Technology space: “Internet of Things”
Cryptographic requirements: authentication

A NOVEL APPROACH TO AUTHENTICATION

Nikolajs Volkovs

Abstract

Recent cyber attacks on government departments and companies in the USA and Canada have demonstrated fundamental issues in existing security technology. Practically all attacks were realized with a similar scenario. Firstly users’ keys were stolen and then the keys were used to get an unauthorized access to informational systems. Therefore the approach when preliminary distributed keys are used more than one time for authentication has to be reconsidered.

We propose a new authentication approach based on ERINDALE-PLUS hashing algorithm.

In 2004 Kumar Murty and Nikolajs Volkovs created a novel hashing algorithm ERINDALE. In 2007 N.Volkovs created ERINDALE-PLUS hashing algorithm which is a more general construction than ERINDALE.

The ERINDALE-PLUS is a stream based algorithm, a hardware implementation of which gives 2.03 Gbps (Xilinx Virtex 5 FPGA). We expect to reach the throughput up to 50 Gbps in ASIC.

The internal state space of the ERINDALE-PLUS is so large that it is possible to generate practically unlimited number of algorithms with different inner structures, but with the same level of security and speed.

In accordance with the new approach the hashing algorithms with different inner structures are distributed between users instead of keys. On the server side the structures of the hash functions that were distributed between users are collected in a database. When a user needs an access to a server he/she sends a request with its ID. Server generates a random sequence of bits (challenge) and sends the challenge to the user. Then the server hashes the challenge with the structured function that corresponds to the user. User hashes the challenge and transmits the hash value to the server. Server compares preliminary generated hash value with the one obtained from a user and authenticates the user. This results in generating a new and unpredictable key during each authentication session.