A Study on Written Communication about Client-Side Web Security

Sampsa Rauti, Samuli Laato, and Ali Farooq

University of Turku, Turku, Finland
{tdhein,sadala,alifar}@utu.fi

Abstract. Today, web services are widely used by ordinary people with little technical know-how. End user cybersecurity in web applications has become an essential aspect to consider in web development. One important part of online cybersecurity is the HTTPS protocol that encrypts the web traffic between endpoints. This paper explores how the relevant end user cybersecurity instructions are communicated to users. Using text-focused analysis, we study and assess the cybersecurity instructions online banks and browser vendors provide with regards to HTTPS. We find that security benefits of HTTPS are often exaggerated and can give users a false sense of security.

Keywords: HTTPS · web application security · cybersecurity education · security guidance

1 Introduction

As online services are often created for and widely used by laypeople with little technical knowledge, end user cybersecurity has become a crucial and relevant aspect to consider in the overall security of information systems (IS) [1, 6, 17, 18]. One of the most popular tools for accessing online services is the web browser. Here, HTTP (Hypertext Transfer Protocol) is the means browsers use to connect to websites. HTTPS (Hypertext Transfer Protocol Secure) is a HTTP connection using modern encryption (currently TLS)[1], securing the connection and preventing man-in-the-middle attacks between communication endpoints. In most browsers, a HTTPS connection to a website has conventionally been indicated with an URL address beginning with HTTPS rather than HTTP, and a small padlock symbol in the address bar [12]. Already introduced in 1994, HTTPS has been steadily growing in popularity. In September 2022, Google reported that HTTPS is used as a default protocol by almost 80% of all web sites [2].

While using HTTPS is indeed important and users should be aware of it, it does not guarantee full protection. For example, malicious websites may simply purchase a cheap HTTPS certificate which makes popular browsers display them as secure despite the content of the website being dangerous. Furthermore, there

[1] https://tools.ietf.org/html/rfc2818
[2] https://w3techs.com/technologies/details/ce-httpsdefault

are many layers of communication between HTTPS and the end user, which may be targeted by adversaries. Recent work has discussed attacks such as man-in-the-browser which are able to completely circumvent the protection offered by HTTPS [23]. As a consequence, there also exists a danger of overemphasizing the security provided by HTTPS in end user cybersecurity communication.

The aim of this work is to investigate how essential end user cybersecurity knowledge is communicated in security critical web applications, in particular bank websites. We analyze and evaluate the cybersecurity guidance they provide with regards to HTTPS using text-focused analysis. Consequently, we formulate the following research questions:

RQ1: *How do bank websites and popular browser vendors communicate to users about HTTPS?*
RQ2: *Do the online banks and browser vendors over- or under-emphasize the security benefits provided by HTTPS?*

2 Background

Accelerated by technology trends such as the utilization of cloud services, a multitude of services are offered online [19]. These consist of old services being transformed online (e.g. banking [16]) and new services emerging such as Internet of things (IoT) management systems and social media [20]. Furthermore, many desktop applications are being replaced with web applications, which are accessible everywhere and updated automatically. At the same time, web security relies heavily on users' knowledge about the environment, including their ability to detect potentially malicious websites and avoid them. One of the key visual cues in browsers indicating that to users that a website is secure is the padlock symbol on the address bar. However, while the users may easily assume that this symbol indicates a completely secure web browsing experience, the padlock merely means that the connection to the server uses the HTTPS protocol. Thus, a detailed analysis on how the meaning of HTTPS and encryption is communicated to users is needed.

2.1 Advantages and misconceptions of the HTTPS protocol

HTTPS has become a significant element in ensuring secure web browsing. Google has campaigned in favor of secure web[3], advocating adoption of HTTPS encryption for websites. Amidst all the hype surrounding the secure web, however, it has often been forgotten that HTTPS and TLS only secure the end-to-end connection, not the security of the client (browser) or the security and integrity of web pages at endpoints.

HTTPS encrypts the communication in transit, but does not provide any protection when the unencrypted data is handled on the client or server side

[3] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

or when it is stored in databases. Therefore, HTTPS does not fully guarantee security, safety or privacy, although users may think so based on many cybersecurity instructions. For example, attacks with malicious browser extensions can effortlessly be implemented on the client side when HTTPS in being used [21].

Moreover, the certificate and necessary infrastructure for HTTPS are easy to obtain for any service provider, also for scammers, and they only guarantees the authenticity of the domain name or the party (e.g. company) maintaining the website. However, users are in no way protected from a website that is malicious to begin with, before it is sent to the client over an encrypted connection.

Motivating and governing HTTPS usage has been incorporated into browsers and web concepts in many ways. These include limitations and guidelines given to developers, such as disallowing mixing HTTP and HTTPS (mixed content) on websites and requiring it as a part of progressive web apps. However, HTTPS has also been acknowledged in cybersecurity communication aimed at end users. Examples of this include directing users to look for a padlock symbol in the address bar to make sure the connection is secure, labeling websites not using HTTPS insecure, and introducing additions like *HTTPS-Only* mode[4] in Firefox and the HTTPS Everywhere[5] extension.

2.2 End user cybersecurity behavior

A major research direction in cybersecurity research concerns the end users and their behavior. This research has focused on aspects such as security policy violations [25], personal data exposure and collection [22], and the impact of personality on cybersecurity behavior [24] among others. It is important to understand the security awareness level of end users, as it is a paramount component in the overall security of IT systems [6]. Therefore, ensuring end users are up-to-date on relevant cybersecurity issues and respective behavior and culture is essential.

There are several factors that impact end-users security behaviour (e.g. see [9, 7]). These include formal and non-formal education [3, 15], offering end users privacy policies that explain potential issues [22, 25], information dissemination [2] and security indicators [12]. Textual information on recommended cybersecurity behaviors are offered by almost all internet browsers and online banking websites, which are in focus in this study.

Researchers have suggested that knowledge of security threats [4, 14] is a crucial part of cybersecurity awareness. However, a recent work (e.g. [5]) suggests that merely knowledge of security threats does not guarantee secure behavior. In addition to threat knowledge, users need to have necessary skills to act in a secure way. Thus, behavioral guidance is needed. This can be achieved through cues and nudges implemented as part of information systems that guide user behavior to a more secure direction [9]. These cues and nudges can be icons, sounds, popups and other sensory cues that inform end users about the state of

[4] https://blog.mozilla.org/security/2020/11/17/firefox-83-introduces-https-only-mode

[5] https://www.eff.org/https-everywhere

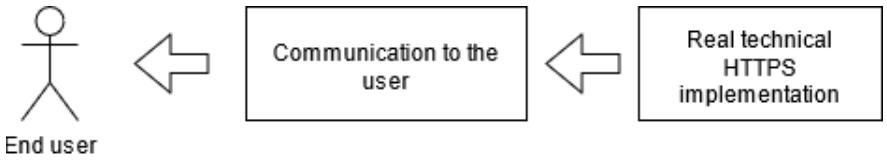

Fig. 1. A visualization how HTTPS technology and implementation are explained and communicated to end users. Instead of end users most often directly being aware of what is going on, they obtain their information through second-hand sources such as the cybersecurity guidance that internet browsers provide.

cybersecurity. The information they convey can indicate either that things are secure or that they are not.

Several studies (e.g. [11, 13, 26]) show that people have a flawed understanding about the internet. This in itself is a cybersecurity concern. Browsers are a way to browse the internet and researchers have suggested a number of ways to improve end user security. Krombholhz et al., [13] summarized a myriad of literature on security indicators in internet browsers and banking apps, and demonstrated that these indicators have advanced on multiple fronts to provide understandable knowledge to end users. The aim of these indicators is not per se to reflect the technical reality, but rather to direct end users towards desired secure behavior. In a work published in 2015, security experts suggest checking for HTTPS as one of the top six measures users should take for their security [10]. To nudge the users towards paying attention to the HTTPS connection, browsers such as Google Chrome and Mozilla Firefox display a padlock symbol in the address bar as an indication of the HTTPS connection. Furthermore, browsers may issue warnings to users if they are about or enter passwords of credit card information on a HTTP site [8].

In summary, end user cybersecurity behavior is influenced by several parties (e.g. browsers, legislators, news outlets) and in many ways (e.g. nudging, informing). It is paramount to ensure that the actions to increase secure end user behavior work as intended and do not, in fact, have adverse effects. In particular, the communication of HTTPS and the padlock symbol are worthy to investigate in this regard.

3 Materials and Methods

In order to respond to the presented research questions, we focus on cybersecurity communication aimed at the users in (1) web browsers; and (2) banks. We analyze these from the perspective of how well they match the technical implementation of HTTPS and the real security aspects it provides. Thus, looking at Figure 1, our focus is on the middle box and its relationship with the technical implementations. Accordingly, our study differs from other cybersecurity user studies which focus on end users via interviews or surveys [6].

3.1 Data sources

We investigate the communication to the users via semantic analysis of two sources. First, how six of the most popular internet browsers (Google Chrome, Firefox, Opera, Safari, Microsoft Edge and Internet Explorer[6]) communicate to their users about HTTPS. These browsers were selected based on popularity as measured by the number of active users globally. We fetched the instructions that the browsers deliver to their users from official sources, which varied between the browser providers. In case varied instructions were given to the PC and mobile version of the selected browser, we preferred the PC version for continuity's sake. The cybersecurity instructions were glanced through and all information relating to HTTPS or the lock symbol on the address bar were stored for more detailed analysis.

Second, we studied how critical high-security web sites, in this case online banks, communicate about HTTPS to end users. Similarly to the web browsers, the banks were also selected for analysis based on their popularity in the target country. We searched a list of the world's 100 largest banks and via random sampling selected 20 banks for analysis.

In order to abide by the standards of ethical research, we have redacted the names of the banks in this work. This is done to avoid targeting specific companies with potentially damaging results.

3.2 Analysis

With these two sets of data were are able to provide an overview of how HTTPS systems are communicated to end users and identify potentially problematic terminology and user guidance. In order to extract potential problems from the selected set of HTTPS related communication, we approached the texts from the perspective of the technical implementation of HTTPS which is depicted on the right hand side in Figure 1. Following the semantic analysis approach, we focused on all communication that was not aligned with the technical implementation. We wrote down these identified issues and classified them into clusters. We present these clusters including direct quotes from the browsers' communication in the following section.

4 Results

Guided by our research method, we identified two separate categories of how the security provided by HTTPS is communicated to end users. We identified issues with (1) terminology, and (2) user guidance. In the following, we discuss these two separately.

[6] Popularity of browsers fetched from Kinsta at https://kinsta.com/browser-market-share/ on 5th of March, 2021

4.1 Issues with Terminology

Table 1 shows the terminology online banks use to describe the security provided by the HTTPS protocol on their pages. We can see that the most common terms to describe HTTPS are "secure website" and "secure connection". In what follows, we will look at the potential problems with this terminology.

Table 1. How is security or privacy provided by HTTPS described? Terms used on 20 studied online bank cybersecurity guidance pages.

Term	N
secure website/webpage/site	10
secure connection	2
authentic certificate	1
encrypted connection	1
legitimate site	1
secure session	1
secure transaction	1
secure data transmission	1

Is the page secure? When cybersecurity guides talk about *secure web pages*, they usually imply that HTTPS and the TLS connection are used. However, it may not immediately be clear to the user that a web page or web application delivered using a secure connection can still be insecure in many ways. For example, a web application can be poorly implemented and contain injection vulnerabilities that leak the user's private data to other users, web pages can be laced with malware, or the owner of the website may simply be a scammer who has acquired a certificate. In all of these cases, the connection may be secure but the web page itself is not.

Accordingly, when cybersecurity guidance calls a web page secure, they merely refer to that the browser connects the remote site using a secure protocol and therefore, attackers cannot tamper with the data between the communication endpoints. However, for the user, security of a web page arguably also means that the web page (the HTML document) they have downloaded for viewing and interact with would be safe to use without compromising their private data and online transactions. Unfortunately, this is not the case. The conception of secure web page can easily become too broad in the user's mind, which makes it problematic to divide web pages into secure and insecure ones just based on their HTTPS usage. Likewise, calling the web where every website would use HTTPS *secure web* can create a false sense of security.

Is the connection secure? Based on the above, calling web pages secure can be confusing and even harmful for users. There is more to the story, however, because HTTPS does not even guarantee a secure connection in the sense users may understand it. If implemented and utilized correctly, TLS guarantees security on the transport layer, preventing man-in-the-middle-attacks that aim

to spy on or tamper with the data sent over the network. However, there is also an alternative interpretation as to what *end-to-end encryption* and secure connections mean.

Whether the connection is secure depends where the end-points of the connection are considered to be and where the "middle" of man-in-the-middle attacks is located. For example, a user might expect every point between the user interface and web server to be secure. Alternatively, the secure connection could be expected to begin when the web application forms a HTTP connection to the server. In both of these scenarios the "connection" is potentially compromised, because the data in the user interface and the data sent from the web application can easily be read and modified for example by a malicious browser extension or an independent piece of malware that has hooked into the browser. These attacks happen on the layers where there is no TLS protection and HTTPS is therefore useless. It is important to understand that TLS is only meant to encrypt the data *during delivery*, not when it is stored or used. The attacker can strike before the application layer data is encrypted or again after the encryption has been removed. From this perspective, Microsoft Edge promises a little too much in its in-browser description of the secure connection, stating that "[...] information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted".

In our sample of online banking websites and browsers, the studied browser vendors used more accurate terminology than the online banks. The browser vendors did not talk about secure websites, but only call the connection secure. However, there was one exception among the browsers. Google Chrome's help page seems to talk about secure connection and private connection interchangeably, which may further confuse readers. Browser vendors also did not go into detail about what parts of data transmission are guaranteed to be secure, which leaves the term "secure connection" vague and open for misunderstandings.

To summarize, the security terminology revolving around the use of HTTPS in online banks' websites and browsers' instructions largely use overoptimistic and exaggerated language when it comes to cybersecurity. While scaring users with threat scenarios may not be wise either, the used terminology makes unwarranted promises about security. This can have negative impact on end users' cybersecurity awareness and give rise to a false sense of security.

4.2 Problems with Guidance

Table 2 shows cybersecurity guidance given on the studied bank websites on how end users can make sure the website and the connection are secure and legitimate. As can be seen from the Table, almost all the banks list "HTTPS" in the web address as a sign of a secure website and connection. Not only is this problematic because HTTPS does not guarantee the security and integrity of a website itself, but it is outright misleading, because at least the Google Chrome browser has discontinued the practice of displaying the "HTTPS" prefix in the

address. Unfortunately, not many security guidance pages have been updated to reflect this change.

Table 2. How to make sure a website or connection is secure? Cybersecurity guidance given on the studied bank websites.

Bank ID	HTTPS in the address bar	Lock symbol	Check the address is correct	Check the certificate is legitimate
1	X	X		
2	X	X		
3	X	X		
4	X	X		
5	X	X		
6	X	X		
7	X	X		
8	X	X	X	
9	X	X		X
10	X	X		
11	X	X		X
12				X
13	X	X		
14		X		
15	X	X		X
16	X	X	X	
17	X	X		X
18	X	X		X
19	X	X		X
20	X	X		X

Another popular alleged sign of a secure website and connection is the padlock symbol. However, even together with HTTPS, this is not an indication of secure or authentic webpage as fraudsters can easily obtain certificates that makes the site appear secure. Almost half of the cybersecurity guide pages only mention the combination of HTTPS and padlock as a sign of security, which is utterly insufficient.

Checking the address in the address bar was only mentioned 2 times, and users were instructed to click the padlock icon to confirm the certificate of the webpage or the bank only in 8 cases. In majority of fraud and phishing scenarios, the displayed URL is something which cannot and has not been fabricated. Therefore, it is concerning that users are not instructed to check and verify the address. Clicking on the padlock and checking that the certificate is legitimate is good advice as well, although it is questionable whether the user wants to go through the trouble of checking this. The user may also not be able to differentiate between a genuine certificate and a fake that the scammer has procured for their fraudulent site. Consequently, users should be made more aware of what the correct URL for their bank's website is and what the correct certificate looks

like. Unsafe practices such as searching for the bank's name in the search engine and possibly clicking a link leading to a fake banking site should be strongly discouraged by the cybersecurity instructions, but this was not the case.

Not surprisingly, the guidance provided by the browser vendors is more accurate than cyber security instructions of online banks. For example, they contain information on secure certificates and explain how to check their authenticity. However, at times they still contain claims that can be seen as exaggerated, such as padlock symbol indicating that entering sensitive information is fully protected[7][8].

5 Discussion

5.1 Theoretical and practical implications

We summarize the key contributions of this work in Table 3. These relate primarily to three areas: (1) cybersecurity communication; (2) security indicator design; and (3) end user cybersecurity. Below we discuss these implications in further detail and how elucidate how they connect to extant literature.

Table 3. Key contributions

Contribution area	Key contributions
Security communication	The security instructions for end users on the world's most popular bank's websites are outdated. Education on how systems work should not be replaced by blind trust on security indicators. It is problematic if end users learn to trust that every time something is wrong with their system they see an indicator.
Security indicator design	Security indicators may provide a false sense of security. In addition to guiding behavior security indicators could be designed to guide learning about potent security measures.
End user cybersecurity	There is a shared responsibility between banks, the government and other related agencies to educate the crowds about the current trends in cybercrime and provide knowledge on how to stay protected. Banks should not fall behind in inadequate security communication that leads to a false sense of security.

With regards to cybersecurity communication, we contribute in to the literature on security indicators in web browsers [13]. Through the performed analysis

[7] https://support.google.com/chrome/answer/95617
[8] https://help.opera.com/en/latest/security-and-privacy/

of cybersecurity communication in the world's largest bank's webpages we offer a unique viewpoint to the literature that largely focuses on empirical user studies [9, 7].

With regards to security indicators and their design, our work offers a fresh perspective reminding of the potential dangers of simplified communication. For example, Krombholz et al., [13] found that end users oftentimes underestimate the security benefits of using HTTPS. Based on our findings, blindly trusting the padlock symbol to make web browsing secure at times when it is quick and cheap to get a HTTPS certificate for any website is unwise. Furthermore, it is problematic if end users learn to trust that every time something is wrong with their system they see an indicator of sorts.

Finally, with regards to end user cybersecurity, our findings align with previous work in that knowledge about cybersecurity threats and education on how the systems work on a general level is needed [4, 14]. Our findings further contradict the argument that security indicators would be better than nothing. In fact, we argue that they may even have a negative impact on cybersecurity for the following reasons:

- They can lure individuals into a false sense of security.
- They may make end users lazy and to not bother to learn how systems actually work.

5.2 Limitations and future work

Our empirical work has the following limitations. First, we reviewed the cybersecurity communication of the most popular online banks and browsers, but it may very well be that this is not the primary source of information for many end users. Other sources including alternative websites, social media, news sites, formal education and mouth-to-mouth sources need to also be considered. To account all these, interview studies with end users could be conducted, an approach adopted by related work (e.g., [13]). Second, we analysed the online banks' and browsers' end user cybersecurity communication specifically with regards to HTTPS. Of course, other important aspects regarding end user cybersecurity behavior and communication exist, and future work could explore these.

6 Conclusion

When used and implemented correctly, HTTPS and TLS are essential technologies to safeguard data when it is transmitted between the user's browser and the server. While saying that HTTPS is secure is not wrong, it is a misconception that using the protocol would keep the user data safe inside the browser or even at every point of the data transmission. HTTPS is only one important piece of cybersecurity, and users and web service providers need to be educated on the threats HTTPS does not protect against and the necessary countermeasures.

HTTPS will no doubt become even more prevalent in the future when a new version of HTTP, HTTP/2 is adopted more widely. Although the protocol

does not require mandatory encryption, in practice it is required by most client implementations. Hopefully, we will soon to be able to move to a web where every site uses HTTPS and trustworthy certificates by default, and developers as well as users can concentrate more on other security issues.

As the world becomes increasingly digital and complex, the pitfall of simplifying things too much for end users via security indicators and visual cues becomes more prominent. Based on our findings here, we stress the paramount importance of end user cybersecurity education as opposed to luring users to potential false sense of security through teaching them to rely on oversimplified security indicators.

In conclusion, we are not arguing that cybersecurity communication to end users should disclose everything about the technical implementation. However, end user communication should make sure to provide a realistic view of the used security measures so that users are not lead into a false sense of security.

References

1. Carlton, M., Levy, Y.: Expert assessment of the top platform independent cybersecurity skills for non-it professionals. In: SoutheastCon 2015. pp. 1–6. IEEE (2015)
2. Dandurand, L., Serrano, O.S.: Towards improved cyber security information sharing. In: 2013 5th International Conference on Cyber Conflict (CYCON 2013). pp. 1–16. IEEE (2013)
3. Farooq, A., Hakkala, A., Virtanen, S., Isoaho, J.: Cybersecurity education and skills: Exploring students' perceptions, preferences and performance in a blended learning initiative. In: 2020 IEEE Global Engineering Education Conference (EDUCON). pp. 1361–1369. IEEE, IEEE (2020). https://doi.org/10.1109/EDUCON45650.2020.9125213
4. Farooq, A., Isoaho, J., Virtanen, S., Isoaho, J.: Information security awareness in educational institution: An analysis of students' individual factors. In: 2015 IEEE Trustcom/BigDataSE/ISPA. vol. 1, pp. 352–359. IEEE (2015)
5. Farooq, A., Jeske, D., Isoaho, J.: Predicting students' security behavior using information-motivation-behavioral skills model. In: IFIP International Conference on ICT Systems Security and Privacy Protection. pp. 238–252. Springer (2019)
6. Farooq, A., Kakakhel, S.R.U.: Information security awareness: Comparing perceptions and training preferences. In: 2013 2nd National Conference on Information Assurance (NCIA). pp. 53–57. IEEE (2013)
7. Farooq, A., Ndiege, J.R.A., Isoaho, J.: Factors affecting security behavior of kenyan students: An integration of protection motivation theory and theory of planned behavior. In: 2019 IEEE AFRICON. pp. 1–8. IEEE (2019)
8. Felt, A.P., Barnes, R., King, A., Palmer, C., Bentzel, C., Tabriz, P.: Measuring {HTTPS} adoption on the web. In: 26th USENIX Security Symposium (USENIX Security 17). pp. 1323–1338 (2017)
9. Howe, A.E., Ray, I., Roberts, M., Urbanska, M., Byrne, Z.: The psychology of security for the home computer user. In: 2012 IEEE Symposium on Security and Privacy. pp. 209–223. IEEE (2012)
10. Ion, I., Reeder, R., Consolvo, S.: "... no one can hack my mind": Comparing expert and non-expert security practices. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 327–346 (2015)

11. Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 39–52 (2015)
12. Kraus, L., Ukrop, M., Matyas, V., Fiebig, T.: Evolution of ssl/tls indicators and warnings in web browsers. In: Cambridge International Workshop on Security Protocols. pp. 267–280. Springer (2019)
13. Krombholz, K., Busse, K., Pfeffer, K., Smith, M., von Zezschwitz, E.: " if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 246–263. IEEE (2019)
14. Kruger, H.A., Kearney, W.D.: A prototype for assessing information security awareness. Computers & security **25**(4), 289–296 (2006)
15. Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., Airola, A.: Ai in cybersecurity education-a systematic literature review of studies on cybersecurity moocs. In: 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT). pp. 6–10. IEEE (2020). https://doi.org/10.1109/ICALT49669.2020.00009
16. Li, F., Lu, H., Hou, M., Cui, K., Darbandi, M.: Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. Technology in Society **64**, 101487 (2021)
17. Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X.: Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management **45**, 13–24 (2019)
18. Lombardi, V., Ortiz, S., Phifer, J., Cerny, T., Shin, D.: Behavior control-based approach to influencing user's cybersecurity actions using mobile news app. In: Proceedings of the 36th Annual ACM Symposium on Applied Computing. pp. 912–915 (2021)
19. Malar, D.A., Arvidsson, V., Holmstrom, J.: Digital transformation in banking: Exploring value co-creation in online banking services in india. Journal of Global Information Technology Management **22**(1), 7–24 (2019)
20. Newman, N.: The rise of social media and its impact on mainstream journalism (2009)
21. Rauti, S.: A survey on countermeasures against man-in-the-browser attacks. In: International Conference on Hybrid Intelligent Systems. pp. 409–418. Springer (2019)
22. Rauti, S., Laato, S.: Location-based games as interfaces for collecting user data. In: World Conference on Information Systems and Technologies. pp. 631–642. Springer (2020)
23. Rauti, S., Laato, S., Pitkämäki, T.: Man-in-the-browser attacks against iot devices: A study of smart homes. In: Abraham, A., Ohsawa, Y., Gandhi, N., Jabbar, M., Haqiq, A., McLoone, S., Issac, B. (eds.) Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020). pp. 727–737. Springer International Publishing, Cham (2021)
24. Shappie, A.T., Dawson, C.A., Debb, S.M.: Personality as a predictor of cybersecurity behavior. Psychology of Popular Media Culture (2019)
25. Siponen, M., Vance, A.: Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly pp. 487–502 (2010)
26. Wu, J., Zappala, D.: When is a tree really a truck? exploring mental models of encryption. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 395–409 (2018)