

Cartoons to Improve Cyber Security Education: Snow White in Browser in the Middle

Christian Catalano¹, Alessandro Pagano², Antonio Piccinno² and Alessandro Stamer²

¹University of Salento, Lecce, LE 73100, Italy

²University of Bari Aldo Moro, Department of Computer Science, Via Edoardo Orabona 4, Bari, Italy

Abstract

Cyber Security Education is considered one of the key challenges of recent years. The increase in cyber attacks requires not only technical experts but also an increase in the awareness of users using technological devices. ENISA (European Union Agency for Cybersecurity) provides a common understanding of the relevant roles, competences, skills and knowledge required in cybersecurity and supports the design of training programs related to cybersecurity. Therefore, the paper proposes using cartoons to educate the user to recognize a cyber attack such as Browser in the Middle. It consists in interposing a transparent Browser between the victim and the attacker in order to steal not only credentials but sessions and sensitive data. Through the story of Snow White and the Seven Dwarfs, one has the possibility to tell how the computer attack can be successful, therefore the evil witch who manages to poison Snow White through the apple, and at the same time a parallel way to save Snow White and therefore prevent the attack from happening, via a mitigation that allows URL parsing. The general aim is therefore to improve the skills, knowledge and skills in cyber security also through the education of cartoons.

Keywords

Browser-in-the-Middle, Cyber Security, Cartoons, Cyber Attack

1. Introduction

Technological development has made the user experience increasingly vulnerable to cyber attacks of various types and various purposes such as scams with financially fraudulent ends or the objective of stealing data and information to blackmail and negatively influence any victim [1, 2].

Therefore in this scenario, cyber security education is considered one of the key challenges facing the modern digitized world [3, 4]. The scientific and reference community is engaged on several fronts in order to be able to raise the level of awareness and education on cyber security such as the ENISA framework (ECSF - European Cybersecurity Skills Framework) that provides a tool to build a common understanding of the cybersecurity professional role profiles and common mappings with the appropriate skills and competences required [5, 6]; CyBOK (Cyber

IS-EUD 2023: 9th International Symposium on End-User Development, 6-8 June 2023, Cagliari, Italy


*Corresponding author.

†These authors contributed equally.

✉ christian.catalano@unisalento.it (C. Catalano); alessandro.pagano@uniba.it (A. Pagano); antonio.piccinno@uniba.it (A. Piccinno); a.stamerra1@studenti.uniba.it (A. Stamer)



© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

Security Body of Knowledge) that aims to codify the foundational and generally recognized knowledge on cybersecurity [7].

In particular, in [7] academia and industry met to discuss the top-level knowledge areas (KAs) that CyBOK should integrate. Supermarket metaphor was used to encourage participants to KAs they considered key to include in the CyBOK.

Consequently, considering the metaphor example, security awareness training can be improved by using pop culture references and gamification techniques to make critical concepts more understandable [8, 9]. Using a cartoon or a familiar icon can leverage the power of familiar images, allowing new data to be better absorbed. [8].

According to a study of Cheung et al. [10], Disney films combine entertainment with life lessons about love, friendship, good versus evil death and loss, and the importance of family. The gamification [11] in cyber security education can bring that sense of healthy competition into the workplace for the better [8].

With this in mind and considering the possibility of using scenarios familiar to the user, the following research proposes the use of cartoons to be able to educate the user to recognize a cyber attack such as Browser in the Middle [12].

We identified, in according to Nice Framework [13], three key elements to the cyber security education through cartoons: (i) *Competencies* that provide a mechanism to assess learns; (ii) *Knowledge*, a retrievable set of concepts within memory; (iii) *Skill*, the capacity to perform an observable action. Figure 1 shows the schema that we adopted to explain cyber attacks with cartoons.

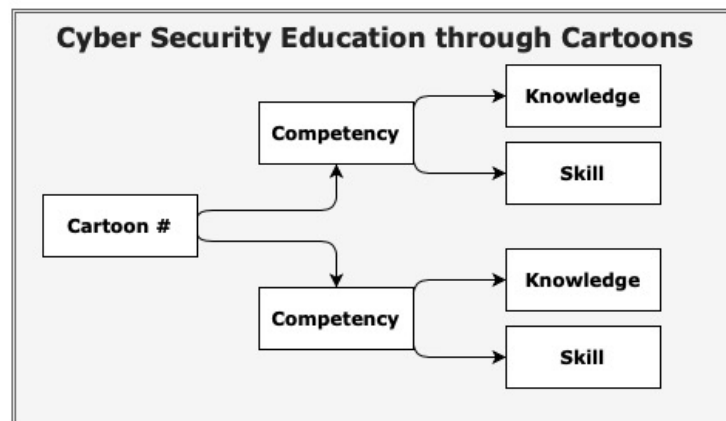


Figure 1: Cyber Security Education through Cartoons

2. Snow White and the Seven Dwarfs in the Browser in the Middle attack

The goal of various types of attacks such as Man in the Middle, Man in the Browser, Browser in the Browser, Browser in the Middle, Mobile Application in the Middle, is to use malware

generally managed between victim client, server and attacking client to obtain important access data or manage active sessions.

In order to educate users to recognize these types of attacks, we propose mitigation that tries to briefly explain defence techniques in an elementary way. The general steps to educate the user on correct navigation are described, thus avoiding various types of attacks such as DoS, phishing or MitM (Man in the Middle).

To analyze an example of attack simulation, the Browser-in-the-Middle study was deepened by carrying out a parallel analysis between the fairy tale of "Snow White and the Seven Dwarfs" and the attack itself. In the same way, a mitigation proposal is made, explaining how various techniques developed can guarantee the protection of the user and in the story of "Snow White and the Seven Dwarfs", the protection of the protagonist from the poisoned apple represented by the computer attack. The goal is to raise awareness of correct navigation by explaining in a fun way, through a fairy tale, what could happen in the event of an attack and possibly defending against it.

2.1. Browser-in-the-Middle

The Browser in the Middle (BitM) attack differs from the Man in the Middle (MitM) attack precisely in the ease of implementation through various techniques such as phishing [12]. Continuous monitoring allows real-time analysis of the victim's actions and behaviors. The latter is unaware that someone can control it because the victim's browser is replaced with a malicious browser that is located on the attack server. A transparent browser is then placed between the victim's official browser and the web server used by the user to use the services. The purpose, on the part of the attacker, is to intercept, record and manipulate any data exchange in order to steal information.

In order to better explain the various stages of the BitM attack, reference is made to the Walt Disney animated story "*Snow White and the Seven Dwarfs*" where the characters are represented in the figure of **Snow White** (the victim of the attack), **the seven dwarfs** who help the protagonist (the mitigation of the Browser-in-the-Middle attack), **the queen** who turns into the wicked witch (the phishing attempt to carry out the BitM attack). From the perspective of the victim (Snow White), the steps are listed as follows [Fig.2]:

- Snow White receives from the wicked witch the poisoned apple represented in reality by the victim who, through social engineering techniques, receives the malicious URL from the attacker. Snow White trusts the received apple to be able to make her actually poisoned apple pie. The user therefore does not check the connection and does not notice what the "onclick" event points to;
- Snow White eats the apple and makes a wish but receives the poison. In the event of the attack the server then sends the JavaScript code to the client ("noVNC client");
- The poison starts circulating in Snow White's body, therefore the JavaScript code, once present on the victim's machine, starts a WebSocket connection (through the HTTP channel);
- The received apple looked as inviting as a normal apple. Even phishing sites look inviting as clones of official sites in terms of graphics. Through the JavaScript client then, the web

server exposes a web page that is configured to encapsulate the page at the URL that the victim tried to access and thus be the legitimate one, hence showing the same appearance. The victim was then tricked into being Snow White herself with the poisoned apple;

- The last step is the phase in which the unaware user enters the credentials on this page, credentials that end up in a database on the malicious server useful to the attacker who will use them on the official site to access them in the name of the user to whom the attack took place. The goal is also to continue interception by manipulating traffic and the session itself. The user then loses her identity, a bit like Snow White who momentarily dies. She can only be awakened with the first kiss of love represented with an attack mitigation technique to prevent it.

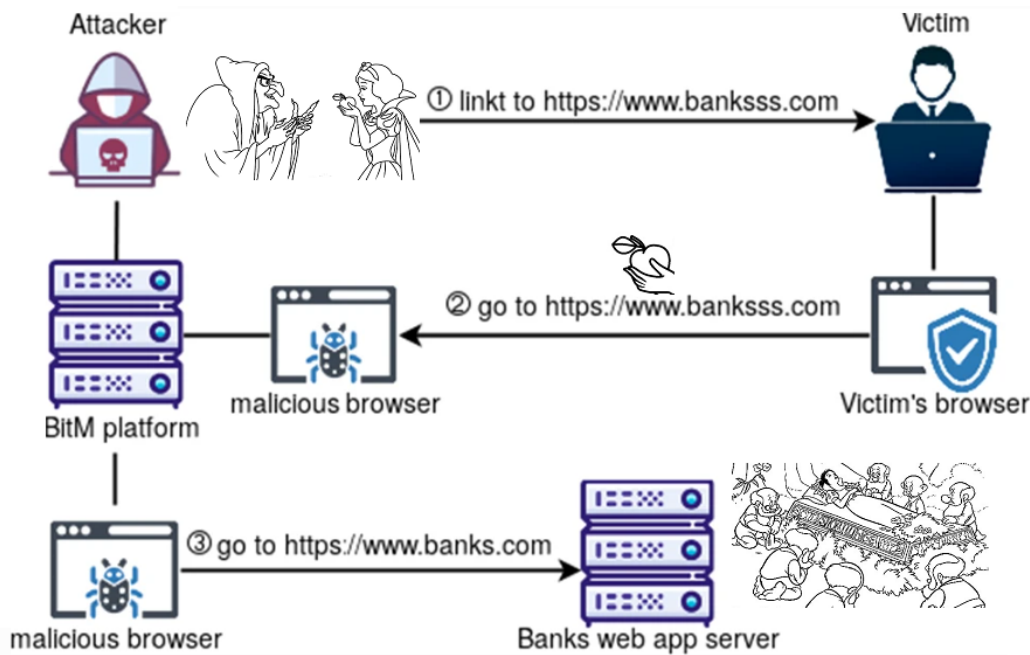


Figure 2: Browser in the Middle [12] in the story of "Snow White"

3. BitM mitigation on Desktop devices

The goal of the mitigation is the creation of a protocol useful for mitigating BitM attacks on both Desktop and Mobile systems, on which attention is paid precisely due to the recent diffusion compared to older attacks such as Man in the Middle and Man in the Browser [14, 15].

The proposed mitigation consists in the development of software for the real-time control of the websites accessed by the user. Since the *Browser in the Middle* attack consists precisely in an attempt to induce the user to open a link through *phishing*, the mitigation software developed in Python allows the user to be protected and warned through the following steps briefly [Fig.3]:

1. Get the real-time history of the page viewed by the user on his browser, then save each URL;
2. Check the following URLs using the online tool *Safe Web* for trustworthiness rating i.e. how websites affect on users' computers. The evaluation will report the following results: "Secure", "Untested", "Dangerous" or "Caution" (in the fairy tale it can be compared to the fruit basket that the wicked witch carries containing only a poisoned apple);
3. The result is shown on the Python terminal by performing a *Web Scraping* of the *Safe Web* site, then grafting the respective URL you want to test;
4. If the analysis returns the certainty of the website's security as a result, then the user can continue browsing normally (the apple is not poisoned so Snow White is safe);
5. If instead the analysis returns: "Untested", "Dangerous" or "Caution", then a warning is shown to the user, notifying that the same URL, not being safe, is blacklisted in the Windows hosts file in so that any subsequent action is rejected (the apple is poisoned; if it is not discarded then it can lead to the death of Snow White).

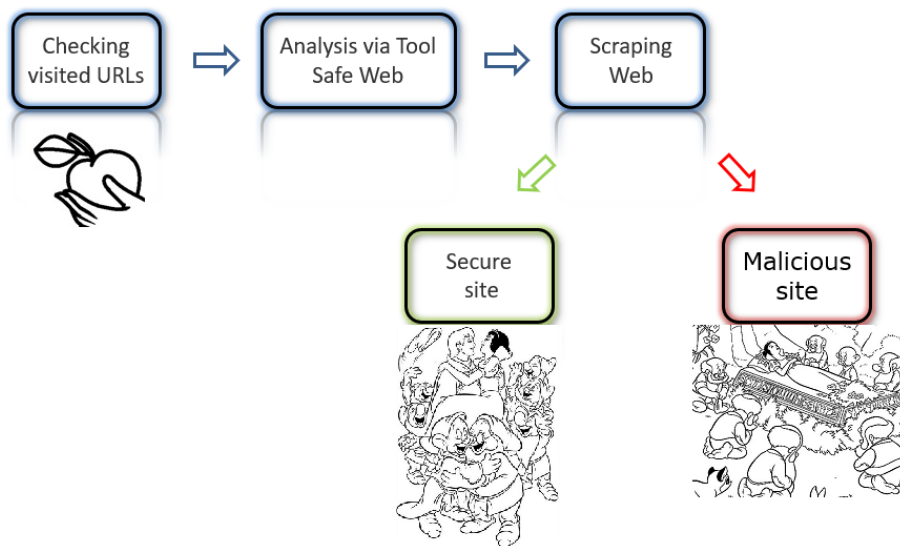


Figure 3: BitM mitigation steps

3.1. URL classification control

The ultimate goal of the mitigation is to ensure that the website that is scanned and classified as "safe" can function properly. The characters of the fairy tale "Snow White and the Seven Dwarfs" describe various situations that can happen. In the case of checking a secure site, it means that the wicked witch fails to deliver the poisoned apple to Snow White (phishing attack) with the help of the seven dwarfs (database check).

In case the scanned site is classified as "Untested", "Dangerous" or "Caution", the newly executed site is automatically moved to a blacklist. A message box is then shown through the

use of the "easygui" library, which warns the user of the actions that will be performed precisely to prevent the attack *Browser in the Middle* to be successful, also specifying which URL is the one classified as unsafe. In case the scanned site is classified as "Not Tested", "Dangerous" or "Warning", the newly run site is automatically moved to a blacklist. A message window is then shown through the use of the "easygui" library, which warns the user of the actions that will be performed to prevent the attack *Browser in the Middle* is successful, also specifying which URL is the one classified as unsafe.



Figure 4: Navigation awareness

In the story of Snow White and the Seven Dwarfs, the classification of the unsafe site can be compared to the actual encounter between the Wicked Witch and Snow White.

- In the case of "Untested" classification, the story can be compared to the queen who turns into an evil witch. No one can therefore carry out an immediate evaluation of the new witch (therefore of the new site which will be a phishing attempt, therefore it is blocked);
- In the case of classification "Dangerous", the story can be compared to the evil witch who gives Snow White the poisoned apple (the victim who receives the malicious link to launch the Browser-in-the-Middle attack);
- In the case of classification "Attention", the story can be compared to Snow White meeting a poor old lady who asks for help but who is actually the wicked witch (site that apparently looks like the official one but is actually a phishing attempt).

Subsequently, the site is written to the Windows "hosts" file with the "append" function in order to add parts of text and not overwrite the existing ones. In the file it will be allowed to add the IP address (always set to the local 127.0.0.1 as a redirect) and the URL considered malicious.

4. Conclusions

The paper aims to investigate how the use of Disney cartoons can improve cyber security education. In particular, in this first step, we focused on being able to map a security attack such as Browser in the Middle to the fairy tale of "Snow White". This was performed with

consideration of the *skills* a user must acquire to recognize a BitM attack, the *knowledge* from the application of the fairy tale characters in explaining the various steps of the attack, and finally the *Competency* to assess learns.

The latter element will be verified in the next step of the research. We are planning an experiment with bachelor's degree students to assess the skills acquired through the explanation of "Snow White and the Seven Dwarfs in the Browser in the Middle", and both in the company to be able to improve the awareness of non-technical employees about cybersecurity.

Briefly, the mitigation of the attack, explained through the fairy tale, reported as a positive aspect the ability in real time to be able to block the execution of the attack through the analysis of the URLs, while as a negative aspect the non-protection of privacy, as the mitigation software reads every URL the user navigates to and hardware performance usage as the program is continuously running [16]. For future developments, in fact, we are thinking of developing a Chrome extension that performs the same operations, so as not to have to use an external program [17].

Acknowledgments

This study has been partially supported by the following projects: SSA (Secure Safe Apulia – Regional Security Center, Codice Progetto 6ESURE5) and KEIRETSU (Codice Progetto V9UFIL5) funded by "Regolamento regionale della Puglia per gli aiuti in esenzione n. 17 del 30/09/2014 (BURP n. 139 suppl. del 06/10/2014) TITOLO II CAPO 1 DEL REGOLAMENTO GENERALE "Avviso per la presentazione dei progetti promossi da Grandi Imprese ai sensi dell'articolo 17 del Regolamento"; and SERICS (Security and Rights In the CyberSpace - PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

- [1] F. Tommasi, C. Catalano, M. Fornaro, I. Taurino, Mobile session fixation attack in micro-payment systems, *IEEE Access* 7 (2019) 41576–41583.
- [2] V. S. Barletta, D. Caivano, M. De Vincentiis, A. Magri, A. Piccinno, Quantum optimization for iot security detection, in: V. Julián, J. Carneiro, R. S. Alonso, P. Chamoso, P. Novais (Eds.), *Ambient Intelligence—Software and Applications—13th International Symposium on Ambient Intelligence*, Springer International Publishing, Cham, 2023, pp. 187–196.
- [3] R. Pirta-Dreimane, A. Brilingaitė, G. Majore, B. J. Knox, K. Lapin, K. Parish, S. Sütterlin, R. G. Lugo, Application of intervention mapping in cybersecurity education design, *Frontiers in Education* 7 (2022). URL: <https://www.frontiersin.org/articles/10.3389/educ.2022.998335>. doi:10.3389/educ.2022.998335.
- [4] V. S. Barletta, F. Cassano, A. Pagano, A. Piccinno, New perspectives for cyber security in software development: when end-user development meets artificial intelligence, in: *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2022, pp. 531–534. doi:10.1109/3ICT56508.2022.9990622.
- [5] ENISA, European cybersecurity skills framework role profiles (2022). URL: <https://www>.

enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles?v2=1.

- [6] ENISA, European cybersecurity skills framework (ecsf) - user manual (2022). URL: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf?v2=1>.
- [7] A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis, C. Peersman, Scoping the cyber security body of knowledge, *IEEE Security Privacy* 16 (2018) 96–102. doi:10.1109/MSP.2018.2701150.
- [8] S. Poremba, What cartoons can teach us about cyberattacks, *Security Intelligence* (2019). URL: <https://securityintelligence.com/articles/what-cartoons-can-teach-us-about-cyberattacks/>.
- [9] M. T. Baldassarre, V. S. Barletta, D. Caivano, D. Raguseo, M. Scalera, Teaching cyber security: The hack-space integrated model, in: *Italian Conference on Cybersecurity*, 2019.
- [10] M. Cheung, C. A. Leung, Y.-J. Huang, Absentee parents in disney feature-length animated movies: What are children watching?, *Child and Adolescent Social Work Journal* (2022). URL: <https://doi.org/10.1007/s10560-021-00799-0>. doi:10.1007/s10560-021-00799-0.
- [11] V. S. Barletta, F. Caruso, T. Di Mascio, A. Piccinno, Serious games for autism based on immersive virtual reality: A lens on methodological and technological challenges, in: M. Temperini, V. Scarano, I. Marenzi, M. Kravcik, E. Popescu, R. Lanzilotti, R. Gennari, F. De La Prieta, T. Di Mascio, P. Vittorini (Eds.), *Methodologies and Intelligent Systems for Technology Enhanced Learning*, 12th International Conference, Springer International Publishing, Cham, 2023, pp. 181–195.
- [12] F. Tommasi, C. Catalano, I. Taurino, Browser-in-the-middle (bitm) attack, *International Journal of Information Security* 21 (2021) 179 – 189.
- [13] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, G. Witte, Workforce framework for cybersecurity (NICE framework), *NIST Special Publication 800-801* (2020). URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>. doi:10.6028/NIST.SP.800-181r1.
- [14] M. Angelelli, C. Catalano, D. Hill, H. Koshutanski, C. Pascarelli, J. Rafferty, A reference architecture proposal for secure data management in mobile health, in: *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*, 2022, pp. 1–6. doi:10.23919/SpliTech55088.2022.9854277.
- [15] C. Catalano, P. Afrune, M. Angelelli, G. Maglio, F. Striani, F. Tommasi, Security testing reuse enhancing active cyber defence in public administration., in: *ITASEC*, 2021, pp. 120–132.
- [16] M. T. Baldassarre, V. S. Barletta, D. Caivano, A. Piccinno, A visual tool for supporting decision-making in privacy oriented software development, in: *Proceedings of the International Conference on Advanced Visual Interfaces, AVI '20*, Association for Computing Machinery, New York, NY, USA, 2020. URL: <https://doi.org/10.1145/3399715.3399818>. doi:10.1145/3399715.3399818.
- [17] M. Teresa Baldassarre, V. Santa Barletta, D. Caivano, A. Piccinno, Integrating security and privacy in hcd-scrum, in: *CHIItaly 2021: 14th Biannual Conference of the Italian SIGCHI Chapter, CHIItaly '21*, Association for Computing Machinery, New York, NY, USA, 2021. URL: <https://doi.org/10.1145/3464385.3464746>. doi:10.1145/3464385.3464746.