Palaiseau (France), January 12th, 2006

SCIENTIFIC REPORT, ERCIM FELLOWSHIP

Fellow: Javier HERRANZ.

Contract Nr. **2005-18**.

Period: 01/05/2005 – 31/01/2006.

Institute: INRIA (École Polytechnique, with prof. François Morain), France.

SERAC Project

During my stay in the cryptology group of the Laboratoire d'Informatique of the École Polytechnique (LIX), whose head is François Morain, I have participated in the French project SERAC (Security Models & Protocols for Ad-Hoc Networks). The idea of this project is to analyze how cryptography can help in order to achieve security in the implementation of routing protocols in ad-hoc and mobile environments. Since some of the participants in this project are the designers of the routing protocol OLSR, the project takes this protocol as practical example.

I have attended some meetings of this project, and also a workshop dealing exclusively with protocol OLSR (see [W1] below). A clear conclusion of these meetings is that, in order to provide security to routing protocols, a necessary condition consists in signing most of the messages that nodes broadcast in the protocol. The problem is that standard techniques of public key cryptography result in quite expensive protocols of digital signature, so implementing an efficient and secure routing protocol in this way seems really hard. To do this, one can use some other cryptographic techniques related to digital signature. For example, aggregate signatures are very useful to save storage memory and computational resources when many signatures on different messages (probably signed by different nodes) must be stored and/or verified.

My research in this period has mainly focused on aggregate signatures. First of all, I have worked on ID-based aggregate signatures (see [P1] below). On the other hand, in a joint work with other members of INRIA, we have considered the aggregation of designated verifier signatures (the results will be published in [P2]).

As an extra activity related to SERAC, Dr. Fabien Laguillaumie and I are giving two seminars (2 hours each one, December 1st, 2005 and January 19, 2006) to explain in detail the concept of digital signature and some of its extensions, addressed to the participants of project SERAC.

Visit to Radboud University

I have spent one week of October 2005 in the Radboud University of Nijmegen (Netherlands), invited by the Security of Systems group of that university. There I gave a talk entitled 'Aggregate Signatures', and I worked with Dr. David Galindo about some topics related to public key encryption. The results obtained from those works have been written in a paper which will be published soon (see [P3] below).

I hope that this professional relation with Dr. Galindo will be maintained in the future, specially during the 9 months I am going to spend at CWI (Amsterdam) as the 2nd period of my ERCIM Fellowship.

Other work

- I have maintained the professional relation with some members of the cryptography research group at UPC (Barcelona, Spain) where I obtained my PhD. Some of these works were initiated while I was still there, before I started this Fellowship. A work with Dr. Germán Sáez has been accepted to be published (see [P4] below), and three other papers are currently submitted to international journals and conferences.
- I have given a talk entitled 'Cryptography and Routing Protocols' during the workshop cited in [W3] below.
- I have reviewed papers for international journals and conferences such as IEE Proc. Information Security, Journal of Systems and Software, Indocrypt'05, PKC'06, Eurocrypt'06.
- I am a member of the Program Committee of the conference ACIS'06 (Applied Cryptography and Information Security), to be held in Glasgow (UK): May 8-11, 2006.

PUBLICATIONS and Abstracts

[P1] Javier Herranz. 'Deterministic *identity-based signatures for partial aggregation*'. To appear in The Computer Journal (Oxford University Press). See: http://comjnl.oxfordjournals.org/cgi/content/abstract/bxh153v1

Abstract: Aggregate signatures are a useful primitive which allows to aggregate into a single and constant-length signature many signatures on different messages computed by different users. Specific proposals of aggregate signature schemes exist only for PKI-based scenarios. For identity-based scenarios, where public keys of the users are directly derived from their identities, the signature schemes proposed up to now do not seem to allow constant-length aggregation.

We provide an intermediate solution to this problem, by designing a new identity-based signature scheme which allows aggregation when the signatures to be aggregated come all from the same signer. The new scheme is deterministic and enjoys some better properties than the previous proposals; for example, it allows to detect a possible corruption of the master entity. We formally prove that the scheme is unforgeable, in the random oracle model, assuming that the Computational Diffie-Hellman problem is hard to solve.

[P2] Raghav Bhaskar, Javier Herranz and Fabien Laguillaumie. '*Efficient authentication for reactive routing protocols*'. To appear in the proceedings of SNDS 2006: 2nd International Workshop on Security in Networks and Distributed Systems. Vienna, Austria, April 18-20, 2006.

Abstract: Ad hoc networks are dynamic networks formed “on the fly” by a set of nodes. Achieving secure routing in such networks is a big challenge. The typical way to prevent or reduce the possible attacks is to use mechanisms to authenticate the origin of all the messages. Standard (asymmetric) signatures schemes provide these mechanisms, but may result in inefficient implementations, specially when many nodes (and so many signatures) are expected.

Some of these efficiency problems can be mitigated with the use of aggregate signatures, which reduce the space and computations required for managing many different signatures. In this work we propose a new concept, aggregate designated verifier signature schemes, which are suitable to authenticate the establishment of routes in reactive protocols. We give formal definitions for the new primitive and we explain the required security properties. Then we propose a specific and efficient scheme which uses message authentication codes, and we prove its security in the random oracle model.

[P3] David Galindo and Javier Herranz. '*A generic construction for token-controlled public key encryption*'. To appear in the proceedings of FC 2006: 10th International Conference on Financial Cryptography and Data Security. Anguilla, British West Indies, February 27 – March 2, 2006.

Abstract: Token-controlled public key encryption (TCPKE) schemes offer many possibilities of application in financial or legal scenarios. Roughly speaking, in a TCPKE scheme messages are encrypted by using a public key together with a secret token, in such a way that the receiver is not able to decrypt this ciphertext until the token is published or released. The communication overhead for releasing the token is small in comparison with the ciphertext size.

However, the fact that the same ciphertext could decrypt to different messages under different tokens was not addressed in the original work. In our opinion this is an essential security property that limits the use of this primitive in practice. In this work, we formalize this natural security goal and show that previously proposed schemes are insecure under this notion. In the second place, we propose a very simple and efficient generic construction of \TCPKE schemes, starting from any trapdoor partial one-way function. This construction is obtained from a slight but powerful modification of the celebrated Fujisaki-Okamoto transformation. We prove that the resulting schemes satisfy all the required security properties, in the random oracle model. Previous to this work, only particular instantiations of TCPKE schemes were proposed.

[P4] Javier Herranz and Germán Sáez. '*Distributed ring signatures from general dual access structures*'. To appear in the journal Designs, Codes and Cryptography.

Abstract: In a distributed ring signature scheme, a subset of users cooperate to compute a distributed anonymous signature on a message, on behalf of a family of possible signing subsets. The receiver can verify that the signature comes from a subset of the ring, but he cannot know which subset has actually signed.

In this work we use the concept of dual access structures to construct a distributed ring signature scheme which works with vector space families of possible signing subsets. The length of each signature is linear on the number of involved users, which is desirable for some families with many possible signing subsets. The scheme achieves the desired properties of correctness, anonymity and unforgeability.

We analyze in detail the case in which our scheme runs in an identity-based scenario, where public keys of the users can be derived from their identities. This fact avoids the necessity of digital certificates, and therefore allows more efficient implementations of such systems. But our scheme can be extended to work in more general scenarios, where users can have different types of keys.

CONFERENCES AND WORKSHOPS Attended

[C1] CRYPTO 2005, organized by IACR, in the University of California in Santa Barbara (USA): August 14-18, 2005.

[W1] 2nd OLRS Interop / Workhop 2005, in the École Polytechnique, Palaiseau (France): July 28-29, 2005.

[W2] Research meeting of ECRYPT (European Network of Excellence in Cryptography), in Montrouge (France): November 23-24, 2005.

[W3] INRIA Security Workshop, in Grenoble (France): December 12-14, 2005.