Multi factor authentication as a necessary solution in the fight with information technology security threats

Anita Jansone, Kaspars Lauris, Ivars Šaudinis
Liepaja University, Faculty of Science and Engineering,
Address: Liela iela 14, Liepaja, LV-3401, Latvia

Abstract. **In the publication multi factor authentication solutions are offered as a necessary tool for decrease of information technology security risks. The work includes description of authentication process from the viewpoint of information technology security aspect, as well as authentication factors are described, which can be used in authentication process modules. Some recommendations for decrease of security risks are given using multi factor authentication solutions. In the work a multi-factor authentication security testing experiment is described, which involves use of Linux remote console - SSH service. Analysis of data of unauthorised access efforts obtained during tests is described: it is determined from which countries or regions, as well as in which days there is the highest threat to information technology security.**

Keywords: **authentication, authentication security testing, authentication factor, authentication security risk, identification, password.**

I INTRODUCTION

Nowadays in the world of information technologies static authentication data - passwords or the same in combination with other authentication factors are less and less used in newer authentication solutions. Use of static passwords in authentication process involves high security risk. Even if a user of a system composes a "secure" password, there are no guarantees that the same user will not use this password in another system, where the security level is low, thus putting other systems to risk. As Jonathan Klein, the president of a well-known company *Usher*, which deals with mobile identification solutions for enterprise needs, says *„I think the password is going the way of the dinozaur”* [11]. He believes that use of passwords will come to the end one day because there are more modern and secure authentication technologies being able to substitute the use of passwords. Multi factor authentication solutions are offered to decrease authentication security risks. In case of multi factor authentication, even if the lawbreaker obtains your passwords it is impossible to access your data in the system, because he does not have the code card assigned to you by the bank or a code calculator or your mobile phone, where an application generates a dynamic password, which is an additional authentication factor.

There have been lots of publications, where IT security experts make qualitative statements about the fact that multi factor authentication solutions significantly decrease security risk. But there are not any publication providing quantitative data for proving those statements. Therefore, it was decided to perform multi factor authentication security tests and obtain quantitative data about multi factor authentication security risk, providing and proving the hypothesis - *if the process of authentication is organized in several stages, and at each stage different authentication factors are used, then it is possible to decrease authentication security risk.*

To determine what authentication solutions it is possible to create, it is important to find out what authentication data or factors it is possible to use in the authentication process.

II AUTHENTICATION SOLUTIONS AND FACTORS

Identification is a quite simple process. A person should submit own data to the system and the system can launch authentication and authorisation processes. To submit data to the system it is enough to enter only a user name or to scan a fingerprint etc. Without identification the system cannot associate authentication factors with the person. During authentication the person's identity is checked by comparing one or several factors to the information about this person, kept in the data base. Authentication data used to check person's identity is the information of restricted access. Ability of the person and the

ISSN 1691-5402

DOI: http://dx.doi.org/10.17770/etr2015vol3.183

system to keep authentication data confidential reflects the security level of a certain system.

Identification and authentication processes always happen as a single two-step process [2]. User identification is always done at the first step followed by authentication at the second step. Without having completed both processes the person cannot get access to the system.

From the viewpoint of information technology security authentication processes can have one-stage, two-stage and multi-stage authentication mechanisms [3]. At each stage the authentication process can be static, dynamic or biometric depending on the authentication data used in the authentication process.

The number of stages and factors used in the certain authentication process depends on the authentication solution. In its turn, the authentication solution depends on how important or sensitive are the data in the system, where user authentication needs to be performed. It is important to use different authentication data or factors at each stage of the multi-stage authentication process.

The authentication data used at each stage can be put into several categories [4]:

1. something you **know** – password, personal identification number - PIN;
2. something you **have** – code card, code calculator, smart card, mobile device etc.;
3. something you **are** – user biometric data, for example, voice, fingerprints, etc.

*A. „Something you **know**" authentication factor*

As it was mentioned before, there are three factor groups. The first of them corresponds to the condition „something you **know**". This authentication factor group is formed by passwords, PIN, phrase or cognitive passwords. However, this authentication factor group contains only static authentication data. Insecure passwords create the main authentication risk, but if the person composes a safe password, it is a powerful authentication factor, which decreases the security risk [4].

Companies usually elaborate information system security policy due to this is defined by legal standards. Such document is elaborated by an information system security expert, and should be certified and approved by the head of institution. Usually such documents also include password composition and application policies. The password composition policy determines the frequency of password changes, the length of passwords and the complexity of password composition algorithm. Furthermore, it is also important to keep in memory all the composed passwords and to implement prohibition in the system for users to use only two passwords all the time, by changing them periodically. Information system users usually choose phrase-type passwords. Such passwords are easier to remember, but are more difficult to guess by using *„brute-force"* methods. They perform the same functions as traditional passwords, and usually are easier to remember because users put some meaning into them. Phrase-type passwords are simple sentences with some modifications. For example – the phrase „Neviens nav ideāls", where „s" is substituted by „$" and „a", or „ā" by „@", and as the result a phrase-type password is obtained – „Nevien$N@vIde@l$".

Another interesting password composition mechanism is used by cognitive passwords [2]. Usually cognitive passwords are formed as a number of questions, which can be answered only by a certain person. For example - "What is your date of birth?", "What is your mother's name?", "What is your pet's name?" etc. The most effective way would be answering a series of such questions during authentication, however, that would significantly delay the authentication process. Therefore cognitive passwords are usually used in case users forgot their passwords. In this case, by providing the correct cognitive password a user can renew the usual password.

*B. „Something you **have**" authentication factor*

The second authentication factor group corresponds to the condition "something you have". This means that the user has a device, which either contains identified authentication data or is able to generate them. Such devices are called "smart-cards" or "tokens", or just security system devices. However, such devices are prone to risk - they can be stolen, lost or duplicated.

Smart-cards have integrated microprocessors and memory, where one or several certificates are stored. The certificates contain subject identification and/or authentication data, which a person can use for identification and/or authentication. The certificates are generated using asymmetric cryptography, such as encryption or digital e-signature. Smart-cards represent a secure authentication factor, they are easy to carry and use complex encryption keys in the identification or authentication process. When a smart-card user wants to perform authentication process, the smart-card is inserted into the reader. Afterwards, the user is usually asked to enter the PIN code or the password, which is another authentication factor. Smart-cards are able to provide both identification and authentication processes. However, it is to admit, that smart-cards are not effective identifiers, because they can be easily given to other persons, changed or stolen [2], therefore, they should be always used together with other authentication factors.

A security system device is a password generating tool. Security system devices are equipped with informative displays, they generate passwords, which have limited usage time interval, for example, 30 seconds. Security system devices use several elements - a unique security system device identifier, which is different for each device, time and encryption key. Security system devices usually are not the only one authentication factor in the authentication process. When using the security system device usually a multi-stage authentication process is created, where at the first authentication stage static authentication data are used - passwords or phrase-type passwords, but at the second authentication stage only a single-use password is used, which is generated by the security system device. But even such authentication devices are prone to security risk. Such devices can be lost, compromised, the battery can expire or the device can malfunction and as the result the device will not be suitable for authentication process. The security system devices are usually activated by entering the *PIN* code, which decreases the authentication security risk. If the device is lost, it will not be easy for the finder to activate and use it.

Two of the most popular security system device types are synchronous and asynchronous dynamic password generators. However, in the authentication process static security system devices are used as well. Synchronous and asynchronous security system devices work as single-use password generators. Single-use passwords are dynamic authentication data, which are changed after the certain time interval or they can be used in the authentication process. Synchronous dynamic password generators generate passwords within the known time period, for example, within 30 second interval, and one of the password generation elements is time. That means that there should be time synchronisation between the security system device and the authentication system. In order for the person to be identified, it is necessary to enter the password generated by the security system device into the authentication system interface. Moreover, the security system device itself shall be activated by using the *PIN* code or the password, which is the second authentication factor. The generated single-use password can provide user identification and/or authentication, but the *PIN* code or the password provides only authentication. Asynchronous dynamic password generators do not use time as the password generating element. In this case, the security system device generates a password only when the person has entered the code generated by the authentication system. By using asynchronous dynamic password generators the authentication process includes also the*„challenge-response"* process. For example, when a person wants to be authenticated in the system, at the first stage it is necessary to enter a user name and a password. After the authentication system has checked the entered credentials, it generates a request code by using the security system device identifier, which is then displayed in the interface. The request code is unique for each authentication. The person enters this request code into the own security system device, which then generates a single-use password that has to be entered by the person into the authentication system in order to finish the authentication process.

Static security system devices can be magnetic cards, smart-cards, *RFID* cards and tags, diskettes, USB devices [2] etc. Various static security system devices contain encryption keys, such as electronic signature, private encryption key *„private key"* or encrypted authentication data. In order to provide authentication process, static security system devices usually require an additional authentication factor - a static or a biometric authentication factor. However, there are cases, when the private encryption key serves as the only authentication factor. Such authentication type is widely used in Linux/Unix system administration in order to perform remote console connection from one resource computer to another.

*C. „Something you **are**" authentication factor*

The third authentication factor group corresponds to the condition "something you are". These are called biometric authentication factors. Biometric authentication factors can be used both for person's identification and authentication. Biometric authentication data can be obtained from person's biological parameters or behaviour features [5]. As to behaviour features, it is possible to say that they correspond to the authentication factor group "somehow you do it". The most popular biologic parameters used during authentication process in companies are fingerprints, venous structure of palms and fingers, eye cornea features, voice or face structure. The last three parameters do not anticipate physical contact with the biometric sensor, thus becoming less reliable. Behaviour features, used in authentication process, relate to keyboard use dynamics. To identify the person, the interval between pressing keys is measured when a word or a phrase is entered. Previously use of biometric authentication in companies was hard to implement due to high expenses, it was necessary to purchase biometric sensors and to perform complex implementations in authentication modules of information systems. However, nowadays smart-phones are very popular, which have such equipment that can be used as biometric sensors, thus making biometric authentication available for the enterprise information systems. Smart-phones are equipped with digital cameras able to perform face or eye cornea recognition, microphones for voice recognition and a keyboards for determining the rhythm of key usage.

Biometric authentication data cannot be easily lost, stolen, broken, guessed, copied or shared. Comparing with passwords, smart-cards or security system devices, biometric authentication factors are much more resistant to social engineering attacks, because it is necessary for a person to be present during authentication process. Google Intelligence security analyst Alan Goode believes that *„Biometric systems can be much more convenient than tokens and other systems, and are useful to augment existing security methods like passwords. For added security they are also sometimes used as a third factor."*

The main shortage of biometric systems is inability to provide 100% precision in its functioning [5]. To use a biometric system, it is firstly necessary for a person to submit one or several biologic data samples to the system for configuration, for example, fingerprints. When the person tries to perform authentication, the fingerprint is compared with the saved sample and, if it is similar enough to the sample stored in the authentication system, the person's authentication is performed. Measuring precision of a biometric system is usually described by two error rates – *„False Non Match Rate"* and *„False Match Rate"* [5]. The first one "False Non Match Rate" describes the number of authentication efforts in the system containing person's biometric data samples, which were not approved by error. The second one "False Match Rate" describes the number of successful authentication efforts in the system, not containing the person's biometric data samples. The majority of biometric systems can be adjusted to decrease one of these rates, however, this happens at the expense of the other rate. Mark Diodati, the analyst of the company Gartner, said: *„It's important to understand that when a user supplies a password or a number from an OTP (one time password) token, it is either correct or it isn't. With biometrics you never get a definitive yes or no"*. Various biometric systems provide different security levels, determined by error rates. A good fingerprint sensor offers low error rates, thus providing a better security level in comparison to the non-contact biometric sensors, for example, microphone or digital camera for voice or face recognition. Fingerprint readers do not work properly in the environment, where users may have dirty fingers. Thus, voice recognition sensors are not suitable for the environment with high noise level. Sensors with low error rates can be used as the only authentication factor. But if error rates are high, then biometric authentication factors should be used together with other authentication factors, organizing a multi-stage authentication process, which significantly decreases the security risk.

III MULTI FACTOR AUTHENTICATION SECURITY TESTING

In order to start testing of authentication security, a testing server was created with the name Omega:

- the chosen equipment *AMD Athlon II X3 440* three core processor, *DDR3 4GB* RAM, *SATAII 500Gb* hard disk, network card *1 Gbit*;
- the installed operation system *Gentoo GNU/Linux* with minimal configuration;
- *Omega* testing server was assigned a real *IP* address;
- *ssh* service installed for server console connection;
- installed *Google authenticator* for a two-stage authentication process implementation [6];
- configured so that in case of successful *ssh* service authentication, the work author receives an e-mail about unauthorised connection and the server shuts down. In order to implement this, *Mutt* e-mail client *GNU* software and *Postfix* e-mail server *GNU* software was installed that will forward a message sent by the *Mutt* client to the given e-mail;
- for the privileged user *root* an insecure password is set *„password"*, users *admin*, *test* are created with passwords *„admin"* and *„test"*.

The aim of the test is to determine whether a multi-factor authentication solution decreases the security risk, by proving the hypothesis of this publication. The research is done in two parts:

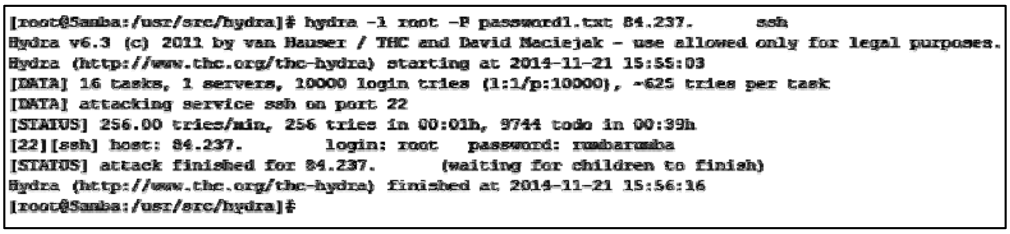
a) In the first part of authentication security testing, for *ssh service* authentication a single-factor authentication is chosen with static authentication data - passwords, which were composed as "insecure";
b) In the second part of authentication security testing, for *ssh* service authentication a two-stage authentication is activated, where in the first stage static authentication data are used - passwords, and in the second stage - a single-use password is generated by *Google authenticator*.

After all the installation and configuration works are finished, all the functions of the test server *Omega* are checked prior to testing of the authentication security in the internet environment. Various password guessing tools are considered, such as*Ncrack, Medusa, Hydra*, in order to be able to perform password guessing using the remote *ssh* service console [7]. For Omega test server password guessing a tool *Hydra* was chosen, because the newest version of it was available. *Hydra* software was downloaded and installed on another test server. From the web-site *http://xato.net/* 10000 of popular passwords were downloaded and saved in the file *passwords1.txt* [8]. To perform the test, the superuser *root* was assigned a password *„rumbarumba"*, which was added to the file *passwords1.txt*. In the console of Omega server the corresponding command was entered to start the password guessing.

Example:

```
#hydra –l root –P password1.txt 84.237.XXX.X ssh
```

At the time of password guessing simulation the *Omega* test server was configured for the first part of authentication security testing, a single stage was used during authentication with static passwords without dynamic password generation by means of *Google authenticator*.



```
[root@Samba:/usr/src/hydra]# hydra -l root -P password1.txt 84.237.      ssh
Hydra v6.3 (c) 2011 by van Hauser / THC and David Maciejak - use allowed only for legal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2014-11-21 15:55:03
[DATA] 16 tasks, 1 servers, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking service ssh on port 22
[STATUS] 256.00 tries/min, 256 tries in 00:01h, 9744 todo in 00:39h
[22][ssh] host: 84.237.        login: root   password: rumbarumba
[STATUS] attack finished for 84.237.      (waiting for children to finish)
Hydra (http://www.thc.org/thc-hydra) finished at 2014-11-21 15:56:16
[root@Samba:/usr/src/hydra]#
```

Fig.1. Hydra password guessing tool in action

After a known period of time the *Omega* server was compromised, and after sending the e-mail message the *Omega* test server shut down. In the Fig. 1 it is possible to see the *Hydra* password guessing tool in action. In the Fig. 1 it is seen that within a comparatively short period of time - 73 seconds, for the *Omega* server superuser *root 9744* passwords were tested. In order to start authentication security testing of the *Omega* test server in the internet environment, the superuser *root* was assigned an insecure password *„password"* and in the firewall of the network router access from the internet was activated for the port 22 of the *Omega* server. Such password was not chosen randomly. According to the researches this is the most popular password in the year 2014 chosen by computer users [9].

The first part of authentication security testing started on 21.11.2014 and.16:34 and on 23.11.2014 at 1:47 a hacker with *IP* address beginning with *176.102.3XX.XXX* registered in Ukraine, guessed the user name *admin* and the password *„admin"*. The duration of the test was 33 hours and 14 minutes until the moment the *Omega* test server shut down, sending an e-mail message about the compromised system.

As the privileged user password was not guessed, the authentication security test was retaken. The repeated test started on 24.11.2014 at 9:00 and on 25.11.2014 at 1:51 a hacker with *IP* address beginning with *222.161.XXX.XXX* registered in the Public Republic of China, guessed the privileged user *root* password *„password"*. The repeated test took 16 hours and 51 minute.

In the second authentication security testing part for *ssh* service the above-mentioned two-stage authentication was activated using *Google authenticator* dynamic passwords at the second stage and no one except the test server administrator could be able to perform authentication. In five months it has been more than 1.7 million unauthorized connection attempts, approximate 10335 in a day. Unauthorized connection attempt statistics has been published in the portal *http://ssh-stats.liepu.lv*. At the site can be seen the statistics of the unauthorized connection attempt geographic and *Logwatch* application ssh service original log files.

IV TESTING RESULT ANALYSIS AND RECOMMENDATIONS

The testing security experiment proves the stated hypothesis, because from the moment the multi-factor authentication was activated, no one was able to compromise the test server. Such authentication security testing proves that dynamic passwords represent a secure authentication tool, which is hard to compromise nowadays. However, it is possible to decrease the security risk to a larger extent if at the first stage of authentication a secure password is used. The company *TrustWave* published a research in IT security field *„Trustwave Global Security Report 2014"* stating that more than 31% of all IT incidents happen due to insecure passwords [1][10]. This indicates that each third password composed by users is *„insecure"*. From this it follows that it is unsafe to use static authentication data - passwords as the only authentication factor. In authentication solutions it is necessary to use the authentication data, which are not created by a person, for example, single-use dynamic passwords. In order to decrease authentication security risk, it is necessary to use multi-factor authentication solutions and static authentication data should always be used together with other authentication factors.

The unauthorised connection effort data obtained during authentication security tests can be analysed. What do we get from it? It is possible to determine regions and countries with the highest threat level. It is possible to estimate whether it is necessary for business to have contacts from such countries or regions and to make decision about blocking access to IT resources or to improve system authentication security by introducing multi-factor authentication.

At the beginning of the research *IP* address origin is analysed with the aim to determine the countries or regions with the highest threat level. The results are shown in Fig. 2. According to the results, the highest threat level is from Hong Kong, which makes 58.42% of the total threat volume. Likewise, high threat level is from the Public Republic of China – 28% and from

Australia – 9.65%, France – 2.46%, Italy, Moldavia, Korea, Kazakhstan, Portugal and Germany. If it is not important for your business to have connections with Hong Kong and China, restrict the access to your IT resources for these countries. If you have collaboration partners in such countries, it is necessary to perform access control and use multi-factor authentication in authentication solutions.

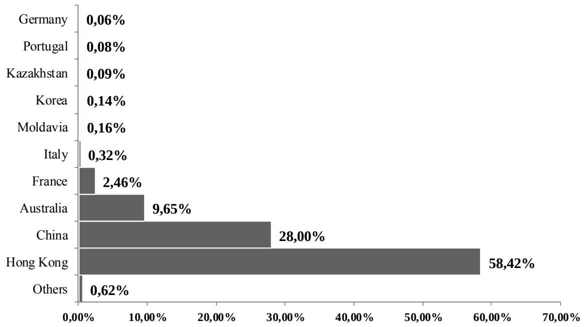


Fig.2. *SSH service* unauthorized connection attempts geographic statistics

Further, the data acquired from the statistics of unauthorised connection efforts to *SSH services* are analysed in order to determine the days of week, when the security threat level is the highest. Analysis of data obtained within 23 weeks was performed. The results are shown in Fig. 3.

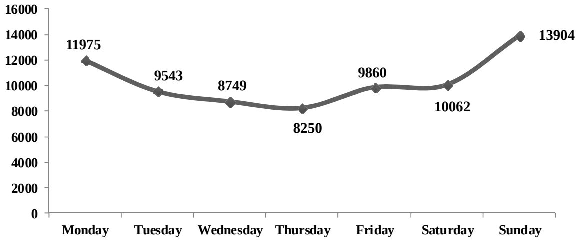


Fig. 3. SSH service average unauthorized connection attempts by days of week

According to the obtained data shown in Fig. 3, the highest IT security threat level is observed on Saturdays, Sundays and Mondays. The reason why exactly in these days IT security threat level is the highest is a good topic for another research. However, authors of this paper can express some qualitative statements regarding this situation. Namely, on Saturdays the threat level can be high, because on weekend the number of employees in corporations decreases thus decreasing the level of IT resource monitoring. A lawbreaker, having obtained the access to the system on Saturday, will be able to perform lots of actions during the weekend without being noticed. In its turn, on Sundays the threat level is high for IT resources because on this day availability and application level of IT resources is the lowest. Therefore, it is recommended to monitor and control IT resources not only during working days, but also in the weekends and on holidays, so that in case of IT incidents the responsible person could perform the necessary actions to prevent the incident.

V CONCLUSION

When applied, various authentication technologies prove that there are more secure solutions rather than password authentication solutions, which use dynamic and biometric authentication factors. This statement is proven also by the authentication security testing experiment described in this publication. The multi-factor authentication process, which uses static and dynamic passwords, provides lower authentication risk even if the static password is considered as unsafe. At the moment in the world passwords are being replaced by other authentication technologies and this is the question of time, when passwords will no longer be used in the authentication process!

There will always be authentication security risks for each authentication solution, and it is impossible to create a 100% secure authentication solution in the nearest future. Therefore, it is necessary to continue the research in the field of authentication solutions and security risks, determining what security risks are new authentication solutions prone to. Using theoretical research methods, performing direct and indirect observations and tests of authentication security, it is necessary to find out, what security risks are authentication security system devices and biometric sensors prone to.

In another research it would be interesting to find out, why such high level of IT security threats comes directly from the Public Republic of China, including the special administrative region thereof - Hong Kong. It would be interesting to find out whether inhabitants of this country are initiators of IT threats or is it the politics of the country, which is favourable for hackers from other countries to perform unlawful actions from IT resources of PRC.

VI REFERENCES

[1] A. Jansone, K. Lauris, “Authentication solutions and security risks”, presented at International Joint Conferences on Computer, Information, Systems Sciences & Engineering (CISSE 14), Dec. 9, 2014.

[2] J.M. Stewart, D. Gibson, M. Chapple, “Certified Information Systems Security Professional – Study Guide (Sixth Edition)”, Canada, John Wiley & Sons, 2012, pp. 1-47.

[3] L. Lāce, “Divpakāpju autentifikācija”, Riga, CERT.LV - the Information Technology Security Incident Response Institution of the Republic of Latvia, Feb. 19, 2013. [Online], Available: https://www.esidross.lv/2013/02/19/divpakapju-autentifikacija/ [Accessed: Feb. 20, 2015].

[4] C.P. Pfleeger, S.L. Pfleeger, “Analyzing Computer Security – A Threat/Vulnerability/Countermeasure Approach”, USA, Pearson Education, 2012, pp.38–64.

[5] P. Rubens, “Biometric Authentication: How It Works”, Aug. 17, 2012. [Online]. Available: http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html [Accessed: Feb. 20, 2015].

[6] "Install Google Authenticator". [Online], Available: https://support.google.com/accounts/answer/1066447?hl=en [Accessed: Feb. 21, 2015].

[7] "Brute Forcing Passwords with ncrack, hydra and medusa". [Online], Available: http://hackertarget.com/brute-forcing-passwords-with-ncrack-hydra-and-medusa/ [Accessed: Feb. 21, 2015].

[8] M. Burnett, "10,000 Top Passwords" Jun. 20, 2011. [Online], Available: https://xato.net/passwords/more-top-worst-passwords/#.VI7ZHnvLLCD [Accessed: Feb. 26, 2015].

[9] A. Kooser, "Worst passwords of 2014 are just as awful as you can imagine", Jan. 20, 2015. [Online], Available: http://www.cnet.com/news/worst-passwords-of-2014-are-just-as-awful-as-you-can-imagine/ [Accessed: Mar. 2, 2015].

[10] D. Kaplan, "2014 Trustwave Global Security Report", May 21, 2014. [Online], Available: https://www.trustwave.com/Resources/Trustwave-Blog/The-2014-Trustwave-Global-Security-Report-Is-Here/ [Accessed: Mar. 4, 2015].

[11] L. Eadicicco, "Passwords Are A Horrible Way To Keep Us Safe — Here Are The Potential Alternatives" May 11, 2014. [Online], Available: http://www.businessinsider.com/password-alternatives-2014-5 [Accessed: Mar. 5, 2015].