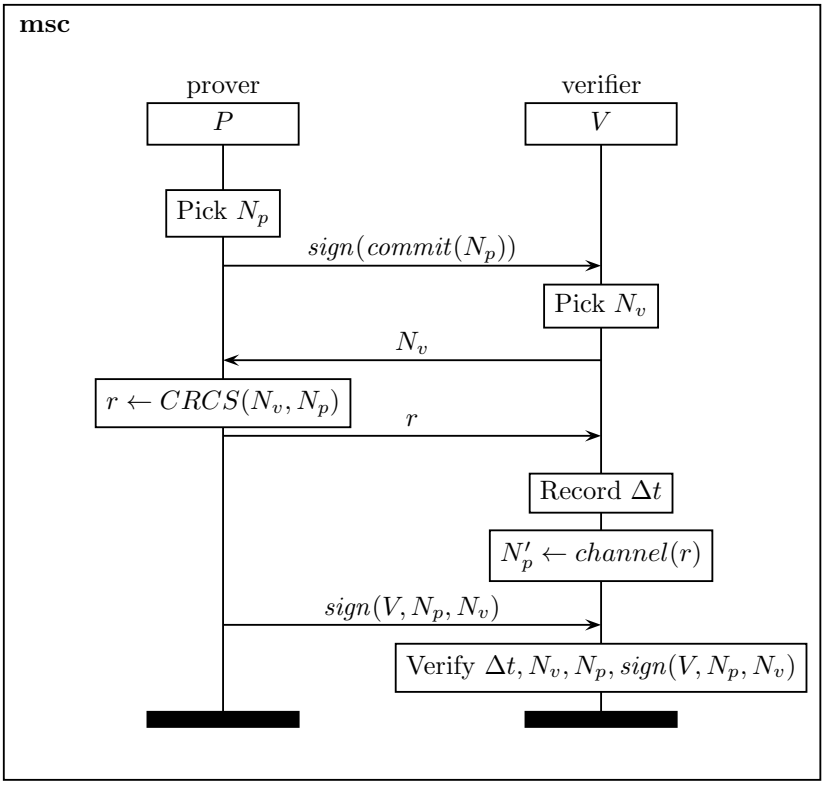

Figure 1: the CRCS protocol

In the original CRCS description, the fact that the prover's identity is equated with his signature key and this key is assumed to be unique, is left implicit. This link can be made explicit by writing the signing operation as $sign_P(\ldots)$. We will use this convention in the following.

Additionally, in order to allow for practical verification of the signature, the identity P should be included in plain text in one of the protocol messages. This can be delayed until the last message. We assume in the following that the identity P is included in plaintext in the final message.

3 Distance hijacking attack on the CRCS protocol

In the attack, there are two provers, P and Q. Q is further from the verifier than P. Q aims to convince the verifier that he is closer than he actually is; in fact, he will convince the verifier that he is as close as P is. The attack requires P to attempt to start the protocol with the verifier. Q replaces P's signed messages with identical messages, except that they are signed by Q.

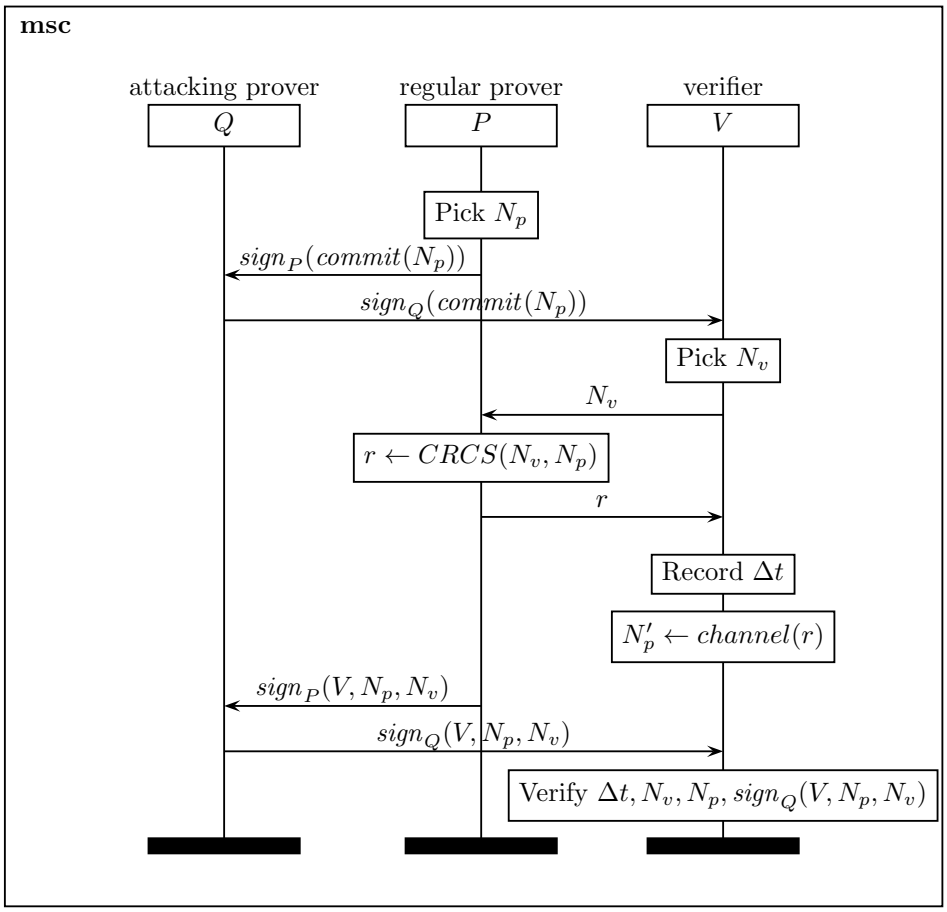

Figure 2: attacking the CRCS protocol

Note that in the attack, Q does not learn N_p from the first message, nor does it need to.

The practicality of the attack is not directly relevant for our analysis. However, it seems that a combination of selective jamming and eavesdropping during jamming would be sufficient to make this attack practical.

Analysis

We observe that the attack depends on the fact that the information exchanged during the distance bounding does not depend on the identity of the prover. The link is assumed to be made through the nonces. The conclusion about the distance is P is drawn on the basis of the assumption that it is P's nonce that is used during the reflection phase. However, the verifier cannot rely on the prover to honor this convention, and the attack exploits the weak binding between the nonces and the identities. In the attack Q claims to be at P's distance by using P's nonce and having P perform the reflection phase.

Cleary, the distance hijacking attack works in scenarios where a verifier accepts proofs from multiple provers. However, this assumption is not strictly required for the attack. Consider an implementation with multiple pairs of provers and verifiers, i.e., $(P_1, V_1), \ldots, (P_n, V_n)$, where verifier V_i only accepts proofs-of-distance from prover P_i. Even in such a scenario, a prover P_i can hijack a session initiated by a prover P_j to a verifier V_j $(i \neq j)$ to make V_i believe that P_i is at distance $dist(P_j, V_i)$.

4 Conclusions

It seems distance hijacking attacks were not considered before and many protocols are vulnerable to them. For example, distance hijacking attacks are possible on all protocols in [1] and the noise resilient MAD protocol from [3].

References

[1] S. Brands and D. Chaum. Distance-bounding protocols. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. Springer Berlin / Heidelberg, 1994.

[2] K. B. Rasmussen and S. Čapkun. Realization of RF distance bounding. In *USENIX Security 2010: Proceedings of the 19th USENIX Security Symposium*. USENIX, 2010.

[3] D. Singelée and B. Preneel. Distance bounding in noisy environments. In *Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks*, ESAS'07, pages 101–115, Berlin, Heidelberg, 2007. Springer-Verlag.

[4] S. Čapkun, L. Buttyán, and J.-P. Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, SASN '03, pages 21–32, New York, NY, USA, 2003. ACM.

A Changes

Version 1.0, February 17, 2011 Initial version.

Version 1.1, February 25, 2011 The original MAD protocol [4] assumes absence of jamming or jamming detection leading to protocol abortion. This seems to prevent a straightforward distance hijacking attack, and hence we replaced the reference to the MAD protocol in the conclusions by the noise resilient MAD protocol, which lacks this feature.