DB-Verify

Sjouke Mauw, Zach Smith, Jorge Toro-Pozo
and Rolando Trujillo-Rasua

University of Luxembourg

This document contains specifications of various distance-bounding protocols by using the specification language introduced in [2]. Each of the protocols listed below have been formally verified with the protocol-verification tool Tamarin[1]; all source codes can be downloaded from `http://satoss.uni.lu/software/DB-Verify/dbverify-tamarin.rar`. The outcome of such analysis is summarized in the following table.

Protocol	Discovered attack
Brands and Chaum [3]	Distance-hijacking
Weak Brands and Chaum	Mafia-fraud
Tree-based [1]	None
Poulidor [11]	None
Hancke and Kuhn [5]	None
CRCS [4]	Distance-hijacking
Meadows et al. [8]	Distance-hijacking
Weak Meadows et al.	Mafia-fraud
Kim and Avoine [6]	None
Munilla and Peinado [9]	None

Table 1: Attacks found (if any) in Tamarin on distance bounding protocols. Note that, the presence of one attack does not discard the presence of other attacks.

It is important to remark that the described protocols slightly differ from the original protocols descriptions. The reason is that distance bounding protocols typically use 1-bit messages during the fast phase, and the specification language represents messages as terms. So we have collapsed 1-bit messages into a single (typically n-bit) message.

[1] `http://tamarin-prover.github.io/`

Brands and Chaum's protocol. The first protocol of this list is the Brands and Chaum's protocol [3]. A description of the protocol can be found in Figure 2. Furthermore, for the sake of illustration we also describe and implement a modification of this protocol where the commitment scheme is different and the final message is only used to open the commitment. We call such a toy protocol the *Weak Brands and Chaum's protocol*.

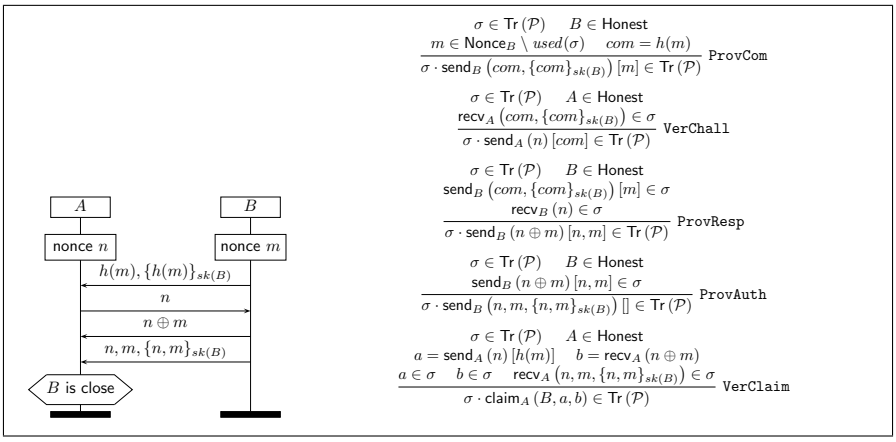

Figure 1: Brands and Chaum's protocol.

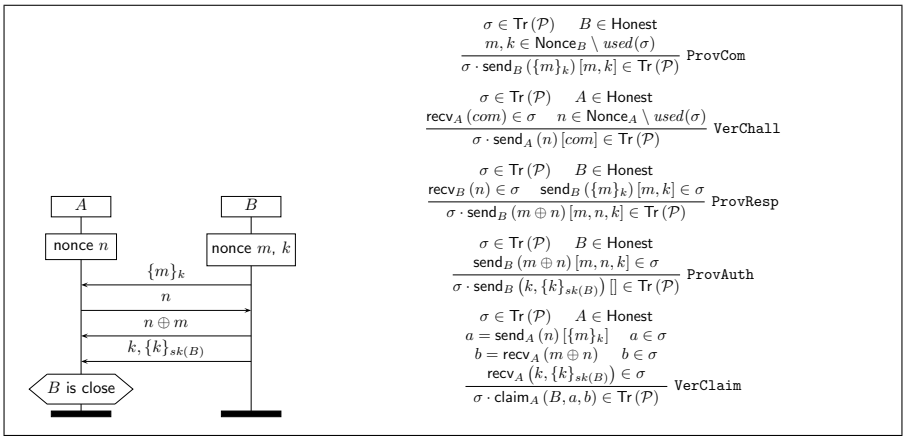

Figure 2: Weak Brands and Chaum's protocol.

CRCS protocol [10]. Figure 3 shows the CRCS protocol proposed by Rasmussen and Čapkun. Both h and f are considered hash functions.

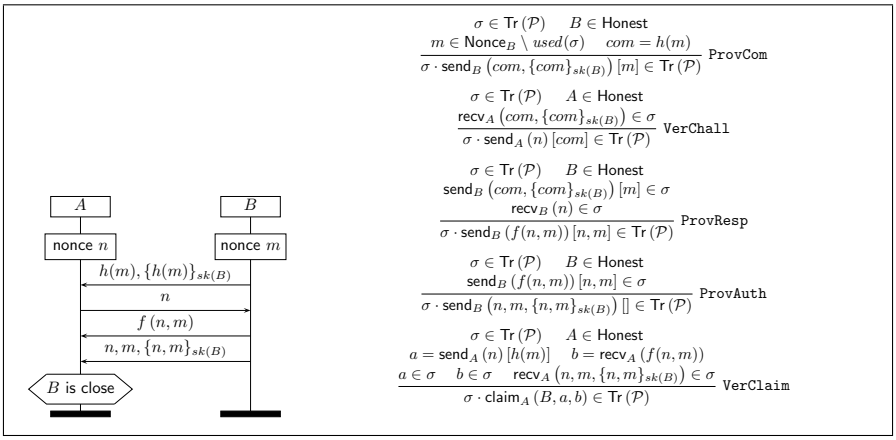

Figure 3: CRCS protocol.

HK-like protocols. By HK-like protocols (see Figure 4) we refer to the Hancke and Kuhn's protocol [5] and other similar protocols based on pre-computation, namely the Tree-based [1], Poulidor [11], and Kim and Avoine's protocol [6]. These type of protocols can be analyzed in a unified model, as shown in [7], and we do the same in this document. In the figure, h is a hash function and $k(A, B)$ stands for the secret shared key between A and B.

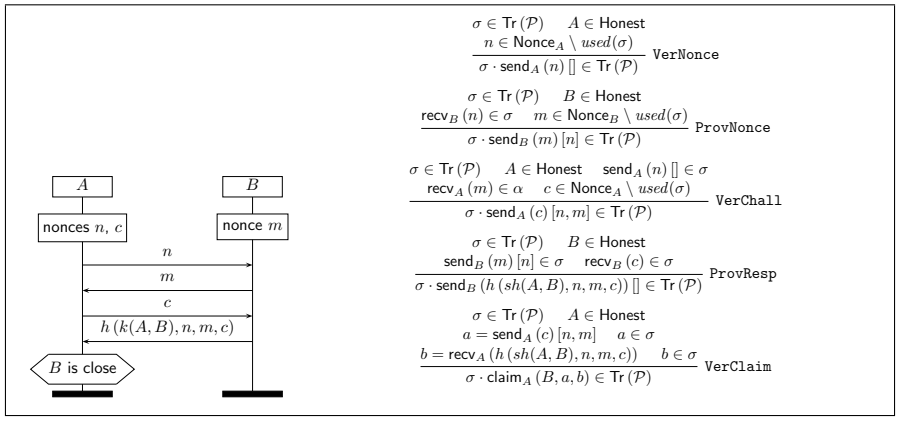

Figure 4: HK-like protocols.

Meadows et al.'s protocol [8]. In Figure 5 we describe the Meadows et al.'s protocol where h is a hash function and $k(A, B)$ denotes the secret shared key between A and B. We also verified (for illustration purposes only) a weaker version of this protocol that does not include the prover's location in the final message nor the verifier's nonce. The *Weak Meadows et al.'s* protocol is depicted in Figure 6.

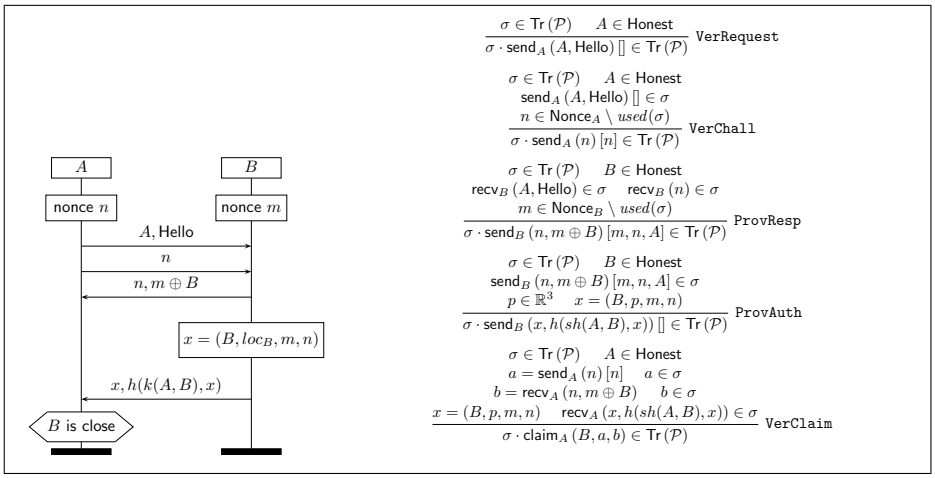

Figure 5: Meadows et al.'s protocol.

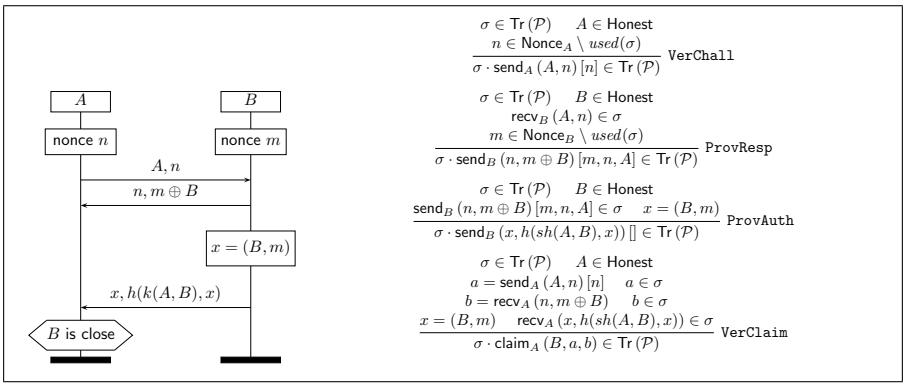

Figure 6: Weak Meadows et al.'s protocol.

References

[1] Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement. In *ISC'09*, pages 250–261, 2009.

[2] David A. Basin, Srdjan Capkun, Patrick Schaller, and Benedikt Schmidt. Let's get physical: Models and methods for real-world security protocols. In *TPHOLs'09*, pages 1–22, 2009.

[3] Stefan Brands and David Chaum. Distance-bounding protocols. In *EUROCRYPT'93*, pages 344–359, 1993.

[4] Cas J. F. Cremers, Kasper Bonne Rasmussen, Benedikt Schmidt, and Srdjan Capkun. Distance hijacking attacks on distance bounding protocols. In *S&P'12*, pages 113–127, 2012.

[5] Gerhard P. Hancke and Markus G. Kuhn. An RFID distance bounding protocol. In *SecureComm'05*, pages 67–73, 2005.

[6] Chong Hee Kim and Gildas Avoine. RFID distance bounding protocol with mixed challenges to prevent relay attacks. In *CANS'09*, pages 119–133, 2009.

[7] Sjouke Mauw, Jorge Toro-Pozo, and Rolando Trujillo-Rasua. A class of precomputation-based distance-bounding protocols. In *EuroS&P'16*, pages 97–111, 2016.

[8] Catherine A. Meadows, Radha Poovendran, Dusko Pavlovic, LiWu Chang, and Paul F. Syverson. Distance bounding protocols: Authentication logic analysis and collusion attacks. In *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, pages 279–298. 2007.

[9] Jorge Munilla and Alberto Peinado. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. *Wireless Communications and Mobile Computing*, 8(9):1227–1232, 2008.

[10] Kasper Bonne Rasmussen and Srdjan Capkun. Realization of RF distance bounding. In *USENIX Security'10*, pages 389–402, 2010.

[11] Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine. The poulidor distance-bounding protocol. In *RFIDSec'10*, pages 239–257, 2010.