Dr. Eng. Sc. Vasyl Yatskiv,
Head of the Department of Cyber Security,
West Ukrainian National University,
8 Chekhov str., Ternopil, 46003,
UKRAINE
E-mail: vy@wunu.edu.ua

Review Report on the doctoral thesis of Libor Dostálek entitled " Multifactor Authentication in Mobile Networks "
Supervisor: Prof. Ing. Jiří Šafařík, CSc.
Consulting specialist: Ing. Jiří Ledvina, CSc.
Department of Computer Science and Engineering

Nowadays cybersecurity statistics reveal a huge increase in the incidents that involve disruption of computer systems and networks, including mobile devices. Significant part of them is aimed at stealing personal data and gaining unauthorized access to sensitive information.

The dissertation «Multifactor Authentication in Mobile Networks» is devoted to improvement of authentication in mobile networks combining different authentication methods in a common multi-factor authentification that is an actual scientific task.

In the introduction the authentication methods and problems of their implementation in mobile devices, in particular, the organizational disadvantages of Authentication and Key Agreement protocol are described.

The basic categories of authentication methods (knowledge, ownership and inherence factors) are considered in Chapter 2. The Authentication and Key Agreement security protocol which is used for mutual authentication and cryptographic material agreement in mobile networks is analyzed in this chapter.

Chapter 3 presents the aims of the work and formulates the basic requirements for the proposed authentication methods. Combining of AKA mechanism with the secure hash-based password authentication protocol using smartcards for multifactor authentication is proposed in Chapter 4.

In chapter 5 merging of AKA authentication mechanism and robust two-factor authentication is described. The comparison of proposed strong authentication method for internet application with other methods is presented in Chapter 6. The authentication model that allows application to dynamically request stronger authentication based on resource is developed and the results of experiments are given in Chapter 7. In Chapter 8 strategies of defender and attacker in Cyber Security Game are defined.

The procedure of the solved problem.

The purpose of the dissertation is fully achieved through: 1) clear statement of research objectives; 2) development of multifactor authentication by combining AKA authentication mechanism and reliable two-factor authentication; 3) comparison of the proposed authentication method with known ones; 4)

development of a multifactor authentication model that can be used in fraud detection systems and experiments; 5) development of the game model which considers defender and attacker strategies based on the proposed methods and game theory.

Results of the dissertation:

- The multifactor authentication method based on merging of AKA mechanism with the Secure Hash-Based Password Authentication Protocol using Smartcards has been developed. The mobile user U and application function S during authentication exchanges three messages. The proposed solution uses two factors: hardware authentication and strong password authentication.
- A new method of multifactor authentication for the Internet applications has been developed, which is based on combining the mechanism of AKA authentication and reliable two-factor authentication.
- A multi-factor authentication model has been developed that allows to work effectively with user authentication when an application provider offers multiple authentication tools of varying strength.

Systematic and clear of work

The PhD thesis represents original and high level of scientific work. The conducted experiments are well arranged and methods are clearly described. The results are very well presented and the explanations are reasonable as well as suitable and focused on the relevant topics.

The author obtained science-based results, which in conjunction solve current applied problem of improving the efficiency of authentication in mobile networks.

Questions for the defense of the doctoral dissertation:

- In which Fraud Detection Systems can your model be implemented?
- Experiments use "External authentication from Facebook", but some users may use two-factor authentication to log in to Facebook, has this option been considered and how will it affect the results of the experiment?
- Did mathematical economic models analyzing the optimal investment level in information security, such as the Gordon-Loeb Model, taken into account when developing a defender strategy in a computer game?

Conclusions

Summarizing, the candidate for PhD degree has performed large amount of insightful research and obtained new original results which broaden our understanding of authentication process in mobile networks. The Dissertation work has been performed at a high scientific level. All important results presented in the Dissertation are published. The thesis and the publication list shoe that Mr. Libor Dostálek is able to perform research independently. For this reason, I recommend the acceptance of this thesis for granting the academic degree Ph.D.

Vasyl Yatskiv

26.04.2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
Božetěchova 2, Brno, 612 66, ČR
Doc. Dr. Ing. Petr Hanáček.
http://www.fit.vutbr.cz/~hanacek

Review of the dissertation thesis

Author: RNDr. Libor Dostálek

Title of thesis: Multifactor Authentication in Mobile Networks

Reviewer: Doc. Dr. Ing. Petr Hanáček, FIT VUT v Brně

The dissertation of Libor Dostálek entitled "*Multifactor Authentication in Mobile Networks*" deals with the issue of authentication schemes in which multiple authentication is performed by multiple protocols and potentially against multiple verifiers.

The thesis consists of three parts. In the first part of the thesis (Chapters 1 and 2), the author introduces us to the issue of authentication in networks, where he discusses the mechanisms and methods used for authentication in different types of communication networks, ranging from simple to quite complex. This section presents the result of an analysis of the current state of the art. The description of some systems is quite thorough, the author goes into quite a lot of detail. However, it is not entirely clear why the authentication systems presented were chosen and why in this order - the reader is somewhat missing something of a guide to the chapter. However, the description is thorough and indicates a well conducted survey of the state of the art. In scope, this section represents almost half of the entire work. In conclusion, the author has sufficiently mastered the current state of the subject.

In the second part of the thesis (Chapters 3, 4, 5 and 6), the author states the objectives of the thesis and then presents two new multifactor algorithms - *Strong Authentication for Internet Mobile Application* and *Strong Authentication for Internet Application*. I consider the objectives of the thesis (*To design algorithms that are used by multiple independent verifiers, to analyze and compare proposed solutions, to design a model for multi factor authentication, and to model game attacker with defender*) to be well defined.

In the last, third part of the thesis (Chapters 7 and 8), the author presents two models - a model that allows to dynamically change the requirements for the authentication method depending on the strength of the authentication based on the current level of security risk, and a *Cyber Security Game* model based on game theory, where a foreign power attacks the defender's assets. In particular, the first of these two models builds well on the previous chapters and is accompanied by corresponding experiments. The second model is more of an extension of another perspective and is not as elaborated.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
Božetěchova 2, Brno, 612 66, ČR
Doc. Dr. Ing. Petr Hanáček.
http://www.fit.vutbr.cz/~hanacek

I conclude:

- I consider the topic of the thesis to be well chosen and the relevance of the thesis to the field of security to be sufficiently high.
- The thesis has a good structure and contains all the parts it should contain. The methods and procedures chosen are appropriate.
- In my opinion, the thesis has fulfilled its objectives, the results are adequate and the thesis contains a sufficient amount of original results of the author.
- The language level of the thesis is satisfactory. The graphic and formal level of the thesis is good. The thesis has the graphical form it should have and contains all the necessary parts in the correct form and structure.
- I consider the author's publication results to be of sufficient quality.
- I recommend the thesis for defence.

Questions for defence: none.

Brno, 16. 3. 2022

.....

Petr Hanáček