INFORMATION OF THE DISSERTATION

Title: **SECURITY IN BIOMETRIC-BASED REMOTE AUTHENTICATION SYSTEM**

Major: **COMPUTER SCIENCE**

Major code: **62.48.01.01**

PhD student: **NGUYEN THI AI THAO**

Scientific advisor: **ASSOC. PROF. DANG TRAN KHANH**

University: **University of Technology – Vietnam National University Hochiminh City**

Dissertation summary

Biometric-based authentication systems offer more undeniable benefits to users than the traditional ones. However, biometric features seem to be very vulnerable - easily affected by different attacks, especially those happening over transmission network or those aiming at the stored biometric templates. In this work, we will propose a novel biometric-based remote authentication framework to deal with malicious attacks over the transmission channel as well as at the untrusted server. The main contribution of this work is the notable biometric template protection scheme in the authentication system. This is a hybrid scheme combining the fuzzy commitment and random projection techniques. This combination is refined to limit the drawbacks and also take advantages of two techniques. The other contribution is embedding a proper secure coprocessor into the main server. Therefore, the administrator is incapable of utilizing information saved in its database to impersonate its clients and deceive the whole system because all the sensitive data is computed in the secure coprocessor. Last but not least, the recognition rate is maintained while the security of the whole system is significantly improved.

Main contributions

- This dissertation has applied the hybrid approach for biometric template protection. The proposed technique is the combination between the fuzzy commitment and the random projection techniques. It is refined to limit the drawbacks and also take advantages of these two techniques.
- Another contribution is embedding a proper secure coprocessor into the untrusted server to solve the problem of insider attacks. This proposal aims at guaranteeing all computations related to clients‘ sensitive date are safe. The protocol suggests how the control server and the secure coprocessor communicate with each other for minimizing not only the computations on the coprocessor but also the contact with sensitive data of the control server.
- The proposal framework has ability to apply for every biometric data which can be extracted to a vector. The experimental results show that the recognition performance of this proposal is competitive with the non-template protection scheme. The system also guarantees the mutual authentication between the client and the server, which makes the whole system resistant against attacks on the unsecure network.

Scientific advisor **PhD student**

Assoc. Prof. Dang Tran Khanh **Nguyen Thi Ai Thao**