Cryptographic Dysfunctionality-A Survey on User Perceptions of Digital Certificates

Dimitrios Zissis, Dimitrios Lekkas, and Panayiotis Koutsabasis

Department of Product and Systems Design Engineering,
University of the Aegean, Syros Greece
{Dzissis,Dlek,Kgp}@aegean.gr

Abstract. In this paper we identify and define cryptographic dysfunctionality and within this context we perform a study to evaluate user perceptions of public key cryptography concepts. The study makes use of user testing, questionnaires and wrap-up interviews with 121 young, but experienced Internet users during their interactions with selected secure Internet locations. The results show that the vast majority of users are not familiar with fundamental concepts of cryptography, and that they are not capable of efficiently managing digital certificates. This case study serves as first evidence supporting our hypothesis that user interface design is deteriorating cryptographic solutions effectiveness due to usability issues.

Keywords: Public Key Infrastructure, Usability, Security, Digital Certificates.

1 Introduction

In recent years, we have witnessed an explosion in the adoption of social media websites, electronic commerce, electronic banking and cloud solutions. As the popularity of these tools is increasing, stakes are now higher than ever in the field of information and communication security, as profits to be made from scams, extortion, online theft, identity theft have risen analogously. Malware is rapidly on the rise and becoming even more sophisticated. The percentage of computers infected with banking Trojans and password stealers has risen to 17% in 2010 while experiments are now showing a success rate of over 70% for phishing attacks on social networks [1]. While emails containing links to malicious sites continue to increase as a major means of leading new victims to attack sites, sophisticated phishing attacks are now poisoning search engine results with hyperlinks to web pages hosting numerous security risks.

In 2010 we witnessed the most sophisticated malware attack to date, the STUXNET worm [2][3]. STUXNET appeared to target highly sensitive Supervisory Control And Data Acquisition *(*SCADA) systems, which monitor and control industrial, infrastructure or facility-based processes, and was remarkable for the sophistication of its code and the amount of work involved in its creation. The STUXNET attack, constituted a serious attack on the notion of “trusted software” in information systems [2].

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 80–87, 2012.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

Trust is not a new research topic in computer science. The notion of trust in an organization could be defined as the customer's certainty that the organization is capable of providing the required services accurately and infallibly. A certainty which also expresses the customer's faith in its moral integrity, in the soundness of its operation, in the effectiveness of its security mechanisms, in its expertise and in its abidance by all regulations and laws, while at the same time, it also contains the acknowledgment of a minimum risk factor, by the relying party[4]. This trust is represented in the digital world using Digital certificates which are realized by Public Key Cryptography. Digital Certificates are used to establish secure connections to servers, authorize and authenticate users, but also validate software source code origins and guarantee its integrity. A digital certificate presented to an end user, published by a trusted Certification authority, can be defined as the conceptual delegation of this trust from the certificate issuer to the certificate owner. This exact trust was exploited by the STUXNET worm. In addition to exploiting four zero-day vulnerabilities, STUXNET used two valid digital certificates for source code signing, giving it credibility and trusted privileges, thus helping keep the malware undetected for quite a long period of time [3]. These sophisticated attacks, open Pandora's box for information system security as they put in doubt the effectiveness of one of the pillars upon which security in the digital world is built, cryptography and digital signatures.

2 Digital Signatures and Certificates

In 1976, Diffie and Hellman published a pivotal paper in the field of cryptography [5], which introduced a number of pioneer ideas in cryptography, including Public Key Encryption , Digital Signatures, One way functions and Trapdoor functions; the need to preserve the availability, integrity, authenticity and confidentiality of exchanged data and communications had already been identified. Digital signatures and Public key certificates have been perceived as an effective and efficient solution for achieving secure communications and transactions. Public Key cryptography currently realizes the concept of digital signatures; it provides a practical, elegant mechanism for symmetric key agreement. At present numerous Internet Protocols (SSL/TLS, IPsec/IKE, SSH, DNSsec, etc) employ digital certificates and thus public key cryptography to secure online transactions. For years scholars, experts and implementors throughout academia and industry have scrutinized the underlying mathematics and algorithms that enable cryptographic applications. Paradoxically though, 30 years after their inception and in contrast to the rise of information system threats, cryptographic applications have never met with wide public awareness. Even though the usage of PKI's in closed and controlled business environments is quite common, interoperability and usability problems arise when shifting to a broader, open environment [6].

A devastating majority of Internet users, either business or social, seem to lack the basic ability, knowledge or even willingness to effectively use cryptographic applications, in a way that can successfully deter imminent threats. A PKI system trusts

its users to validate each other's certificates and effectively protect their private keys. PKI strength can be summarized down to specific end user trust judgments regarding the trustworthiness of certificate issuers and ultimately certificate holders. As no automated mechanism for evaluating and managing the trust relationships exists, to make an effective trust judgment about the validity of a specific public key certificate, an end user is required to evaluate an extensive list of critical parameters, certificate repositories and cross certified authorities[7]. The complexity of this task, dawns on user friendliness and overall usability. When users fail to manage their private keys securely or when they fail to validate each other's public keys rigorously, then authenticity and privacy guarantees weaken and overall security deteriorates. Security software is only defined as usable if the people who are expected to use it [8]:

- are reliably made aware of the security tasks they need to perform;
- are able to figure out how to successfully perform those tasks;
- don't make dangerous errors;
- are sufficiently comfortable with the interface to continue using it.

To achieve secure and authenticated communications, a web server presents its own digital certificate to an end-user in order to prove its identity and to facilitate the establishment of a secure end-to-end session. The end-user is required to:

- Validate the subject on the digital certificate. In this case the subject of the certificate is a domain name, which must match the domain currently visited.
- Validate the signed content of the digital certificate. Typically, the hash value of the certificate's content is signed and the signature is included in the certificate.
- Validate the trustworthiness of the certification path, up to a trusted certification authority
- Check the validity period of the digital certificate (effective and expiration dates)
- Check if the certificate has been revoked
- If executable signed software is implicated, validate the signature of the source code

The above steps are by default performed by the web browser of the end-user and thus it is presumed that the end-user trusts the web-browser program and expects to be properly notified if any of these steps fail. Often these validations require the end user to participate effectively in the process, as is the case if the certification publisher is not pre included in the browsers root certificate repository; thus unknown to the browser or a check fails. At this point overall security is as strong as the end user trust decision. For the user to effectively participate in this process, and for security to adhere to the above definition of usable security, the user is required to have the necessary knowledge and understanding, to evaluate a list of critical parameters, certificate repositories and cross certified authorities. Hence the problem. Realistically only sophisticated users can be expected to meet fully the demands of PKI. Users are unable to effectively make decisions regarding digital certificates in daily transactions due to the lack of informativeness of the user interface and usability issues. Cryptography in its essential form appears to be greatly dysfunctional in every day environments, not due to the inherent complexity of the underlying mathematics, but

due to the intricacy of the application interface, lack of informativeness and risk acknowledgment on a user side.

The severity of this vulnerability is critical, as a growing number of sophisticated malware attacks are exploiting end users inability to effectively validate digital certificates. Besides STUXNET, the Zeus Trojan exploited this same vulnerability to steal banking information. Zeus during installation exhibited an expired certificate belonging to Kaspersky's Zbot product, which was designed to remove Zeus [9]. Although this certificate was expired, and contained a different hash value, a plethora of users accepted it as trusted, thus enabling its propagation. Another version of malware exhibited a digital certificate claiming to be published by a trusted CA Avira [10]. When taking a closer look, Microsoft Windows shows a note "A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider". This message simply means that the certificate has not been created by Avira.

Within this context we define cryptographic dysfunctionality. At present, we identify the problematic dimension of PKI as being a usability and user interface design problem. During application usage, a detachment seems to occur between the application interface, informativeness and operation, which ultimately leads to user exclusion. In this exclusion cryptographic dysfunctionality has its deepest roots.

3 A Study on User Perceptions of Digital Certificates

We identify and define cryptographic dysfunctionality and within this context we perform an investigation, using questionnaires, to evaluate user understanding of cryptographic applications, application informativeness, user friendliness and usability. The results shed light on several aspects of these applications that deter cryptographic functionality in every day transactions. Our case study serves as a test of our hypothesis that user interface design is deteriorating cryptographic solutions effectiveness due to usability issues.

3.1 Goal, Method and Participants

This study's goal was to investigate the extent to which Internet users can (a) understand the most essential concepts of digital certificates, and (b) manage digital certificates effectively during their interactions with a number of selected and familiar web sites. The methods selected for this survey included user testing, questionnaires and wrap-up interviews with students of the department of Product and Systems Design Engineering at the University of the Aegean, Greece. It needs to be noted that all students of the department make daily use of computers for their studies, in various ways, including using email to communicate with academic and administrative staff and using an asynchronous e-learning platform to access electronic content for most of their courses. All participants can be defined as experienced Internet users, if we take into account that they make daily use of the Internet. A total number of 121 users participated in this survey. Users were recruited by an e-mail invitation.

The user testing phase of the study required users to connect to the academic e-mail server and access their accounts using the Mozilla Firefox, Internet Explorer and Opera web browsers, in a step-by-step process. To connect to the server, users were required to establish a secure SSL connection with a server exhibiting a valid digital certificate, which is not included in the Trusted Certification Authority Repository. This process required from the users to bypass the browser warning message to establish a secure connection, and in doing this add the CA to the Trusted Repository. For this, users should review the certificate critical parameters. For each step of the process users were asked about basic aspects of digital certificates and filled in the questionnaire (the questionnaire was available electronically via Google docs). This simple user testing process was followed in order to help users concentrate on the task of establishing an SSL connection, and to allow for a brief search of the issues that they would be enquired about in the questionnaire. At the end of the process, we conducted a number of wrap-up interviews with a selected set of users on the basis of their answers in order to provide some clarifications and interpretations.

The questionnaire comprised of a total of 20 (twenty) questions: the first four (4) were demographic, and the other 16 (sixteen) were about basic concepts of digital certificates and certificate management issues. For three (3) of these questions, users were told where to look for answers: they were also provided with screenshots of browser messages and they were asked whether they could understand their content and purpose.

3.2 Results

A total number of 121 participants took part in this survey; they were all between 18-23 years of age: 18y: 51 users (42%), 19y: 31 users (26%), 20y: 18 (15%), 21y: 7 (6%), 22y: 9 (7%), 23y:5 (4%). All participants are of young age and have considerable experience with using the Internet: 83 users (69%) reported that they have been using the Internet for more than 5 years, 15 users (12%) for more than 10, and 23 users (19%) for less than 5 years. The vast majority of participants make daily use of the Internet (102 (84%), while a total of 81 users (67%) have performed some kind of an electronic transaction, concerning e-commerce (49 users (41%)), e-banking (9 users (7%)), e-government (5 users (4%)) and other (18 users (15%)).

Obviously, users with the above demographic and Internet usage data should be at least aware of basic concepts regarding digital certificates, if not capable of understanding related complex concepts, able to efficiently manage certificates and establish secure connections. User responses raise serious concerns on the effectiveness of many security implementations used in online transactions and shed light on the true nature of the problem. We shall go through the most important answers received and attempt to provide an unbiased interpretation of these.

Users were asked if they have ever established a secure connection to an Internet website in order to protect their online information exchange (Fig. 1). Although 90% of participants had previously stated that they regularly make use of e-commerce and e-banking websites (meaning that they often establish SSL connections), a striking 67 users responded ‘no’ (56%), 39 users responded ‘not sure’ (32%), while a poor 12%

answered 'yes'. This answer was a first contradiction to the aforementioned participants' experience of Internet usage, and it is largely due to the fact that the secure connection is quite seamless from the user point of view. However, it need to be noted that even their specific and repeated interaction experience with their web e-mail accounts (during which they are prompted to connect to a 'potentially unsecure location', according to Firefox terminology) has not proved informative enough for the vast majority of users to realize that they are actually establishing secure connections every time they accessed their web e-mail account.

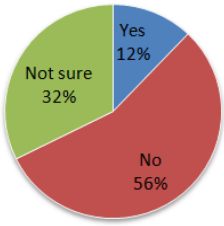

Fig. 1. Have you ever established a secure connection?

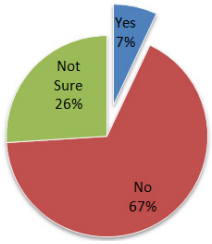

Fig. 2. Do you understand what a digital signature is?

An even more surprising set of answers was provided for the following question: "When you connect to a safe Internet location the URL changes to https. Do you understand what this means/does?" The vast majority of users (88%) lack any understanding of the concept of https (66%: 'no'; 22%: 'not sure').

Following this, users were enquired about their basic understanding of digital signatures and their ability to manage these (import, export and delete them), as this is one of the basics tasks users are required to perform in a secure PKI environment. A total of 93% (Fig. 2) responded that they "do not know or understand what a digital certificate is" (67%: 'no', 26%: 'not sure'). In the following question, answers revealed that an 85% of all respondents lacked the necessary knowledge to effectively manage digital signatures, this includes deleting a comprised Certification Authority from the trusted rooted certificate repository. When enquired about their understanding of SSL, 93% responded that they were unable to understand this, 3%: were 'not sure', and a small 4% responded 'yes'. These answers reveal that there is an astonishing majority of young experienced Internet users that are not aware of the most basic terms and concepts of secure online transactions.

Alarmingly when users were asked if they had ever viewed a digital certificate to validate it, only 2 % responded positively [2 responded positively (2%); 111 responded negatively (91%) and 8 responded not sure (7%)] (Fig. 3). As a PKI strength can be summarized down to specific end user trust judgments, regarding the trustworthiness of certificate issuers, after reviewing the validity of a specific public key certificate, an extensive list of critical parameters, certificate repositories and cross certified authorities, an end-user inability to participate effectively diminishes the solutions overall effectiveness. What is even more striking is that a total 60% of users, responded that they were able to bypass the browser warning message and

accept the digital certificate, thus visiting the website that had previously been deemed "unsecure" [32 users responded that they were able to bypass the message (26%), 41 that they believed they knew how to (34%) and 48 that they were unable to (40%)]. This was done without reviewing the certificate parameters.

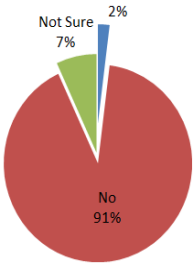

Fig. 3. Have you ever reviewed/validated a digital certificate?

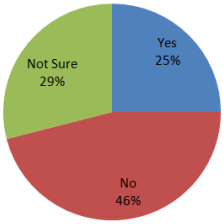

Fig. 4. Do you know how to bypass such a warning message?

At this point we can state that the data clearly points towards users being unable to effectively perform in this situation. These questions were made while users were required to interact with the web site and check out related Firefox messages and pages. However, a very small number of users responded satisfactorily, which certainly rings a bell. Despite the fact that there has been over a decade since the first studies on the usability of cryptographic user interfaces (with most influential that of Whytten & Tygar [8]), it seems that current web-based user interfaces are still not 'passing the message' to online users.

In the following questions we enquired about users understanding of the messages presented to them when visiting a web server exhibiting a certificate issued by a RootCA not included in the Trusted Certificate Repository. A user's knowledgeful participation in this process is vital, as if a user accepts a certificate from an untrusted publisher, the user could be a victim of a plethora of malicious attacks, including password and information stealing, enabling malicious code execution etc. When visiting a website that exhibits a certificate not trusted by the Firefox browser, a message is presented to warn the user, such the following one, "This Connection is Untrusted- You have asked Firefox to connect securely to (domain name), but we can't confirm that your connection is secure". On many occasions trustworthy websites use certificates that are not included in the Trusted Root Certificate Repository. When enquired about this only 16% responded to understanding the nature of such a message.

Following this users were asked if they understood the message "The certificate is not trusted because the issuer certificate is not trusted". An overall of 93% does not seem to understand the nature of such a message (7% responded yes, 63% Responded No, 30% responded not sure). When users were asked if they understood what "This certificate is untrusted because it is self-signed" means, only 3% appears to understand. While most users do not understand the nature of these messages 60% knows how to override such a message and visit an untrusted site.

Acknowledging the issue the Extended Validation Certificates have been issued. EV Certificates use color-coding of the Web browser's address bar to signal secure connections. The browser navigation window turns green to indicate an authentically validated site with an EV Certificate, full security, and encryption in place, and turns red when it encounters an untrustworthy site. When enquired about these, only 39% responded to have ever noticed the coloring [47 responded had noticed the coloring (39%), 63 had not (52%) and 11 were not sure (9%)], while a total of 98% had no idea as to what the purpose of this coloring was [3 responded positively (2%), 106 negatively(88%) and 12 were unsure(10%)].

4 Summary and Conclusion

Overall, the collected data indicates that users are unable to effectively complete specific tasks that are required from an end-user to establish secure communications in the context of PKI environments. In view of these tasks, while users are required to validate the domain name, expiration date on the digital certificate or check if a certificate has been revoked, 98% of responders (from a group that is considered above average) have never viewed a digital certificate or are not sure how to view one. Even in the case that one of these checks fails, 92% of responders does not know how to manage (delete) certificates. While users are required to validate the trustworthiness of the certification authority, 93% of responders do not understand what a certification authority is but most dangerously 54% does know how to get past a warning security message and add an exception to a specific certificate. The exponential rise of risks in the digital world demands a redesign of applications interface that manage, use and interact with digital certificates, as the problematic dimension in a PKI environment, appears to be a usability problem.

References

1. APWG: Phishing Activity Trends Report 2nd Quarter 2010 (2010)
2. Matrosov, A., Rodionov, E., Harley, D., Malcho, J.: Stuxnet Under the Microscope. ESET Technical Report (2011)
3. Kaspersky Lab: Kaspersky Lab provides its insights on Stuxnet worm. Kaspersky Lab Technical Repost (2010), http://www.kaspersky.com/news?id=207576183
4. Lekkas, D.: Establishing and managing trust within the Public Key Infrastructure. Computer Communications 26(16), 1815–1825 (2003)
5. Diffie, W., Hellman, M.E.: New Directions in Cryptography. IEEE Trans. on Info. Theory IT-22, 644–654 (1976)
6. Massimiliano, P., Smith, S.: Finding the PKI needles in the Internet haystack. Journal of Computer Security 18(3) (2010); The 2007 European PKI Workshop: Theory and Practice (EuroPKI 2007)
7. Davis, D.: Compliance Defects in Public-Key Cryptography. In: Proc. 6th Usenix Security Symp., San Jose, CA, pp. 171–178 (1996)
8. Whitten, A., Tygar, D.: Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, pp. 169–183 (1999)
9. Kirk, J.: Zeus malware used pilfered digital certificate. In: Computer World (2010)
10. Wegele, T.: Malware signed with fake Avira Certificate. Computer Security News & Articles (2011)