Increasing Usability of TLS Certificate Generation Process Using Secure Design

Giorgi Iashvili[a], Maksim Iavich[a], Avtandil Gagnidze[b] and Sergiy Gnatyuk[c]

[a]*School of technology Caucasus University Tbilisi, Georgia,*
[b]*Business and engineerig faculty East European University Tbilisi, Georgia*
[c]*IT-Security Academic Dept. National Aviation University Kiev, Ukraine*

Abstract

Based on the researches, usually users are not familiar with different security mechanisms of the systems and do not understand how to use them in everyday life. Special research field analyzing user behavior in the technological systems and in computer security world is called human computer interaction (HCI), is also known as usable security. TLS or Transport Layer Security is one of the most commonly used secure protocols today. It is used to protect data that travels between client and server using HTTPS. Data protection is critical issue, especially when users are sending sensitive information. TLS uses cryptographic algorithms to protect data transmitted via HTTPS protocol. In this paper we will offer balanced and more user-friendly generation process of one of the most frequently used security mechanism on websites Transport Layer Security (TLS) certificate for establishing HTTPS connection between client and server. Our system will check all the requirements of the website and its services to make users run more balanced systems. If system will found another approach with better value based on user requirements, client will be informed in understandable and easy to read form. As a result, user will get the best option for both security and usability sides in shortest period of time

Keywords

TLS, encryption, user, usability, user security

1. Introduction

Secure communication is one of the most important factors in digital world today. Every day users of internet are sending and receiving a huge amount of data, the information transmitted through the special channels also known as protocols. With the grow of internet and networking systems, users tend to share data increasingly over communication channels. Nowadays there are many different data transfer protocols for different purposes. For better security level communication between client (internet browser) and server must be performed through encrypted protocol – Hypertext Transfer Protocol Secure (HTTPS).

In most cases users of the systems are not paying enough attention to their security. Based on the researches, usually users are not familiar with different security mechanisms of the systems and do not understand how to use them in everyday life [1, 2]. This fact significantly reduces security level of the users in different systems, especially of websites or different web-based multi user systems. Stilling personal information, data breaches, phishing and different social engineering methods, all these user-oriented attacks are very popular today because of not enough knowledge of the users. This fact is also caused by problems of usability of some security mechanism. Users cannot understand why and how to use these security models in practice.

In this paper, we will offer balanced and more user-friendly generation process of one of the most frequently used security mechanism on websites Transport Layer Security (TLS) certificate for establishing HTTPS connection between client and server. This approach will increase usage of TLS certificates by website owners, consequently the level of user security on such websites will also be improved.

2. Security Agains Usability

2.1. Understanding User in the System

Serious researches were performed to make user-oriented system more comfortable and understandable for people. The aim of such studies is to increase security level of the users in different systems [3]. Special research field analyzing user behavior in the technological systems and in computer security world is called human computer interaction (HCI), is also known as usable security. The studies in this direction are oriented on user understanding of different systems, the

IVUS 2020: Information Society and University Studies, 23 April 2020, KTU Santaka Valley, Kaunas, Lithuania

kulyabov-ds@rudn.ru (G. Iashvili); kulyabov-ds@rudn.ru (M. Iavich); kulyabov-ds@rudn.ru (A. Gagnidze); kulyabov-ds@rudn.ru (S. Gnatyuk)

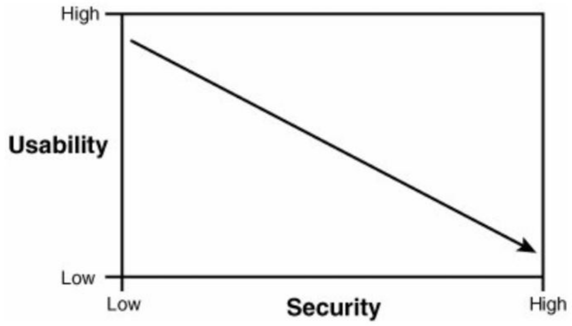


Figure 1: Balance Between Security and Usability

most important part of HCI is to learn user preferences, abilities and limitations using technologies. Based on this data friendlier and more understandable user security mechanisms can be implemented to the different web-based multi user systems or websites [4].

There are different parameters to measure usability of the system:

- Speed – is a way of measuring how quickly a user can accomplish the task.
- Efficiency – measures how many mistakes are made in accomplishing the task.
- Learnability – measures how fast user can learn the working process of the system.
- Memorability – how memorable the system is for the user. User feedbacks – based on user feedbacks we can understand weak points and not usable segments of our system.

Better level of usability of the system means more comfortable work for the users. This approach obviously will have great positive impact on multi-user systems security level.

But as we can see on Figure. 1 , that too much of usability in the system might have negative impact on security level. Important factor in this process is to find the balance between security and usability. System must have strong security mechanism, but users must feel comfortable working with it.

2.2. Less Usable Security Mechanism

Some of security mechanisms implemented to different multi-user systems today from point of view of usability are not efficient enough. Together with high level of security, usually such mechanisms are complex and hard to understand for average users of the system. The best method of implementation of complex security mechanisms is background processing. In this case user has interaction only with needed part of the system and all security processes are running behind the scene. But if user must take a part in security process of the system – usability becomes a key factor for ensuring relevant security level [5]. Example of it is visiting unsecure website and transmitting data through Hypertext Transfer Protocol (HTTP). In this case data is sent as plaintext, which makes the process of sniffing attack much easier. User itself must make a decision for transmitting personal data through insecure website. If user has no enough technical knowledge it can cause serious security problems. To improve the security of website users more user-friendly security mechanisms must be offered.

3. Need of Transport Layer Security

TLS or Transport Layer Security is one of the most commonly used secure protocols today. It is used to protect data that travels between client and server using HTTPS. TLS is also might be used to protect email or host of the other protocols. TLS is also known as SSL or Secure Socket Layer which is an old version of TLS. Data protection is critical issue, especially when users are sending sensitive information. TLS uses cryptographic algorithms to protect data transmitted via HTTPS protocol [6]. TLS certificate provides user with the following components:

- Authentication – during the visit of the website client gets a copy of TLS certificate from the server. It happens to ensure that web browser is connected to right website. Data in TLS certificate includes the name of domain and company information.
- Integrity – transport layer security ensures the integrity of data. Which means that data must not modified during transition. With strong cryptographic algorithms the hacker is not able to change the content. The information is confirmed through special Message Authentication Code (MAC) also known as tag.
- Confidentiality – data confidentiality prevents information from being leaked. It must be very difficult to intercept encrypted information for the hacker.

4. Types of TLS Certificates

In order to get Transport Layer Security for the website, user must choose the correct type of TLS certificate [7, 8]. There are different types of certificates, which must be chosen based on category of the website. Most widely used representatives of TLS certificates are: General purpose TLS certificates – the certificates used for small and medium business websites; Extended Validation (EV) TLS Certificates – used for bigger organizations and needs special documentation audit of the website and company; Multi-Domain EV TLS Certificates – one certificate can be used for multiple website domain names; Wildcard TLS Certificates – is used for subdomains of the website; Personal Authentication/Email Certificates – used for personal or email clients encryption. Each certificate has its purpose and special features, which vary depending on type, industry and globalization of the website. The website owners must understand which type of TLS certificate should be used in particular case.

4.1. Free and Paid Certificates

Some of the hosting providers offering free versions of TLS certificates. The main difference between paid and free TLS certificates is, that free could be only General purpose certificates also known as Domain Validation certificates (DV) without any support from CA. Another difference between free and paid certificates is validity of TLS. Free certificates usually are issued for 30 – 90 days and the owner of the website must re-generate them manually. But in some cases hosting provides users with auto re-generation service for TLS certificates. Validity period for paid TLS certificates usually is 1-2 years.

4.2. Trusted Certificate Authorities

Together with the type important factor to take into account is issuer of certificate. TLS certificates today are issued by different trusted organizations called Certification Authorities (CA). Biggest Certification Authorities are Comodo, Symantec, GoDaddy, DigiCert, Trustwave. Technically certificates issued by different authorities are similar and using the same security mechanisms during client-server protected communication. The only difference is in support and index of trust. Every modern web browser has special certificate authority built-in database. Once client wants to establish connection with the server, browser checks the authority of TLS certificate installed on concrete website by comparing it to the names in the list.

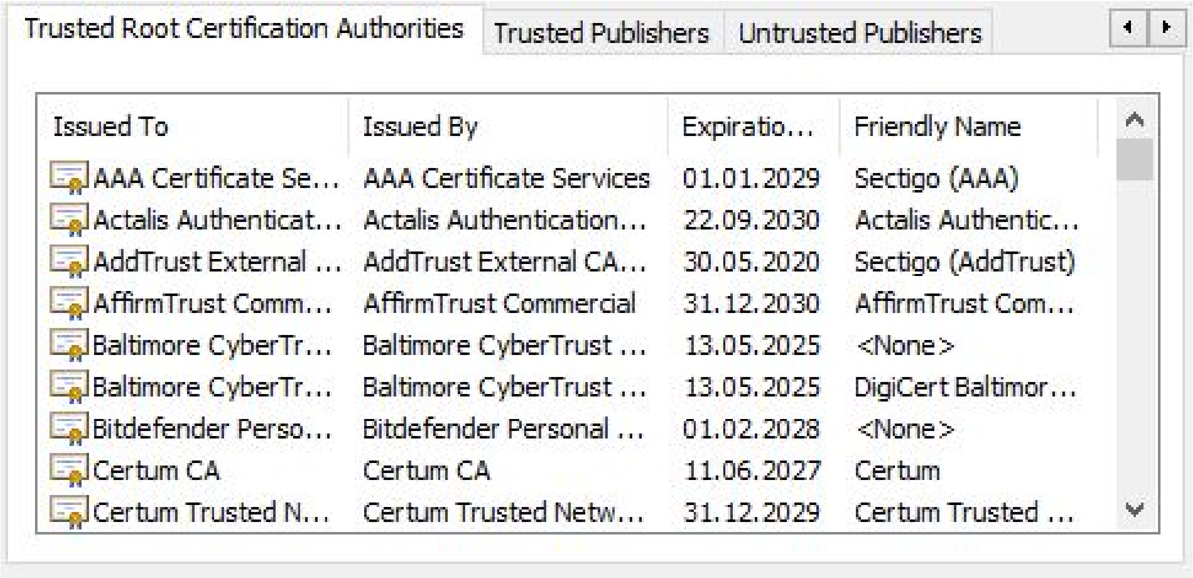
Figure 2 demonstrates the list of Trusted Root Certification Authorities in Google Chrome web browser. Together with issuer TLS certificate has two more important parameters. Issued to, which means the domain name this certificate was issued for and validation. This last parameter holds information about generation date and validity of the certificate. Outdated TLS certificate will not work on the website.

5. TLS Certificates Generation Process

All types of Transport Layer Security certificates must be installed and well configured on server side. Usually clients are using default settings to configure TLS certificates, which is normal for beginners. After more detailed research we can say, that in some cases clients are using default settings during TLS certificate generation because they have no enough understanding of what is really happening and why it must be done. In Transport Layer Security certificate technology both symmetric and asymmetric cryptography are used.

Asymmetric cryptography is used every time when client is establishing connection with server. RSA cryptographic algorithm is used at the first stage. Once connection is established and special key called session key is transmitted, symmetric cryptography begins the work. In working process of TLS hybrid encryption methods are used, and it is because of two main reasons - security and efficiency. Asymmetric cryptography is more secure due to public key encryption mechanism, but this method has lower speed. To ensure higher speed, on the second stage, when session key is already transmitted, TLS security mechanism uses symmetric cryptography. Instead of using heavy asymmetric cryptography for transmitting data, it is used only once during establishing connection between client and server. It is done to provide secure transmission of session key. User of the website can check the data of TLS certificate used on the website including the information about public key length and used algorithm [9].

On figure 3 we can see that website uses RSA encryption algorithm and length of public key is 2048 Bits, which is standard based on National Institute of Standards and Technology (NIST) recommendations. Some hosting companies with free certificates included services provide management system to configure TLS manually. Hetzner Online GmbH is hosting provider with different data centers located in Germany. For some packages they offer free TLS certificate gener-



Issued To	Issued By	Expiratio...	Friendly Name
AAA Certificate Se...	AAA Certificate Services	01.01.2029	Sectigo (AAA)
Actalis Authenticat...	Actalis Authentication...	22.09.2030	Actalis Authentic...
AddTrust External ...	AddTrust External CA...	30.05.2020	Sectigo (AddTrust)
AffirmTrust Comm...	AffirmTrust Commercial	31.12.2030	AffirmTrust Com...
Baltimore CyberTr...	Baltimore CyberTrust ...	13.05.2025	<None>
Baltimore CyberTr...	Baltimore CyberTrust ...	13.05.2025	DigiCert Baltimor...
Bitdefender Perso...	Bitdefender Personal ...	01.02.2028	<None>
Certum CA	Certum CA	11.06.2027	Certum
Certum Trusted N...	Certum Trusted Netw...	31.12.2029	Certum Trusted ...

Figure 2: List of Trusted Authorities in Browser

ation models right inside the managing panel of the hosting. Users can manually generate and use certificates provided by Let's Encrypt Authority X3. Transport Layer Security certificate generation process for such certificates has two stages – issue procedure and DNS validation processes. On the first stage to run certificate generation process user must define the following: Domain name; DNS validation; TLS certificate name; Common names; Key length; Such certificates support Domain Name Service (DNS) based validation, which is requires special TXT records in configuration of the hosting. Once information is entered, TLS certificate obtaining procedure is starting.

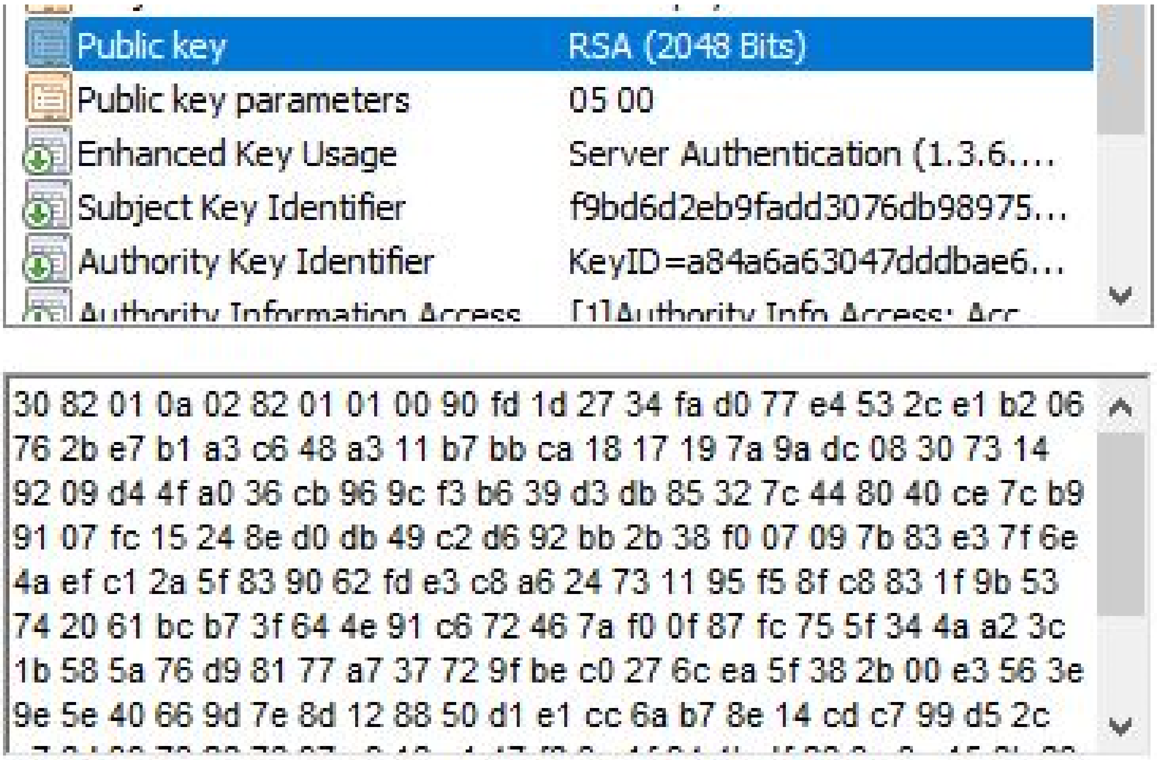
The system automatically generates self-signed certificate with parameters entered by user during first stage. Every five minutes the system is trying to get the certificate. Once the certificate is obtained self-signed certificate becomes Let's Encrypt certificate instead and the website is ready to establish secure connection trough HTTPS protocol.

5.1. Usability Problems for The Client

Sometimes Transport Layer Security (TLS) certificates generation process is done by the owners of the websites. Wrong configuration of certificate can have negative impact on security and efficiency of the website. User must know each parameter of certificate which will be used for generation process. We think that more efficient way of generating TLS certificate for the website is to make user act based on concrete scenario. If the website is used only for informational purposes we need one balanced security mechanism, but if website holds different sensitive information, like user personal data, it is completely different situation and in this case security level must be increased [10]. We already know that with growth of security level, the usability of the system inevitably decreases. Some user-friendly TLS certificate generation mechanisms are offered but they still have problems with efficiency. From example of Let's Encrypt TLS certificates generation process provided by Hetzner Online GmbH we can learn, that main parameters of certificate configuration must be set by user, which could lead to a problem of security on the website, especially if the website is built as online commerce or data exchange platform, where users are sending and receiving personal data.

5.2. Security Problems

While user has problems with understanding of security mechanisms he will try to not use complicated systems despite their importance. Most security problems in multi user systems are coming from lack of client knowledge. Well- formed and easy to use security mechanisms will solve a lot of cyber security problems and will help to avoid different user-oriented attacks in real life [11].



Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Key Identifier	f9bd6d2eb9fadd3076db98975...
Authority Key Identifier	KeyID=a84a6a63047dddbae6...
Authority Information Access	[1]Authority Info Access: Acc

```
30 82 01 0a 02 82 01 01 00 90 fd 1d 27 34 fa d0 77 e4 53 2c e1 b2 06
76 2b e7 b1 a3 c6 48 a3 11 b7 bb ca 18 17 19 7a 9a dc 08 30 73 14
92 09 d4 4f a0 36 cb 96 9c f3 b6 39 d3 db 85 32 7c 44 80 40 ce 7c b9
91 07 fc 15 24 8e d0 db 49 c2 d6 92 bb 2b 38 f0 07 09 7b 83 e3 7f 6e
4a ef c1 2a 5f 83 90 62 fd e3 c8 a6 24 73 11 95 f5 8f c8 83 1f 9b 53
74 20 61 bc b7 3f 64 4e 91 c6 72 46 7a f0 0f 87 fc 75 5f 34 4a a2 3c
1b 58 5a 76 d9 81 77 a7 37 72 9f be c0 27 6c ea 5f 38 2b 00 e3 56 3e
9e 5e 40 66 9d 7e 8d 12 88 50 d1 e1 cc 6a b7 8e 14 cd c7 99 d5 2c
```

Figure 3: Information About TLS Certificate on Website

6. Secure Design Methods Implemetation

Based on the researches in cyber security, the most efficient user-oriented security systems are built with high level of usability in mind. While security system is partly or fully managed by the human secure design concepts and methods will have great impact on entire security level of that system [12],[13]. Secure design is aimed on developing strong security mechanism with user-friendly and understandable interface and functionality. The design cycle consists of different stages of building the main structure:

- Requirements – defining the requirements for interaction with the system. Main direction, tasks and rules inside the system.
- Analysis – building the conceptual model of entire system based on research and practical analysis of the requirements.
- Design – main structure of the system, which is the most important part in human system interaction process. Must be considered different factors. Interface must correspond to use cases.
- Implementation – on this stage technical part of the system must be integrated. All security measures must be considered and different scenarios must be analyzed.

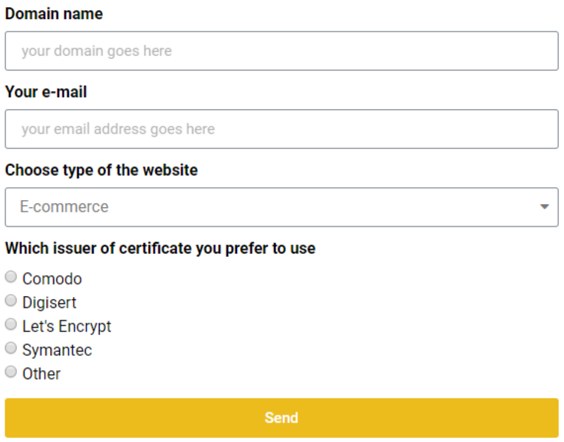
6.1. Increasing Usability With Secure Design Methods

Based on researches in secure design and cyber security mechanisms implementation techniques we created more usable Transport Security Layer (TLS) certificate generation method, which will help owners of different web-based systems make secure decision during certificate generation. As generation process of TLS certificate consist of different parameters, we included most commonly used types of the websites, certificate authorities and some user data to special web-based form. As we can see on figure 4, form has field for client email, type of the website based on industry, domain name and issuer or certificate authority. After submitting this simple data, system will automatically generate the best balanced option of generation certificate. Full instruction and details will send to email of the user in understandable and easy to read form.

6.2. System Automation Process

Firstly, the system will check information about the server from domain name provided by the user. For this process an open sources of information will be used. Based on information about services running on the server, system will generate the first part of recommendation for the user, which includes performance and information about optimized services running on the server of website. Afterwards the system will choose optimal length of the key for TLS certificate based on selected category of the website. If category of the website is related to financial operations or transmitting sensitive information like personal information of the users, conversations and file sharing – security level will be improved by increasing the length of generated key [14]. The next step is choosing of trusted certificate authority (CA). Prices and services of different CAs varies, usually it is based on customer service, support frequency and high trust index of different web browsers by default. If chosen by user CA meets all the requirements of concrete usage scenario, the system will approve it. But in the case when system can find more secure and usable way for the user, it will offer another option together with detailed explanation why suggest version of security and usability mechanisms combination and also selected certificate authority is better for this particular case. The system will check all the requirements of the website and its services to offer the best and balanced option. As a result, user will get the best option for both security and usability sides in shortest period of time. This approach must increase the level of usability of generation correct TLS certificate based on the needs of the user.

As the offered system is web-based, we are always working on improvements and making it more comfortable and easy to use. The main aim of such systems is to make end users and owners of different multi user web platforms understand importance of security mechanisms together with high level of usability. Because any usable system won't work without good security level behind it.



Domain name

your domain goes here

Your e-mail

your email address goes here

Choose type of the website

E-commerce

Which issuer of certificate you prefer to use

○ Comodo
○ Digisert
○ Let's Encrypt
○ Symantec
○ Other

Send

Figure 4: Web-Based Recommendational Form

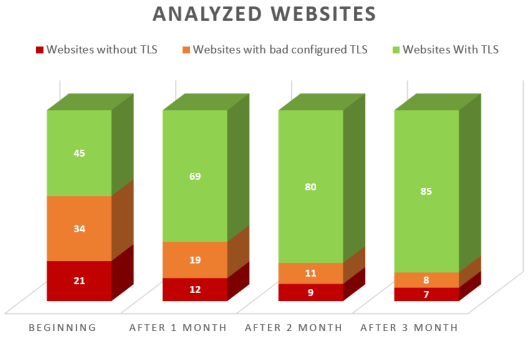


Figure 5: Configuration on Different Websites

7. Work of The System on Pratice

Only installation of TLS is not enough to make the website work securely. There are different factors to take into account while working with TLS certificate configuration. In some cases, users are getting errors on websites like mixed content. Which means that certificate is installed but not well-configured. Mixed content error occurs when the webpage is loaded over HTTPS protocol, but some other resources such scripts, graphics or another media are loaded over HTTP insecure protocol. It this case, both HTTP and HTTPS content is loaded at the same time. This situation might be problematic in the case of Man in the middle attack. During this attack hacker can eavesdrop on a network and make some modifications of the traffic.

In the frame of our research, we shared information about optimized TLS certificate generation mechanism with different organizations. In total information about the system being sent to owners of 100 websites of different industries like sport, news portals, personal blogs of organizations and informational websites. In the frame of our work we from 100 websites TLS certificates was installed and configured correctly only on 45 websites. On 34 websites certificates was not fully configured and on 21websites TLS was not installed at all. Figure 5 demonstrates the number of websites with installed TLS, installed but not well-configured TLS and without TLS at all. We collected data about certificates usage on web platforms and divided research process into different stages: beginning; after first, second and third month. As we can see on Figure 5 after getting information about TLS certificates installation and correct configuration, security of a lot of website in the frame of our research was increased.

8. Conclusions

Based on the work performed in the frame of our research we can say that well-chosen Transport Layer Security certificate has serious impact on security level of entire web-based application or website. So, correct configuration and type of certificate is extremely important for multiuser systems which are using web protocols. The offered system is developed to improve usability of certificate generation process, consequently the owners of web-based systems and websites can easily understand which configuration is needed for particular scenario. Based on recommendations of the system, web-based applications and websites owners can perform generation of needed security mechanism with better understanding. This fact will seriously increase the level of security of web-based applications and websites.

Acknowledgments

The work was conducted as a part of PHDF-19-519 and the grant financed by Caucasus University.

References

[1] D. Nicholson, Advances in human factors in cybersecurity, Proceedings of AHFE 2017 International Conference on Human Factors in Cybersecurity (2017).

[2] G. Lo Sciuto, S. Russo, C. Napoli, A cloud-based flexible solution for psychometric tests validation, administration and evaluation, in: CEUR Workshop Proceedings, volume 2468, 2019, pp. 16–21. URL: www.scopus.com, cited By :1.

[3] G. C. Cardarilli, L. Di Nunzio, R. Fazzolari, M. Re, Tdes cryptography algorithm acceleration using a reconfigurable functional unit, in: 2014 21st IEEE International Conference on Electronics, Circuits and Systems (ICECS), IEEE, 2014, pp. 419–422.

[4] Hci for cybersecurity, privacy and trust, 2020.

[5] S. Garfinkel, H. R. Lipford, Usable security: History, themes, and challenges, Synthesis Lectures on Information Security, Privacy, and Trust 5 (2014) 1–124.

[6] B. Rothke, Ssl and tls essentials: Securing the web, Security Management 44 (2000) 106–106.

[7] G. M. Farinella, C. Napoli, G. Nicotra, S. Riccobene, A context-driven privacy enforcement system for autonomous media capture devices, Multimedia Tools and Applications 78 (2019) 14091–14108.

[8] S. Battiato, G. M. Farinella, C. Napoli, G. Nicotra, S. Riccobene, Recognizing context for privacy preserving of first person vision image sequences, in: International conference on image analysis and processing, Springer, 2017, pp. 580–590.

[9] I. Ristic, Bulletproof ssl and tls: Understanding and deploying ssl, TLS and PKI to Secure Servers and Web Applications (2014).

[10] S. Mangard, A. Y. Poschmann, Constructive side-channel analysis and secure design, Lecture Notes in Computer Science 9064 (2015).

[11] A. Gagnidze, M. Iavich, G. Iashvili, Novel version of merkle cryptosystem, Bull. Georg. Natl. Acad. Sci 11 (2017).

[12] R. Baskerville, Information systems security design methods: implications for information systems development, ACM Computing Surveys (CSUR) 25 (1993) 375–414.

[13] E. B. Fernandez, A methodology for secure software design., Software Engineering Research and Practice (2004) 130–136.

[14] M. Iavich, A. Gagnidze, G. Iashvili, S. Gnatyuk, V. Vialkova, Lattice based merkle., IVUS (2019) 13–16.