International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

Two-factor Authentication through Flash Calls: Technical and Economic Analysis

Borovikov Evgeny*

Head of DevOps, HFT Fund (under NDA), Dubai, UAE

Email: borovikov.ea@gmail.com

Abstract

This study explores flash call verification as an innovative approach to two-factor authentication (2FA), addressing modern security and cost-efficiency challenges. The research examines the theoretical foundations and technical implementation of flash call authentication, comparing it against conventional SMS-based methods. The proposed methodology utilizes telephone network infrastructure to deliver authentication codes through incoming call numbers, showcasing notable improvements in both security and economic viability. Results indicate that flash calls offer substantial cost savings relative to SMS authentication, while preserving high-security standards through channel isolation. Although the method is particularly relevant for markets with elevated SMS costs, it holds global applicability in diverse digital systems. By providing a comprehensive analysis of flash call architecture, security mechanisms, and operational benefits, this study contributes new insights into scalable and cost-effective 2FA solutions.

Keywords: two-factor authentication; flash calls; telecommunication security; digital authentication; voice channel security; cryptographic verification; authentication protocols; telecommunications infrastructure; authentication costs; emerging markets security.

1. Introduction

In the modern digital world, ensuring secure user authentication has become critically important. According to Positive Technologies, the number of cyber incidents in the first quarter of 2024 increased by 7% compared to the previous quarter, with data breaches accounting for 72% of incidents involving individuals and 54% involving organizations [1].

Received: 10/2/2024
Accepted: 10/16/2024
Published: 12/25/2024

----

* Corresponding author.

Traditional two-factor authentication methods, such as SMS codes, authenticator applications, and hardware tokens, exhibit several significant limitations. SMS authentication, despite its widespread adoption, is vulnerable to message interception and SIM swapping. Flash calls, proposed in this study as an alternative method, are also susceptible to some of these vulnerabilities, particularly SIM swapping [2]. Hardware-based solutions, while offering a high level of security, create additional barriers for users and require substantial infrastructure investments [3]. Biometric authentication, although an innovative approach to security, often faces challenges related to recognition accuracy and high implementation costs [4].

In the context of emerging markets, particularly in the MENA (Middle East North Africa) region, the search for solutions that combine high security levels with economic efficiency is especially relevant. Flash calls represent an innovative approach to two-factor authentication, where the confirmation code is integrated into the incoming call number, fundamentally differing from traditional methods of delivering authentication data.

The objective of this study is to analyze the technological and economic efficiency of using flash calls as a method of two-factor authentication. The research aims to address the following tasks: evaluate the security and reliability of the method and analyze its cost-effectiveness compared to traditional solutions.

2. Materials and methods

In modern digital systems, access security is ensured through multi-layered authentication mechanisms. The fundamental principle of two-factor authentication (2FA) is based on the combination of two independent factors from three possible categories: "something you know" (passwords, PIN codes), "something you have" (physical devices, phones), and "something you are" (biometric data) [5]. This approach significantly enhances security since the compromise of one factor does not result in the breach of the entire system [6].

The technical process of two-factor authentication relies on secure data transmission protocols (protocols like TLS) and specialized authentication protocols such as TOTP and HOTP [7]. Both TOTP and HOTP use time- or event-based one-time passwords. Security can be enhanced by storing the shared secret on separate authentication devices, such as hardware security keys (e.g., YubiKey) and mobile applications, reducing the risk of unauthorized access. Similarly, the flash call methodology utilizes the telephone network infrastructure (SS7, SIP) to transmit authentication data. While flash calls differ in implementation, all these methods share comparable susceptibilities, such as risks associated with SIM swapping [8].

Table 1: Comparative analysis of SMS and flash call authentication methods

Security Parameter	SMS Authentication	Flash Calls
Resistance to interception	Low (due to inherent vulnerabilities in the SS7 protocol, which allows attackers to intercept or spoof communication)	Low (due to inherent vulnerabilities in the SS7 protocol, which allows attackers to intercept or spoof communication)
Protection against phishing	Moderate	High
Protection against SIM swapping	Low	Low
Reusability of data	Possible (SMS codes can be reused during their validity period for 2FA requests)	Possible (the last digits of a missed call number can similarly be viewed within its validity period)
Complexity of compromise	Moderate	Moderate
Implementation cost	High	Low
Delivery speed	10-30 seconds	1-3 seconds
Transmission protocol	SMS (MAP/SMPP)	Voice (SIP/SS7)

The flash call method represents an innovative approach to two-factor authentication, utilizing the last digits of an incoming phone number (3-5 digits) as a temporary verification code. This method is applied to verify various operations, including banking transactions, registration in digital services, and user identity confirmation [8].

The theoretical security model of flash calls is based on the following principles:

1. Cryptographic randomness: Code generation employs cryptographically secure algorithms to ensure the unpredictability of values [7].

2. Temporal synchronization: Each code has a strictly limited validity period, synchronized with server time [9].

3. Atomicity of operations: Each authentication attempt is treated as an indivisible transaction with a clearly defined state [6].

The methodology for evaluating effectiveness includes an analysis of the following parameters:

- Delivery latency of the authentication code;

- Reliability of the data transmission channel;

- Resistance to various attack vectors;

- Economic efficiency of the solution;

- User experience (UX) metrics [8].

In the context of telecommunications protocols, flash calls leverage the advantages of existing Voice over IP (VoIP) infrastructure and traditional Public Switched Telephone Network (PSTN). This ensures high service availability and the ability to utilize existing telecommunications channels without requiring additional infrastructure deployment [9].

The flash call method also demonstrates an optimal balance between security, usability, and economic efficiency, making it particularly relevant for emerging markets such as MENA At the same time, for example, in UAE the high cost of traditional authentication methods is not a decisive factor due to the country's overall economic conditions. Obtaining local phone numbers for new telecommunication-based services in the UAE can be challenging for startups due to regulatory requirements and restrictions.

3. Results and discussion

The proposed two-factor authentication (2FA) solution based on flash call technology demonstrates notable advantages compared to traditional SMS-based methods. This approach relies on a short “instant” voice call, where the verification code is embedded directly into the Caller ID. As a result, it achieves both cost reduction for the business and enhanced protection against attacks involving SMS interception [2,6,13]. Successful large-scale implementation requires a comprehensive approach that includes a microservices architecture, cryptographically secured code generation, and robust interaction with telecommunications networks.

Within this research, we have analyzed the structural features of the proposed 2FA system, focusing on its architecture (Figure 1) and the functionality of its key components. The foundation rests on a microservices model, where each module (code generation, telephony, validation, etc.) operates independently [8,10]. For clarity, the main technical characteristics of system modules are summarized in Table 2, providing an overview of potential implementation choices.

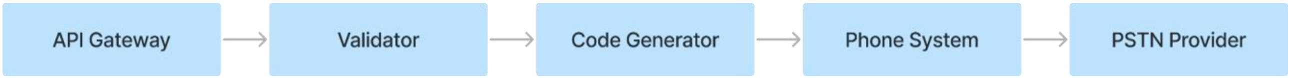

Figure 1: Flash Call System Architecture

Table 2: Technical Specifications and Possible Implementations of the Flash Call 2FA System

Component	**Basic Requirements**	**Additional Features**	**Implementation Options**
API Gateway	- REST/HTTPS as a single entry point - Rate limiting - JWT authentication	- Role-based security model - Multiple API version support	- **Kong, Nginx**: ready-to-use gateways with plugin flexibility [10] - **Custom gateway**: custom-built for specific business logic
Code Generator	- Cryptographically secure pseudorandomness (CSPRNG) - TOTP model with a limited lifespan - 3–5 digit verification codes	- Adaptive logic (context-aware, e.g., geo data, device ID) - Replay attack prevention	- **Simple PRNG**: basic .NET or Java generator - **Crypto libraries**(OpenSSL, etc.), utilizing hardware RNG [7]
Telephony	- SIP/SS7 infrastructure - Multi-operator routing - Large phone number pools (hundreds to thousands of lines)	- Automated carrier selection based on QoS/cost - Load balancing across voice call routes	- **SIP Providers** (Twilio, Infobip) - **Custom VoIP gateway** (Asterisk, FreeSWITCH) with direct integration into operator networks
Validation Module	- Caller ID comparison within a limited time window - Transaction atomicity	- Hybrid checks (flash call + fallback SMS/push) - Context-based validation (geo location, timestamp)	- **Standalone microservice**: stores session data in Redis - **Integration**with frameworks like Spring Security, ASP.NET Identity
Monitoring	- Real-time tracking of latency and success rate - Authentication attempt logging	- Alert systems and dashboards (Prometheus, Grafana) - ML-based anomaly detection	- **Prometheus + Grafana** - **ELK stack** (Elasticsearch, Logstash, Kibana) [2] - **Cloud-based** solutions (AWS CloudWatch, Azure Monitor)
Containerization	- Orchestration of microservices (Kubernetes, Docker Swarm) - Automatic scaling	- Potential serverless approach for unpredictable load	- **Docker/Kubernetes** [10,11]- **FaaS platforms** (AWS Lambda, Azure Functions)

One of the central benefits of flash call authentication is its reliance on voice telephony instead of SMS. Each inbound call corresponds to a cryptographically generated code, valid only within a short time window [7]. The likelihood of replay attacks is further minimized by an atomic verification model, where each authentication attempt is treated as a distinct, indivisible transaction [9]. Additionally, monitoring services detect and mitigate anomalies such as sudden traffic spikes or suspicious routing configurations [2].

Amid rising tariffs for Application-to-Person (A2P) SMS, numerous industry players are seeking alternative 2FA solutions [12,13]. Flash call can reduce authentication costs by an average of 40–60% compared to traditional SMS, as noted by multiple CPaaS providers [13]. This cost advantage becomes especially evident for businesses processing millions of transactions monthly, where SMS can quickly escalate into a major operational expense.

Sample Calculation (global scale):

- Let the average A2P SMS cost be $0.03. At 1 million authentications per month, the monthly bill is $30,000.
- In many regions, flash call can be up to twice as economical, potentially saving tens or even hundreds of thousands of dollars annually.

Transitioning to flash calls requires an upfront investment (CAPEX) in phone number pools, along with negotiating SLAs with one or more telecommunication providers. However, at higher transaction volumes, the approach often leads to favorable TCO (Total Cost of Ownership) [12].

The evolution of flash call authentication has quickly spread worldwide. According to industry forecasts, flash call volumes for verification could reach hundreds of billions in the near future [12,13]. This technology transcends regional limitations, making it broadly relevant wherever there is high demand for secure, cost-effective, and fast identity confirmation.

Beyond cost savings, flash call also improves delivery speed (1–3 seconds) and offers a seamless user experience: Many mobile OS platforms (particularly Android) can automatically read the final digits of a missed call, eliminating the need for manual code entry [8]. Nevertheless, large-scale projects must carefully manage call routing and phone number pools to balance load distribution and reduce the risk of carrier blocks.

The results of this study indicate that flash call authentication can capture a substantial share of the 2FA market. Its main strengths include significant operational savings over A2P SMS, faster code delivery, and enhanced security through channel separation [4,7,8]. Coupled with a microservices architecture (see Figure 1 and Table 2), which supports smooth scalability and integration, flash calls cater to diverse services ranging from online banking to e-commerce and social platforms.

Areas for future development include:

1. Refined Financial Modeling: A more detailed cost-benefit analysis (TCO) that accounts for phone number rental expenses, CAPEX, and OPEX [3,12].
2. Expanding Functionality: Integrations of flash call with other 2FA methods (e.g., push notifications) to

provide hybrid scenarios [8].

3. Enhanced Usability: Comprehensive UX studies aimed at reducing user drop-off and optimizing automatic code reading [2].
4. Stronger Telco Partnerships: Direct agreements with SIP providers and operators to ensure top service quality and prevent large-scale blocks [9,12].

In summary, flash call stands out as a flexible and universally applicable 2FA method that has been steadily gaining trust among global digital services and operators. Combining strong security, low latency, and financial benefits, it offers a viable alternative in an era marked by escalating A2P SMS fees and stricter requirements for secure user verification.

4. Conclusion

Analysis of flash call authentication indicates the potential for a paradigm shift in two-factor security methods, where reduced operational expenses are balanced with robust protective measures. The research confirms that leveraging telephone networks as an authentication channel can significantly improve the overall efficiency and reliability of digital transactions.

Moreover, the versatility of flash call technology suggests broad applicability: organizations worldwide can adopt this solution to mitigate the rising costs associated with traditional SMS-based 2FA. The findings highlight the importance of further investigations into integrating flash calls with emerging security technologies and protocols, potentially yielding hybrid authentication models that consolidate multiple protective layers for enhanced resilience. By extending the scope of this methodology, future work could accelerate the global adoption of more secure, cost-effective strategies for user authentication.

References

[1]. Current Cyber Threats: Q1 2024 //Positive Technologies, 2024. [Electronic resource]. Available at : https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (date of access: 11/19/2024)

[2]. Ibrahim T. M. et al. Recent advances in mobile touch screen security authentication methods: A systematic literature review //Computers & Security. – 2019. – T. 85. – pp. 1-24. https://doi.org/10.1016/j.cose.2019.04.008

[3]. Suleski T. et al. A review of multi-factor authentication in the Internet of Healthcare Things //Digital health. – 2023. – Vol. 9. https://doi.org/10.1177/20552076231177144

[4]. Ekpezu A. O. et al. Biometric authentication schemes and methods on mobile devices: a systematic review //Modern Theories and Practices for Cyber Ethics and Security Compliance. – 2020. – pp. 172-192. https://doi.org/10.4018/978-1-7998-3149-5.ch011

[5]. Velásquez I. Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication //Clei Electronic Journal. – 2021. – Vol. 24. – No. 1. – P. 29. Available at: https://www.google.com/url?q=https://clei.org/cleiej/index.php/cleiej/article/download/485/392&sa=D

&source=docs&ust=1739435524855203&usg=AOvVaw2-Bn7-dCnWRzD7aLU0jIZP

[6]. Barkadehi M. H. et al. Authentication systems: A literature review and classification //Telematics and Informatics. – 2018. – Vol. 35. – No. 5. – pp. 1491-1511. Available at: https://www.academia.edu/download/58659909/Authentication_systems_SAR.pdf

[7]. Samy M. A. et al. One-Time Password Authentication Techniques Survey //Data Mining and Knowledge Engineering. – 2017. – Vol. 9. – No. 4. – pp. 69-78. Available at: https://www.ciitresearch.org/dl/index.php/dmke/article/view/DMKE042017001.

[8]. Fneish Z. A. A. M., El-Hajj M., Samrouth K. Survey on iot multi-factor authentication protocols: A systematic literature review //2023 11th International Symposium on Digital Forensics and Security (ISDFS). – IEEE, 2023. – pp. 1-7. https://doi.org/10.1109/ISDFS58141.2023.10131870

[9]. Omas-As, R., Teleron, J. Enhancing Network Security: A Robust Network Access Control and Authentication Mechanism for Secure Data Transmission. International Journal of Advanced Research in Science, Communication and Technology, 2023. – Vol. 3. – No. 1. – pp. 182-187. https://doi.org/10.48175/ijarsct-14023.

[10]. Use API gateways in microservices //Learn Microsoft, 2024. [Electronic resource]. Available at: https://learn.microsoft.com/en-us/azure/architecture/microservices/design/gateway (date of access: 11/19/2024)

[11]. Make secure .NET Microservices and Web Applications //Learn Microsoft, 2023. [Electronic resource]. Available at: https://learn.microsoft.com/en-us/dotnet/architecture/microservices/secure-net-microservices-web-applications/ (date of access: 11/19/2024)

[12]. Global Mobile Authentication Market: 2023-2028, 2023. [Electronic resource]. Available at: https://www.juniperresearch.com/research/telecoms-connectivity/messaging/mobile-authentication-research-report/ (accessed: 26.11.2024).

[13]. Kamra J. Flash Calling: The cheaper, faster alternative to SMS verification, 2024. [Electronic resource]. Available at: https://www.symbio.global/resources/flash-calling-sms-alternative (accessed: 26.11.2024).