Mete Akgün

Thesis Supervisor: Prof. Mehmet Ufuk Çağlayan

Security and Privacy of RFID Protocols

Abstract

This thesis studies security and privacy issues of Radio Frequency Identification (RFID) technology that enhances ubiquitous computing environment. Privacy is one of main issues to adopt RFID technology in daily use. Due to resource constraints of low cost RFID tags in terms circuit size, power consumption and memory size, it is very restricted to design a private authentication protocol based on existing cryptographic functions. Therefore new private authentication protocols should be designed with lightweight cryptography primitives.

In this thesis, we focus on the security of low cost RFID tags. Our contributions are as follows. First, we analyze the security of recent RFID authentication protocols with respect to two security requirements: mutual authentication and availability. We propose impersonation and de-synchronization attacks against recent RFID authentication protocols.

Secondly, we analyze the security of chaotic-map based RFID protocols. We propose secret disclosure, tracking, impersonation and de-synchronization attacks against these protocols. We propose revised protocols resistant to our proposed attacks.

Finally, we study privacy and scalability issues in RFID. All previous RFID protocols giving the desired level of privacy required linear work in the back-end server. There are several PUF-based protocols which requires work logarithmic in the number of RFID tags in a system. We propose PUF-based scalable authentication protocols for RFID systems. They provide destructive privacy according to the Vaudenay's privacy and security model. They defend against compromising attack by using PUFs as a secure storage to keep secrets of the tag. To the best of our knowledge, they are the first to provide this level of privacy with constant identification time.

PUBLICATIONS

Journals

1. **Akgün, M.** and Çağlayan, M. U. (2015). Providing destructive privacy and scalability in RFID systems using PUFs. Ad Hoc Networks, 32:32-42
2. **Akgün, M.**, Bayrak, A. O., and Çağlayan, M. U. (2015). Attacks and improvements to chaotic map-based RFID authentication protocol. Security and Communication Networks, 8(18):4028-4040
3. **Akgün, M.** and Çağlayan, M. U. (2015). Towards Scalable Identification in RFID Systems. Wireless Personal Communications, pages 1-19

Conferences

1. **Akgün, M.** and Çağlayan, M. U. (2015). Weaknesses of two RFID protocols regarding de-synchronization attacks. In International Wireless Communications and Mobile Computing Conference, IWCMC 2015, Dubrovnik, Croatia, August 24-28, 2015, pages 828–833

2. **Akgün, M.** and Çağlayan, M. U. (2014). Vulnerabilities of rfid security protocol based on chaotic maps. In 2014 22st IEEE International Conference on Network Protocols, ICNP 2014, Raleigh, North Caroline, October 21-24, 2014, pages 1–6
3. **Akgün, M.** and Çağlayan, M. U. (2011). PUF Based Scalable Private RFID Authentica- tion. In Sixth International Conference on Availability, Reliability and Security, ARES 2011, Vienna, Austria, August 22-26, 2011, pages 473–478
4. Kardaş, S., **Akgün, M.**, Kiraz, M., and Demirci, H. (2011). Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. In Lightweight Security Privacy: Devices, Protocols and Applications (LightSec), 2011 Workshop on, pages 20–25
5. **Akgün, M.**, Özhan Gürel, A., and Çağlayan, M. U. (2010). Attacks to a lightweight RFID mutual authentication protocol. In 5th International Conference for Internet Technology and Secured Transactions, ICITST 2010, London, United Kingdom, November 8-10, 2010, pages 1–5
6. **Akgün, M.** and Çağlayan, M. U. (2010). Extending an RFID Security and Privacy Model by Considering Forward Untraceability. In Security and Trust Management – 6th International Workshop, STM 2010, Athens, Greece, September 23-24, 2010, Revised Selected Papers, pages 239–254
7. **Akgün, M.** and Çağlayan, M. U. (2010). Server Impersonation Attacks and Revisions to SLAP, RFID Lightweight Mutual Authentication Protocol. In Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on, pages 148–153
8. Özhan Gürel, A., Arslan, A., and **Akgün, M.** (2010). Non-uniform Stepping Approach to RFID Distance Bounding Problem. In Data Privacy Management and Autonomous Spontaneous Security - 5th International Workshop, DPM 2010 and 3rd International Workshop, SETOP 2010, Athens, Greece, September 23, 2010, Revised Selected Papers, pages 64–78
9. **Akgün, M.**, Çağlayan, M. U., and Anarım, E. (2009). Secure RFID authentication with efficient key-lookup. In Proceedings of the Global Communications Conference, 2009. GLOBECOM 2009, Honolulu, Hawaii, USA, 30 November - 4 December 2009, pages 1–8
10. **Akgün, M.**, Çağlayan, M. U., and Anarım, E. (2009). A new RFID authentication protocol with resistance to server impersonation. In 23rd IEEE International Symposium on Parallel and Distributed Processing, IPDPS 2009, Rome, Italy, May 23-29, 2009, pages 1–8

Defense Jury Members

1. Prof. Mehmet Ufuk Çağlayan Boğaziçi University
2. Prof. Fatih Alagöz Boğaziçi University
3. Prof. Emin Anarım Boğaziçi University
4. Prof. Albert Levi Sabancı University
5. Prof. Semih Bilgen Yeditepe University

Defense Date: 11.12.2015