On Security and Privacy Enhanced Authentication of RFID

Mohammad Shahriar Rahman (710079)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 5, 2009

Keywords: RFID, Security, Privacy, Batch-mode Authentication, Aggregate Hash.

In this master graduate thesis, we studied on the security and privacy enhanced authentication of RFID. Privacy and security of RFID is recently a popular research area which has drawn attentions of both the industry and academia. When cryptography is used in RFID tag deployment, concerns rise about the fundamental resources required by an algorithm. The security threats in an RFID tag spans from issues like tracking, denial of service, data authentication, tag and/or reader authentication, communication efficiency, through to a burning issue:- consumer privacy. The range of security threats and their importance varies from application to application.

Cryptographic algorithms are mainly classified into two classes according to how they use key material. If the parties involved in a cryptographic communication are using secret-key or symmetric cryptography then they will share the same key material. If the two parties are using public-key or asymmetric cryptography, then they will use different key material. In this case the key used by the sender of an encrypted message will be publicly available.

Considering the diversified functionality, it can be said that either type of cryptography might be used in principle for RFID. However, one significant difference between them is the supporting infrastructure that they require.

Such considerations may well make one type of cryptography far more suitable than the other. A second difference, and one that is often cited in RFID tag applications, is that symmetric algorithms tend to require less computational resources than asymmetric algorithms.

Estimates vary on exactly what space resources might be available at the low-end of the market. The notion of gate equivalents (GE) corresponds directly to the physical space that is occupied on silicon. This in turn depends on the manufacturing technology used. It is assumed that RFID tags at the lower-end of the market might have a total gate count of around 1000-10,000 GE with around 200-2000 GE being available for security features. While we might be looking at around 2000 GE for security functionality in the cheaper tags today, enthusiasts of Moores Law (Moore, 1965) observes that this suggests around 10,000 GE may be available for a similar price in next few years.

In batch mode, a reader scans numerous tags, collects the replies, and sometimes, performs their identification and authentication later in bulk. The batch mode is appropriate when circumstances prevent or inhibit contacting the back-end server in real time. An inventory control system, where readers are deployed in a remote warehouse and have no means of contacting a back-end server in real time is such an application.

In this thesis, we have studied the recent privacy preserving RFID authentication protocols. We also studied the vulnerabilities and threats in the RFID. Although many works have been done recently on RFID security and privacy, a few works have focused on reducing the communication cost in the RFID environment. Not all the protocols we studied, can satisfy all the security requirements. Some of them also require high communication, computation cost. Elliptic curve based protocols take about 10000 gates, which is well beyond the reach of todays passive tags. Moreover, reader authentication is also not supported by some of them. But reader authentication is required to thwart illegal tracking or cloning of the tags. It is also important to keep the number of messages passed as low as possible. More than 2-pass protocols require more communication overhead, and a tag requires to 'remember' all the intermediate states to complete the protocol. All this translates into needing more resources on the tag. In some protocols, it is assumed that an external device is attached with the tag.

This is not practical for applications where batch-mode authentication is done.

We have introduced a two-way message authentication protocol where both tag and reader authenticate each other. Compared to the previous RFID authentication protocols, our protocol is an improvement from the efficiency's point of view especially for batch-mode; our protocol satisfies security requirements better and the required computation is kept at a minimum. Moreover, we show the use of aggregate function for the reader to server communication. The reader to server communication cost is reduced through introducing aggregate hash function. In our two-way authentication protocol, a reader helps a tag to recover from the non-operative state. Furthermore, our scheme provides reader authentication to thwart tag cloning. In the extended version of our scheme, the reader uses partial authentication to keep the rogue tags out of the aggregate function. One significant point here to notify that, the extended version of the protocol increases communication cost for both the tag to reader and server to reader interaction. However, sacrificing a part of communication cost strengthens the security. The partial authentication by the reader helps filter out malicious tags. This erases inclusion of any rogue tag in the aggregate function, which leads into no anomaly when the server verifies the aggregate value. To be precise, this increases a tag's computation by one hash function and also the tag to reader communication by b bits where b is the bit length of messages (assuming all are equal in bit size). We consider this as a trade-off between security and efficiency. However, the level of security is improved compared to the previous works as it provides resistance against DoS, Cloning, Replay, and Tracking attacks. It also provides forward security and does not allow a tag to become non-operative unless explicitly done by the reader.

We emphasize that, for a batch mode environment where validating a number of tags in a very small amount of time, Algorithm 4 in the chapter 5 is suitable - where the communication cost is the least. In such a batch mode environment, tags are authenticated in a bulk; hence it is enough to verify the authentication of the whole batch together in a least possible time. Even though the extended protocol is not much effective for batch mode environment where validating a number of tags in a small amount

of time is required, it can be used in the settings where the server is not readily available (Police checking drivers' licenses with mobile readers is such a condition, where the bulk of the licenses are finally authenticated later by the server; or, inventory control system where readers are deployed in a remote warehouse and have no means of contacting a back-end server, for examples). In such situations, the reader can partially authenticate the tags. Moreover, the extended version is also suitable for small number of tags or even for individual tag authentications.

As part of the future works, searching cost by the server for individual tags has to be reduced. Till now, many privacy-preserving authentication protocols are proposed. But a few research treats key management of the tags. RFID released within an RFID infrastructure should migrate to another RFID infrastructural domain. Robust, Delay Tolerant computations are also yet to get focused by the researchers. Moreover, still unaddressed is how to handle revocation of rogue readers.