Hungarian Trends in Password Usage, in an International Comparison

Zoltán SOM[1] - Gergely PAPP[2]

Abstract
In the last decade and a half we have seen an accelerating tendency concerning information loss and data leakage. Both the public and the private sectors are affected by embarrassing cases of data leakage all over the world, so experts of both fields are facing a significant challenge concerning this matter. International regulations are at present significantly diverse, but the plan for the future is to unify these regulations. Leaked client data content can be a relevant subject of further scientific research. Concentrating first and foremost on password usage, we attempt to describe the measurable features of passwords in our study, from the point of view of an international comparison. The assessment of passwords has several relevant aspects that determine the quality of passwords mutually. According to our hypothesis, the quality of passwords is in strong correlation with the security-conscious type of behaviour. Enumerating the aspects of assessment, we also attempt to focus on the geographical and language-area diversions of index numbers. We assume that a correlation exists amidst password usage, security-conscious behaviour and e-acceptance. In our study we analyze the current state of information security in Hungary – which have entered a totally new era in 2013, following amendments of the legal regulation – comparing it to international password usage trends. Consequently, in the process of creating a new information security practice for the future, this might be regarded as relevant experience. Furthermore, we are formulating a recommendation, concerning a more dynamic harmonising legislation process. According to our hypothesis, low levels of knowledge and consciousness coupled with easy-to-brake passwords does not offer an adequate level of protection for our data. However, if all documents would appear in digital formats, security risks would get even more significant. Nevertheless, the result of risk analysis shows that more education would be required, in the BA level of higher education. In addition, service providers have to be obliged to provide education for the safe usage of all their products, without limiting education to the level of descriptions.

Keywords: information security, password, international password, international password comparison, information security consciousness education, password rules, password usage habits, administration, Hungary.

[1] National University of Public Service, Doctoral School of Public Administration Sciences, Information Security Department, Budapest, Ménesi út 5. som.zoltan.kdi@office.uni-nke.hu,
[2] National University of Public Service, Doctoral School of Public Administration Sciences, Budapest, Ménesi út 5., papp.gergely.kdi@office.uni-nke.hu

Actuality of the Topic

To state that IT systems are used in general is considered to be true all over the world in all segments of the industry. Data and information are being stored and processed in such IT systems and numerous other operations might be carried out through them. Without limitation, it should also be mentioned that different accessibility and authority levels can be determined and set for such data and systems. In some way or form, these IT systems and concepts are present in every single organization, whether they are SME-s, multinational companies, governmental organizations or operate within the public administration. Nowadays the most common system implementation of accessibility methods and levels that are used as the primary line of defence are the username – password pairings (from here on for the sake of simplicity this will be referred to as "password").
It is a fact that companies nowadays store their knowledgebase: methodologies, patents, contracts, information, etc. Narrowing our research down to EU member states[3] it is true that governments have targeted the digitalization and "electronization" of public administration in every country, this being a featured area of the EU 2020 as well. [61] Each year 40% of EU citizens (approximately 200 million people) make purchases on the internet. The ICT sector alone represents around 6% of the EU's GDP. The EU's ICT sector together with ICT related investments produced approximately half of the total productivity growth and in addition internet-economy provided 21% of EU's GDP growth over the past 5 years. [49] In this study, we would like to highlight that in certain situations there might be an indirect link or connection between habits of password usage and the GDP.
It is also clearly visible that the constantly developing field of e-public administration increasingly affects and represents an increasingly important part of the ICT segment regarding both individual countries and the EU itself, if by no other then through the order of services received directly from governmental bodies. Information security may greatly affect the security and future development of the ICT segment. Within this topic, the scope of our research was focused on habits regarding password use. Indeed, the ICT sector is one of the "growth engines" of the EU. The World Bank estimates that with 10% increase in high speed Internet connections, economic growth would increase by 1.3%. [8] We currently know of only one EU level non-profit initiative that focuses on information security: the EU's Safer Internet Programme. [22] Although this Programme concentrates "only" on the youth, considering them as the target group regarding education.[4] However, numerous other target groups are involved in the operation of the economy, whose knowledge regarding information security is also incomplete. The development of information security and the establishment of an appropriate level of security as well as homogeneity are of particular importance and is a national interest. In Hungary, in 2013 a comprehensive set of measures was started and the round of duties of public and municipal bodies regarding information security was regulated by law.[3], [72] It should also be mentioned that millions of workers and buyers are the "operators" of the economy, who do work on a daily basis in all walks of life, but once their working hours are over they become mothers, fathers, children; users of social networks, or users of the internet in general. According to our research a strong connection can be detected between privacy (private life) and the level of information security awareness at the workplace. It is of national interest as well as an interest of the EU to raise the level of information security awareness and thus to reduce potential abuse. [56] A strong first line of defence should be inner motivation and consciousness regarding simple areas as well, such as choosing a suitable password. There is no exact figure on the number of abuse that already occurred, which might be due to faulty

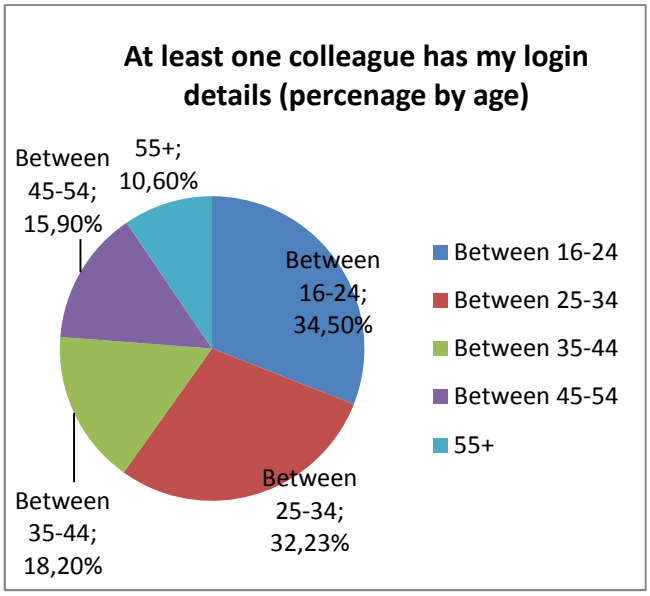
[3] According to Directives, member states are required to make their services electronically accessible in multiple areas. Numerous areas of the EU 2020 Programme strongly support the development of e-services. Specially: Digital Agenda in the Europe 2020 strategy, http://ec.europa.eu/digital-agenda/en/node/1584, last visited: 20.12.2014
[4] The EU SIP programme organizes nation-wide trainings in Hungary with the participation of voluntary trainers and lecturers. The authors have been participating in these programmes for years.

legislation. [68] We can only take into account the number of cases that has come to light, which number is very high on its own. [56] Any case might be included where modern devices are used that are suitable for storing information.

General Habits regarding Password Use

Even though numerous new technologies are available – e.g. the multi-factorial and biometric identification – password-based identification is the most commonly used method. The reasons for this includes easy implementation, and user-friendliness as it does not require any extra hardware. A major problem with basic password-based systems is them being static. It is important to ensure "randomness" in the process of identification in order to make it secure. [27]

Figure 1: *At least one colleague has my login details (percentage by age)*



Source: From Brutus to Snowden a study of insider threat personas, Available at: http://www.isdecisions.com/insider-threat-persona-study/, downloaded: 10.12.2014.

A strong connection can be detected between the general level of information security awareness and habits regarding password use. Many people live in an illusion, where they think users can be influenced to use good passwords through regulations and technical pressure, but this is only partially true. [34]

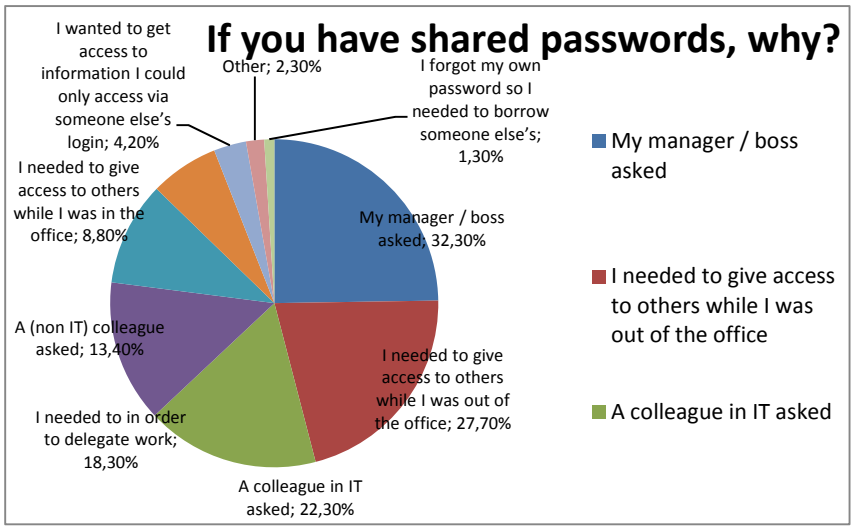
There are numerous ways to launch an attack against a password.[5] Some defence mechanisms are suitable against some ways of attack, through which the general level of security can certainly be raised. According to our opinion, raising the general level of conscious password use would alone be a serious result. Having total defence against most or all forms of attack methods and threats poses a great challenge and thus requires a higher level of maturity.

Based on our experiences and on the relevant information that has come to light on the matter, a shift can be observed in the direction of possible attacks against the "human factor". One of the key reasons for this is that it does not require advanced technical knowledge. Accordingly, our general recommendation would be to apply enhanced defence to such areas, naturally in addition to providing appropriate technical support. Technology however is not some kind of a "miracle cure". Even with the appropriate settings, it can only be an effective supporting instrument of information security awareness. There are numerous recommendations and long lists [47] to help users setting up a good password, but in order to have an effective defence mechanism, one should know exactly what he/she is trying to defend him/herself against primarily. The password should be implemented in such a way that it should take the type of risks associated with the particular organization, application, or situation into consideration, just like in the case of any other defence mechanisms.

[5] Several ways and methods are described in the course material for the "Ethical Hacker" courses organised by international organizations and supervised by the EC-Council, but these are exclusive to the ones enrolled and not publicly available.

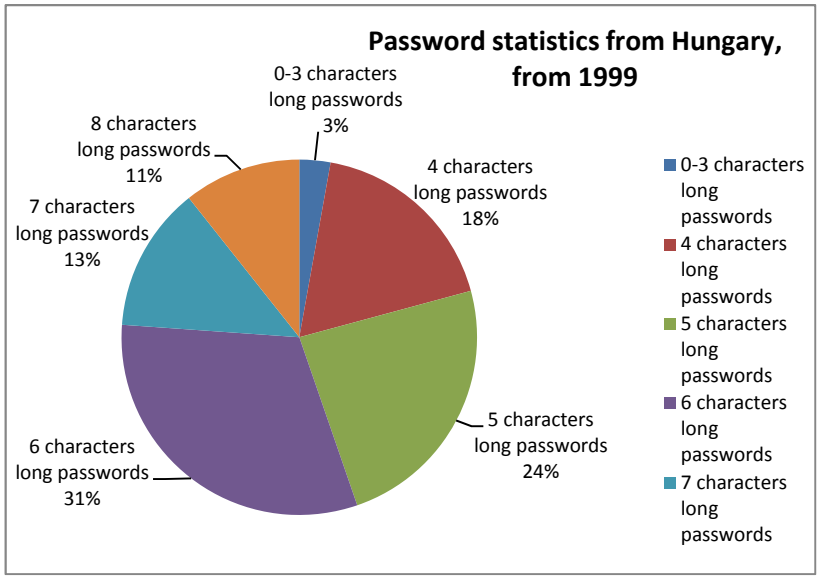
There are dozens of pre-written applications available for free that are especially designed to be suitable for implementing attacks against passwords.[6]
Sharing passwords within the organization seems to be an important issue. [7] According to an international survey with a large sample size, 23% of users share their network passwords with one or more colleagues, but due to some special circumstances or stress, this number may even rise to 49%. An interesting trend seems to unfold [30] when this is broken down by age groups, this is shown in Figure 1. It is also important to examine the factors that stress or even force employees to share their passwords. This is shown in Figure 2. It is also important to take qualitative factors into consideration next to quantitative numbers. If completing a work- and/or private life related task requires the employees to disobey some rules or regulations then the willingness towards disobedience is relatively high. This is why it is advised to define and map the different work processes within the organization according to ITIL[8] standards, as this way it would be possible to detect the processes that cannot seem to be carried out without disobeying regulations.
The shocking result was that only 28% of the interviewed employees knew to whom and how they should report a security incident should it occur, which drives attention to the lack of education. Although we do not examine it in detail but in the mainstream of our

Figure 2: If you have shared passwords, why?



Source: From Brutus to Snowden a study of insider threat personas, Available at: http://www.isdecisions.com/insider-threat-persona-study/, downloaded: 10.12.2014.

Figure 3: *Password statistics from Hungary, from 1999*



Source: Study on the Elender Passwords Come to Light. http://tig.kgk.uni-obuda.hu/targyak/gazdinfo/gyak_KEA/ElenderJelszo.html, [In Hungarian], downloaded: 10.12.2014.

[6] Back Track 5 Linux and Kali Linux (which might be understood as the continuation of the former) contain several hundred utilities and applications that serve as great help in carrying out safety checks and tests. Although in the wrong hands they may be suitable for an attack as well. https://www.kali.org/, last visited: 20.12.2014.
[7] Naturally there are other quality measures as well, but these are not dealt with in detail due to space reasons.
[8] ITIL stands for Information Technology Infrastructure Library, which is a collection of standards established based on a business type approach to support the management of IT processes.

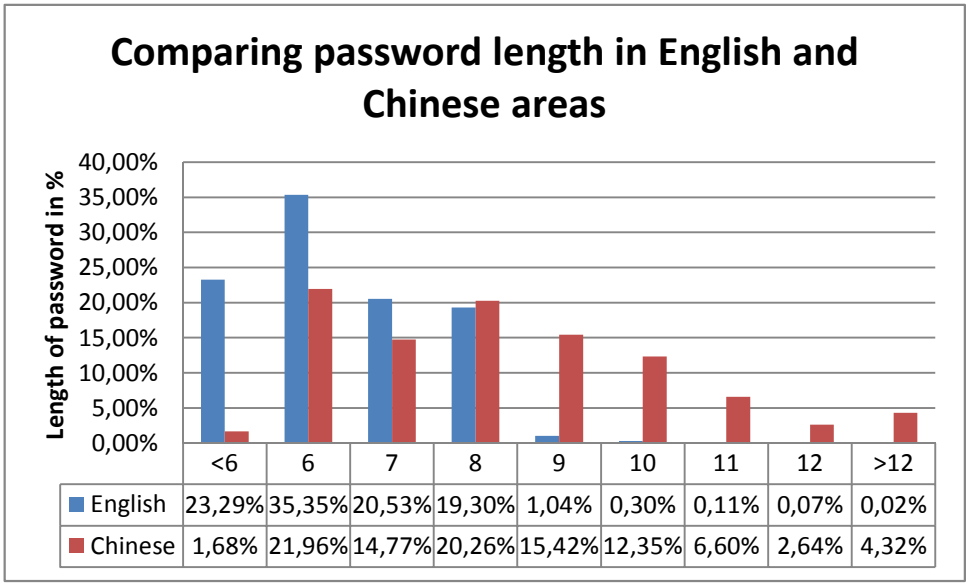
study we mention that 36.3% of employees have continued to have access to systems or data from an employer even after they have left their jobs. [30] This further strengthens our hypothesis that most of the risks are caused by the human factor, or in other words by the people themselves. Between December 1999 and January 2000 an incident occurred at a Hungarian IT system, which resulted in 32,796 passwords being made public. Even after a decade and a half has passed it is worth examining in an international comparison, how much has consciousness regarding password use really changed.[9] 804 of the passwords contained only numbers which made up 10.52% of our total, 559 passwords were one of the 25 most commonly used passwords, which added up to 7.31% of the total. The top 100 most commonly used passwords gave access to 1,100 user profiles. [65] It is a rare occasion to have the opportunity to analyze the passwords made public in further contexts, but this time the date of the last password changes were also made available for us. Available data shows that the average age of the passwords was almost a year (333 days to be exact) in relation to the incident that happened in the beginning of January in 2000. This is very far from the recommended monthly or the suggested quarterly interval for password changes. In relation to the length of passwords (which will be dealt with in detail later) in Hungary and on an international scale it can be concluded that regarding quality measures, user passwords have not changed significantly over the past (approximately) 14 years. This means that generally these passwords do not meet the recommendations regarding length, complexity or further factors. It is also important to note that the analysis of different password databases are not always comparable as in most cases the initial data is only partially accessible or not accessible at all.

International Comparison of Password Use

The question arises as to what differences or similarities can be seen regarding the habits of international password use.

Habits regarding password use can be influenced by numerous factors. These can be technical or regulatory, or even legal [3] terms or conditions, for example only a password of given length and which meets further recommendations is acceptable. This might be regarded as a forced

Figure 4: *Comparing English and Chinese password lengths*



	<6	6	7	8	9	10	11	12	>12
English	23,29%	35,35%	20,53%	19,30%	1,04%	0,30%	0,11%	0,07%	0,02%
Chinese	1,68%	21,96%	14,77%	20,26%	15,42%	12,35%	6,60%	2,64%	4,32%

Figure created by author from data in source The top 10,000 worst passwords[1] and A Large-scale Survey on Password Habits of Internet Users in China [66]

[9] (Should we be in possession of the original password database it would only be a matter of computing capacity to decrypt all of the passwords, but it is important to note that our further analysis is based on data that accounts for 23.3% of the total database.)

attempt on behalf of the supplier.[10] [52], [60] An alternate main category is the knowledge of factors influencing the thinking of users, and knowledge of factors that can influence the process of choosing a password more effectively by adapting to the technical conditions. [34]
National tendencies of password use are not available for every country, although in the past few years a number of international suppliers have provided data records of the order of tens of millions. [46] We have divided our analysis on password use into three main areas. In the first one we concentrated on data from suppliers operating in the United States of America (this will further be referred to as "the first area"), and thus here we primarily focused on habits of English speaking areas.[11] In the second main area we analyzed data from a Chinese report (this will further be referred to as "the second area") [66] which is particularly special as the number of similar cases of data-leakage that has come to light is relatively low. The "third main area" is a Hungarian analysis. By the comparison of these three areas we aim to analyze and uncover significant differences regarding the trends in password use, based on cultural and geographical location (if any). Due to space reasons we have narrowed down our research to only focus on two factors: 1) the length of passwords and 2) how frequently does a given characters occur in the passwords (this way we should be able to determine the most commonly used characters).

In the first area[12] the average password length is 6.29 characters. Figure 4 shows the relation

Figure 5: *Sequences in a Passwords*

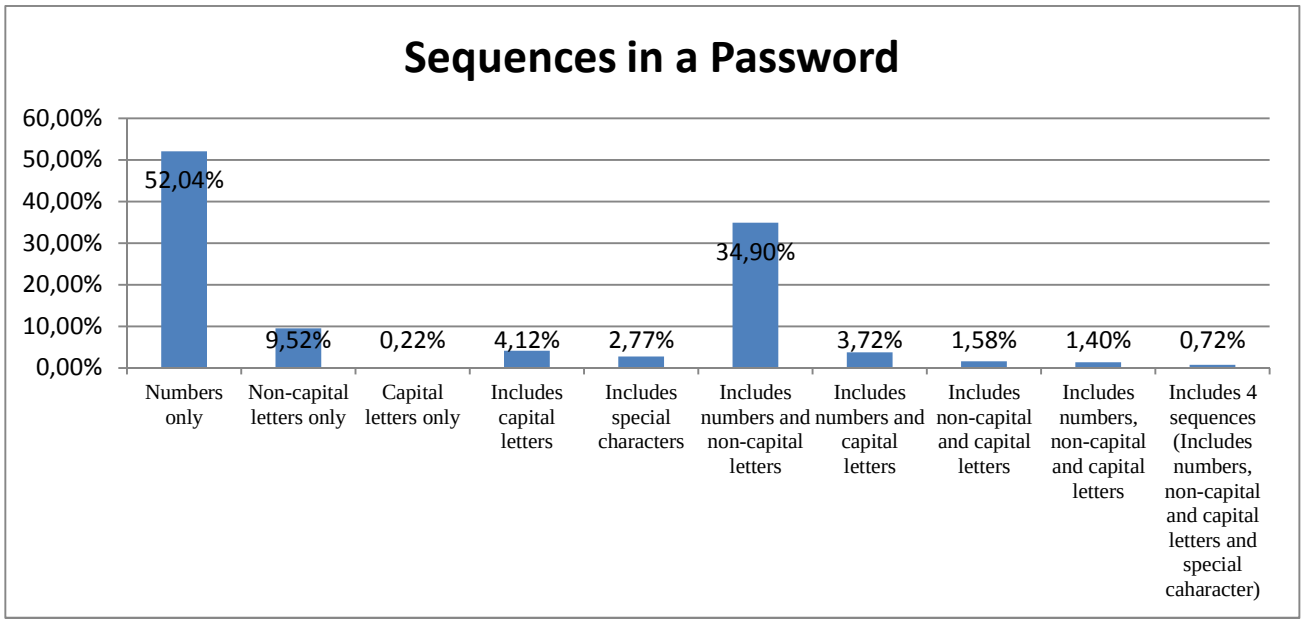


Figure created by author from data in source A Large-scale Survey on Password Habits of Internet Users in China [66]

between frequency of given characters and password length. Compared to the total the number of passwords with less than four or more than nine characters is insignificant (below 1%). It shows a comparison of data from English and Chinese speaking territories regarding the length of passwords. The most commonly used characters are letters: "e", "a", "r", "o", "n" "i", "s", "t", and

[10] This topic could be discussed much further as the opposite of the above tendency (namely "constriction") is also valid, for example in cases when the systems of the supplier are not suitable for storing passwords longer than 6 characters.
[11] We have analyzed the 10,000 worst passwords available for us in detail. The top 10,000 worst passwords. The statistics on password use were prepared after analyzing approximately 6 million data records, https://xato.net/passwords/more-top-worst-passwords/
[12] Data records primarily form English speaking territories, https://xato.net/passwords/more-top-worst-passwords/

"l" respectively. Figure 5 shows how many of the possible four sequences are used in each password.[13] The research shows that in 10.4% of the cases there is a strong connection between the username and the password.[14] In 9.1% of the cases one or more words with an actual meaning were used as a password. Regarding the third area, [46] two sets of passwords were analyzed from different sources. During the summary of the findings we could determine that 33.95% of the total passwords examined had 8 characters. The most common characters used in passwords were letters: "a", "i", "e", "1" and "o". An interesting fact was also uncovered which seems to be a national specificity: approximately 20% of the passwords contained Hungarian names of persons.[15] Only 3.21% of the passwords contained special characters. According to the research it can be concluded that password with 7 to 8 characters are most common. Usually "safe passwords" (those using all four sequences) are not used. It would seem that users are not concerned with the safety of their own data, or that they are ignorant in this field. This poses as a serious threat on both individual and supplier (national, public administrational) level, [36] as most of the passwords could be compromised through the use of an average personal computer and software available for download from the internet for free. [72]

The Connection between Password Use and Information Security

Changing trends: There is only one thing that is constant, and that is change itself. Although the pace of change is not constant or uniform. Unfortunately when it comes to information security and password use the pace of change in behaviour is far slower than it should be to be able to keep up with and adapt to technical development. We could see that there is a significant connection between organizational culture, maturity towards security and habits and trends regarding password use. Instruments available on the internet for free, and the drastic growth in the performance of personal computers result in a high success rate for both acquiring or cracking a password less than 8 to 10 characters under a very short time interval, in some cases in no more than just a couple of days. (Due to space reasons we do not include computing capacity as in the use of cloud services.) Information security culture is an important part of the organizational culture. It is visible through the acts and their implementing orders and regulations enacted by Hungary that the government has also realised that there is a need for legal regulation of the question, as the field of public administration is significantly affected. An important milestone of this procedure is that the training of information security managers has started through a course hosted by the National University of Public Service.[16]

As seen from the above, both the attitude of users and customers using IT systems and e-acceptance are important areas that are capable of influencing the GDP, and should be handled with appropriate care. The Tallin Manual [63] is a good example for the changes that should be handled constantly and in proportion to the risk at hand on an organizational-, member state- and legal level as well. Consciousness towards password use and password habits in general can both be considered indicators when determining information security consciousness. This means that data and trends uncovered regarding these questions might indicate the level and overall behaviour of people when it comes to the question of information security regarding their work or private life as well. Numerous international examples prove that companies might suffer severe financial loss due to

[13] A good password should include all four sequences, this means that a good password should include: non-capital letters, capital letters, numbers and special characters as well.

[14] This means that in 1.54% of the cases the username and the password were the same. In 3.01% of the cases the username was included in the password. In 5.85% of the cases the password was a part or segment of the username.

[15] Given names in Hungarian, Officially registered Hungarian given names, http://www.nytud.hu/oszt/nyelvmuvelo/utonevek/ last visited: 20.12.2014.

[16] National University of Public Service, http://eiv.uni-nke.hu/

information leakage. The IT sector makes up a significant and constantly growing part of a country's (as well as the EU's) GDP. Since information security is considered to be a risk factor at IT companies, habits regarding password use might also be considered indicators for determining the different characteristics (e.g. age, cultural specialties, etc.) and company types which should put special emphasis on information security consciousness.

Recommendations

We may state that there is a need for significant improvement on the field of security awareness regarding the use of IT systems. Furthermore making the necessary information for acceptable behaviours and decision-making transparent is not sufficient in all cases. These should be delivered in the appropriate form while designing both the transmission channel and information to fit the target audience or target group. Apart from all these, the security area should also be able to provide efficient support in everyday use and during the processes of the users. This should also be in accordance with the achievable expectations. Obligating suppliers to prepare users for the major types of attacks against the systems and devices they deal might mean a huge breakpoint. Upon preparing the risk analysis on technical and human attacks, if the given organization was able to determine the primary attack vector, they should be able to prepare their workers and the supporting technical background to fend that particular threat off. On the other hand, the procedure of applying random transformations on a fixed password used in our scheme design is a classic idea to prevent password leakage, but it is not easy to be realized in a human-friendly manner without new user interface technologies only available on modern computing devices. [50], [32] Workplace level information security culture should be an integral part of organizational culture. There is a need for a multilevel awareness programme that includes the employees and differentiates based on age groups, organizational tasks and sectors as well as potential risks during their respective work. Multiple accesses in the same time (concurrent access) should be limited. But technology is only capable of supporting such ambitions and regulations. Due to the transparency of regulations, it is required for penalty items to also be transparent and they should be used consistently. Thus the message sent this way that safety regulations are important will be a valuable piece of information as well as an educational opportunity for all. In the upper third of the maturity model, it is recommended to implement such solutions that assign accesses to given roles and time intervals. Technical limitations in this area only supports creating opportunities for unauthorized access. Such as attempts to access folders or other departments unauthorized or simply trying to access the system after business hours. Processes should be clearly regulated, assigning or transferring tasks or delegation should be more simple. Clearly regulated and monitored processes can effectively promote safety. There is a need for efficient educational models that do not merely share recommendations but also present the possible consequences of not following them in a well exemplified way through potential and actual cases of abuse. Reading through these regulations the following question arises: is it safer to use a password that fulfils the requirements of numerous instructions but is nearly unusable in everyday life or is there an alternate solution? During the course of education we harmonize regulations and the habits of password use so that they would be easy-to-use on a daily basis. In practice various different methods are available to achieve this, which should be dealt with during the trainings and courses. A possible method is through the use of a password safe.[17] In regard of economy it should be kept in focus that e-passport and e-id products and services in general are an up-and-coming field and will account for a large proportion of the GDP and thus will most likely aim the attention to e-acceptance and related areas as well.

[17] Numerous password safe applications are available for free on the internet, e.g.: Keepass.

Drawing a comparison it showed a drastically growing trend over the past decade and a half together with the use of internet. [35]

What Levels Should We Include in Education?

The present educational model (elementary-, secondary- and tertiary education) serves as a good example that education aims to provide students with the necessary knowledge at the given levels of education simplified with respect to students' age and level of perception. This style of education should include information security as well. As an elementary school student usually does not have his/her own cash or debit card yet, but in most cases he/she would have a Smartphone, which makes the danger of someone acquiring their PIN code a valid threat even at that age. According to what I experienced over the years I spent as a trainer and lecturer in the EU SIP programme, using a Smartphone and joining social networks is very common in general. By the age of 11 participation actually becomes nearly 100%. The first cases of fraud, abuse and online harassments might occur as early as at this age which most likely "scar" the young users permanently. Education focusing on the secure use of IT systems on a daily basis, as well as showing best practices presented in an easy-to-understand manner through multi level awareness programmes should be present on both national and EU levels. This is a necessity in order to prevent e-acceptance and the rapidly developing e-services ending up in an irreversible state of distrust, as this would pose as a major economic threat as well. [4] Shaping the culture of password use – as it has been mentioned above – is a necessary condition for achieving willingness to use e-administration [39], as well as the spreading of digital literacy and e-acceptance in general. This culture is not only made up by the intention to come up with solutions for developing and expanding technical methods – which appears on the side of experts –, but knowledge, being informed, trust and motivation (based on the former) also make up an exceptionally important part of it. The instrument to achieve all this is none other than education and raising the level of knowledge, building on the results of which, such a level will become available where users are able to understand multi-factorial identification as well as further alternative forms of identification. [41] There is only a very narrow group of users currently capable of understanding these methods, as most lack not only the knowledge but trust and motivation as well. [48] Based on all these there can only be one motto for improving the culture of password use: *education on all channels*. A cultural and conceptual system of basic skills needs to be set up, which allows to further develop the users' skills due to the clear laying down of basic skills and thus including the users and making them interested in the questions at hand (through the safe knowledge of basic skills and) through giving easy-to-understand answers to the "whys" raised regarding the subject. [40] The consciousness or awareness levels of information security might serve as a good starting point for later in questions and issues and related services (e.g. e-id-s and e-passport services) that require a much larger scale of consciousness. Attention must be drawn to the polarizing power of the internet and IT systems in general, as it is even more easy for disadvantaged people and people more exposed to potential harassment to become victims without proper preparation.

Information security managers and trainers should be well aware of the conditions that can be used to create a password policy and recommendations valid for the organization, application, and user groups. Without such guidelines and principles how would it be possible to develop a password policy proportional to potential risks? The optimal solution most likely would be to come up with a solution that in possession of all the information would be able to serve and protect the password as primary line of defence throughout its lifespan taking the risk appetite of the organization into account as well. Unfortunately according to our current research there are only a very small number of multi-level awareness trainings and multi-level information security protocols

at the organizations. In respect of each of the organizations, education should include the citizens as clients as well. [47]

References

[1] 10,000 Top Passwords, The top 10,000 worst passwords. The statistics on password use were prepared after analyzing approximately 6 million data records, https://xato.net/passwords/more-top-worst-passwords/, last visited: 20.12.2014.

[2] A Brief Analysis of 40,000 Leaked MySpace Passwords, Blog post, http://www.theinterweb.com/serendipity/index.php?/archives/94-A-brief-analysis-of-40,000-leaked-MySpace-passwords.html, last visited: 20.12.2014.

[3] Act 50 of 2013 on the Electronic Information Security of Public and Municipal Bodies, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, [In Hungarian], last visited: 20.12.2014.

[4] András, Lőrincz, Uncertainties of Trust, In the Service of the Country, [In Hungarian], 2014

[5] András, Nemeslaki: Conceptual Foundation and Comparison of ICT Value in Business and Public Administration In: 4th Annual Conference of the European Decision Sciences Institute (EDSI) Budapest, Hungary, 16-19.06.2013. Single-window and time-limit administration, economic benefits deliver value for the entrepreneurs.

[6] András, Nemeslaki: Corporate Internet Strategy, [in Hungarian] Budapest: Akadémiai Publishing, 2012. 271 p. (Management), (ISBN:978-963-05-9189-8)

[7] Burnett M., Kleiman D. Perfect Passwords: Selection, Protection and Authentication, Syngress Publishing Inc, Rockland, MA, 2006.

[8] Commission staff working document impact assessment, Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, /* SWD/2013/032 final */, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013SC0032, last visited: 20.12.2014.

[9] Communication from the Commission to the European Parliament and the Council on the evaluation of the European Network and Information Security Agency (ENISA), COM/2007/0285 http://eur-lex.europa.eu/Notice.do?val=449692:cs&lang=hu&list=547922:cs,542630:cs,699289:cs,449692:cs,531842:cs,533229:cs,514029:cs,&pos=4&page=3&nbl=27&pgs=10&hwords=enisa~&checktexte=checkbox&visu=#texte, last visited: 20.12.2014.

[10] Competitiveness and Innovation Framework Programme (cip) ICT Policy Support Programme , ICT PSP Work Programme 2010, The EU strategic framework, i2010 – A European Information Society for Growth and Employment http://europa.eu.int/information_society/eeurope/i2010/index_en.htm, last visited: 20.12.2014.

[11] DaeHun Nyang, Aziz Mohaisen, Jeonil Kang, Keylogging-resistant Visual Authentication Protocols, TRANSACTIONS ON MOBILE COMPUTING, Vol. 1, Issue. 8, AUGUST 2014, IEEE, https://www.verisigninc.com/assets/labs/tmc14.pdf, last visited: 20.12.2014.

[12] Danuvasin Charoen, Murali Raman, Lorne Olfman, Improving End User Behaviour in Password Utilization An Action Research Initiative, 2007 Springer Science+Business Media, LLC 2007, DOI 10.1007/s11213-007-9082-4

[13] Dell'Amico M., Michiardi P., Roudier Y. Password Strength: An Empirical Analysis, Proceedings of the 29th Conference on Information Communications, San Diego, USA, 15–19 March 2010, pp. 983–991.

[14] Dombi Gábor, Molnár Szilárd: From the Definition of Digital Diversification to E-inclusion Policies, Information Society [in Hungarian] in: 2008 Vol. VIII, Issue 2, ISSN: 1587-8694, http://www.infonia.hu/digitalis_folyoirat/2008_2/2008_2.pdf, last visited: 20.12.2014.

[15] ENISA Threat Landscape 2013, Overview of Current and Emerging Cyber-threats 11 December 2013

[16] ENISA: The Right to be Forgotten – between Expectations and Practice, General Report 2012., ISBN 978-92-9204-065-9

[17] Eszter Bartis and Nathalie Mitev: A Multiple Approach to Information Systems Failure: A Successful System that Failed

[18] EU Inventory of CERT activities in Europe includes publicly listed teams, co-operation, support and standardisation activities. http://www.enisa.europa.eu/activities/cert/background/inv, last visited: 20.12.2014.

[19] EU Legal law, http://www.parlament.hu/biz/eib/link1/jogharm.htm

[20] EU Member Countries, http://europa.eu/about-eu/countries/member-countries/

[21] EU Press releases database, Proposed Directive on Network and Information Security – frequently asked questions, http://europa.eu/rapid/press-release_MEMO-13-71_en.htm, last visited: 20.12.2014.

[22] EU Safer Internet Program, http://www.saferinternet.org/, last visited: 20.12.2014.

[23] Eur-lex, Access to European Union law, About ENISA. http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&lng1=en,hu&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=449692:cs], last visited: 20.12.2014.

[24] European Union, Eurostat. Enterprises having a formally defined ICT security policy with a plan for regular review, by economic activity, EU27, January 2010. http://epp.eurostat.ec.europa.eu/statistics_explained/index.php?title=File:Enterprises_having_a_formally_defined_ICT_security_policy_with_a_plan_for_regular_review,_by_economic_activity,_EU27,_January_2010_(%25_of_enterprises).PNG&filetimestamp=20110304131331, last visited: 20.12.2014.

[25] Featured Project titled Office On The Net, [in Hungarian] Project No.: ÁROP-2.2.18-2012-2012-0001 http://hirlevel.egov.hu/2014/10/07/felmeres-a-kozszferaban-az-elektronikus-kozigazgatas-human-tenyezoirol/, last visited: 20.12.2014.

[26] Florencio D., Herley C. A large-scale study of web password habits, Proceedings of the 16th International Conference on World Wide Web, Association for Computing Machinery, Banff, Alberta, Canada, 8–12 May 2007, pp. 657–666.

[27] Folláth – Huszti - Pethő, Computer Security and Cryptography, 2011, Source: http://www.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch10.html, [in Hungarian], last visited: 20.12.2014.

[28] Frank Bannister: Forward to the Past: Lessons for the Future of E-government from the Story So Far, Information Polity - ICT, public administration and democracy in the coming decade, Volume 17 Issue 3,4, July 2012, p.: 211-226, doi:10.3233/IP-2012-000282

[29] Frank Hogrebe, Wilfried Kruse: One Stop eGovernment for Small and Medium- Sized Enterprises (SME): A Strategic Approach and Case Study to Implement the EU Services Directive, 21st Bled eConferencee Collaboration: Overcoming Boundaries through Multi-Channel Interaction, June 15 - 18, 2008; Bled, Slovenia, https://domino.fov.uni-mb.si/proceedings.nsf/0/7ace7e48c4979a95c125748200347e35/$file/38hogrebe.pdf, last visited: 20.12.2014

[30] From Brutus to Snowden a study of insider threat personas, Source: http://www.isdecisions.com/insider-threat-persona-study/, last visited: 20.12.2014.

[31] Gergely Papp, Customer Satisfaction Measurement for the Customer Service in Public Administration, 2014, [in Hungarian]. Source: http://ktk.uni-nke.hu/kutatas-es-tudomanyos-elet/esemenyek_-konferenciak?tag=2014, last visited: 20.12.2014.

[32] Ginzburg, L., Sitar, P., Flanagin, G. K. (2010). User Authentication System and Method. US Patent 7,725,712, SyferLock Technology Corporation.

[34] Illéssy – Nemeslaki – Som, Electronic Information Security Consciousness in the Hungarian Public Administration System, Information Society [in Hungarian] in: Social Science Journal, Grade XIV, Issue 1 (p.:52-73) ISSN:1587-8694

[35] Internet world stat, http://www.internetworldstats.com/stats7.htm, last visited: 20.12.2014.

[36] István Bukovics, Sustainable Public Administration, the Theory of Sustainable Security [in Hungarian]

[37] István, Bukovics The System Concept of Critical Infrastructures – A Methodological Critique of a Questionnaire In: Szabolcsi Róbert, Horváth Attila, Tóth Bálint, Bukovics István, Gyarmati József, Molnár Ferenc, Németh József Lajos, Pintér István, Csaba Zágon, Dr habil Horváth Attila, Bányász Péter (ed.) Chapters from the Protection of Critical Infrastructure I

[38] Jeffrey E. Kottemann and Kathleen M. Boyer-Wright, Socioeconomic Foundations Enabling E-Business and E-Government

[39] Jenő Reich, Zsolt Döme, Civil Service within Public Administration, ÁROP-2011/1.1.12, For the question(s): "Why didn't you do set it up, what prevented you from doing it?"(The question was asked regarding e-administration) 28% answered that they do not have internet connection, and 12% said that they do not know how to use the internet or how to operate a computer.

[40] Ken H. Guo, Yufei Yuan, Norman P. Archer, and Catherine E., Connelly, Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, Journal of Management Information Systems, ISSN: 0742-1222, Business and Management, Computer Science, Management Information Systems and Information Technology, Volume 28, Pages 203-236, DOI: 10.2753/MIS0742-1222280208, 2011

[41] L. Tama, M. Glassmana, M. Vandenwauverb: The psychology of password management: a tradeoff between security and convenience, Behaviour & Information Technology, Vol. 29, Issue. 3, May–June 2010, 233–244

[42] László Kovács, Csaba Krasznay, A Digital Mohács: A Cyber Attack, Scenario against Hungary, Nemzetésbiztonság III:(Spec. Issue) pp. 49-59. (2011)

[43] Mark Burnet: Perfect Password Selection, Protection Authentication, ISBN 1-59749-041-5

[44] Matthew Reis, Judith Geller, A Manager's Guide to Human Behavior, ISBN-10: 0-7612-1241-8

[45] Nathan Alexander Sales, Regulating cyber-security, Northwestern University School of Law ,Northwestern University Law Review

[46] Norbert Tihanyi, Comparison of Two Hungarian Password Databases, Pollack Periodica, vol. 8, no. 2, pp. 179–186 (2013)

[47] Papp – Som, Password, Password, Trust and E-acceptance and their relations nowadays, [In Hungarian] II. 2014, (Nearly half a hundred recommendations regarding habits in password use)

[48] Péter Erdősi, Trust, Security, Vulnerability, HISEC 2014 Conference

[49] Proposed Directive on Network and Information Security – frequently asked questions, Press release: IP/13/94, Brussels, 7 February 2013, http://europa.eu/rapid/press-release_MEMO-13-71_en.htm, last visited: 20.12.2014.

[50] Qiang Yan, Jin Han, Yingjiu Li, Jianying Zhou, Robert H. Deng, Leakage-resilient Password Entry: Challenges, Design, and Evaluation, Computers & Security 48 (2015) 196 e211, last visited: 20.12.2014.

[51] Reich Jenő, Döme Zsolt, Civil Service within Public Administration, ÁROP-2011/1.1.12,

[52] Reidenberg, Joel R, Lex Informatica: The Formulation of Information Policy Rules Through Technology, Texas Law Review, Vol. 76, 1998/3. p. 584.

[53] René Meier, Tino Schuppan, Esther Ruiz Ben: Influencing Factors on the Employees' Resistance to Change in ICT-enabled Public Sector Organizational Transformation

[54] Reportlinker, Global Cyber-security Market 2013, http://www.reportlinker.com/p01080460/Global-Cyber-Security-Market-2013-2023.html#utm_source=prnewswire&utm_medium=pr&utm_campaign=Security_Systems

[55] Som – Papp, Basics of Information security and Statistics on Password Use. Password, Trust and E-acceptance and their Relations Nowadays, [In Hungarian] 2014

[56] Som – Papp, Computer Crime, or Crime where IT Devices were included, HISEC Conference, 2014

[57] Som, Papp, Basics of Information security and Statistics on Password Use. Password, Trust and E-acceptance and their Relations Nowadays, [In Hungarian] 2014

[58] Susan McLean: Beware the Botnets Cyber-security Is a Board Level

[59] Symantec's Recent Annual Cost of a Data Breach Report http://www.symantec.com/connect/blogs/cost-data-breachstudy-highlights-critical-role-symantec-partners-serve., last visited: 20.12.2014.

[60] Tamás Szádeczky, The Conflict of Regulating IT Security, Info-communication and the Law [in Hungarian]

[61] The EU 2020 Programme also includes the need for setting up and improving broadband internet connections and that of the system of e-public administration. Communication from the commission, EUROPE 2020, A European strategy for smart, sustainable and inclusive growth, http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf, last visited: 20.12.2014., last visited: 20.12.2014.

[62] The European eGovernment Action Plan 2011-2015, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF, last visited: 20.12.2014.

[63] The Tallinn Manual on the International Law Applicable to Cyber Warfare, NATO Cooperative Cyber Defence, Centre of Excellence Tallinn, Estonia, https://www.ccdcoe.org/, last visited: 20.12.2014.

[64] Trilogue system informal tripartite meetings attended by representatives of the European Parliament, the Council and the Commission. ttp://ec.europa.eu/codecision/stepbystep/glossary_en.htm, last visited: 20.12.2014.

[65] Vajda – Bencsáth – Bognár, Study on the Elender Passwords Come to Light. http://tig.kgk.uni-obuda.hu/targyak/gazdinfo/gyak_KEA/ElenderJelszo.html, [In Hungarian], last visited: 20.12.2014.

[66] Wei Wang, Hongwei Wang, Yuan Meng, A Large-scale Survey on Password Habits of Internet Users in China,

[67] Wolf, P.; Krcmar, H. 2006, p3: Collaborative E-Government – Bedarfsorientierung in komplexen Unternehmenslagen [in German]. http://www.winfobase.de/lehrstuhl/publikat.nsf/intern01/547F7EB0B782A86BC1257221003E8EB3/$FILE/06-44.pdf, last visited: 20.12.2014.

[68] Zoltán Som , Cyber security legislation in the EU, NISPAcee 2014,

[69] Zoltán Som, Authentication Issues regarding (e-)Public Administration in Hungary, [in Hungarian] "Tavaszi szél" Conference

[70] Zoltán Som, Cyber security legislation in the EU, NISPAcee 2014,

[71] Zoltán Som, Dangers of the Internet and Recommendations on Handling them, with a Primary Focus on Teens in Elementary School. Information on Methodologies: for Teachers [in Hungarian] 2012- 53:(2) PP. 21-32. (2013)

[72] Zoltán Som, Laws aiding cyber-security in the EU, 2013, Central and Eastern European e|Dem and e|Gov Days 2014

[73] Zoltán Som, With Cyber-Consciousness against Cyber Warfare, 13. Robot Warfare conference,