Security Enhancements for Cloud Applications

Ana-Maria DINCĂ[1], Sabina-Daniela AXINTE, PhD[2]
Faculty of Electronics, Telecommunications and Information Technology,
University POLITEHNICA of Bucharest, Romania
[1] ana_maria.dinca@stud.etti.upb.ro
[2] axinte_sabina@yahoo.com

Abstract

This study scrutinizes the cloud applications infrastructure and the associated vulnerabilities that could allow unauthorized access to users' accounts. The research is based on a Fault Tree Analysis that uncovers various security design flaws and their occurrence probabilities. For each undesirable event, a preventive mechanism is suggested and validated by the testing results, decreasing to a minimum the risk exposure of unauthorized access to users' sensitive data.

Index terms: cybersecurity, cloud platform security, security augmentation, security by design

1. Context

Lately, cloud computing gained more and more popularity because of its broad spectrum of solutions and convenience, especially in the last couple of years. Since the pandemic started, companies started substituting their hardware equipment with cloud solutions, cutting costs and facilitating access to critical resources for the employees that shifted to remote work [1].

With an increase in cloud usage, the number of cybernetic attacks surged and consequently the number of data breaches has risen, as shown in the annual Verizon Data Breach Investigation Report (DBIR): "the number of data breaches showed a significant jump up from 3,950 confirmed data breaches in the 2020 report to 5,258 in 2021" [2].

According to the DBIR, the causes of data breaches in 2021 were related to a human component in 85% of the incidents, while 61% of breaches involved credentials, 13% implicated ransomware and only 3% of the breaches were built upon vulnerability exploitation [3]. The high percentage of data breaches, facilitated by the human component, can be explained by the rise in social engineering and phishing attacks; according to Cisco's 2021 Cyber Security Threat Trends report [4] phishing attacks can be accounted for 90% of data breaches. Users choosing vulnerable passwords to protect their personal data is another security exposure, induced by the human factor and responsible for inadvertently facilitating cybernetic attacks.

The human component caused a concerningly high percentage of data breaches that were confirmed in 2021, which indicates a need for augmented security training for employees and additional security mechanisms in order to boost the sensitive data protection.

2. Pre-requisites

This paper is proposing a research regarding security vulnerabilities that might emerge during the planning or design phases of the software development cycle. The study is conducted on a web application designed and developed as part of the graduation thesis and its intended end-users are the students attending the Faculty of Electronics, Telecommunications and Information Technology and

the faculty members such as teachers, assistants or administrative staff (IT administrators, secretaries). The application's purpose is to provide the schedule for its users for any requested date and to offer support with booking a classroom.

The functional flows were designed to accommodate various information access levels in accordance with different roles and specific permission groups, thus the functionalities differ in perspective between users. The main roles in the application are the following: administrators, teachers and students, each one having less access privileges that the previous ones.

One of the first dissimilarities between the functional flows can be observed during the registration flow, where the teachers and the administrators can begin their account initialization by themselves, but students need to previously be enrolled on the platform by an administrator or a teacher. After enrolling on the platform, the users receive an email that will contains a web address where they can set up their account password.

Once the account is activated and the users can access the application, they can fill in their additional data in order to be able to access their schedule and to find out where the classes take place. They are also able to see how they can get in touch with the faculty members - classroom, office, email address.

Users can also book classrooms for various activities such as an exam preparation or a group study; depending on the user's privileges, if they are a faculty member, they can book lecture halls or regular classrooms whilst students can only book regular classrooms.

Because the accounts created on the platform contain some of the users' personal information, a compromised account can lead to sensitive information exposure and, additionally, could result in material damage for certain scenarios, such as an attacker impersonating a student, booking a classroom and causing material damages; unsensitized fields in the application also represent a vulnerability considering that it can jeopardize the stored data.

In the following sections, the causes that put the users' accounts at risk will be analyzed in order to tighten security validations and to propose adequate solutions to prevent negative scenarios.

3. Fault Tree Analysis

Fault Tree Analysis (FTA) is used to compute the probability of an undesirable event, which can be utilized to compute the occurrence probability of an attacker to access users' sensitive data. One needs to determine the direct root causes for the top event and then, for each of the leading causes, to identify the specific triggering events.

For the FTA presented below there have been identified a total of 10 base events that can facilitate an attacker to gain unauthorized access to users' accounts. The first five events are scenarios that involve setting or resetting a user's password, which sends an email to the associated address, that contains an URL from where they can set a new password. This flow becomes vulnerable in case of previously compromised email accounts; the attacker has the possibility of setting the new password before the legitimate user gets the chance to, and therefore the ownership of the platform account will be lost.

The considered basic events and their associated probabilities are the following: user inserting an expired password - 42% [5], accessing an inactive account - 15%, user forgetting current password - 78% [6], consecutive failed login attempts in a short period of time - 30% and new platform account creation - 40%. The first four events are part of the main scenario where the user loses access to his account and sends a reset password request to the IT department, with a probability of 46%; an user enrolling on the platform is the other main scenario with a probability of 40%. Consequently, the combined probability of these scenarios equals to 16% because there is a reduced possibility that an user's email account has been compromised prior to receiving an access-providing email, more specifically, one in four email accounts are considered already compromised.

The following five events are directly related to the probability that the user chose a vulnerable password and their probabilities are the following: weak password - 64% [5], password reused between multiple accounts - 61% [5], password contains username or publicly available data such as name, age, pet's name - 60%, password leaked online after a cybernetic attack - 55% or user was a target of a phishing attack - 33% [7]. The combined probability of these scenarios is equal to 97% - a concerningly high percentage, which strengthens the necessity of protecting platform accounts enforcing strong passwords and implementing resilient and prompt security mechanisms to protect these accounts during an imminent cybernetic attack.

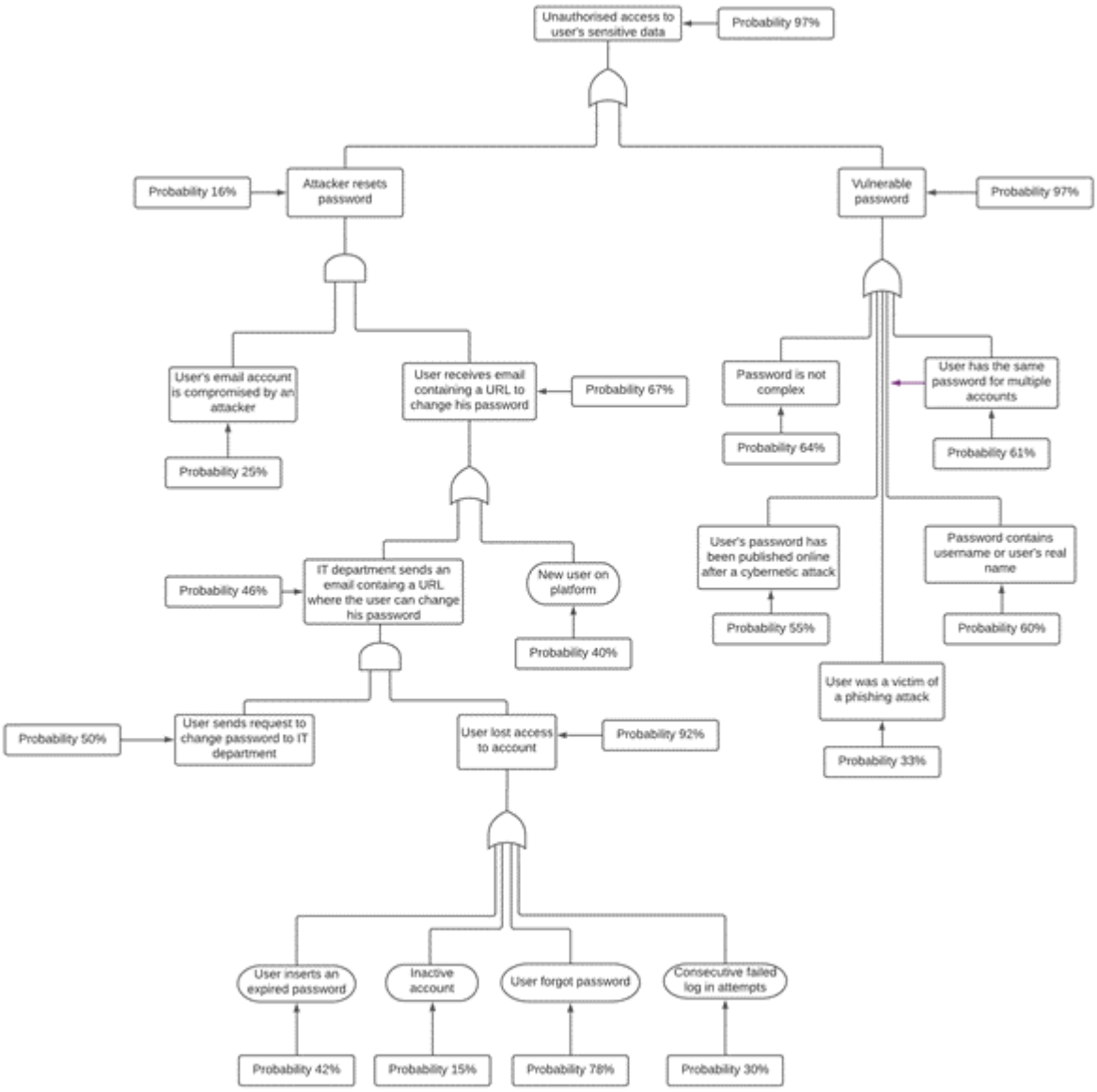

Fig. 1. Fault Tree Analysis

After the final computation, the possibility that users' sensitive data can be accessed by an attacker is up to 97%, which makes it imperative to introduce various security measures with the main goal of protecting the accounts created on the platform, their associated personal information, and mitigating the risk of the top event.

4. Security augmentation in design phase

Continuous improvement is a compulsory requirement in modern cloud architecture. Consequently, we focus on enhancing User Experience and strengthening security in an effort to keep

end-users both engaged and protected. The FTA previously presented stands as a step towards improving the platform, while the next organic one is proposing solutions for the identified problems.

The first issue to be tackled is the possibility that an attacker, who previously compromised the user's email account, is able to set a new password on behalf of the rightful owner and therefore restrict his access. This scenario can be entirely prevented by using two-factor authentication (2FA), which is an additional step to the traditional authentication: after providing the correct username and password combination, the user is asked to insert an one time password (OTP). An OTP is a fortifying layer of protection in order to secure the platform's accounts, that expires once it is used or after a fixed period a time, usually between five and ten minutes for OTPs sent via text messages, and one minute for OTPs generated using dedicated software applications. Also, if the OTP is sent via a text message and the token sent by the user is not an exact match, then it's invalidated and a new one is generated and sent to the user. However, when the OTP is generated by an application, the verification can be attempted multiple times in the one minute interval, which prompts to a small, but risk-exposing probability of bypassing the security layer.

The proposed implementation of 2FA on the platform relies on imposing phone number ownership verification for each platform account; when the user tries to set a new password, the identity will be confirmed only when the received code matches the one on the server. When several successive incorrect OTPs are being received, the account will be locked for a determined period of time and a warning email will be send to both the user and the IT department, informing that the account has been locked due to suspicious activity.

Another concerning problem identified by the FTA is the vulnerable passwords chosen by the user, given that complex password combinations are easy to forget, and that 53% of people rely on their memory to remember passwords [8]. First vulnerable category are the ones of low complexity that can be easily cracked, such as having less than 8 characters or consisting only of letters or numbers in a predictable order (E.g. "12345" or "qwerty"). The second circumstance is when it contains the username or any other personal information about that user that is publicly available and easy to uncover such as birthdate, spouse name, pet name, graduated college, workplace etc. Last situation when a password is believed to be weak is whether it is encountered on the online resources that contain credentials disclosed during cybernetic attacks [9] or extremely common passwords (E.g. "Password1", "Mypass1234", "Admin123", "Password1234").

The designed solution prevents the user from setting a compromisable password combines the resolutions for each of the described scenarios. At first, the passwords will be constrained to be of eight characters length, having at least one lowercase, at least one uppercase, at least one number and at least one special character. If the password passes this validation, it will be sent to the server in order to verify if it contains any trace of personal information associated to that account. If the password does not include predictable information, it will be compared against a database of stored passwords that were leaked online; the server will compute a percentage to decide how similar the combination chosen by the user is to any entry in the persisted data. If the percentage is smaller than 30%, the password is considered secure and associated with the account, the user is redirected to the home page. Otherwise, the password will not be set and the user will be informed which requirement was not fulfilled, followed by a suggestion based on that reason.

The password database for reference will be updated periodically or in case of major cybernetic attacks. Additionally, on the mentioned events, a script will be run, hashing any new entries and comparing them with the stored user passwords, and if any of them are a match, the associated accounts will be blocked and warning email notifications containing the quarantine justification and the URL for password reset will be sent.

From the user's experience perspective, requiring an OTP on each authentication is considered to be disruptive behaviour. Thus, it was opted for a less intrusive approach in the form of IP comparison between the last known one for that specific user, and the one from the current request.

If not identical, user will be prompted to the next screen to confirm his identity by typing in the OTP sent to the phone number associated to the account. If there will be more than three incorrect attempts from the user, the account will pe locked and emails will be sent to both the user and the IT department with the quarantine reason; the user will also be guided through the necessary steps to change the account password.

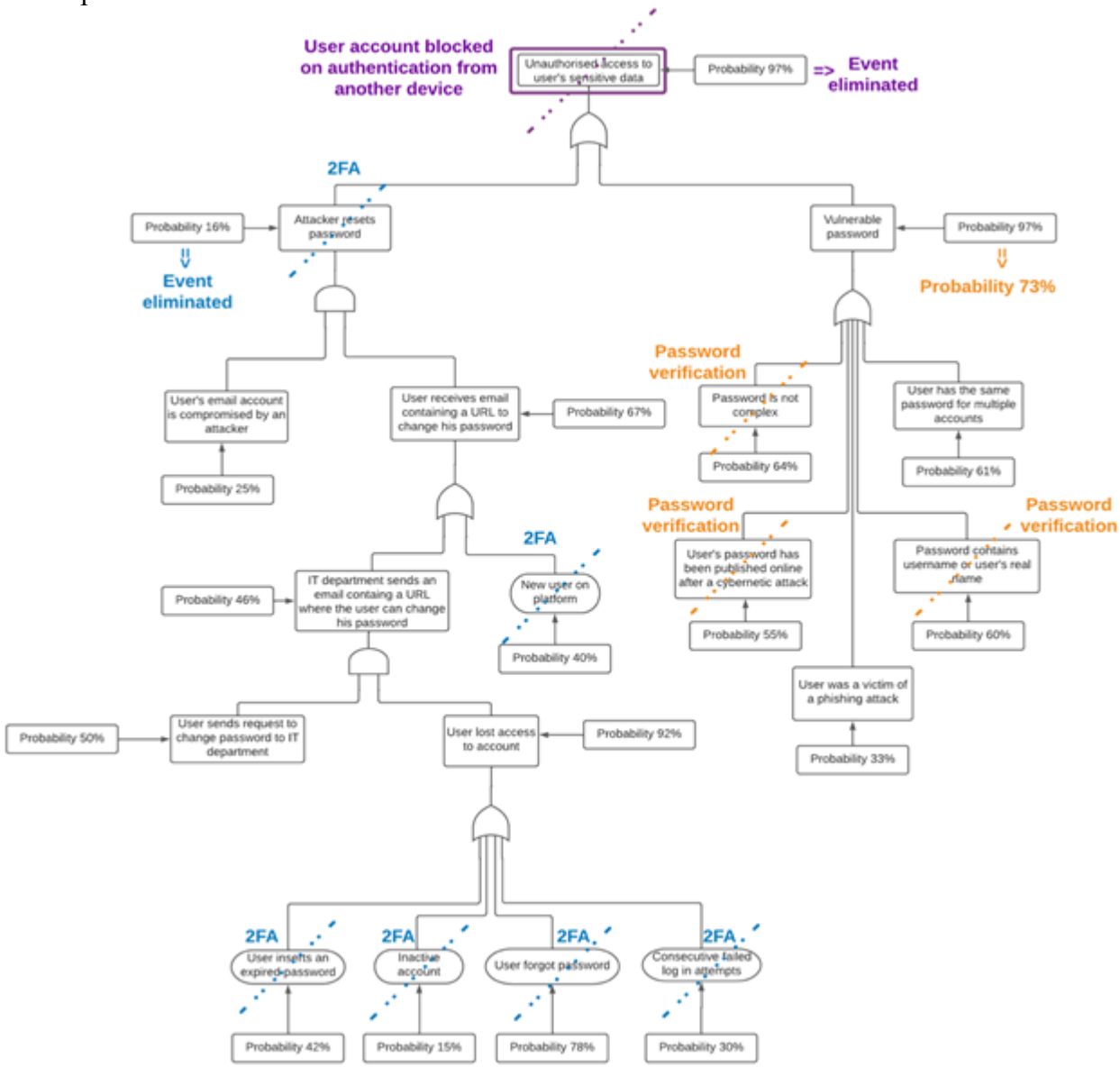

Fig. 2. Enhancement results

5. Conclusions

In the last couple of years there has been a significant increase in cybernetic attacks, as the COVID-19 pandemic has forced the business digitalization to spread all around the world. This has exposed hidden vulnerabilities in the cloud platform infrastructures and the inadequate investment in cybersecurity awareness training for employees, causing unwarranted "costs to the global economy of about $1 trillion — 50% more than predicted in 2018" [10].

This paper conducted a Fault Tree Analysis on a modern cloud platform and it revealed several design vulnerabilities that could leave users' personal data exposed to cybernetic attacks. The first issue was discovered in one of the most important business flows, set or reset password. The main cause is the large percentage of compromised email accounts and, if the reset password URL sent to such a compromised account, will allow an attacker to set the platform account password prior to the

user. The implemented solution was a 2FA integration, which confirms the user‘s identity. If there is suspicious activity, the account will be blocked and the user and the IT department will be notified, eliminating the possibility of an attacker to take control of a user’s account.

The second problem identified by the FTA was the usage of noncompliant passwords: low-complexity passwords, that are vulnerable on brute force attacks, predictable passwords that contain information that is publicly available or passwords that have been disclosed online during previous cybernetic attacks. The chosen prevention mechanism was to enforce a higher complexity for passwords, to identify any trace of personal data in the provided password and to compare it to a database containing previously leaked passwords. If the password passes all the checks, the user will be logged in and redirected to the home page. Consequently, the passwords protecting the planform accounts will be stronger and the possibility to be cracked is considerably diminished.

The third addressed vulnerably is the user impersonation by an attacker with the correct credentials. To cover this, the current IP address is compared to the last registered one, and if they do not coincide, the user will be asked to introduce a newly sent OTP. By comparing the IP addresses used to log in, the account owner’s identity is verified and suspicious connections are blocked.

Given the growing interest in cybersecurity, the exponential evolution of hacking tools and the free available documentation that facilitate the activity of both ethical and malicious hackers, platforms need to be prepared for cybernetic attacks and to implement preventive fail-safe mechanisms against phishing and social engineering attacks.

References

[1] S. Mandal, D. A. Khan, "A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic," 2020 Int. Conference on Smart Electronics and Communication (ICOSEC), pp. 837-842, doi 10.1109/ICOSEC49089.2020.9215374, 2020.

[2] J. Carson, "3 Top Takeaways from the 2021 Verizon Data Breach Investigations Report," 29 06 2021. [Online]. Available: https://thycotic.com/company/blog/2021/06/29/verizon-data-breach-investigations-report-top-takeaways/. [Accessed 25.02.2022].

[3] Verizon, "Data Breach Investigations Report," 2021. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2021/. [Accessed 27.02.2022].

[4] C. Umbrella, 2021. [Online]. Available: learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list. [Accessed 27.02.2022].

[5] N. Lord, "Uncovering Password Habits: Are Users’ Password Security Habits Improving? (Infographic)," 2020. [Online]. Available: https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic. [Accessed 23.03.2022].

[6] L. Leuthvilay, "New Password Study by HYPR Finds 78% of People Had to Reset a Password They Forgot in Past 90 Days," 2019. [Online]. Available: https://blog.hypr.com/hypr-password-study-findings. [Accessed 23.03.2022].

[7] J. Lapienytė, "Top 5 industries that fall victim to phishing scams," 28.10.2020. [Online]. Available: https://cybernews.com/security/top-5-industries-that-fall-victim-to-phishing-scams/. [Accessed 23.03.2022].

[8] P.I. LLC, "resources.yubico.com," 2019. [Online]. Available: https://resources.yubico.com/53ZDUYE6/as/q3tmql-974v8g-g8llc3/Ponemon_2019_State_of_Password_and_Authentication_Security_Behaviors_Report.pdf. [Accessed 13.03.2022].

[9] Have I been pwned, https://haveibeenpwned.com. [Online]. [Accessed 01.04.2022].

[10] A. Lukehart, "2022 Cyber Attack Statistics, Data, and Trends," 04.01.2022. [Online]. Available: parachute.cloud/2022-cyber-attack-statistics-data-and-trends/. [Accessed 18.03.2022].