Master project in Information Security at the University of Luxembourg

Title: Distance Bounding: a graph theoretical approach

The Security and Trust of Software Systems group, led by Prof. Dr. Sjouke Mauw, is looking for outstanding master students who want to develop their master thesis within our group.

Project description

Like the air we breath, wireless channels are intangible and openly accessible, which make them a convenient communication means. These features, however, increment the likelihood and severity of various security threats. Outstanding examples are *mafia* and *distance fraud*; two attacks proposed in 1988 [3] and 1993 [2], respectively, that were brought back to popularity in 2005 [4] thanks to the worldwide adoption of the RFID technology. Mafia fraud, sometimes called relay attack, is a man-in-the-middle attack where the adversary actively participates in an authentication protocol by relaying messages between two parties, making them believe that they have a direct communication. This attack can easily break a proximity claim that appears in many cryptographic applications and standardized contactless interfaces, such as ISO 14443, ISO 15693, and ISO 18092.

Physical proximity is indeed a common requirement in access control policies in the physical world. One normally expects someone to be present when opening a door or turning on a car. In practice, the very design of many access control mechanisms enforces physical proximity naturally, e.g., mechanic locks or biometric identification. In wireless systems, however, providing the same kind of guarantee is far from being trivial. The most reliable approach to proximity checking in wireless systems is distance bounding, that is, a cryptographic protocol where the propagation time of messages traveling at the speed of light determine an upper bound on the distance between two devices.

The purpose of this project is to improve the security of graph-based distance bounding protocols; a prominent family of distance bounding protocols based on random walks in graphs. Graph-based distance bounding protocols are efficient building blocks suitable to be implemented in low-cost devices such as RFID tags. One based on trees [1] and another one based on a peculiar graph structure named Poulidor [5], are the two graph-based distance bounding protocols proposed up to now. They remain unbroken, and no other distance bounding protocol has proven to outperform them. Nevertheless, very little is known about this type of protocols.

General goal. In this project, we will study the relation between graph properties and the security properties of graph-based distance bounding protocols. We observe that the Poulidor graph belongs to the well known family of Cayley graphs. Therefore, understanding and studying the relation between graph-based hash functions (where Cayley graphs are used) and graph-based distance bounding protocols, may lead to better designs of this type of security protocols.

Contact Information

For further inquiries please contact:

- Prof. Dr. Sjouke Mauw (`sjouke.mauw@uni.lu`) or
- Dr. Rolando Trujillo (`rolando.trujillo@uni.lu`)

References

[1] Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement. In *Information Security, 12th International Conference, ISC 2009, Pisa, Italy, September 7-9, 2009. Proceedings*, pages 250–261, 2009.

[2] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, EUROCRYPT '93, pages 344–359, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[3] Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and sbuses of the fiat-shamir passport protocol. In *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, CRYPTO '87, pages 21–39, London, UK, UK, 1988. Springer-Verlag.

[4] Gerhard P. Hancke and Markus G. Kuhn. An rfid distance bounding protocol. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, SECURECOMM '05, pages 67–73, Washington, DC, USA, 2005. IEEE Computer Society.

[5] Rolando Trujillo-Rasua, Benjamin Martin, and Gildas Avoine. The poulidor distance-bounding protocol. In *Radio Frequency Identification: Security and Privacy Issues - 6th International Workshop, RFIDSec 2010, Istanbul, Turkey, June 8-9, 2010, Revised Selected Papers*, pages 239–257, 2010.