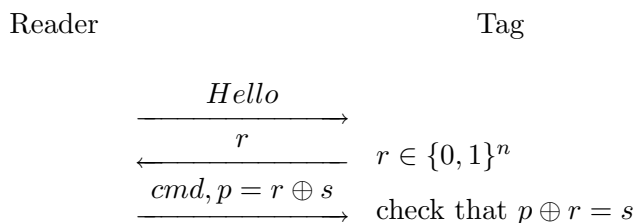


Excercises “Privacy in Sensor Networks (RFID)”

It has been observed by several authors that the channel from tag to reader is much harder to eavesdrop than the channel from reader to tag. With that in mind, Molnar and Wagner present a simple protocol for enhancing passwords in RFID tags [1]; the same protocol was independently discovered and proposed as part of the EPCglobal Gen II standards process. The main idea is for the tag to send a random nonce to the reader; an adversary who misses the nonce cannot recover the password from reader to tag communication alone. Let s be the shared secret password, and cmd the command to execute. Schematically, their protocol is:



The tag then returns the result of the check to the reader by either responding to the command or raising an error. This protocol is only intended to provide security against passive eavesdropping on the reader-to-tag link; in particular, it does not provide security against man-in-the-middle attacks or attacks that modify transmitted messages. If the adversary does not see the nonce value r , then, assuming the tag picked the nonce uniformly at random, the secret s is information-theoretically secure. Further, an adversary cannot replay protocol messages, as the nonce required by the tag changes each time. Moreover, the adversary cannot even determine whether authentication succeeded from the protocol run. Finally, because the nonce r is independent of tag data or serial number, it cannot be used to distinguish different tags. However, it requires a good source of randomness, either physical or pseudo-random, for the RFID tag; finding such a source given the limited capabilities of a tag is an open problem.

Excercise 1:

HB+, developed Ari Juels and Stephen Weis, builds on a protocol for human-to-computer authentication originally developed by Nick Hopper and Manuel Blum. It is a secure authentication protocol that is extremely simple to implement in hardware and therefore could make HB+ useful in preventing “skimming”, counterfeiting, or cloning of cheap pervasive devices like RFID tags. Describe the HB+ protocol and argue whether it may make sense to use it in a supply chain application.

See the Web page of Stephen Weis for papers and presentations on HB+ and successor proposals <http://saweis.net/hbplus.html>.

Excercise 2:

In the context of increasing debates in the European Union over the RFID policy, Peter Hustinx, the European Data Protection Supervisor (EDPS), published on 20 December 2007 his opinion

on the growing use of RFID chips in consumer products and other new applications affecting individuals http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf. On 12 May 2009, the Commission of the European Communities has published recommendations on the implementation of privacy and data protection principles in applications supported by radio-frequency identification http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf. Did the Commission adequately address the concerns of the European Data Protection Supervisor?

Excercise 2:

Literatur

- [1] D. Molnar and D. Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In *11th ACM Conference on Computer and Communications Security (CCS)*, pages 210–219. ACM Press, 2004.