

Timed Analysis of RFID Distance Bounding Protocols

Yu Lu¹

Alice Miller²

¹ School of Computing Science, University of Glasgow, UK, y.lu.3@research.gla.ac.uk

² School of Computing Science, University of Glasgow, UK, alice@dcsc.gla.ac.uk

Abstract: Modelling real time is fundamental to reason about pervasive systems. The formal analysis of some time sensitive security protocols, such as distance bounding protocols, could lead to a more formal approach to time dependent properties formalisation and verification of pervasive systems.

1 Introduction

Pervasive systems often contain devices which must operate in very different environments and connect together in different ways, and still satisfy all the desired security properties. The rapid development of wireless technologies (such as RFID) has led to new application areas for pervasive systems with novel security requirements for the protocols employed. Unlike traditional security protocols concerning message secrecy or different types of authentication, these new protocols employed in new applications usually establish security properties coupled with the wireless network environment.

Physical location is used as a measurement of trust in wireless networks, RFID-based systems and vehicular communication that require secure localisation, time synchronisation, neighbour discovery, and neighbour verification. For such location services, it is crucial to securely estimate distance between two nodes in a wireless network and thus impede man-in-the-middle attacks. The main countermeasure against such attacks is the use of *Distance bounding (DB) protocols*. DB protocols are a class of identification protocols in which one “verifier” node in wireless networks measures an upper bound on its distance to another “prover” node in the network. Accordingly, the security of DB protocols is applicable to most pervasive computing applications.

So far, DB protocols have been extensively studied: a large number of protocols have been proposed and analysed in the past decade. Regardless of the different type of DB protocols, the distance bound is obtained from a rapid exchange of messages between the verifier and the prover in the fast bit phase. In this phase, the verifier sends a challenge to the prover, to which the prover responds after some processing time. The verifier measures the round-trip time between sending its challenge and receiving the responses from the prover, subtracts the prover’s processing time, and based on the remaining time, computes the distance bound between the devices.

Typically, DB protocols are designed and analysed with respect to three different classes of attack scenarios:

- *Mafia fraud* attacks where the attacker $\mathcal{A}$ relays communication between a honest prover P and a honest verifier V in different sessions
- *Distance fraud* attacks where a malicious prover P

claims to be closer to the verifier V than it actually is

- *Terrorist fraud* attacks where the attacker $\mathcal{A}$ gets limited active support from the prover P to deceive the verifier V

All attacks aim to make the verifier believe that the prover P is physically closer to the verifier V than it really is. Recently, a fourth type of real time attack on DB protocols, called *Distance hijacking* attacks, has been defined and analysed [4]. Although nowadays many proposed DB protocols are resistant to mafia fraud, verifying DB protocols using existing informal and formal frameworks still does not guarantee the absence of other attacks, e.g., the distance hijacking.

2 Related Work

The first DB protocol was proposed in [3] in 1993, but the first formal analysis of DB protocols was presented in 2007 ([9]). In [9], the authors not only proposes a new protocol for distance bounding that requires less message and cryptographic complexity, but also uses authentication and secrecy logics to analyse its security. Their logical framework is only based on qualitative analysis and does not provide any extended analysis of the timing properties. Since then, several quantitative frameworks for the verification of real time sensitive protocols have been proposed.

The constraint solver tool, which is a protocol security analyzer taking advantage of constraint programming techniques, was used to automatically analyse DB protocols in [8]. A natural limitation of their analysis is that it cannot tackle unbounded analysis since the constraint solver only considers bounded number of protocol processes. Meanwhile, a related approach to modelling and verifying physical properties (namely communication, location, and time) of DB protocols using HOL/Isabelle was presented in [10]. Being a verification effort, the two approaches in [8] and [10] differ in the classical way that model checking differs from theorem proving: the former tests for attacks while the latter proves their absence of.

It seems that since the introduction of the first RFID distance bounding protocol [7] in 2005, numerous DB protocols have been proposed, in an attempt to make them appropriate for the RFID systems. Unfortunately, many protocols in the literature address no rigorous cryptographic

security models, nor the case of clear security proof. Also, they are commonly designed without any formal methods, which lead to inaccurate analyses. We consider that distance bounding for RFID systems is more difficult to achieve due to constrained resource of RFID tags.

During the last two years, there has been a recent surge in interest and research, in the arena of formal approaches to RFID-based distance bounding protocols. A new framework [6] was proposed, based on common game-based notion on cryptography, to analyse the security of the RFID DB protocols. Although this new approach addresses RFID authentication and can also be applied to general DB protocols, it still abstracts away from timed analysis. Another systematic method [2] aims to improve analysis and design of RFID DB protocols. Although the unified framework includes a thorough terminology about frauds, attackers, and provers, thus clarifying many misleading terms, the generic model only allows for the refinement of the security analysis, but not to verify security properties.

3 Our Approach

To the best of our knowledge, all the existing techniques for verifying security protocols specifically for pervasive systems abstract away from real time, focusing only on the sequencing of events. Although this has many advantages, it is a serious limitation for reasoning about RFID protocols for secure distance bounding, which rely on real time considerations. Furthermore, past efforts to analyse DB protocols have only been manual. Automated analysis would avoid the problems and distrust in manual analysis of protocols that have often been reported. Thus, we consider that automated approaches are critical since they are quite likely to find flaws that manual approaches cannot.

Our contributions will be threefold: (1) To give in-depth and rigorous analyses of how to formalise time dependent properties in security protocols using modelling languages such as applied pi calculus [1], (2) to define the time dependent security properties formally against attacks RFID distance bounding protocols could address. Finally, (3) we will extend existing formal verification techniques (such as model checking and process calculi), towards a automated verification of such protocols.

The most two popular approaches are based on automated methods, such as model checking, and interactive methods, such as theorem proving. In both scenarios, it is standard to formalise an intruder model based on the Dolev-Yao model [5], which identifies the intruder with the network. However, the conventional Dolev-Yao style analysis of security protocols is inappropriate to analyse DB protocols in our case. Analysis of RFID DB protocols involves examining whether it is possible to make a tag appear closer than it really is, to an honest reader. The problem is different and difficult compared to standard Dolev-Yao analysis of protocols that only consider whether an attacker can generate messages required to violate some security properties. Thus, we need to consider the timing required for genera-

tion and transmission as well.

Formal verification using automatic verifier ProVerif has been discussed in [8] as an extension of their analysis. In particular, it suggests adding four events in the DB protocols, two each for the verifier and prover, corresponding to sending and receiving the challenge and rapid response in the fast bit phase. The security property they formulate is a time-based trace equivalence that we plan to formalise in applied pi calculus as a starting point for our timed analysis.

4 Conclusion

The timed analysis of RFID distance bounding protocols will enable us to tackle the problem of modelling real-time aspects in timed process calculi and thus define and formally verify time dependent security properties. This will be essential to formally verify pervasive systems.

References

- [1] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. POPL '01*, pages 104–115, 2001.
- [2] G. Avoin, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin. A framework for analyzing RFID distance bounding protocols. *Journal of Computer Security*, 19(2):289–317, 2011.
- [3] S. Brands and D. Chaum. Distance-bounding protocols. *LNCS*, 765:344–359, 1994.
- [4] C. Cremers, K. B. Rasmussen, and S. Capkun. Distance hijacking attacks on distance bounding protocols, 2011.
- [5] D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.
- [6] U. Dürholz, M. Fischlin, M. Kasper, and C. Onete. A formal approach to distance-bounding RFID protocols. In *Proc. ISC'11*, pages 47–62, 2011.
- [7] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *Proc. SECURECOMM '05*, pages 67–73, 2005.
- [8] S. Malladi, B. Bruhadeshwar, and K. Kothapalli. Automatic analysis of distance bounding protocols. *CORR*, 2010.
- [9] C. Meadows, R. Poovendran, D. Pavlovic, Chang L., and P. Syverson. Distance bounding protocols: Authentication logic analysis and collusion attacks. *Advances in Information Security*, 30(Part II):279–298, 2007.
- [10] P. Schaller, B. Schmidt, D. Basin, and S. Capkun. Modeling and verifying physical properties of security protocols for wireless networks. In *Proc. CSF '09*, pages 109–123, 2009.