Basic authentication procedure modelled by Petri nets

J. Capek, M. Hub, R. Myskova

Abstract— This paper presents modelling of the basic authentication procedure. The Petri net technique as a tool was chosen in this study. Experiments were made with two groups of models according the quantity of used attributes. One consists of combination of the User name and Password with and/or without repeating. The second group consist of the user name, password and biometrics with and/or without repeating. The goal of this paper is to demonstrate that security increasing with attributes quantity and decreasing with possibility to repeating wrong sequence of symbols.

Keywords— Authentication, biometrics, passwords, Petri nets, user name,

I. Introduction

With the rapid growth of network applications, network security has become an important issue, and authentication protocols are the basis of security in networks. Therefore, it is essential to ensure these protocols correctly. Unfortunately, it is difficult to design a robustness and effective security protocol for networks. Not only because of the characteristics of networks, but also because good analysis techniques are lacking. The technical means to achieve information security in an informatics society are provided through cryptography. The cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, access control, and authentication. Confidentiality is a service used to keep the contents of information from all but those authorized to have it. There are numerous approaches to provide confidentiality, e.g. the mathematical algorithms which render data incomprehensible. Access control is the ability to limit the access to authorized users and applications. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be assigned to individuals. Authentication is a service related to identification. It is a fundamental building block for a secure networked environment. If a server knows the identity of a client, it can decide whether to provide the service, whether the user should be given special privileges, and so forth. In other words, authorization and accounting schemes can be built on top of authentication resulting in the required security to the computer network system. Authentication based on some knowledge shared by the system and the user, user name and a password [1], is one of mechanisms used in achieving one's security goals. Nowadays the user name and passwords are still commonly used for authentication purposes, although recently they are thought as not being secure as some of other forms of authentication mechanisms [2].. The reason behind this is probably because the implementing of passwords is easy and not so expensive [5].

Protocols play a major role in cryptography and are essential in meeting cryptographic goals. We need protocols to apply cryptographic algorithms and techniques among the communicating parties. Encryption schemes, hash functions, and random number generators are among the primitives which may be utilized to build a protocol. A cryptographic protocol is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective. The whole point of using cryptography in a protocol is to detect or prevent attacks.

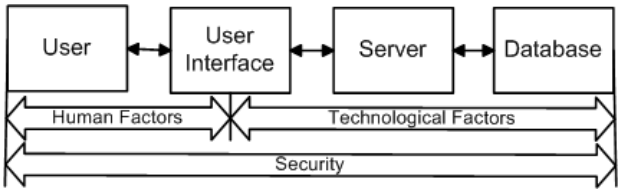

Fig. 1: Factors of User Name and Password Authentication Security (Source: modified on the base of 0)

Human factors can be divided to two categories:

- Type of user name and password (length, randomness, used characters, etc.)
- Mode the user guards a password (how often a user change his password, whether the user writes a password down, and so on)

Since users are thought to be the weakest link of every security solution, it is necessary to study their behaviour. We are convinced of the need to study how users choose their passwords, because it evidently infers of security of this kind of authentication.

A lot of authors frequently discuss about the factors that influence password security, for example: length, randomness, and the period the password is used. Some authors are trying to make a distinction between a "weak" and a "strong" password, commonly by using an expert's opinion 0. Other authors are trying to break passwords, and the results of their experiments are present as a proof of the passwords weakness 0, 0. The authors of this paper are convinced about the need for an exact number that represents the security level of some password.

The characteristic of password security will serve for various purposes:

- Decisions on how password authentication will be implemented (password security evaluation as a part of risk analysis).
- Surveys on long-time term trends in password selection.
- Surveys in password selection by different types of users.
- Studies on the effect of different modes of trainings in password selection.

After passing into computer systems, for example in case e-business according (fig.2.)

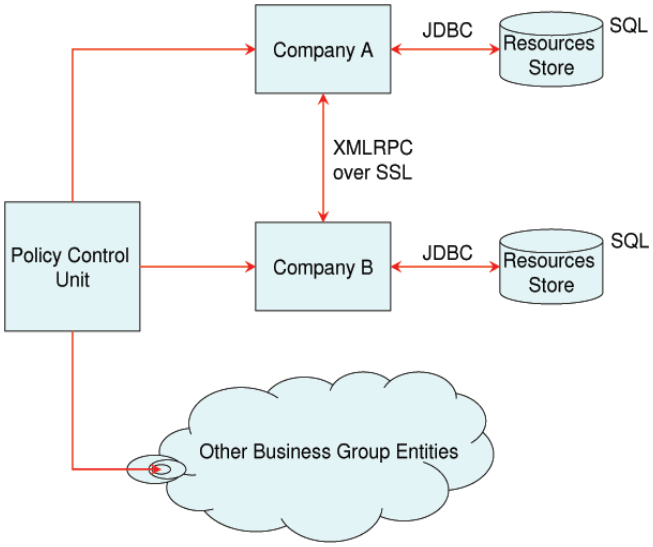

Fig 2 Secure communication infrastructure according [35].

we need protocols to apply cryptographic algorithms and techniques among the communicating parties. Encryption schemes, hash functions, and random number generation are among the primitives which may be utilized to build a protocol. A cryptographic protocol is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective. The whole point of using cryptography in a protocol is to detect or prevent attacks.
Within e-Commerce the agent system is used for example [35]. Fig.3 shows that the first step is authentication.

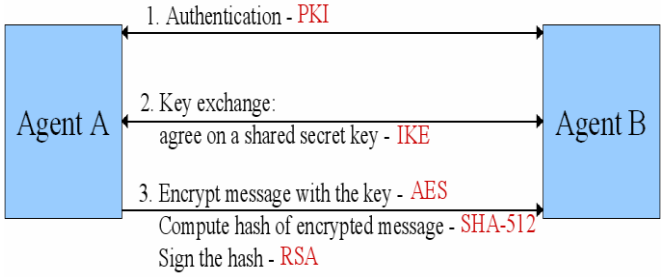

Fig. 3 Agent based system of authentication.

Before sending any messages, the client and the server need to authenticate themselves. In [35] they use a Public Key Infrastructure (PKI) with X.509 certificates for authentication. But the early bird step is use the user name and password and then, after this first step is successful is possible to use PKI and other techniques.

We will begin with describing the motivation for the Kerberos approach and its environment because is obvious that Kerberos is vulnerable to password guessing attacks. Then, we will present a brief overview of the related work. After that, we will use a Petri nets for modelling access to network and/or information systems by user name and password fill in keystroke dynamics technique. Finally, we will summarize our conclusions and our future work.

II. RELATED WORK

There are many client/server applications that use passwords for authentication, for remotely logging onto a supplier's web database and/or bank systems [3], [4].. In these applications it is often possible for an attacker to intercept the password and then replay it to the server. This replay problem can be overcome by using a system called Onetime - Password System (OTP) [5], [11]. An OTP system has an advantage over a regular password system in that the former generates a different password for each time authentication is required. In the one-time-password system, the password entered by the user does not traverse the network. This enables the OTP systems to protect users against passive attacks [8], [11].

The problems with mobile authentication are solved in [42], some tasks from the general problem of the security can be found in [41].
The probabilistic risk assessment (PRA) is the most powerful approach to quantifying risks has been used for the information security risk assessment [36]. Key concepts such as assets, threats, vulnerabilities, impacts, likelihoods, and safeguard emerged during the 1990's, yielding a qualitative approach called GMITS (Guidelines for the Management of safeguards of IT Security) [37]. The information security accident is defined as a breach of confidentiality, integrity, or
availability [38], [39]:
1) Confidentiality: The information is protected from unauthorized or accidental disclosure.
2) Integrity: The information is as intended without inappropriate modification or corruption.
3) Availability: Authorized users can access applications and systems when required to perform their jobs.
GMITS calculates the risk value of the information asset that is to be protected by multiplying each value of the information asset, threat, and vulnerability:
Risk value = (information asset value) × (threat value) × (vulnerability value)
It is true that GMITS has the simplicity in that risk is evaluated with the scores of these three factors, but GMITS cannot describe the scenario of individual information accident.
A scenario enumeration from the initiating event to the accident has not been performed.

The Kerberos protocol allows a client to repeatedly be authenticated to multiple servers assuming that there is a long-term secret key shared between the client and Kerberos infrastructure. Security of Kerberos has been analyzed in many works, e.g. [10], [11], [12], [13], [14], [15] and [16]. Most commonly analyses identify certain limitations of Kerberos and sometimes propose fixes. This leads to the evolution of the protocol when a new version patches the known vulnerabilities of the previous versions. The current version Kerberos V5 is already being revised and extended [9], [17], [18] and [19].

From the rich information sources dedicated to Petri nets we chose [21], [22], [23], [24] and [25]. Within recent years was Petri nets successful used for modelling authentication protocols from many, we choose [26], [27], and [28].

III. KERBEROS MESSAGE EXCHANGE

Kerberos has grown to become the most widely deployed system for authentication and authorization in modern computer networks. Kerberos is currently shipped with all major computer operating systems and is uniquely positioned to become a universal solution to the distributed authentication and authorization problem of communicating parties [11].

A simplified overview of the Kerberos actions is shown in Fig.4. Exchange between the client and the Kerberos AS (Authentication Server) in messages 1 and 2 are used only when the user first logs by his/her user name and password, in to the system. Exchange between the client and the Kerberos TGS (Ticket Granting Server) in messages 3 and 4 are used whenever a user authenticates to a new server. Message 5 is used each time the user authenticates itself to a server. And finally, message 6 is the mutual-authentication response by the server. The ticket plus the secret session key are the user credentials to be authenticated to a specific server.

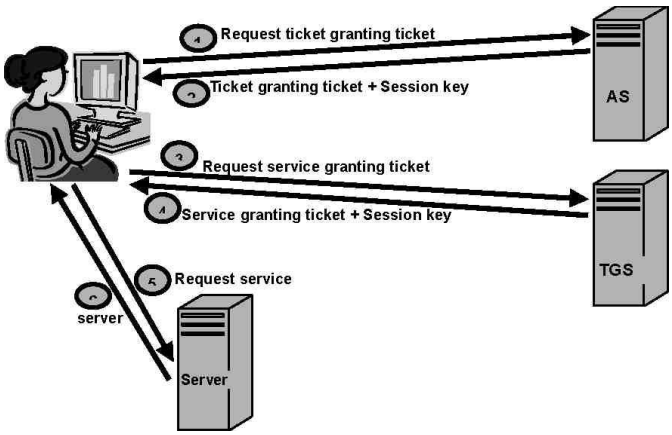

Fig. 4 Overview of the Kerberos actions according [20]

The client long-term secret key was generated using the client's user name and password ([22] describes the password to key transformation technique that is presented by the standard specification). This first step of the authentication process will be modelled in the next part of this contribution.

IV. MODELLING BY PETRI NETS

A gentle introduction into Petri net modelling approach is made for example by [29] where Petri nets are described as follows: "**Petri Nets** are a graphical and mathematical modelling notation first introduced by Carl Adam Petri's dissertation published in 1962 at the Technical University Darmstadt (Germany). A Petri Net consists of **places**, **transitions**, and **arcs** that connect them. Places are drawn as circles, transitions as rectangles and arcs as arrows. Input arcs connect places with transitions, output arcs connect transitions with places. Places are passive components and are modelling the system state. They can contain **tokens**, depicted as black dots. The current state of the Petri Net (also called the **marking**) is given by the number of tokens on each place. Transitions are active components modelling activities which can **occur** and cause a change of the state by a new assignment of tokens to places. Transitions are only allowed to occur if they are **enabled**, which means that there is at least one token on each input place. By occurring, the transition removes a token from each input place and adds a token on each output place. Due to their graphical nature, Petri Nets can be used as a visualization technique like flow charts or block diagrams but with much more scope on concurrency aspects. As a strict mathematical notation, it is possible to apply formal concepts like linear algebraic equations or probability theory for investigating the behaviour of the modelled system. A large number of software tools were developed to apply these techniques, a comprehensive overview can be found in the Petri Net tools database." Classical Petri Nets (PN) are defined as a structure $N = (S; T; F)$, where S means set of places, T is set of transitions and F is $F \subseteq (S \times T) \cup (T \times S)$, where $(\forall t \in T)(\exists\ p;\ q\ \in\ S)(p;\ t);\ (t;\ q)\ \in\ F$. Graphical representation is set up by following symbols as was described above:

- Places - rings ◯
- Transitions - rectangle ▌
- Relations - pointers between transitions and places or places and transitions ⟶
- Tokens •

Petri net models consist of two parts: First the net structure that represents the static part of the system and Second a marking that represents the overall state on the structure. The token distribution among the places of a Petri net is called its marking. When one or more tokens reside in a place, the place is said to be marked, otherwise it is unmarked. The number of tokens at a place represents the local state of the place so that the marking of the net represents the overall state of the system. The dynamic behaviour of the system is then modelled by the flow of token and the firing of transitions. Roughly, transition firing means that tokens in the input places are evidently moved to the output places.

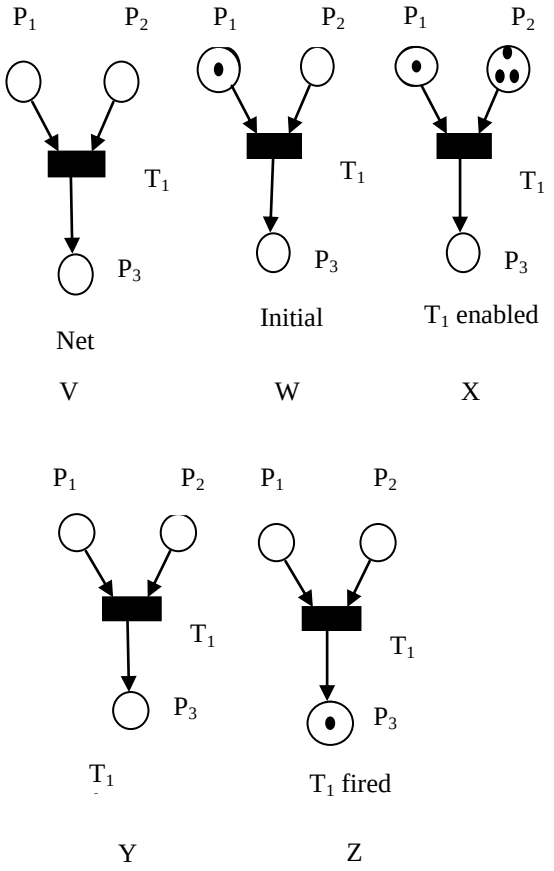

Fig. 5 Petri net elements and firing sequence modified according [33]

Transition firing involves the following steps:

- A transition is said to be enabled if each input place has at least as many tokens as the weight of the arc connecting them (Figure 5 X).
- Enabled transition may be fired by removing from each input place the number of tokens equal to the weight of the arc connecting them (Figure 5 Y).
- When the transition is fired, tokens will be added to the output places connected to the transition. The number of tokens to be added to each output place is equal to the weight of the arc joining them (Figure 5 Z).

It should be noted, for step 2, that enabled transitions are never forced to fire. In practical modelling, transitions can be related to external conditions that determine whether they may fire or not when enabled. Besides, in ordinary Petri net model with no temporal feature, firing occurs instantly (Figure 5 Y).

The above-described mechanism is usually called firing rule.

Mathematically, analysis of Petri nets can be based on enumerating of all possible markings to form reach ability trees and/or through methods and theories in discrete mathematics like matrix equations. We summarize the behavioural properties of Petri nets as below [33]:

1. Reach ability — this determines whether a system can reach a specific state or exhibit a particular functional behaviour. The reach ability set can be denoted by $R(M_0)$, where M_0 is the initial marking.
2. Liveness — this detects whether deadlock situation will be occurred in the system or not.
3. Boundedness and Safeness — a Petri net is said to be bounded and safe if no overflow condition is detected.
4. Conservativeness —a Petri net is described as conservative if the number of tokens in the model remains constant irrespective of the markings it takes on.
5. Reversibility — a Petri net is reversible if $\forall M \in R(M_0)$, M_0 is reachable from M.
6. Denotes a specific marking. This property determines whether system re-initialization is possible or not

With respect to modelling, Petri nets offer the following advantages:

- Using Petri nets to model features like precedence relation, concurrency, conflict and mutual exclusion of real-time system is simple and straightforward.
- The formal graphical representation provides a medium of visual representation of the complex system under modelling for both modellers and users.

With respect to the analysis, Petri nets have the following advantages:

- Having a well developed mathematical foundation; the analysis can be carried out to detect deadlock, overflow and irreversible situations, etc.
- Performance evaluation is possible through the mathematical analysis of the model of the system (using Deterministic Timed Petri Nets or Stochastic Timed Petri Nets).

The major weaknesses of Petri nets are: (1) to model the notion of time, it is not straightforward [34]; (2) as the system size and complexity evolve, the state-space of the Petri net grows exponentially, which could become too difficult to manage both graphically and analytically; (3) control logic is hard-wired, i.e. inflexible to cope with system change. A lot of research has been carried out in order to tackle, in particular the first two weaknesses. Most of them attempt to enrich the modelling power of ordinary Petri nets by incorporating the notion of time, which leads to Timed Petri nets and associating data to the token, leading to high level Petri net like Coloured Petri nets.

We will not describe any more into details the idea and properties of basic PN and for deeper understanding of this problem we recommend basic literature [21], [22], [23], [24], [25], [40] and [43].

A basic PN representation of the User Name, Password and Biometrics, is depicted in Fig. 6.

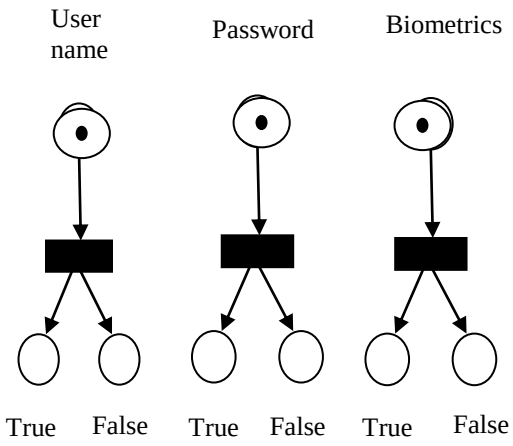

Fig.6 A PN Representation of the User Name, Password and Biometrics.

We can build various authentication models by means of these basic elements. The first one is model when the user name and password is used without possibility to repair wrong sequence of symbols (Fig. 7).

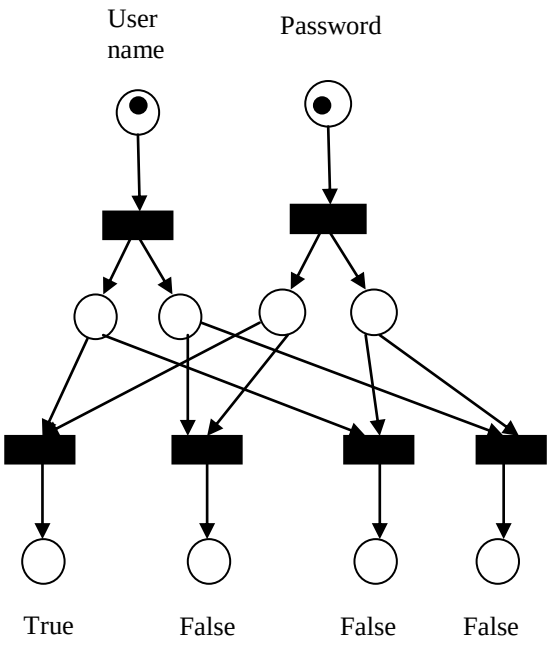

Fig 7 A PN authentication model using user name and password without possibility to repair wrong sequence of symbols.

Next model allows repair wrong sequence of symbols (Fig. 8)

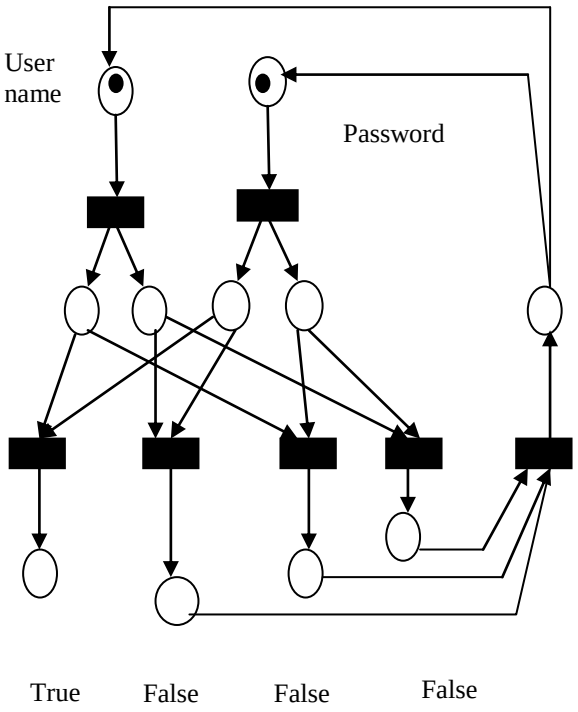

Fig.8 A PN authentication model using user name and password with possibility to repair wrong sequence of symbols.

Next model take into account combination of authentication by knowledge and authentication by attribute, where as the attribute the biometrics was chosen. (Fig. 9)

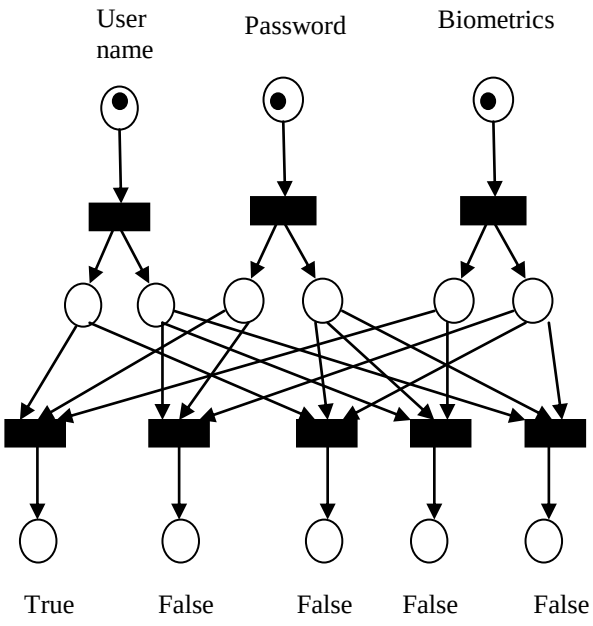

Fig. 9 A PN authentication model consist of the user name, password and biometrics, without possibility to repair wrong sequence of symbols.

The last model is previous one, but with possibility to repair wrong sequence of symbols. (Fig. 10)

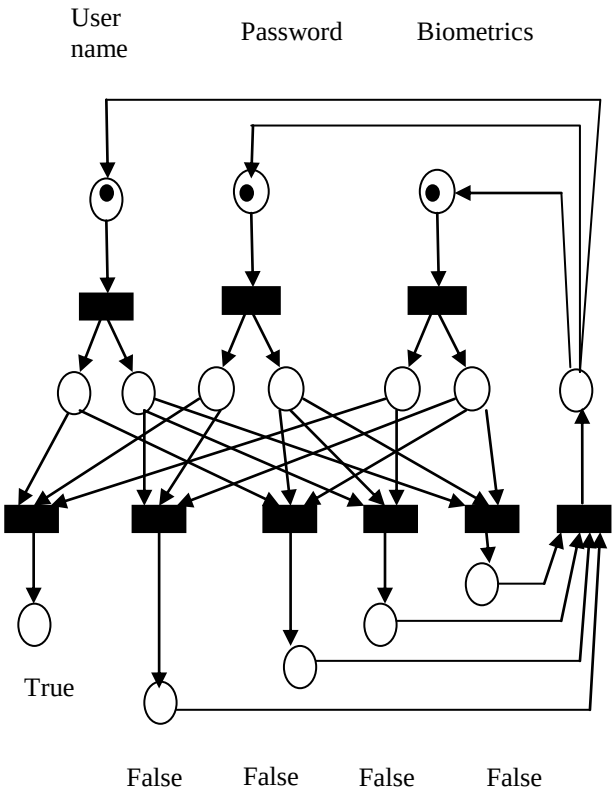

Fig. 10 A PN authentication model consist of the user name, password and biometrics, with possibility to repair wrong sequence of symbols.

V. RESULTS

All models work under the same conditions in HPSim environments and are liveness. The results of the experiments are summarized in Tables 1 and 2.

Within Tables 1 and 2 a cases A (Fig. 7) and C (Fig. 8) describing situation without possibility to repair wrong sequence of symbols within systems User name, Password and/or Biometrics, while a cases B (Fig.9) and D (Fig.10) describing situation with possibility to repair wrong sequence of symbols within the same systems. It should be noticed that in the cases A and C was experiment arranged for three times access possibility, only. From tables 1 and 2 one can see the access percentage of offered combinations. From the following graph is clear that most safety is the case C, follows the case A. (Case C include more attributes, than case A). Both are without possibility to repair wrong sequence of symbols when the accessing procedure works. In comparison the cases B and D, naturally is safety the case D, because include more attributes, than the case B (only User name and Password).

Table 1 Access situation modelled by Fig 7 and Fig. 8

User name	**Password**	**Case A access for Fig. 7 [%]**	**Case B access for Fig. 8 [%]**
True	True	21,4	46,2
True	False	28,6	15,3
False	True	21,4	17,1
False	False	28,6	21,5
Total percentage unsuccessful access:		78,6	53,8
Total:		100	100

Table 2 Access situation modelled by Fig. 9 and Fig. 10

User name	**Password**	**Biometrics**	**Case C Fig. 9 [%]**	**Case D Fig. 10 [%]**
True	True	True	13,3	37,7
True	False	True	8,3	5,0
True	True	False	13,3	11,3
True	False	False	13,3	2,6
False	True	True	8,3	4,4
False	False	True	11,7	11,9
False	True	False	15,0	4,6
False	False	False	16,7	22,5
Total percentage unsuccessful access:			86,7	62,3
Total:			100	100

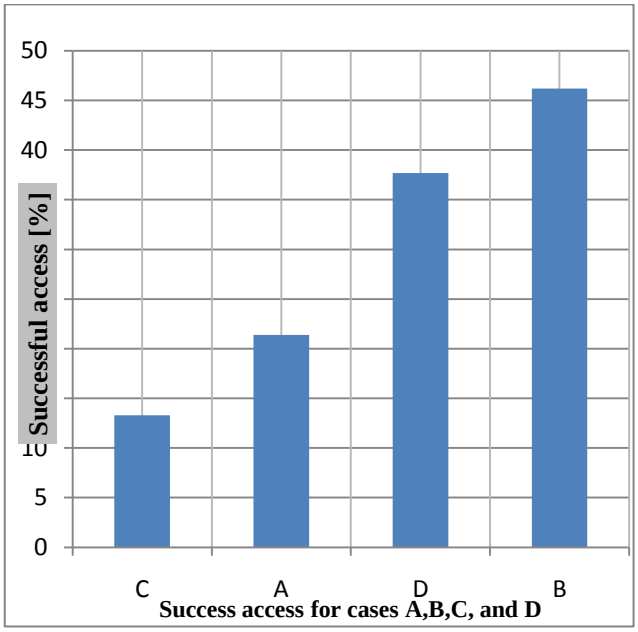

Fig 11 **Success access for cases A, B, C and D.**

In fig. 11 one can see the sequence of the success access from security point of view. The most unsuccessful access (the most secure system) is the case C; consist of the three attributes without possibility of repeating wrong sequence of symbols, following the case A, consists of the two attributes, only. Interesting is, that in percentage the successful access in the case C was roughly half of the case A.

VI. Conclusion

The modelling first steps within authentication process by Petri nets were not done in the literature, yet. This modelling method does not cover the training needs in case of keystroke dynamics. From our previous works [30], [31], and [32] the learning algorithm for depressing false acceptance errors and false rejection errors need at least five repeating the same password by user before starting access procedure. The Petri net modelling technique seems to be a good tool for experiments with authentication processes for accessing to information systems.

Further work will be focused into experiments with coloured Petri nets (CPN) for the possibility to modelled whole accessing process including encrypt communication protocols.

REFERENCES

[1] W. Stallings, "Cryptography and Network Security principles and practices", Pearson Education 2003, ISBN 0-13-111502-2.

[2] K. Renaud, Evaluating Authentication Mechanism. Security and usability. O'Reilly Media, Inc. 2005. pp 103-128. ISBN 0-956-00827-9.

[3] Y. C. Lee, Y. C. Hsieh and P. S. You, A New Improved Secure Password Authentication Protocol to Resist Guessing Attack in Wireless Networks, In *Proceedings of the 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08)*, Hangzhou, China, pp. 160-163, 2008.

[4] W. G. Shieh, M. T. Wang. An improvement on Lee et al.\'s noncebased authentication scheme . In *WSEAS Transactions on Information Science and Applications.* Vol.1, WSEAS Press, 2007. pp. 832-836. ISSN 1790-0832.

[5] L. J. Hoffman, Modern Methods for Computer Security and Privacy. 1st ed. New Persey: Prentice-Hall, Engelwood Cliffs, 1977.

[6] M. Burnett, D. Kleiman. ed. Perfect Passwords. Rockland, MA: Syngress Publishing. 2006. p. 181. ISBN 1-59749-041-5.

[7] D. Klein, A Survey of, and Improvements to, Password Security. In *Unix Security Workshop II, USENIX Association*, 1990.

[8] Ch. P. Garrison, An Evaluation of Passwords, On line CPA Journal-May 2008, Accesable http://www.nysscpa.org/cpajournal/2008/

[9] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos network authentication service (V5)".Network Working Group. Request for Comments: 4120. Available at http://www.ietf.org/rfc/rfc4120.txt, 2005.

[10] S. Bellovin & M. Merrit, "Limitations of the Kerberos Authentication System," SIGCOMM Comput. Commun. Rev., 20(5):119–132, 1990.

[11] G. Bella and E. Riccobene, "Formal analysis of the Kerbero authentication system". Journal of Universal Computer Science, 3(12):1337–1381, 1997.

[12] G. Bella and L. Paulson, "Kerberos version IV: Inductive analysis of the secrecy goals". In *ESORICS '98*. Springer, 1998.

[13] J. Kohl, "The use of encryption in Kerberos for network authentication". In *CRYPTO '89*. Springer, 1989.

[14] S. Stubblebine and V. Gligor. "On message integrity in cryptographic protocols". In *Symposium on Security and Privacy '92*. IEEE, 1992.

[15] T. D. Wu. "A real-world analysis of Kerberos password security". In *NDSS '99. The Internet Society*, 1999.

[16] T. Yu et al. "The perils of unauthenticated encryption: Kerberos version 4". In *NDSS '04. The Internet Society*, 2004.

[17] K. Raeburn. "Encryption and Checksum Specifications for Kerberos 5". Network Working Group. Request for Comments: 3961. Available at http://www.ietf.org/rfc/rfc3961.txt, 2005.

[18] K. Raeburn. "Advanced encryption standard (AES) encryption for Kerberos 5". Network Working Group. Request for Comments: 3962. Available at http://www.ietf.org/rfc/rfc3962.txt, 2005.

[19] http://www.kerberos.org/index.html

[20] E. el Emam at all „A Network Authentication Protocol Based on Kerberos" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009 ISSN 1738-7906

[21] J.Peterson: Petri Net Theory and the Modelling of Systems. Prentice Hall, 1981

[22] M.Češka: Petriho sítě /Úvod do teorie a nástrojů aplikací Petriho sítí/. CERM, Brno, 1994.

[23] K. Jensen, "Coloured Petri Nets: basic concepts, analysis methods and practical use," Vol. 1–3, Basic Concepts. Monographs in Theoretical Computer Science, Springer-Verlag, 1997.

[24] C.Girault, R.Valk, Petri Nets for Systems Engineering (A Guide to Modeling, Verification, and Applications), Springer-Verlag Berlin Heidelberg 2003

[25] http://www.informatik.uni-hamburg.de/TGI/PetriNets/

[26] J.P. Thomas at all, Modeling of Web Services Flow. In *Proceedings of the IEEE International Conference on E-Commerce (CEC'03)* 0-7695-1969-5/03

[27] R.Bouroulet at all, Modeling and Analysis of Security, In *Protocols Using Role Based Specifications and Petri Nets K.M. van Hee and R. Valk (Eds.): PETRI NETS 2008*, LNCS 5062, pp. 72–91, 2008.

[28] J. McDermott, G. Allwein, „A formalism for visual security protocol modeling", Journal of Visual Languages and Computing 19 (2008) 153–181

[29] WoPeD (2005) http://193.196.7.195:8080/woped/PetriNets

[30] J.Čapek, M. Hub.: Fuzzy approach in Biometric Autentication by Keystroke Dynamics. WSEAS Transaction on Systems. Issue 4, Vol. 4, April 2005, pp. 256-262, ISSN 1109-2777

[31] J.Čapek, M. Hub: Authentication by keystroke dynamics. In.*Proceegindgs of the 4th CONTECSI – International conference on information systems and technology management* , May 30 – June 01, 2007 TECSI – FEA USP São Paulo/ SP Brazil pp 2023-2032, ISBN 978-85-99693-02-5

[32] M. Hub, J.Čapek: Method of password security evaluation. In. *Proceedings of the 8th International Symposuim on Distributed*

Computing and Applications to Busiess, Engineering and Science. 16-19. Oct. 2009 Wuhan, China, pp401-405, ISBN 978-7-121-09595-5

[33] W. Reisigs , G. Rozenberg: Informal introduction to petri nets In. *Lecture Notes in Computer Science*, 1998, Volume 1491/1998, 1-11, DOI: 10.1007/3-540-65306-6_13

[34] U.Rembold, B.O.Nnaji, A.Storr: Computer integrated manufacturing and engineeting, Addison-Wesely Longman Publishing Co., Inc.,Boston, MA, 1993

[35] C. Bobolia: Secure Communication Framework for E-Commerce Environmets. In *Proceedings of the 9th WSEAS International Conference on APPLIED COMPUTER SCIENCE, (2009) pp 45-49 ISBN: 978-960-474-127-4*

[36] N. Satoh, H. Kumamoto: An Advantage Factor of Probabilistic Risk Assessment in Information Security. In.*Proceedings of the 8th WSEAS International Conference on Applied Computer and Applied Computational Science* (2008) pp 400-407, ISBN: 978-960-474-075-8

[37] ISO/IEC TR 13335 (2001).

[38] IS-2 Inventory, classification, and repase of university electronic information, IS Series Information Systems, Business and Finance Bulletin, University of California(2007).

[39] T.R. Peltier: *Information security riskanalysis,* Second Edition, Auerack publications (2005).

[40] R. Baťa, I. Obršálová, J. Volek,.: Využití Petriho sítí pro varianty nakládání s biologicky odbouratelným komunálním odpadem In. SCIENTIFIC PAPERS OF THE UNIVERSITY OF PARDUBICE Series D, 13 (2008),pp 4-17, ISSN 1211 – 555X

[41] J. Valášek, P. Linhart: Východiska bezpečnostního výzkumu ČR SCIENTIFIC PAPERS OF THE UNIVERSITY OF PARDUBICE Series D, 11 (2007**)** pp 203-208, ISSN 1211 – 555X

[42] P. Kopeček:Two-Way Mobile Authenticator.In *Proceedings of the 10th WSEAS International Conference on APPLIED COMPUTER SCIENCE (ACS'10)* pp 251-254,ISBN: 978-960-474-231-8

[43] A.S. Staines Using Petri Net Classes for System Requirements Engineering ,*WSEAS Proceedings of the International Conference on Applied Computer Science (ACS) Malta September 15-17,* 2010, pp214-219, ISBN: 978-960-474-225-7