Teaching Computer Security in a Secondary School

J. Mottl
Faculty of Science, University of Hradec Králové/Department of Applied Cybernetics,
Hradec Králové, Czech Republic
jan.mottl@uhk.cz

***Abstract* - The article focuses on computer security, especially on the teaching of this topic in secondary schools. From the broad topic of security, the article focuses mainly on authorization and authentication and the related tools used for these processes in web development. The main objective of the paper is to determine the extent of education on these topics in secondary schools. The paper provides an insight into the issue by means of a questionnaire survey conducted in a secondary vocational school with a focus on computer science. The results of this survey were compared with the results of the same questionnaire given to students of the Bachelor's degree programme in Applied Informatics at the Faculty of Informatics and Management at the University of Hradec Kralove. The paper summarizes the results of the analysis of these questionnaires and provides insight into the importance of teaching computer security in secondary schools.**

Keywords - computer security; authorization; authentication; secondary school

I. INTRODUCTION

Computer security is a very broad topic that has been addressed in many research papers. This paper focuses on teaching cyber security and provides insight into teaching this topic in a secondary school.

The paper also attempts to provide a basic theoretical insight into the topic, so the first chapter focuses on computer security itself, specifically the principles of authorization and authentication, as well as basic methods of data encryption. In addition, a preview of the basic tools used to secure websites is provided.

Subsequently, the paper discusses the teaching of these topics, and, in particular, the articles focused on the topic of security itself.

The main contribution is the practical part of the paper, which builds on the topic and provides insight into the current situation of teaching the topic at Delta High School in Pardubice, Czech Republic. The level of knowledge and familiarity with computer security tools was determined using a questionnaire survey conducted at the school. The paper compares the results with a smaller sample of students at a higher education institution, specifically the University of Hradec Kralove, Faculty of Informatics and Management.

II. THEORETICAL BASIS

Cybersecurity is a broad topic; this chapter is intended to provide a basic insight into the subject at a theoretical level so that it can be linked to education.

Security can be summarised in two key points: defending against threats and dealing with the consequences. For the latter, it is necessary to include not only dealing with the damage caused but also the skill of immediate response during an attack [1].

Author in [2] summarizes cybersecurity into six points: confidentiality, integrity, authorization, availability, authentication, and accountability. In this paper, the important point is the authorization process, which ensures the authenticated user has access to secured data, the transmission of which is protected by encryption.

Authorization is defined as determining which data is accessible. Individual operations on these data are subject to authorized control, which is provided by the authorized owner or server. Similarly, an authentication system works by continuously verifying that the entity connected to the data is the authorized owner. Authentication serves as the primary authentication property that ensures the integrity of data manipulation [3].

There are two types of attacks on computer systems: one targeting users and known as social engineering (e.g., phishing, pharming). The second type of attack is aimed directly at the system, most often attacking the operating systems, servers, applications, or data stores. Often the attacker gets access to the data through a breach of the authentication or authorization process [1].

The most common identity attacks are phishing, spear phishing, credential stuffing, password spraying, and man-in-the-middle.

Phishing is a part of social engineering; it is an attempt to obtain login credentials by using a deceptive email or message on a social network.

Spear phishing is a targeted phishing attack on an organization or individual.

Password spraying is a brute force attack where an attacker, ignoring the basic rules of a given server, tries to guess the password in a crude manner. The defense against this type of attack is two-factor identity verification.

Man-in-the-middle is a targeted attack that tries to get between the user's communication and the server. An example is attacking communication through a public Wi-Fi network, where the server and the user's computer are secure, but the network that mediates the communication is insecure [4].

A. Data encryption

The security of all communication through the network is ensured through encryption methods. These methods focus on encrypting the content of messages and authenticating the users, which is done through substitution and transposition.

Substitution is the replacement of characters in a message with other characters, and transposition is changing the order of characters in a message. The science that deals with this is cryptography [5].

The encryption can be symmetric in asymmetric; in either case, a encryption key is important. In symmetric encryption, a one (private) key is shared between the communicating parties. In asymmetric encryption, two keys are used, public and private. The private key is not shared within the communication [3].

Symmetric encryption is typical for dealing with large amounts of data. This type of encryption emphasizes the transmission speed [6]. An example of such encryption is the DES (Data Encryption Standard) algorithm, developed by IBM in 1967. The encryption blocks that determine the length of the key are typical of this type of encryption. Its successor was the AES (Advanced Encryption Standard), also known as the Rijndael algorithm. It uses keys 128 to 256 bits long and is used in web communication as well as file encryption [7].

Asymmetric encryption, as mentioned earlier, uses a pair of keys (private and public), with one being important for encryption and the other for decryption. In the process of decryption, each party generates its own private key and is responsible for keeping it secure. Compared to symmetric encryption, this method is slower.

The Diffie-Hellman algorithm is one example of asymmetric encryption. However, this algorithm has a major weakness and cannot defend against a man-in-the-middle attack, where one party can be presented with a fraudulent key.

The Rivest-Shamir-Adleman algorithm is often used for electronic communications, digital signatures, and building private networks. This algorithm uses keys over 100 decimal digits long and is therefore considered to be strongly secure. Asymmetric encryption is also used in certification and signature authority [6].

B. Identity management (authentication and authorization)

Identity management, which includes authentication and authorization, uses various tools and protocols. An example of this is the SAML 2.0 protocol, which is difficult to implement. OpenID Connect layer on top of the OAuth 2.0 protocol and SAML 2.0 are significant standards in authorization and authentication [8].

Identity management is often described as a cycle, at the beginning of which is registration, where a user account receives its unique identification number/symbol. Subsequently, the new account is assigned the available actions it can perform (there is a difference between an administrator account and a regular user within the system privileges). At the same time, the user's identity must be continuously verified (by the authentication process).

The most common authentication is by password or by sending an authentication email. Two-factor authentication, which helps to ensure account security, is standard. After the user has been authenticated, the process of enforcing the content that the user is entitled to, depending on the type of account, takes place. Next, the length of the login (session) is limited; at the end of this time, the user is re-authenticated or directly logged out. That ensures the secure length of the connection. Subsequently, either at the user's request or at the expiration of the session, the user is logged out.

The identity management cycle ends only when an account is deleted, which is the ultimate termination of access to the server [8].

OAuth 2.0 is an authorization protocol that allows third-party Application Programming Interface (API) calls via tokens without the protocol sharing sensitive user information. In addition, the protocol makes the content available for a limited time. The use of tokens is crucial, as their interception does not compromise the client or the server [8].

Authentication is handled by the OpenID Connect protocol. In particular, protocol ensures only limited user authority as well as limited token accesses and validity [8].

SAML (Security Assertion Markup Language) is based on an XML framework. It allows single sign-on from multiple domains. The key factors are identity providers and service providers who communicate with each other to verify the user's identity and possible credentials [8].

Currently, there are several modern open-source identity managers. These include the Ory and Gluu projects and, most importantly, the Keycloak project.

This project offers an identity and access manager, as well as single sign-on services, federated identities, and REST APIs. Keycloak was originally developed by Red Hat, which later abandoned the project. It has been further developed by the community and now offers the ability to style the login page, set up strong authentication, and a large range of ready-made programming flows. In its basic toolset, it offers the possibility to reset passwords and encourages users to update them. Keycloak includes a single sign-on system and management of the length of that sign-on [9].

Compared to Keycloak, Gluu offers the possibility to log a user in without a password, using, for example, a mobile phone, but otherwise using a similar set of tools. Ory, on the other hand, focuses mainly on working with cookies in a web environment.

III. TEACHING COMPUTER SECURITY

Awareness of computer security is being raised outside the school environment in the Czech Republic. The primary organizations dealing with the topic of prevention are the Police of the Czech Republic and the Primary Prevention Centre. The largest organization concerned with cyberspace is the National Cyber and Information Security Agency, which also serves as an educational institute for cybersecurity. Other examples of raising awareness of cyber security include various courses, competitions, and other educational events.

One of the larger projects that educate about cybersecurity is Counties for a Safe Internet. It is an e-learning course established in 2013 and supported by the Ministry of the Interior and Microsoft. A similar e-safety project called Czech Children and Facebook 2015 focused on safe behavior within saidsocial network. It was a part of a broad research project of the Faculty of Education of Palacký University in Olomouc.

A. Related works

In this subsection, several research studies concerning teaching cybersecurity at different levels of education in different countries are presented.

In the Netherlands, 140 primary school students and 96 secondary school students were asked (through a form) about their behavior in terms of password handling and cyber security. The questionnaires revealed that secondary school students were much better able to recognize a phishing site or email than elementary school students. Both groups were shown to at least check the security of a given website when accessing it. Both groups handled downloaded files similarly, as they did not check if they are secure. Overall, cybersecurity appeared to be slightly more discussed among high school students, while it was completely absent among elementary school students [10].

Similar research has been conducted at the University of the Western Cape in South Africa, where the primary focus was on the cybersecurity of university students, specifically smartphone usage behavior. This research spanned the years 2016 and 2017, while a total of 252 students were interviewed. The results were positive; students demonstrated knowledge of safe smartphone usage [11].

The quantitative study was conducted in Bartin province, Turkey. Several secondary schools and a total of 8 299 students participated in this study, thus, it provides comprehensive results. The data were collected using a voluntary questionnaire offered to the students. The research primarily dealt with model situations and investigated how students behave in them. These situations were related to cybersecurity, whether it was sharing login credentials or logging out of the system. Similarly, the research was interested in sharing personal information within social networks. The results were primarily positive as they showed that students were aware of the various threats. However, the research showed a weakness in recognition of social engineering [12].

In 2017 and 2018, extensive research was conducted on secondary school students, focusing on students' social media behavior. As part of the research, the social network Fakesbook was created. This platform allowed the authors to conduct simulations of student behavior within this network. Within these simulations, it was found that students share sensitive data and information within social networks. Students have little awareness of the interconnectedness of accounts and share content across networks. In follow-up work with students and using graphs to show account and data interconnectedness, the authors sought to educate and try to make students aware of the threats in disseminating information within such networks [13].

Research conducted in China had a similarly alternative approach to teaching computer security. In research realized between 2014 and 2016, a series of simulations were conducted to teach students computer network security. This study revealed wide gaps in understanding basic terms and principles [14].

These papers provided insight into how security is taught across countries as well as levels of education. All of these works have become essential sources for the development of the research for this paper.

IV. RESEARCH

The research of this paper aimed to test the knowledge of theoretical and practical computer security. This research took place in the fall of 2022 and was conducted at Delta secondary school in Pardubice, Czech Republic. Delta is a private school that focuses on teaching computer science and management.

The results from the secondary school were compared to a smaller sample of college students studying Applied Computer Science at the University of Hradec Kralove, Faculty of Informatics and Management.

A. Method

This quantitative research was conducted through a voluntary questionnaire administered to secondary school students. The same questionnaire was administered to college students in order to compare the results.

The questionnaire was constructed with an emphasis on the topics described in the theoretical part of the paper an emphasis on data encryption and identity management, specifically, specifically the level of knowledge on these topics. In the questionnaire, respondents answered fully anonymously; neither gender nor the age of the student was asked, only the year in which the student was. Similarly, the undergraduate students were asked only about the year of study.

The questionnaire was divided into a section dealing with cryptography and a section dealing with identity management.

The first section focused primarily on the difference between asymmetric and symmetric encryption, specific encryption algorithms (DES, AES, etc.), and their categorization.

The second section dealt with identity management, specifically the processes of authorization and authentication. Here, the focus was particularly on the use of multi-

TABLE I. ANSWERS TO ATTITUDE QUESTIONS

Statement	Secondary school				University			
	Agreed	*Rather agree*	*Rather disagree*	*Disagree*	*Agreed*	*Rather agree*	*Rather disagree*	*Disagree*
I am familiar with cryptography and have been involved in this field in school or self-study.	15	30	42	36	0	6	6	2
I am familiar with the concepts of authorization and authentication and have been involved in this field in school or self-study.	27	55	30	11	6	5	3	0
I used one of the well-known authorization protocols when creating the website.	9	10	22	82	3	3	4	4

factor password authentication and password management through software developed for this purpose.

As both schools are focused on teaching computer science, the final part of the questionnaire focused on questions related to the use of authorization and authentication tools in web development.

The questionnaire includes attitude questions, where students comment on individual statements and whether they agree or disagree with them (or to what extent). They are further divided into factual questions, where the aim is to determine the degree of realistic insight, especially regarding the different types of encryption. The questionnaire then contains questions directed towards specific written responses, mainly in terms of how students use multi-factor identity authentication and, where applicable, for which services or tools. For such questions, multiple choice was often used, as well as the option to enter one's own answer if none of the selected ones were suitable.

B. Results

123 secondary school students and 14 college students participated in the survey. Specifically, for the secondary school, there were 51 first-year students, 15 second-year students, 26 third-year students, and 31 fourth-year students. The questionnaire was voluntary. The large number of first-year students represented is due to the larger number of students in these years, while the upper years have a smaller number of students per class. For the college students, there were 14 students third-year undergraduate students.

I have decided to analyze the results within individual categories, with cryptography being the first to be looked at in depth. The results of the attitudinal question of cryptography knowledge are shown in Table I. It can be seen that the majority of the secondary school respondents (82/123), as well as college respondents (8/14) are not familiar with the topic of cryptography. In the case of the college, it should be noted that none of the respondents fully agreed they were knowledgeable about this question. 28 of the negative responses come from first-year secondary school students who have not yet discussed the topic in their lessons and so have knowledge from primary school.

The questionnaire also addressed the issue of cryptography by asking whether students were able to distinguish between symmetric and asymmetric encryption. Students were asked to identify which of these encryptions uses one and which uses two keys, as well as to distinguish which of these encryptions is faster. In the second series of questions, students were asked to match specific encryption algorithms to the correct category, whether the encryption type was symmetric or asymmetric.

The results of these knowledge questions are presented in Table II. Students were given the option of not answering the question to see the difference between those who had poorly grounded knowledge and those who had never encountered the terms and thus were unable to answer the question at all.

As can be seen in Table II., both groups of students have positive results in the basic distinction of encryption types by key and speed. In both cases, more than half of the respondents answered correctly. In contrast, knowledge of specific algorithms is very low. It is interesting to note that the results achieved by high school students were better than those achieved by university students. That, however, may be caused by the small number of university respondents, so it cannot be considered conclusive..

The second category studied was related to identity management, specifically authorization and authentication processes. This category was divided into topics related to identity management itself and a final section that dealt with the development of websites and the tools used in these processes as part of their creation.

Regarding the attitude question, the results are shown in Table I., which clearly indicates that the respondents' attitude is more positive towards this topic than cryptography. There are 82 positive responses for the secondary school, which is over half of the respondents. The results are similar for college, with 9 positive responses; it is also worth noting not a single respondent disagreed with the statement they were unfamiliar with the topic.

The next question in the questionnaire was directed at

TABLE II. RESULTS OF CRYPTOGRAPHY KNOWLEDGE QUESTIONS

Type of question	Secondary school			University		
	Correct answer	*Incorrect answer*	*No answer*	*Correct answer*	*Incorrect answer*	*No answer*
Numbers encryption keys	47%	16%	37%	64%	7%	29%
Encryption speed	49%	13%	38%	64%	11%	25%
Algorithm assignment to encryption type	17%	16%	67%	10%	16%	74%

the use of two-step identity verification. Here, I did not differentiate between secondary school and university students, as their responses did not differ significantly. Fig. 1 shows the results of where students use two-factor authentication; it demonstrates that two-factor authentication is now the standard. The students use it not only for online banking, where two-factor authentication is usually mandatory, but also for other online services, whether it is a mailbox, social networking or discussion forums, or gaming clients (such as Steam). On the contrary, there were 3 respondents who do not use two-factor authentication at all.

In terms of the specific method of two-factor authentication, the majority of respondents (133) chose to authenticate using a phone device, whether it is via SMS or an application. Another common verification method (108 respondents) was a second verification through sending an email with a check password. Other methods, such as USB keys or specific identity verification programs, were also present in units of responses. Again, it confirms how widely used two-factor authentication is today.

Another part of the questionnaire was devoted to password managers. It started with a simple question about whether students use identity managers. For secondary school, 55.3% (or 68 respondents) do use a password manager, while for university, only 28% (4 respondents) do. Here, it can be seen password managers are more likely to be used in secondary school, where students often manage various accesses to many systems and use software tools to remember passwords.

The most commonly used tool was Google Password Manager. Similarly, the corresponding Apple tool often appeared among the responses. In addition, software such as Bitwarden, LastPass and, KeePass was represented among the respondents. The results can be seen in Fig. 2.

The last part of the questionnaire was devoted to web development and the use of authorization programs. Here, the attitudinal type responses, which can be seen in Table I., show that vast majority of secondary school students are not familiar and even less of them are experienced with web development. However, results are somewhat better for university students who generally have more experience in web development. When asked about their knowledge of specific tools, the secondary school respondents appeared to have better knowledge, with 18 respondents knowing and sometimes using KeyCloak, which was mentioned in the theoretical section, followed by the secondary school respondents mentioning their knowledge of Glu and Ora (4 and 3 responses, respectively). Amongst college students, only one respondent knew one of these tools.

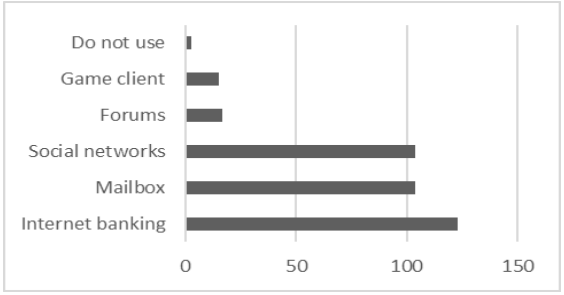

Figure 1. Using two-step identity verification

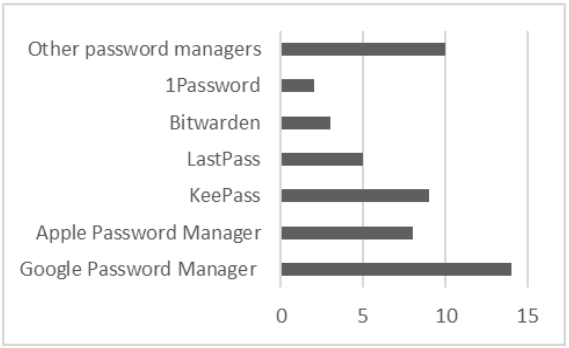

Figure 2. Password Manager

V. Conclusion

The aim of the paper was to introduce cybersecurity, especially data encryption and identity verification processes, as well as provide insight into teaching these topics within topics in secondary schools.

The main contribution is the research conducted in a secondary school with a focus on Computer Science and a university in Applied Computer Science. The results of this questionnaire showed that there is still little knowledge among students of symmetric and asymmetric encryption as fundamental knowledge in understanding how to send data across a network. However, even if students were lacking in theoretical knowledge about cryptography, they demonstrated very good knowledge of practical topics such as identity management, students from both schools appeared to have very good knowledge, as two-factor authentication of that identity has proven to be standard among students. In password management, the situation was similar; it became apparent that more education is needed in web development and using tools for user authorization and authentication processes.

This paper is just a light insight into the issue and I believe it can help with a deeper investigation in this regard.

Acknowledgment

I would like to thank Mgr. Josef Horálek, Ph.D., who helped me with the selection of the topic and cooperated as a supervisor of the article itself. I would also like to thank Mgr. Long Do, whose work provided me with a good insight into the topic and provided an overview of inspiration for the research.

I would like to thank the Department of Applied Cybernetics, Faculty of Science, University of Hradec Králové for financial support.

References

[1] J. Kolouch and P. Bašta, CyberSecurity. Praha: CZ.NIC, 2019.

[2] P. C. Van Oorschot, Computer security and the internet: tools and jewels from malware to bitcoin. Switzerland: Springer, 2021

[3] R. Pužmová, TCP/IP v kostce, 2. upravené a rozšířené vydání. České Budějovice: Kopp, 2009.

[4] “Identity is key to stopping these 5 cyber security attacks,” Okta. [Online], 2001. Available: https://www.okta.com/resources/whitepaper/identity-is-key-to-stopping-these-5-cyber-security-attacks/. [Accessed: 03-Feb-2023]

[5] S. Singh, The code book : the science of secrecy from Ancient Egypt to quantum cryptography. New York: Anchor Books, 2000.

[6] K. Burda, Kryptografie okolo nás. Praha: CZ.NIC, 2019.

[7] L. Dostálek, Velký průvodce protokoly TCP/IP: Bezpečnost, Praha: Computer Press, 2003.

[8] Y. Wilson and A. Hingnikar, Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0,. Berkeley, CA: Apress, 2019.

[9] S. Thorgersen and P. I. Silva, Keycloak - identity and access management for modern applications: harness the power of Keycloak, OpenID Connect, and OAuth 2.0 protocols to secure applications, Birmingham: Packt, 2021.

[10] J. W. A. Witsenboer, K. Sijtsma and F. Scheele, “Measuring cyber secure behavior of elementary and high school students in the Netherlands,” Computers & Education, vol. 186, pp. 104536, Sep 2022.

[11] I. M. Venter, R. J. Blignaut, K. Renaud and M. A. Venter, “Cyber security education is as essential as “the three R's”,” Heliyon, vol. 5, issue 12, e02855, Dec 2019.

[12] R. Yilmaz, F. G. Karaoğlan Yilmaz, H. T. Öztrük and T. Karademir, “Examining secondary school students' safe computer and internet usage awareness: An example from Bartın province,” Pegem Journal of Education and Instruction, vol. 7, issue 1, pp. 83–114, Feb 2017.

[13] M. Zikus, O. Curry, M. Moore, Z. Peterson and Z. J. Wood, “Solving A social networking platform for teaching security and privacy concepts to secondary school students,” in Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19), pp. 892–898, New York, NY, ACM, 2019.

[14] X. Dai and S. Tsai, “Experimental Teaching of Information Security Based on Virtual Simulation,” Mobile Information Systems, vol 2021, 8062065, Nov 2021.