Open problems pertaining to RFID anti-cloning and some observations

Benjamin Arazi
Dept. of Computer Engineering and Computer Science
University of Louisville
Louisville, KY 40292

March 24, 2007

1 Motivation

RFID (Radio Frequency IDentification) facilitates the identification and tracing of an object by wireless communication. Its main purpose is to provide automated and efficient product traceability along the entire supply chain.

RFID security issues have been identified and analyzed. In this presentation we treat the threats posed by cloned tags that transmit wrong information, or transmit pre-recorded genuine information at the wrong time or place. This presents a vital need for technologies that facilitate authenticity validation of the tag itself (known as 'object integrity') and its stored and transmitted information. A GAO report on the use of RFID technology dedicates considerable attention to security issues [1], explicitly treating cloning and re-play. Identifying a product at a cashier's terminal, for payment purposes, based on RFID communication with the product, is also associated with cloning and replay threats. Supply chain management reliability depends on information authenticity. Recording valid communication and transmitting it later at the wrong time or place can cause a havoc. It should be noted that a hostile party that wishes to disturb an RFID-based system does not even need to have RFID tags. It can use any kind of transmitter in order to transmit misleading information.

The FDA treats the use of RFID in preventing drug counterfeiting [2]. The following is taken from [3]. "*The inherent problem with EPC technology, from a pharmaceutical perspective, is the lack of anti-cloning features in the EPC chip itself....* With current EPC specifications, it is possible to programme one chip with the exact data of another, effectively cloning the first chip. Without guaranteed authentication, the usefulness of RFID is significantly reduced. META's analysts believe *RFID use within the pharmaceutical industry will be limited to a "track and trace" role until EPC specifications are revised to make cloning more difficult.*" (EPC is Electronic Product Code, the value stored in an RFID tag.)

RFID anti-cloning techniques should basically enable the tag to prove that it stores a secret key unique to the tag. The key should not leak out from the tag, either by physical means or by eavesdropping. Furthermore, the communications should include a random element, to prevent invalid replay.

2 Physical-level considerations

A secured system is as strong as its weakest link. There is no point in protecting a communication channel, if the security at the edges is compromised. As RFID tags can be physically accessed by any party, either a friend or a foe, the secret key stored at the tag should be protected based on techniques whose security strength is not inferior to that of the techniques used in protecting the transmitted data. However, while channel security techniques reached sophistication to an extent where the level of security can be *proved* based on mathematical theorems, current approaches to physical security are based on technical considerations that are more 'art' than science. (e.g., special glue, special coating techniques, clock irregularities.) No fundamental proofs are employed here, beside 'good feeling' of the designers.

Security strength is based on the extent of the inability of an adversary to perform an operation that is easily performed by valid users. This poses two challenges: devising means for executing this principle and devising means for accurately evaluating the adversary's inability. The following are some fundamental considerations that can be applied when implementing provably secured memories.

In nonvolatile molecular memory, a molecule is used to store a charge. Setting and resetting a memory cell is implemented by applying appropriate electric bias. Multilevel molecular memory involves nanowires whose electrical conductance is adjusted by molecules that accept or give electrons. Such principles provide ample possibilities for preventing external probing, whereby the interaction between the probe and the molecule disrupts the stored charge or the electrons that control the conductance of nanowires. The energy needed for reading a stored value by an external tampering probe, and the meaning of the interaction between the probe and the charge or electrons that support the memory, can be exactly evaluated using rules from classical physics. A provably secure memory should be based here on an approach whereby the mere attempt to read a stored value by resorting to illegal means would provably destroy the value attempted to be read.

Secured memories based on established theories from mechanics should also be considered. For example, possible implementation of electromechanical supports that would collapse when an outside probe approaches the structure.

Physical security considerations can also be employed in providing functionality obfuscation. This security application concerns the inability of an adversary to 'reverse-engineer' a transformation, meaning that the entire transformation acts as a secret key. Energy-preserving considerations can also be applied here using thermodynamics laws.

3 Implementation-level considerations

HMAC - keyed Hash Message Authentication Code - is a hash implementation parameterized with a secret key. The output value strongly depends or a variable input and the fixed parameterizing key, whose leakage should be protected when choosing any number of the variable inputs. RFID anti-cloning based on HMAC are an obvious choice, implementing what is known as challenge-response interrogation. However, implementation difficulties have also been raised.

The following representing statement [4] summarizes the issue: "*Tag MAC functionality would allow tags to authenticate themselves, but is beyond current low-cost tag resources*". An accurate analysis [5] states: *"the implementation of the hash standard SHA-1 requires 12,000 logic gates, while the cost constraints of an RFID tag permit the use of no more than 2,500 gates"*.

The main problem with current HMAC implementations concerns the need to execute a software code using a general processor. The software code runs a well analyzed mathematical algorithm. However, should resource-demanding highly complex cryptographic schemes be enforced just because they can be mathematically well analyzed? Shouldn't it be the other way around? That is, *an implementation that suits the conditions under which it is intended to operate should first be designed, and then analyzed, with subsequent possible modifications that enhance security while keeping the fundamental infrastructure.*

The very low processing power of an RFID-tag inherently cannot support software-specified HMAC. *There is a need to devise direct hardware implementations of HMAC, in which the security is enforced and analyzed based on hardware design considerations.*

We consider the possibility of using a variation of a stream cipher in implementing an HMAC. The cipher is a symmetric encryptor (i.e., the transmitter and receiver share the same secret key). The shared key forms a seed which generates a pseudo random stream, XORed with the cleartext stream, yielding a ciphertext stream. The receiver, having the same seed key, generates synchronously the same pseudo random stream. XORing this stream with the received ciphertext yields the cleartext back. Stream ciphers operate at a higher speed than block ciphers and have significantly lower hardware complexity.

A fundamental security requirement that should be satisfied by a stream cipher concerns noise characteristics of the generated pseudo random stream and inability to recover the secret seed key, knowing the generated stream. The security of the proposed HMAC is associated with the latter chracteristics of the cipher.

As low-cost anti-cloning is based on symmetric cryptography, the issue of key management deserves here special considerations. For example, in pharmaceutical implementations there is a need to provide all intended legal validators with means to check the authenticity of drugs they received. The drug producer that initiates the RFID tags accompanying his shipments, and the validating parties, can be at different locations on the globe. Furthermore, the identity of intended validators is even not known to the drug producer when he seals his shipments. The key-management challenges here are clear.

4 Presentation content

The issues raised above will be treated in detail at the presentation. The possibility of harnessing nanotechnology tools in providing proved physical security will be exhibited. Functionality obfuscation will also be discussed.

A complete compact hardware-based HMAC implementation based on stream ciphers will be presented, accompanied with security analysis. System-level key-management issues will also be treated.

References

[1] GAO, "Radio frequency identification technology in the federal government," United States Government Accountability Office, May 2005.

[2] FDA, "Fda counterfeit drug task force report: 2006 update," June 2006.

[3] PharmaTechnologist, "Rfid take-up by pharma will be rapid - eventually," in-Pharmatechnologist.com, August 2004.

[4] S. Sarma, S. Weis, and D. Engels, "Rfid systems and security and privacy implications. cryptographic hardware and embedded systems," *CHES 2002*, vol. 2523, pp. 454–469, 2002.

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags," in *RFID Privacy Workshop*, MA, USA, November 2003.

[6] D. Henrici and P. Müller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," in *First International Workshop on Pervasive Computing and Communication Security, PerSec'04*. Orlando, FL, USA: IEEE Press, March 2004.

[7] eSTREAMPHASE2, "Ecrypt network of excellence," Update on eSTREAM and SASC 2007, November 2006.

[8] J. Lano, "List of stream ciphers," homes.esat.kuleuven.be/ jlano/stream/ designs.htm.