University of East London

Pioneering Futures Since 1898

School of Architecture, Computing and Engineering

Module Code: CN7016 2425 (T1)

Module Title: Computer Security

Module Leader: Dr. Tauseef Ahmed
Dr. Athirah Mohd Ramly

Case Study: Security Analysis of SMS as a Second Factor Of Authentication
Author: Roger Piqueras Jover

By:

Student Name: Saurav Gurung
Student ID: u2773653

Contents

Introduction

As per Roger Piqueras Jover's article, "Security Analysis of SMS as a Second Factor of Authentication," the paper discusses security challenges related to cellular SMS-based Two Factor Authentication (2FA). There is maximum usage of this mechanism because it is SIMple to use and available for everyone. SMS-based Two-Factor Authentication (2FA) has numerous drawbacks that impact its trustworthiness in safeguarding valuable online accounts. The man-in-the-middle attack (MITM) on GSM (Global System for Mobile Communication) and LTE (Long Term Evolution) networks is one of these vulnerabilities (Jover, 2020).The vulnerabilities, such as SIM swapping, which allow attackers to transfer the victim's phone number to a SIM card under their control and exploit faults in legacy telecommunication protocols like SS7 (Signaling System No.7) allow for the intercepting of SMS communication.

Apart from that, the report highlights the growing complexity of cyberattacks and their ability to exploit SMS-based multi-factor authentications with the purpose of stealing money or sensitive data. Deploying Two-Factor Authentication (2FA) based on SMS as the primary defense for account security could potentially generate a serious threat. As there is an increase in global cyber threats, the vulnerabilities of SMS-based two-factor authentication are more visible, making it one of the least trustworthy options for safeguarding high-risk accounts. (Chaudhari, no date)
According to the findings of the research, it is essential to make the move to greater powerful authentication methods such as hardware tokens, authenticator applications, or biometrics, which provide a more effective safeguard against modern cyber-criminal activity. This article aims to motivate individuals, organizations, and programmers to implement more reliable and secure methods to protect sensitive data in today's increasingly interconnected society.

Summary

Roger Piqueras Jover's work "Security Analysis of SMS as a Second Factor of Authentication" explores the security drawbacks of two-factor authentication (2FA), a popular technique for strengthening accounts. Although SMS-based 2FA is widely used today because of its readily available infrastructure and user-friendly nature, it does have some significant security and reliability limitations such as SIM swapping attacks, man-in-the-middle attacks, otp delayed delivery, SS7 protocol weakness and more. With the evolving cybersecurity landscape, the study highlights the need to explore safer and more dependable alternatives.

Main Result and Contribution

This paper takes a close look at the weaknesses of SMS-based two-factor authentication, highlighting how issues within cellular networks leave it vulnerable. The main risks include SIM swapping, outdated communication protocols like SS7 (Signaling System No. 7), and man-in-the-middle (MITM) attacks on GSM and LTE networks. Attackers can exploit SIM swapping to take over someone's phone number, allowing them to receive verification codes and break into personal accounts. On top of that, older telecommunication protocols like SS7 do not offer strong protection, making it easier for criminals to eavesdrop on text messages while they are being sent.

By analyzing these weaknesses, the study establishes a technological basis for comprehending the dangers associated with SMS-based two-factor authentication. This highlights that the ongoing use of this authentication approach exposes users to sophisticated cyber threats, especially for accounts containing sensitive or high-value information.

This study points out the challenges of SMS-based two-factor authentication, which many people still rely on despite its risks. It takes a closer look at how attackers exploit weaknesses in cellular networks and outdated protocols, making it easier to understand the vulnerabilities in this system and their real-world impact.

The paper also emphasizes the need to step up cybersecurity practices by recommending more secure alternatives, such as app-based authenticators, biometric verification, or hardware security tokens. These options are less reliant on vulnerable cellular networks and are better equipped to defend against modern cyber threats. The article looks at the weaknesses of SMS-based 2FA and encourages using stronger authentication methods. It is a helpful resource for cybersecurity experts, researchers, and organizations working to make their systems more secure and keep up with changing threats.

Support for the Conclusion

With enough data and rational analysis, the study fairly supports its findings. It uses technical descriptions of cellular communication systems, including SS7, which lacks contemporary security protections, thereby providing an easy target for intercepting SMS messages. Real-world examples support the actual viability of SIM switching attacks by showing how attackers control telecom carriers to reroute phone numbers. These revelations support the author's assertions on the shortcomings of SMS-based 2FA very strongly.

The report makes suitable and dependable use of the tools and statistics. The study is based on knowledge of well acknowledged cellular network protocols and attack strategies in cybersecurity research. The article guarantees trustworthy and well-supported results by referring to both technical research and recorded occurrences of violations. The argument is strengthened even more by the reliance on recognized flaws in GSM and LTE networks as these are accepted shortcomings of the sector. This research explains the challenges of using SMS-based two-factor authentication, which many people still rely on despite its risks. It takes a closer look at how attackers take advantage of outdated technology and weaknesses in cellular networks, showing the real-world impact of these vulnerabilities.

The study shows the importance of improving end-point privacy by promoting safer practices for two-factor authentications like hardware security, biometrics methods or one-time token authenticators. These authentication mechanisms provide better security against cyber risks related to multi-factor authentication on mobile network systems which are more vulnerable.
This essay addresses the issues with two-factor authentication using SMS and suggests using better ways to prove who you are. To keep the system safe from any kind of cyber difficulties, IT professionals, big tech companies, and schools should keep their system up to date against new threats.

New Learnings

The paper provided important insights into how deeply embedded vulnerabilities in mobile communication networks may harm SMS-based two-factor authentication. The analysis of the SS7 protocol shows that its implicit trust model may enable attackers to steal authentication codes from miles away. In a similar way, the specifics of SIM-swapping attacks show how hackers trick telecom service providers to access the unauthorized accounts. The research also talks about non-technical attacks, like social engineering, where attackers trick customer service centers to commit large-scale fraud. The article explains the creation of security issues due to technical flaws and weak procedures and highlights the need for proper strategy to protect users and accounts. The paper reveals the procedure of attackers gaining access to cellular networks like SIM swapping and outdated protocols like SS7 could be vulnerable and allow attackers to steal authentication codes and authorize into accounts. To prevent accounts from being compromised, there should be proper security systems which should be improved along with the findings of new security weaknesses.

Critique

Evaluation of Argument

Before critically evaluating the arguments from the article, let us break the evaluation into two sectors, i.e., strengths of argument and weakness of argument.

Strengths of Arguments

The research article provides deep information related to the importance of multi-factor authentication systems embedded in an online account. It highlights the security and vulnerabilities which are possible with both the SMS-based and one-time token applications of two-factor authentication mechanisms. The article introduces the attention to the real-world issues that should be minimized to enhance cybersecurity. The article highlights the risk which could be generated using SMS-based multi-factor authentication like SIM swapping, MITM attacks on GSM/LTE protocols and traffic interception on SS& protocol. The article addresses wide flawed authentication method used in our daily life. It shows the attention toward the critical area of technology where many individuals and enterprises are still using the mechanism which could make the system or environment vulnerable in the future. The article suggests alternatives for the SMS-based two-factor authentication like app-based authenticator, biometrics used for authentication or some secure but costly authenticators such as hardware security tokens used in high tech enterprise level named RSA keys, Yubi key and many more. The article suggests aligning the security industry trends and securing best practices for improving the authentication mechanism for multi-factor authentications.

Weakness of Argument

The article totally focuses on the weaknesses of SMS-based 2FA, neglecting its advantages such as accessibility and ease to use for non-technical users. The research paper provided only slight alternatives to SMS-based 2FA. There could also be flaws in the alternatives which are provided in the article. For example, for app-based 2FA there will be a dependency on smart phones, there could be a risk with biometrics spoofing and the cost of the hardware tokens are expensive which could never be affordable for regular users. There is a lack of proper statistical data regarding flaws related to SMS-based 2FA. There is a high chance of challenges while implementing from old mechanisms to new complex authentication mechanisms. The article lacks focus on non-technical vulnerabilities such as social engineering or phishing attacks which may also compromise the robust modern authenticators. Even if the article recommends the modern 2FA in the place of SMS-based authentications, it is not an innovation for now. There are millions of people using app-based 2FA which limits this article from its originality.

Unsolved Problems

There are different problems that remain unsolved for SMS-based two-factor authentication.

Lack of secure implementation of SMS-based 2FA alternatives

While the paper points out the flaws in SMS-based two-factor authentication (2FA), it does not address the challenges of implementing or the potential risks of alternatives like hardware tokens, biometric systems, or app-based authenticators.
This makes it unclear if these options are realistic or practicable in varied circumstances, especially in low-resource or technological areas.

Poor awareness of social engineering and user behavior

The paper focuses on technological weaknesses but fails to discuss how human factors like phishing and social engineering may compromise even the most secure authentication methods.
This limitation is crucial since human mistakes typically occur because of security vulnerabilities, making the research less complete.

Limited exploration of cellular network dependencies

The paper questions the dependence on cellular networks for SMS delivery but does not provide specific ways to lower or remove this reliance for consumers without access to consistent internet connections for app-based approaches.
This is a major problem as it influences customers in rural areas difficulty in switching from SMS-based authentication.

Emerging threats in 5G networks

Although the study briefly covers 5G protocol weaknesses, it does not assess how these may affect 2FA system security in the future.
Understanding the security context for 5G networks is essential for predicting and tackling future difficulties in mobile communication.

Lack of industry-wide standards

The document does not address the lack of industry- and region-wide secure 2FA standards.
This difference highlights the difficulty of adopting security standards measures in an international digital economy.

Future Research Directions

The article highlights different gaps in the current implementation and security of SMS-based two-factor authentication mechanisms, and there are few ideas which could help to tackle these gaps in future.

Deploying secure and accessible alternatives to SMS-based 2FA

The alternatives should be secure, user-friendly, and cheap compared to SMS, such as app-based authenticators.
This approach will reduce cellular network dependency and provide safe authentication.

Examining 5G network security

There should be proper research regarding new emerging 5G network's vulnerabilities and capacities for authentication mechanisms.
This research could stop upcoming networks like 5G acquiring LTE and SS7 protocol's vulnerabilities by recognizing and identifying newer risks.

The impact of human behavior and social engineering

This research should focus on human behavior and social engineering strategies like phishing attacks that hamper bypass authentication systems.
The study could result in the development of enhanced security 2FA mechanisms.

Implementing international 2FA standards

The research should develop a security standards framework which should be internationally accepted by 2FA mechanisms developers. This security framework must offer security, usability and accessibility.

Implementing this standard can reduce the errors and weaknesses to develop general trustworthiness of two-factor authentication mechanisms.

Discussion of Similar Problems

Comparison with Similar Research

The article critically analyzes the SMS-based two-factor authentication (2FA). SMS-based authentication can be attacked in numbers of ways which make it vulnerable to accounts even though it is used widely because it is easy to use. The article also explains the vulnerabilities like SIM swapping, SS7 protocol exploitation and Phishing Attacks.
According to Jessa Mikka Convocar, there are several key findings for SMS-based authentication like highly vulnerable to different attacks, weakness in SMS-2FA could lead to unauthorized access to accounts, and it has recommended alternatives like authenticator apps, biometric and hardware tokens against modern cyber threats.
The article has also highlighted some of limitations like implementation challenges faced during the migration from SMS-based 2FA to alternatives, user adoption barriers and accessing with biometrics in rural areas or old smartphones could have some limitations. Convocar (2023)

According to the authors of this article, there are several key findings like the long delay to send One-Time-Password (OTP), SS7 and SIM swapping attacks, SOS (SMS OTP Security) uses authenticated key exchange (AKE) mechanism and the usability of SOS remains same as traditional SMS-based 2FA.
There are several limitations highlighted in this article, like there are multiple occurrences for this delay, which may be bad network coverage, a lot of network traffic, SMS service provider defects, or cellular service provider defect. The article describes problems raised with delay on receiving OTP to customers which could lead to OTP expiration, unsuccessful transactions and rise in the user's frustration. The study addresses the weakness of SMS as a communication tool which includes its dependence on a reliable network and SMS queuing mechanism for message delivery. In conclusion, SMS-based 2FA is a popular and easily accessible mechanism but it calls the security issues and development of more secure alternatives are required for authentication solutions.(Peeters et al., 2022)

Reference

Chaudhari, A.S. (no date) ‘Security Analysis of SMS and Related Technologies Master’s Thesis’. Available at: https://pure.tue.nl/ws/files/46916565/840165-1.pdf (Accessed: 18 December 2024).

Convocar, J.M. (2023) *Why You Should Stop Using SMS Two-Factor Authentication [Updated 2023]*. Available at: https://www.itsasap.com/blog/why-stop-using-sms-2fa (Accessed: 12 December 2024).

Jover, R.P. (2020) ‘Security analysis of SMS as a second factor of authentication’, *Communications of the ACM*, 63(12), pp. 46–52. Available at: https://doi.org/10.1145/3424260.

Peeters, C. *et al.* (2022) ‘SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication’, *ASIA CCS 2022 - Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security*, pp. 2–16. Available at: https://dl.acm.org/doi/pdf/10.1145/3488932.3497756 (Accessed: 12 December 2024).