Foundations of Cryptography

Notes of lecture No. 10A (given on June 11, 1989)

taken by Ehud Hausman

Summary

The topic of this lecture is "Digital Signature systems". We present a falacious folklore argument concerning digital signatures, and point out its hidden and unjustified assumptions. Thus, this lecture can be titled "The need for formalism in Cryptography. - An example"

1. Introduction

In this lecture we present what problems can arise when one lets his intuition lead him to conclusion, on a subject that one does not fully understand. As a consequence formalism is mandatory. We specificly deal with a "theorem" introduced in the late 70'S. The scientific community accepted it, because it seemed to be intuitively clear. However, when it is confronted against formalism it turned out to be false.

MOTO: "If the fact that something is selfevident does not imply its validity
then selfevidence can not be considered a proof of correctness".
[L. Wittgenstein, 1918]

2. The Folklore theorem.

The motivation for this "Theorem" is in Rabin's signature system (for detailed discussion refer to Rabin's paper). In this system the signer (A) choses two large primes p, q and keeps them as his secret key for signing purposes. He then calculated their product n, and deposits it in a public file. The signature σ of a message m (regarded as an element of the multiplicative group of n) is computed by taking a square root modulo n of either m or "perturbation" of m (the perturbation is used to make the element a quadratic residue mod n). The signee (B) will use n to verify the authenticity of message signed by A by squaring σ modulo n and comparing the result to the original m (or perturbation of m). The security of the system is based on the fact that the factorization of number which is a product of two large primes is considered to be "hard". Rabin proved that forgery is not easier than factoring, and Rivest observed that the very structure of this proof gives raise to a chosen message attack (*CMA*).

Rivest mistakenly generalized this observation and claimed that any "Digitalize Signature System" which stands against CMA cannot have a constructive proof of security against forgery. This claim ("formalized" below) was considered valid for several years.

"Folklore Theorem" There cannot exist a signature system "based on factorization", such that:

(i) There is a Turing-reduction of factorization to "breaking" the signature system (e.g. "breaking" the system leads to factoring algorithm).

(ii) There is a Turing-reduction of "breaking" the signature system to factorization (e.g. knowing the factorization implies "breaking" the system).

(iii) The signature system stands against CMA .

By "breaking" the system in (i) and (ii) we mean the ability to create with non-negligible probability a pair of strings consisting of message and its signature. For sake of simplicity, we stated the Folklore Theorem with respect to a particular intractability assumption. We shall now present a false proof which consists of some hidden and unjustified assumptions.

3. A false proof

Assume that (i) and (ii) hold. We shell show that (iii) cannot be true. By (i) we know that exists an oracle machine G which on input n and access to a forgery oracle F, outputs p, q such that $p \cdot q = n$.

The oracle machine G proceeds as follows:

1) Generates public file P_k.
2) Generates message m to be signed.
3) Supply m to oracle F, which yields signature σ with respect to m and P_k.

Steps 1-3 are repeated and the factorization is computed from the output of the oracle answers.

CMA can now be successful using the following method:

We run machine G using the real signer A instead of the oracle F . i.e. we ask A to sign the messages chosen by the oracle machine G. As consequence, (i) ensures that the output of G will be the factorization. Now, (ii) yields that factorization implies "breaking" the signature system. We now can forge signatures. Thus, we showed a mechanism for forgery using CMA , a contradiction to (iii).

4. Falscies in the proof

In the false proof above we used a vague notation for the public file P_k, "hoping" that the reader will assume that P_k contains n (to be factorized). Furthermore, in the computing iteration we expected the reader to assume that in **every** step # 1 the public file P_k is the same, and that this public key is equal to the public key attached by (ii). This assumption need not be true. Thus, in general the theorem is not valid as will be explicitly shown (by an example) in the next lecture. In such general system the real signer cannot play the role of the oracle because the oracle must answer questions with respect to different values of P_k whereas the real signer answers questions only about his public file.

Only in special cases, as in the proof of unforgability of Rabin's system, in every iteration the same and expected public key P_k is used. In such cases the claim and the proof are valid!!