Hitachi Unveils Digital Signatures on Stand-Alone Memory Chips

September 25 2008

Hitachi announced today the development of a mechanism for attesting the authenticity of memory chips using highly secure digital signatures in a worldwide breakthrough. Since the mechanism requires neither a CPU nor a computational unit, high security can be attained at a very low cost. As a result, counterfeited or altered memory devices can be recognized as such, with a wide range of applications, including memory cards for digital cameras or handheld video game consoles, cartridges for consumer products, admission tickets or gift coupons.

On the one hand, barcodes, seals or signatures are useful for establishing the authenticity and the integrity of physical goods or paper documents; on the other hand, digital signatures can achieve similar results in the electronic world, for example for computer software or electronic documents. In order to establish that digital contents are authentic and have not been tampered with, digital signatures usually involve cost-intensive computations and require an important processing power.

For instance, in some schemes, large integers with hundreds of digits are multiplied hundreds of times using a powerful CPU. As a consequence, conventional memory chips without CPU cannot handle digital signatures and are confined to the use of basic identification(A) techniques based for example on serial numbers. Moreover, adding a CPU with sufficient processing power for digital signatures to such chips would considerably raise their cost. However, although the market of removable storage devices such as memory cards for digital cameras and game cartridges for handheld consoles has enjoyed a sustained growth,

in the same time, the impact of counterfeits and piracy on this market is larger and larger, and this issue has attracted the attention of the industry.

This is the original motivation behind Hitachi's effort to develop a digital signature technique which, for the first time in the world, does not require any CPU and can be readily integrated in a memory chip. In this new scheme, data required for digital signatures is pre-calculated and stored in memory. Later, this data is re-combined appropriately in order to assemble a digital signature. Unlike conventional digital signatures which require an important processing power, the new digital signature system can be realized in simple memory chip. Now, with Hitachi's technology, CHAP(B) systems may be used in applications where highly secure authentication is required, at a low cost. In particular, the digital signature scheme can serve as building blocks for anti-copy and anti-tampering mechanisms for a wide range of products, including memory cards for digital cameras or handheld video game consoles, authentication tokens, replacement parts for consumer electronics, admission tickets or gift coupons.

(A) Identification is a mechanism that allows distinguishing subjects in a group. Usually, it is realized with unique attributes of subjects such as passwords or serial numbers. Identification mechanisms do not provide protection against malicious third parties able to intercept passwords or serial numbers.
(B) Challenge Handshake Authentication Protocol (CHAP) is an authentication method where a verifier sends a random challenge to a prover who replies with a digital signature of the challenge.

In addition, part of this work was realized in a joint research effort with the Technical University of Darmstadt, Germany. The result will be announced at the 9th International Workshop on Information Security Applications (WISA 2008) which will be held in Jeju Island, Korea,

from September 23 to 25, and in the Second Workshop on Post-Quantum Cryptography (PQCrypto 2008), which will be held in Cincinnati, Ohio, USA, from October 17 to 19.

Anti-counterfeiting mechanism

In order to check the authenticity of a removable memory device, when the memory device is paired with a contained device, a random numerical sequence called "challenge" is sent from the container to the memory device. Next, the memory device replies with a numerical sequence corresponding to the challenge. This response sequence consists of pieces of enciphered data initially loaded to the memory device, and is a digital signature of the challenge. The container verifies the digital signature, and if it is correct, accepts the memory device, following the principles of CHAP. However, a counterfeit will fail to deliver a proper digital signature and will be rejected by the container.

Interception of correct digital signatures

Counterfeits may include correct digital signatures gathered from authentic memory devices, but even in this case, will fail to authenticate. The reason is that a new challenge is sent for every new authentication. Since signatures gathered in the past cannot be the correct response to a new challenge, they are not of any help for successfully authenticating. In that sense, the security offered by the technique is much higher than that of identification systems based on passwords or serial numbers.

Provided by Hitachi