Sixth Framework Programme
Information Society Technology

RE-TRUST

Remote EnTrusting by RUn-time Software auTthentication

June 19th-20th, 2008

Abstracts

User's Identification and Key Generation Based on Human Biometrics

Prof. Valery Korzhik - *Invited Speaker*
(State University of Telecommunications, Russia)

User identification and key generation are very important problems concerning software security. Direct solution to these problems is to use passwords for user's identification and generate keys by special hardware based on physical properties of thermal noises or radioactivity. But good password can be forgotten by users whereas short passwords can be found easily by adversary and both passwords and keys which are saved in memory increase the risk of their theft. The way out of this situation is the use of biometrics or psychology of users owing to the slogan –"My body is my password". The main types of biometric information (BI) are: palmprint, iris, face, fingerprint, speech, signature, keystroke, favorite objects (like movies). But the use of BI has the following defects: it is not truly random and it is very difficult to reproduce it repeatedly. Moreover, some of users are strongly disagree to present their BI for storing in data bases. In the talk we are not going to say about the technique of BI extraction (say about sensors of BI) but we want to present some methods that transform BI in such a way to provide its randomness, robustness and security. As examples of BI we will consider basically three types: iris, fingerprinting and favorite objects. Firstly we consider such notions as
secure sketches and *fuzzy extractors*. Definitions, the main properties and practical implementation of them are given. Next we present such approach that uses BI in order to "encrypt" truly random keys that can be used next for user's identification. Because BI suffers to be reproducible repeatedly it is necessary to use power error correcting codes in order to remove this defect. Another technique executes *nonlinear encryption* of random keys by BI. It was called by its inventors as *fuzzy vault*. Performance evaluation of these methods and their complexity are discussed in the lecture.
We try to compare all mentioned above methods of users identification based on BI and to formulate open problems for further investigations.

Cryptographic mechanisms for information authentication and unauthorized copying software protection

Prof. Nikolay Moldovyan - *Invited Speakers*
(Specialized Center of Program Systems "SPECTR", Russia)

Encryption and information authentication are discussed as protection mechanisms against unauthorized copying the software. It is considered the use of digital signature algorithms for confirmation the legal copies of the software products. New computationally efficient digital signature schemes are presented, which are based on new finite algebraic structures defined over the vector spaces of different dimensions.

Remote Entrusting by Orthogonal Client Replacement

Mariano Ceccato, Mila Dalla Preda, Anirban Majumdar, Paolo Tonella
(UNITN)

In a typical client-server scenario, a trusted server provides valuable services to a client, which runs remotely on an untrusted platform. Of the many security vulnerabilities that may arise (such as authentication and authorization), guaranteeing the integrity of the client code is one of the most difficult to address. This security vulnerability is an instance of the malicious host problem, where an adversary in control of the client's host environment tries to tamper with the client code. We propose a novel client replacement strategy to counter the malicious host problem. The client code is periodically replaced by new orthogonal clients, such that their combination with the server is functionallyequivalent to the original client-server application. The reverse engineering efforts of the adversary are deterred by the complexity of analysis of frequently changing, orthogonal program code. We use the underlying concepts of program obfuscation as a basis for formally defining and providing orthogonality. We also give preliminary empirical validation of the proposed approach.

Private Circuits Revisited: Provable Security Guarantees on Boolean Circuits

Sebastian Faust
(KUL)

Ishai et al. studied in [1] the security of Boolean circuits against invasive adversaries that are allowed to probe a number of t wires in a circuit. In practice, however, non-invasive adversaries are the more dangerous threat to security. We present a new formal treatment to analyze the security of Boolean circuits against non-invasive adversaries that have access to the circuit's power consumption. This kind of attack is frequently referred to as power analysis. Power analysis is based on the fact that the power consumption of a circuit depends on the (possibly secret) inputs, and (possibly secret) state of a circuit. In CMOS logic, which is the common standard for circuit design, the power consumption mostly depends on the transitions that occur in the circuit when the input of the circuit switches from x to x'. We formally analyze the security of frequently used countermeasures such as Dual Rail Pre-Charge Logic and Masking, and show which assumptions are necessary to prove the circuit's security in our new model.

[1] Yuval Ishai and Amit Sahai and David Wagner, Private Circuits: Securing Hardware against Probing Attacks, *CRYPTO 2003*.

Preliminary Analysis of the Reverse Engineering Complexity

Mariano Ceccato, Jasvir Nagra, Massimiliano Di Penta, Marco Torchiano,
Paolo Tonella, Paolo Falcarin, Filippo Ricca
(UNITN, POLITO)

Although general purpose obfuscation algorithms satisfying any strong definition of obfuscation do not exist and some argue they are impossible to construct, in practice available code obfuscation is considered a useful protection against malicious reverse engineering by obstructing code comprehension. In previous works, the difficulty of reverse engineering has been mainly estimated by means of metrics, by the computational complexity of static analysis or by comparing the output of de-obfuscating tools. In this paper we take a different approach and assess the difficulties attackers have to understand and modify obfuscated code through controlled experiments involving human subjects.

Design and Analysis of Entrusting Protocol

Vasily Desnitsky, Igor Kotenko
(SPIIRAS)

In the talk we outline the current state of Entrusting Protocol development including analysis of some additional security requirements that could be put in claims. A model of possible attacks on the entrusting protocol and its analysis are considered. Some initial principles of assessment of attacks on the protocol are also suggested.

Analysis of verification tools for security protocols

Sergey Reznik, Igor Kotenko
(SPIIRAS)

The talk reviews the approaches for verification of security protocols. Description of the approaches is accompanied with consideration of corresponding tools implementing them. Classification of verification tools from several standpoints is provided. Their weak and strong points are estimated. This survey is a necessary basis for design and analysis of entrusting protocol in framework of RE-TRUST.

Verification of Entrusting Protocol using AVISPA and Isabelle

Sergey Reznik
(SPIIRAS)

The talk justifies the use of AVISPA and Isabelle to verify the Entrusting Protocol designed in RE-TRUST for exchanging messages between server and client. General approaches to verification of Entrusting Protocol using these two tools are described. Examples of application of AVISPA and Isabelle to proof the confidentiality and authenticity are demonstrated.