Transparent password policies: A case study of investigating end-user situational awareness

Alberto Bullo, Eliana Stavrou
Computing department, Applied Cyber Security Research Lab, University of Central Lancashire, Cyprus

Stavros Stavrou
Faculty of Pure and Applied Science, Open University of Cyprus

ABSTRACT

Transparent password policies are utilized by organizations in an effort to ease the end-user (e.g. customer) from the burden of configuring authentication settings while maintaining a high level of security. However, authentication transparency can challenge security and usability and can impact the awareness of the end-users with regards to the protection level that is realistically achieved. For authentication transparency to be effective, the triptych security – usability – situational awareness should be considered when designing relevant security solutions / products. Although various efforts have been made in the literature, the usability aspects of the password selection process are not well understood or addressed in the context of end-user situational awareness. This research work specifies three security and usability-related strategies that represent the organizations', the end users' and the attackers' objectives with regards to password construction. Understanding each actor's perspective can greatly assist in increasing situational awareness with regards to the authentication controls usage and effectiveness. Furthermore, a case study is presented to evaluate if, and in what way, transparent password policies, that isolate users' involvement can affect the perspective of the end-user with regards to the

security situation. Results showed that the transparent approached utilized has created a negative situation, users were not aware and never dealt with changing or trying to alter default security settings configured on their wireless access point, leaving their home network vulnerable to external attacks. Finally, initial recommendations are made to organizations that would like to implement and evaluate transparent authentication controls.

Keyword: Transparent security; transparent password policy; password cracking; usable security; end-user cyber situational awareness.

1 INTRODUCTION

One of the most challenging aspects of information security is user authentication (Payne and Edwards, 2008). Users utilize passwords in everyday life to access their accounts and support their activities. Although user authentication is a topic well studied, the practice of using passwords as a means of providing identity is challenging security and usability design aspects (Flechais, Mascolo and Sasse, 2007) and can hinder situational awareness (Barford et al., 2009). Authentication controls such as password creation policies, try to balance between strong security (which dictates more diverse passwords that are not easily cracked) and usability of authentication mechanisms (relating to the ease of use and memorability of passwords). Assessing if authentication controls can successfully balance security and usability can lead individuals and organizations to predict and respond to potential threats that might arise. By identifying vulnerabilities relevant to authentication controls and by anticipating relevant threats, we can increase situational awareness and empower end-users and organizations to develop effective countermeasures.

Authentication mechanisms, and particularly password utilization, combines both technical and human factors. From a technical perspective, appropriate password policies are utilized to drive the construction and implementation of strong passwords. The human factor (Sasse and Flechais, 2005) plays a crucial role in user authentication. Often, the human factor is considered the weakest link with regards to security and password creation. If users are allowed to create their own passwords, this could lead to weak passwords. Easily guessable passwords constitute a vulnerability that can be exploited by malicious people to gain unauthorised access to a system and relevant resources. This vulnerability could occur due to reasons such as users' lack of awareness and training or because convenience (e.g. short and easy to remember passwords) is chosen over security.

Many organizations address the aforementioned problem by designing services/products that utilize transparent security policies (Shay, 2016) in an effort to prevent end users, e.g. customers, from choosing weak passwords. Therefore, the organizations produce the password and provide it to the end user, often without the possibility for the user to change the password. With this approach, the user is isolated in an effort to ensure that the security policy is always applied to meet the expected security requirements. Transparent security may be desirable by users, especially by those who are not familiar, for example, with the security settings of a product that need to be configured to protect its operation and data. Transparency could promote usability as the user is not troubled with security aspects he/she may not be familiar with. However, one should consider that transparent security could also lead to vulnerabilities. Transparent security could greatly impact the end-user understanding of the situation by creating a false sense of security, as users could rely on good faith upon the organization to achieve the desirable level of security. Therefore, it is imperative to evaluate transparent security controls, identify negative situations and address them accordingly in a timely manner before attackers have the chance to identify and exploit vulnerabilities.

The objective of this research work is to: a) specify usability and security related strategies with regards to the password construction process, b) investigate through a case study if, and in what way, transparent password policies utilized by wireless access points (that isolate end users' involvement) can hinder situational awareness, and c) provide recommendations to increase situational awareness through transparent password policies. Section 2 discusses related work. Section 3 specifies appropriate usability and security related strategies with regards to the password construction process. Section 4 presents the case study and section 5 provides recommendations related to the design and assessment of transparent authentication controls. Section 6 constitutes conclusions.

2 RELATED WORK

Wireless networks, while being very popular and accessible, face a variety of security challenges. Zou et al. (Zou, Wang and Hanzo, 2015) explain how an intruder in the wireless medium can penetrate the network without "breaking in the building" as he would in a wired network, by remotely attacking from a distance. Waliullah et al. (Waliullah, Moniruzzaman, and Rahman, 2015) point out that the wireless medium, due to its open nature and long coverage of areas, can become the only target by outsiders because it is hardly traceable by authorities. So attackers remain invisible. Wireless

signal transmissions can be intercepted, and different techniques are able to perform attacks capable to collect and analyze sensitive data which can cause severe loses to companies and users (Solms and Marais, 2004). Jiantao et al. (Jiantao, Jinghong and Tao, 2012) explain how some of these attacks are feasible on the existing wireless security protocols, considering the data link MAC layer of the OSI model where beacons are transmitted with no encryption, leaving attackers the ability to spoof or sniff radio signals. To mitigate these issues, cryptographic protocols were introduced to encrypt data communication in the WLAN such as WEP, WPA and WPA2 encryption (Kumar and Gambhir, 2014). Even though these protocols added a layer of encryption, they failed to remain invulnerable with WEP encryption being the weakest and now obsolete (Naamany, Shidhani, and Bourdoucen, 2006). WPA and WPA2 protocols provide a greater level of protection and are widely used by all networking vendors today. However, some vulnerabilities have been discovered for WPA and WPA2. These vulnerabilities relate to offline dictionary attacks, allowing an attacker to try different key combinations from a list of words in order to find the correct wireless network authentication key (Lashkari, Danesh and Samadi,, 2009). This attack utilizes the authentication information collected from the four-way handshake used for the initial communication of the client with the access point. The four-way handshake packet, once collected by an attacker, can be brute forced to match the authentication key of the wireless access point. Since it is an offline attack, this means that it can be performed in any location without the need to be close to the access point (Hytnen and Garcia, 2006). Depending on the authentication key complexity and length, a brute force or dictionary attack can be successful if only the password is weak and not configured correctly. If the key is found, then the attacker has access to the wireless network unless additional security measures, such as MAC filtering, are applied. It is crucial then for networking manufacturers and Internet service providers to ensure the devices are secured by default with all important security protocols preconfigured (Loo, 2008). More recently, another vulnerability related to WP2 was demonstrated by (Vanhoef and Piessens, 2017). The authors demonstrated the key reinstallation attack. This attack abuses design or implementation flaws in cryptographic protocols to reinstall an already-in-use key. This resets the key's associated parameters such as transmit nonces and receive replay counters. By forcing nonce reuse in this manner, the data-confidentiality protocol can be attacked, e.g., packets can be replayed, decrypted, and/or forged.

Another important issue that needs to be taken into consideration when securing a network is users' usability (Ho, Dearman and Truong, 2010). Bly et al. (Bly et al, 2006) identified that non-tech savvy users have difficulties

or are unable to understand the security principles. (Durbin, 2011) showed the importance of users' awareness and attitude for correctly configuring the security of their networks and computers due to the increased reliance on the internet (Arachchilage and Love, 2014). Previous studies as in (Sheng et al, 2006) demonstrated that users might become victims if they are unable to use the security features properly. Some solutions focusing on the users were then proposed by researches. (Calvert, Edwards and Grinter, 2007) proposed a self-configuring home network with no interaction of users able to secure it-self and administer automatically. As mentioned in (Furnell, 2005), transparent security overcomes irresponsible users' actions. However, even if transparent security solutions can solve some of the issues related to the users, they usually do not help with user security situational awareness. (Whalen and Inkpen, 2005) identified transparent security as a weakness because users were not aware if they were at risk or secure at the end. A trade-off between these usability studies was proposed in (Ho, Dearman and Truong, 2010). Ho et al. (Ho, Dearman and Truong, 2010) suggested a guided initial configuration wizard of the wireless access point when first powered up, helping the users making the most secure choices and explain at the same time which security protocols and features to enable. By using this method, home users get the information needed on best security practices and understand the basic secure configurations. (Shay, 2016) has focused on constructing different password-composition policies and evaluating which have been more usable and secure. They have observed that by forcing users to break their password construction habits, they made the password selection process more difficult but have also achieved the creation of stronger passwords.

3 PASSWORD CONSTRUCTION: SECURITY VS USABILITY STRATEGIES

Password utilization (Payne and Edwards, 2008) is a typical authentication method, with the achievable security level highly depended on the password construction policy. For the password construction process to be effective, both security and users' usability aspects should be considered.

In terms of security, it is desirable to prohibit attackers from easily cracking passwords. There are a variety of tools, e.g. John the Ripper, HashCat, AirCrack, etc., that can attempt to crack users' passwords. Typically, a dictionary or a brute force attack is launched against users' passwords. A dictionary attack considers wordlists that contain predefined words, often mangled based on a variety of rules to create even more possible passwords. A brute force attack considers all possible combinations of characters,

numbers and symbols, thus it could be a very time consuming process compared to the dictionary attack. From an organization's point of view, constructing diverse, random passwords of minimum 8 characters, mixing upper case and lower case characters, numbers and symbols, could decrease the possibility of account compromisation (Payne and Edwards, 2008). Therefore, a high security level can be achieved. From an attacker's perspective, a low security level is desirable that can be achieved by either a non-restrictive password policy or due to bad password construction practices followed by the end users. Finally, the security level that is pursued by end users typically depends on their level of security awareness and training.

In terms of usability, there are also different strategies depending on the objectives pursued by organizations, end users and attackers. The usability strategy of the user mainly considers constructing passwords that are memorable so they can be easily recalled and used. On the other hand, the usability strategy of the attacker considers making the password cracking process more efficient by decreasing the password-creation space. To achieve this, the attacker relies on the fact that users focus more on their convenience and the memorability of their password than the underlying security that can be achieved. Therefore, the attacker hopes for the users to produce passwords that are easily remembered and potentially easily cracked. Furthermore, in terms of usability, the attacker relies on various user-related error-prone conditions to increase the efficiency of the password cracking process, e.g. write down a difficult to remember password, use personal information that can be obtained through social engineering attacks, etc. Another user-related usability aspect that is of interest to the attacker is the learnability of good password construction policies. If user learnability is low, there is a higher possibility for user errors to occur.

In an effort to address the usability strategies of both the end users and the attackers, organizations focus on a different set of usability aspects and promote transparent password construction policies. Transparency means that the interaction with the password construction process is low, even avoided, and the visibility of the password construction policy is obscured. The organizations' aim is to minimize the users' errors, e.g. bad password construction practices, and the attackers' efficiency of the password cracking process. However, by doing so, they remove the users' (e.g. customers') control and freedom to manage their passwords, including the ability to change it. Of course, the successfulness of the transparent password policies highly depends on the ability of the organization to

balance usability and security for its users. If it is not well balanced, user errors could still happen, e.g. write down the password. Another important aspect that needs to be considered with transparent security is users' expectations. Users can consider that the organisation has alleviated the burden of security configurations from their shoulders, and now they rely entirely on the transparent services to achieve the desirable security level. This creates a false sense of security on behalf of the end users that do not feel the need to investigate any further and setup their security configurations. However, end users should consider the possibility of vulnerabilities caused by the organizations' actions. The following section presents a case study, considering an existing transparent password policy and investigates how situational awareness may be affected.

4 CASE STUDY

This section presents a case study, investigating whether, and how, transparent authentication controls can affect situational awareness, especially from the end-user perspective. The case study involves testing the security of a wireless access point, from a specific Company, that utilizes a transparent password policy, where end users' (customers') involvement has been isolated.

4.1 Initial observations

The investigations have started when an initial gathering of passwords from some end-users who had acquired the same type wireless device from the Company had led to the following observations:

- The password length was 8 characters long
- The password was constructed using only hexadecimal characters [A-F] and [0-9]

Also, it worth mentioning that the Company did not allow the end-users to change the password (devices have been shipped with a predefined password) and that very recently it provided this feature through a web portal.

4.2 Case study design

Initially, all participants provided their consent for the practical testing to be conducted against their wireless device at their house premises. A laptop with a built in wireless card able to monitor the wireless signals in monitor mode was required to perform the test. The test was comprised of two attack attempts. For the first attempt, the client was legitimately connected and the attack was performed. If the attack was successful then the information such as password, required time or any other comments was collected. In the

second attack, the laptop was legitimately trying to connect to the wireless network. If it required an extensive time to conclude, it was left at the house overnight and collected the next day to view the results.

4.3 Methodology

The initial stage was to collect as many passwords from customers (of the particular Company) as possible to identify if there are any relations between: the SSID (Service Set Identifier or WiFi name of the device), MAC address of the wireless device and the wireless password. After extensive review an observation had been made. The MAC address of the device had something in common with the wireless password. The wireless password as noted earlier consisted of 8 characters in length, using only hexadecimal characters, thus 0-9 and A-F, in the form of "112213A4". What was noticed is that the 5th and 6th character of the password was the same as the device MAC address 9th and 10th digit. For example, in the password "112213A4", part "13" was the same as the MAC address 11:22:33:44:13:AF, which 9th and 10th digit is "13". This was considered a good starting point as it applied to every password gathered in the initial stage. Another observation was that the first 4 characters of the password were always numbers (0-9). For example, the passwords started with 2354XXXX or 7698XXXX. That was a very promising discovery because, if that was true, that meant that a dictionary could be created containing all possible combinations for passwords with the first four characters being numbers and the last four containing all hexadecimal characters. This would allow an attack such as the four-way handshake to collect the password and test it against the dictionary list. With a decent computational power calculating around 2000 keys per second, that would require around 3 days to find the key, always considering that the list contains the correct key otherwise the process will fail. Further in the review process, something else was noticed. Sometimes the 6th, 7th and 8th character of the password was changing and did not match the first observation that the 5th and 6th character matched the MAC address. For example, consider the password "1122A4FD" with the respective MAC address 11:22:33:44:A5:05. After extensive review of this password, another theory emerged. If the last digit of the MAC address in the 12th position was below number 8 (<8), the character was somehow changing in those positions. For example, if the MAC address was 11:22:33:44:AE:48 then the password would be "XXXXAE40", and only the last digit changed. But if the MAC address was 11:22:33:44:AE:40, then the password was different "XXXXAE38". If the MAC address was in this form 11:22:33:44:A4:04, with 0 in the 11th digit position and lower than number 8 in the last 12th position digit, then the password was changing all last 3 digits "XXXXA3FC". With these

observations in mind, the last digits once converted in binary values from hexadecimal characters (0 and 1), made some sense. In the example with MAC “AE:48”, the password became “AE40” and the difference was MAC last digit – 8. In the second example where MAC was “AE:40”, the password became “AE38” and the third example with MAC “A4:04” the password became “A3FC”. If the difference of MAC – 8 still applies in the last two examples, then there is some consistence if the hexadecimal character is converted to binary value or decimal number as shown in Figure 1. In that case, the decimal number 10 represents the hexadecimal character “A”, the decimal number “11” represents the hexadecimal character “B” and so on until the last character which is “F” maps to the decimal number 15. So in the end, the theory of MAC address – 8 at the last digit is correct. As shown in Figure 1, the hexadecimal characters are represented by decimal numbers in the form of numbers [0-15]. If the last example is considered where the MAC “A4:04” became the password “A3FC”, the MAC’s last digit 4 – 8 = -4 which is represented by hexadecimal character C, since with the subtraction value 0 was passed (going minus value), then there is a subtraction of 1 in the 6th and 7th password digit. So from 40 – 1 = 3F because F is the last character before moving to zero. A MAC address can be in the form of 00:00:00:00:00:00 to FF:FF:FF:FF:FF:FF. Second example was MAC “AE:40” that became password “AE38” so the theory is still consistent with 0 – 8 = -8 (hexadecimal character 8) and since the zero number was passed there is another subtraction of E4 – 1 = E3.

Binary	Hex	Decimal	
		US	S
0000	0	0	0
0001	1	1	1
0010	2	2	2
0011	3	3	3
0100	4	4	4
0101	5	5	5
0110	6	6	6
0111	7	7	7
1000	8	8	-8
1001	9	9	-7
1010	A	10	-6
1011	B	11	-5
1100	C	12	-4
1101	D	13	-3
1110	E	14	-2
1111	F	15	-1

Figure 1. Hexadecimal characters representation in decimal and binary values.

By using this theory, all gathered MAC addresses were converted to passwords and matched the last four characters of the password correctly. In this way the last four characters of the wireless password could be calculated by only having the MAC address of the wireless device which can be easily viewed by any software able to visualize the wireless access points. This discovery leaves the first four characters to be calculated which as discussed before they were observed to only contain numeric characters [0-9]. Considering this then the possible range of any access point password is: 0000XXXX – 9999XXXX. There are then 10000 possibilities or otherwise 10000 passwords contained in a list to be compared with the four-way handshake containing the correct wireless password. If a decent modern computer can calculate 2000 keys per second, then only 5 seconds are required to find the correct key (assuming that the four-way handshake packet is gathered).

With this information collected, the password strength of any wireless access point of the Company is considered very weak. For confirming the experiment, the practical part had to be done by simulating an attacker trying to penetrate the network. Since the Company used WPA2 encryption, the only method for finding the wireless password was to perform the Denial of Service attack to collect the four-way handshake and compare it against the dictionary list. Since the password was weak and there were only 10000 possibilities, another way of attacking these wireless networks was feasible. If an application went over all possibilities in the dictionary against the wireless access point directly, without the need to collect the four-way handshake, that would eliminate the need to wait for a legitimate client to connect to the access point allowing to perform the attack anytime. By using this theory, a bash script was created in Linux which reads all lines of the dictionary one by one and tried to connect to the access point like any other normal device would in the process to connect to a wireless network. This method, compared to the normal attack via four-way handshake, will require significant amount of time due to the limitation of the wpa_supplicant client which was used to perform the connection operations and required around five seconds for each key inside the dictionary (5*10000 = 50000 seconds, 13.8 hours). If the wpa_supplicant connection was successful, then the application stopped, and the correct key was presented. For speeding up the process two laptops were used, one starting from 0000XXXX towards 9999XXXX and one starting from 9999XXXX towards 0000XXXX.

4.4. Discussion

For the first experiment two practical tests were performed, one using the traditional WPA dictionary vulnerability and another one using only a dictionary and an automatic script which tries to connect legitimately to the wireless access point. Both tests were successful with the sample used. Approximately in 65% of the cases, the participants' networks were accessible by using the four-way handshake dictionary attack within minutes (since the clients were connected and present) and the rest 35% of the cases the networks were accessible by using the automated method which required around 7 to 10 hours to complete. This finding raises a danger in the security strength of the customers' wireless networks. An attacker finding its way inside the network might continue to perform credit card stealing, impersonation, data stealing attacks, etc., which can cause serious issues. As it has been observed throughout the experiment, participants lacked security awareness and had difficulties understanding the relevant security issues. Also, 85% of the users weren't aware of the new feature provided by the Company that permitted them to change their password. As a result, they have left the default security configurations (transparent security). We would also like to mention that due to confidential information issues, the name of the organization and the actual passwords discovered cannot be revealed.

The case study demonstrated that it is challenging to design effective transparent password policies that can balance security and usability while empowering the end-user (customer) to maintain a good level of awareness. It is widely recognized that end-users represent the weakest link in the cybersecurity chain. Increasing end-users cyber situational awareness is imperative to successfully address cyber threats. The research community should investigate further how transparency in security can affect situational awareness and propose measures to balance the triptych security – usability – situational awareness. The following section provides initial recommendations related to the design and assessment of transparent authentication controls.

4 RECOMMENDATIONS

Usability is often set aside when designing security solutions. Even if a highly secure system is developed, if user usability is not taken into consideration, then users will probably try to find ways to increase their convenience, having a negative impact on the overall security effectiveness. Transparent security has been proposed to address the tradeoff between security and usability. The challenge when working behind the scenes is to

simplify things, reduce configurability while at the same time provide to the users the means to understand the situation and control the security of their systems. As confirmed by the case study, it is a bad practice to remove entirely the control from the end user when it comes to configuring the security of their wireless networks. The best approach to apply, in an effort to balance usability – security - awareness, is to implement understandable security solutions that are easy to manage by the novice users. In the context of novice users, understandable security would mean to provide high level security information, focusing on key technical terms only, so that the users will be able to realize easily the related security concepts and select the appropriate configurations. Implementing a wizard to guide end users through the configuration process is a good approach and organizations should consider it more actively. Moreover, since transparent security often means that the end users will overlook security since they consider that it is already configured, the application should force the users to interact (at least once) with the configuration options. This way the users are made aware of the existence of the configurations and also are given the opportunity to investigate them further, if they want to. Organizations should also make sure to communicate to their users, new security features and provide support through different channels (e.g. email announcements, forums, training videos, etc.) in an effort to meet the requirements of both novice and expert users. Furthermore, transparent password policies should be constructed taking into consideration users' expectation, memorability, learnability, freedom and error avoidance (avoid bad practices). Finally, appropriate tools (Stavrou, 2017) need to be developed that can evaluate the level of protection that can be established through the transparent policies.

5 CONCLUSION

Transparent security is one way to ease users, especially novice ones, from the burden of security configurations. Implementing transparency on password construction and utilization policies is challenging, as the tradeoff between usability and security has to be balanced in order to promote an effective authentication solution and end-user situational awareness. Human factors play a significant role in the tradeoff that occurs between usability and security and organizations should consider these factors in order to achieve usable and understandable security. This case study proofed that transparent password policies are indeed challenging and could lead to vulnerabilities that can be exploited by attackers. The Company's regulations, to have full transparent security, affected negatively the awareness of end-users and the overall security of the wireless networks. To achieve effective security and end-user awareness, both security experts

and end users need to take into consideration each other's security requirements. It is important for security experts to have an understanding of how people will interact with the systems they develop and with the configurations they setup, and develop solutions that will be understandable and not burdensome the end user. On the other hand, end users should be security aware and try to make good security decisions. As a future work, authors are planning to extend the presented investigations and provide more recommendations as to the construction and utilization of transparent password policies.

6 REFERENCES

Arachchilage, N., Love, S. "Security awareness of computer users: A phishing threat avoidance perspective". Computers in Human Behavior, 2014, 38, pp.304-312.

Barford, P. et al. 2009. Cyber SA: Situational Awareness for Cyber Defense, Advances in Information Security, Springer, 46, pp. 3-13.

Bly, S., Schilit, B., McDonald, D., Rosario, B. and Saint-Hilaire, Y. "Broken expectations in the digital home", CHI '06 extended abstracts on Human factors in computing systems - CHI EA '06, 2006.

Calvert, K.L., Edwards, W.K. and Grinter, R.E. "Moving Toward the Middle: The Case Against the End-to-End Argument in Home Networking", In HotNets, 2007.

Durbin, S. "Tackling converged threats: building a security-positive environment". Network Security, 2011(6), pp.5-8.

Flechais, I., Mascolo, C. and Sasse, M. A. "Integrating security and usability into the requirements and design process", Int. Journal of Electronic Security and Digital Forensics, vol.1 no.1, pp.12-26, 2007.

Furnell, S. (2005), "Why users cannot use security", Computers and Security Journal, vo. 24, no. 4, 2005, pp. 274-279.

Ho, J., Dearman, D. and Truong, K. "Improving users' security choices on home wireless networks". Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10, 2010.

Hytnen, R. and Garcia, M. "An analysis of wireless security". Journal of Computing Sciences in Colleges, 2006, 21(4), pp.210-216.

Jiantao, G., Jinghong, F. and Tao, W. "Analysis of Current Wireless Network Security", International Journal of Education and Management Engineering (IJEME), 2012, vol. 2, no. 10, p.34.

Kumar, U. and Gambhir, S. "A Literature Review of Security Threats to Wireless Networks", International Journal of Future Generation Communication and Networking, 2014, vol. 7, no. 4, pp.25-34.

Lashkari, A.H., Danesh, M.M.S and Samadi, B. "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)". In Computer Science and Information Technology, 2009. ICCSIT 2009, pp. 48-52.

Loo, A. "The myths and truths of wireless security". Communications of the ACM, 2008, 51(2), pp.66-71.

Naamany, A.M. Al, Shidhani, A. Al and Bourdoucen, H. "IEEE 802.11 wireless LAN security overview", International Journal of Computer Science and Network Security, 2006, vol. 6, no. 5B, pp.138-186.

Payne, B. D. and Edwards, W. K. “A brief introduction to usable security”, IEEE Internet Computing, vol.12, no. 3, pp. 13-21, 2008.

Sasse, M. and Flechais, I. “Usable security: What is it? how do we get it?” In: Cranor, L. F., Garfinkel, S. (Eds.), Security and Usability: Designing Secure Systems that People can Use. O'Reilly Books, pp. 13-30, 2005.

Shay, R. “Designing password policies for strength and usability”, Journal ACM Transactions on Information and System Security (TISSEC), vol. 18, no. 4, May 2016, Article No. 13.

Sheng, S., Broderick, L., Koranda, C.A. and Hyland, J.J. “Why johnny still can’t encrypt: evaluating the usability of email encryption software”, In Symposium On Usable Privacy and Security, 2006, pp. 3-4

Solms, B. von and Marais, E. “From secure wired networks to secure wireless networks – what are the extra risks?”, Computers & Security, 2004, vol. 23, no. 8, pp.633-637.

Stavrou, E., “A situation-aware user interface to assess users’ ability to construct strong passwords A conceptual architecture”, 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 19-20 June 2017, UK.

Vanhoef, M. and Piessen, F. “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, ACM Conference on Computer and Communications Security (CCS), 2017

Waliullah, M., Moniruzzaman, A.B.M. and Rahman, M.S. “An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network”, International Journal of Future Generation Communication and Networking, 2015, 8(1), pp.9-18.

Whalen, T. and Inkpen, K.M., “Gathering evidence: use of visual security cues in web browsers”. Proc. of Graphics Interface 2005 (pp. 137-144). Canadian Human Computer Communications Society.

Zou, Y., Wang, X. and Hanzo, L. “A survey on wireless security: technical challenges, recent advances and future trends”, 2015. arXiv preprint arXiv:1505.07919.

KEY TERMS

- Transparent security – The implemented security is not visible to the end-users.
- Transparent password policy – A password policy that is not visible to the end user.
- Password cracking – A process to evaluate if a password can be recovered.
- Usable security – Solutions that assist users to perform their tasks securely, in an effective and efficient manner.
- End-user cyber situational awareness – The perception of the end-user with regards to a cybersecurity issue.

BIOGRAPHICAL NOTES

Alberto Bullo obtained his MSc degree in Computing in 2016, from the University of Central Lancashire Cyprus. Before that, he received his Bachelor degree in Communication and Internet studies in 2012, from Cyprus University of Technology. His research interests include computer security and gamification.

Eliana Stavrou is a Lecturer in the Computing Department of the University of Central Lancashire, Cyprus, and leads the MSc Cybersecurity programme. She is also the founder and director of the Applied Cybersecurity Research Lab. Her research interests include situational awareness, security in the IoT, intrusion recovery, cyber threat profiling and cyber security capabilities development. She has published a number of scientific papers at premier international journals and conferences and has participated in EU and national funded projects in the area of cyber security.

Stavros Stavrou is an Assoc. Professor in the Faculty of Pure and Applied Sciences of the Open University of Cyprus. He is currently the Dean of Faculty and leads the Telecommunication Systems Research Lab he founded in 2009. His research interests span through different cross layer topics in Communication Networks and Telecommunication systems. Topics include the design of optimum and secure networks for 5G, IoT and smart cities, and wireless user localization aspects. He has published extensively in the above areas, and has participated in over 25 successful EU and national research proposals, targeting mainly research councils and industry. He is a fellow of the Higher Education Academy (U.K.) and an appointed member of the executive academic board of the European Defence and Security College.

REFERENCE

Reference to this paper should be made as follows: Bullo, A., Stavrou, E. & Stavrou, S. (2017). Transparent password policies: A case study of investigating end-user situational awareness. *International Journal on Cyber Situational Awareness*, Vol. 2, No. 1, pp85-99.