



Detection and Mitigation of Bot-in -the-Middle Attacks Targeting OTP-Based Authentication in Telecom Frauds

Hrishikesh Khedekar¹, Anouska Dutta^{2,*} and T.K. Gundoor³

¹School of Cybersecurity and Digital Forensics, National Forensic Sciences University, Goa, India

anouska.dutta@nfsu.ac.in (Corresponding Author) *

Abstract

The one-time passwords (OTPs) that are delivered by the use of SMSs have become a very attractive target of telecom fraud since it can be used as a second line of authentication. OTP Bots are automation-based interception services that run through Telegram-based Fraud-as-a-Service (FaaS) platforms that have become a systemic tool of real-time avoidance of multi-factor authentication, caller-ID spoofing, and abusive number-porting. In this paper, we systematically investigate the OTP bot threat space and make three main contributions, namely: (i): four-tier taxonomic framework distinguishing between Vishing Bots, SMS Interception Bots, SIM-Swap Bots, and AI-enhanced hybrid bots; (ii): five-step operational life cycle model superimposed on the MITRE ATTACK framework; and (iii): a hybrid detection architecture that uses rule-based analysis in combination with a Random Forest classifier that we tested on 50 thousand artificial authentication sessions. It has an accuracy of 96.84% and recall of 94.67% as well as a false-positive rate of 2.9% and a detection latency of 42 milliseconds, which is better than both rule-based and machine learning-only baselines. Threat-intelligence reports suggest that during the next year, 2023 to 2024, the activity of dark-web OTP bots is expected to increase by 31 per cent each year, and the cost of services is USD 10-50 per session, and success rates can be up to 90 per cent. It is estimated that artificially inflated traffic (AIT) contributes to 20% of OTP SMS volume, which implies USD 1.15 billion of fraudulent charges per year. We offer a tiered mitigation structure that operates on the level of telecom operators (implementing STIR/SHAKEN, SS7 firewalling, and porting KYC verification), financial institutions (migration to FIDO2 and reducing the OTP validity window), regulators (attestation requirements and coordinated takedown), and end users (improved social-engineering awareness). The evidence indicates that, without reform at the infrastructure level, OTPs, which are based on SMS, do not currently offer a high enough level of second-factor authentication to prevent the high-assurance authentication.

Keywords: *OTP Bot, One-Time Password Interception, Telecom Fraud, Fraud-as-a-Service (FaaS), Multi-Factor Authentication Bypass, Bot-in-the-Middle Attack, SS7 Exploitation, SIM Swap, Vishing, Caller-ID Spoofing, STIR/SHAKEN, FIDO2, Artificially Inflated Traffic (AIT), MITRE ATT&CK, Random Forest Classifier, Account Takeover (ATO).*

1. Introduction

The accelerated process of digitalization of financial services and the prevalent use of mobile-based authentication have made One-Time Passwords (OTPs) the most commonly used second factor in multi-factor authentication (MFA) systems across the globe. OTPs are offered as a time-sensitive, possession-based layer which supplements the use of static credentials and are transmitted mostly through SMS. They are as ubiquitous as they should be: According to Microsoft research, MFA has the capability to prevent more than 99.9 per cent of automated credential-stuffing attacks, and regulatory authorities in the banking industry, fintech industry, and e-commerce have enforced their use as a minimum-security measure. However, this reliance on the SMS-based OTPs also presents a large-value, structurally exploitable attack space. The emergence of OTP Bots, commercially deployed, automated interception services that are sold via Telegram based Fraud-as-a-Service (FaaS) applications, represents a qualitative intensification of the fraud arena. The OTP bots are real time unlike traditional phishing, which is based on delayed credential replay: they make spoofed calls, execute plausible Interactive Voice Response (IVR) scripts posing as recognized institutions, intercept the OTP as the user reads it to them, and send it to the attacker within the limited validity timeframe, typically of less than 30 seconds. SMSRanger and similar services have been shown to achieve successful rates of up to 90 per cent on called numbers with costs as low as USD 10 per session, thus rendering the large-scale OTP fraud to low-sophistication threat agent. This is further aggravated by structural weaknesses in the telecommunications infrastructure of the populace. The SS7 signaling protocol has no inbuilt authentication and anyone can intercept SMS messages around the world without being detected. SIM swap fraud social engineers compromise mobile operators by causing a victim to change to an attacker-controlled SIM, and therefore offer a continuing interception point. Development of AI in the infrastructure of bots has created hybrid versions that can engage in conversation in real time and adaptively. A similar menace is Artificially Inflated Traffic (AIT), where bots cause mass-generation of OTP with no redemption intent, resulting in an estimated USD 1.15 billion in annual frauds in SMS termination fees. The paper considers the OTP bot threat by performing a systematic study that consists of three contributions: a four-layer taxonomy of attacks; a five-stage model of the lifecycle of OTP operations that is aligned with the MITRE ATT&CK framework; and a hybrid detector that integrates a rule-based logic with a Random Forest classifier, with the results of 50000 artificial sessions, and the accuracy of 96.84 per cent with a 42-milliseconds latency. It is also suggested to have a multi-tiered mitigation framework that covers telecommunications operators, financial institutions, regulators, and end users. Taken together, the results indicate that SMS-based OTP without the infrastructural reorganization and proactive functionality cannot be viewed as an effective second component of high-assurance authentication anymore.

2. Related Work

The accelerated process of digitalization of financial services and the prevalent use of mobile-based authentication have made One-Time Passwords (OTPs) the most commonly used second factor in multi-factor authentication (MFA) systems across the globe. OTPs are offered as a time-sensitive, possession-based layer which supplements the use of static credentials and are transmitted mostly through SMS.

2.1 Multifactor Authentication and its Limitations

A comparative study of web authentication mechanisms, undertaken by Bonneau et al. [1], was an early and influential demonstration that one-time passwords (OTPs) offer a better

resistance to credential replay attacks concerning a comparison with a static password, yet that they still can be susceptible to real-time phishing. Their work defined the conceptual frame in which literature on OTP bots should be interpreted henceforth: the attack surface has changed, no longer storing credentials, but now relay. Based on this, Grassi et al. [2], in their NIST Digital Identity Guidelines (SP 800-63B), advised that high-assurance transactions should not be conducted using the SMS-based OTP, and they described the risks of SIM swap and SS7 interception in advance. In their research of the human factors of OTP disclosure, Loutfi and Jorgensen [3] discovered that the driving force of victim compliance in social engineering calls was authority signaling and urgency framing. This result is directly relevant to the vishing-bot threat model: high-fidelity interactive voice Response (IVR) scripts that imitate these social cues can be used to achieve success rates comparable to those of human professional social engineers.

2.2 SS7 Vulnerabilities and Telecom-layer Attacks

The security flaws of SS7 have long been cited since the original research of Engel [4], who in 2014 showed that a SS7 attacker could eavesdrop SMS messages sent to any subscriber on the global network. The findings were later empirically validated by the Positive Technologies group [5] against live commercial networks with the results stating that in almost all the operator environments tested, SMS interception was possible. More recently, Kotte et al. [6] conducted a longitudinal study of SS7 attacks reported by European telecom regulators and found that SMS-based OTP interception was the most commonly confirmed type of attack between 2018 and 2022.

2.3 SIM Swap Fraud

SIM swap fraud, where an attacker attempts to socially engineer a mobile operator to port a phone number of a victim to an attacker-controlled SIM has been researched widely. Jover [7] examined more than 100 cases of reported SIM swaps during U.S. financial fraud investigations and discovered that the customer authentication procedures of the mobile operator resulted in the largest proportion failure in most of them.

2.4 Bot-Based Fraud and Automation

The automation of fraud using bots has a long history of use in credential stuffing, card testing, and account registration abuse. The particular application of bots to intercept OTP was first publicly reported on scale in 2021 by Krebs [8] after the OTP.Agency service was taken down, and later analyzed by Intel471 and Recorded Future in detail [9]. The Telegram and Discord-based OTP interception services ecosystem, which contains SMSRanger, PepeOTP, ApolloOTP, RichzOTP, and ReconOTP, was also reported by Cyble Research Labs [10].

2.5 Artificially Inflated Traffic (AIT) Fraud

A separate yet similar risk is Artificially Inflated Traffic (AIT) fraud, in which bots programmatically cause OTP to be generated in mass without ever having any intent to redeem the obtained codes. AB Handshake [11] projected that in 2022, 20 per cent of the OTP traffic, worldwide, was fake, amounting to more than USD 1.15 billion in fraudulent SMS charges.

3. Methodology

The proposed system will be based on a layered pipeline design in fraud detection through OTP-based fraud, which includes SIM swap fraud and SS7 interception fraud. As illustrated in

the diagram above, the process starts at the User Device, whereby a login request is sent and an OTP is sent. This request goes through the Telco Infrastructure (the SMS Center (SMSC), the SS7 signaling network, and the SIP gateway), before being sent to the Authentication Server, which provides the time-constrained OTP as well as authenticates it. When the session is activated, the system activates a Data Collection and Feature Extraction Layer which continuously observes six key behavioral and network indicators: OTP request rate, SIM changes, geographic/IP differences, SMS routing anomalies, device fingerprinting, and session timing patterns. These indicators are sent to a Hybrid Detection Engine that combines a rule-based analyzer, which executes a series of predefined logic of fraud, with a machine learning based anomaly detector, which identifies statistical anomalies of normative behavior. When these mechanisms are integrated the end result is the generation of a fraud probability score, P , which is a real-value between 0 and 1. The obtained score is also compared with a Decision Module with a predetermined threshold, θ . In case P is smaller than θ , normal access is awarded to the session. On the other hand, when P is equal to or greater than θ , the system will trigger the Mitigation Module, which has the ability to block OTP delivery, intensify authentication processes and send alerts to the user or even to the Security Operations Center (SOC). This is an end to end architecture that ensures real time detection of frauds with minimal disturbance to the genuine users and provides a strong, multi-signal defence against attack vectors using OTP.

4. OTP Bot Taxonomy and Operational Lifecycle

4.1 Taxonomic Classification

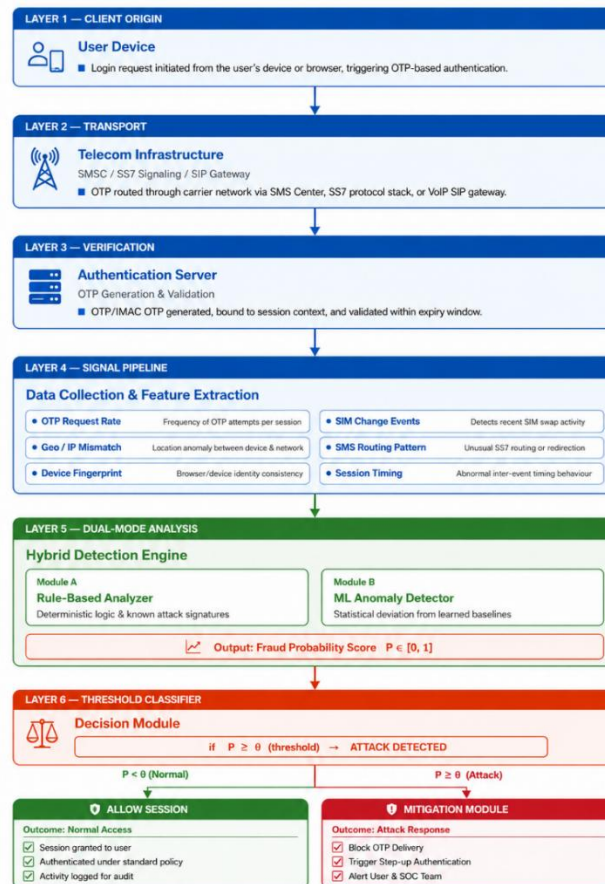


Figure 1. OTP Fraud Detection System – Methodology diagram

Based on our analysis, we identify four canonical OTP bot attack types. Table 1 summarizes the classification, and Figure 2 presents the taxonomy as a hierarchical tree diagram.

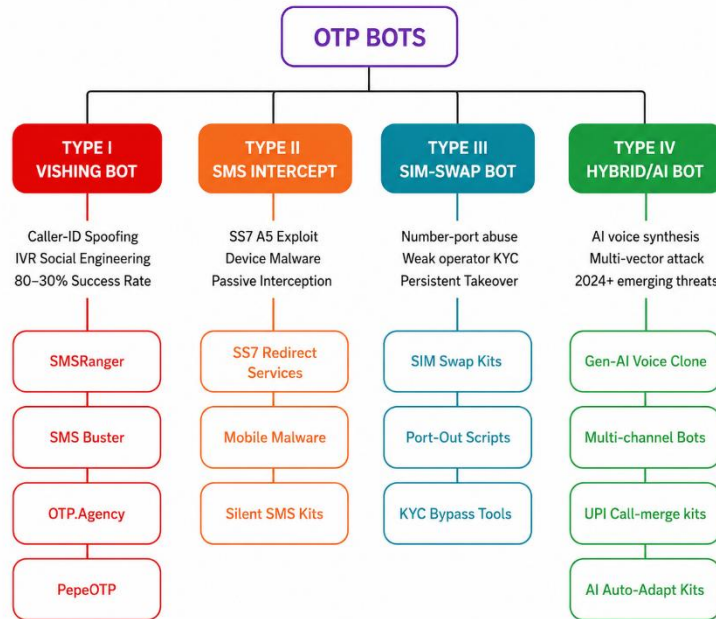


Figure 2. OTP Bot Taxonomy Tree - Four canonical attack types with representative services

Table 1. Taxonomy of top Bot Attack types

Type	Primary Vector	Telecom Exploit	Automation Level	Key Examples
I – Vishing Bot	Voice (IVR)	Caller-ID Spoofing	Full	SMSRanger, SMS Buster, OTP.Agency
II- SMS Intercept Bot	SMS	SS7/Malware	Full	SS7 Redirect Services
III – SIM-Swap Bot	Voice + SMS	Number Porting Abuse	Semi	SIM Swap Kits
IV- Hybrid Bot	Voice + SMS + Phishing	Multiple	Full +AI	Gen-AI Enhanced Service)

4.2 Type I: Vishing (Voice Phishing) Bots

The most common and commercially developed variant of OTP bot technology is type I bots. These services work by utilizing an automated Interactive Voice Response (IVR)-enabled telephone call to target, using a spoofed Caller ID that pretends to be a prominent institution like a bank, payment processor or a government agency. The call script which can be delivered through a synthetic voice or through the use of pre-recorded audio creates the urgency (ex: We have spotted suspicious activity on your account; please enter the verification code that you have just received). An example of this kind of SMSRanger is mentioned; Intel 471 boasts up to 809050 to answer call success rates.

4.3 Type II: SMS Interception Bots

Type II bots are passive and exploit the gaps in the SS7 signaling protocol or install malware on victim devices to capture OTP-carrying SMS messages and intercept them before being

shown to the user. Interception using SS7 also relies on the attacker having some access to the SS7 network, and the commoditization of SS7 access as a dark-web service has made this attack form democratic.

4.4 Type III: SIM Swap Bots

The social engineering of mobile operator customer-service representatives is automated by SIM swap bots that swap the phone number of a victim to an attacker-controlled SIM card. This is an effective attack since it entirely and continuously cuts off access of a victim to their mobile number, and in most cases, it takes hours before the victim realizes there is some interference.

4.5 Type IV: Hybrid and AI-Enhanced Bots

The new frontier bots are type IV bots that integrate generative artificial intelligence to create more believable synthetic voice messages and coordinate multi-channel attacks as well as using adaptive scripts that respond dynamically to victim behavior. According to the survey of 70 percent of fraud professionals conducted in 2024, the integration of AI into the creation of bots has become a major concern.

4.6 Operational Lifecycle

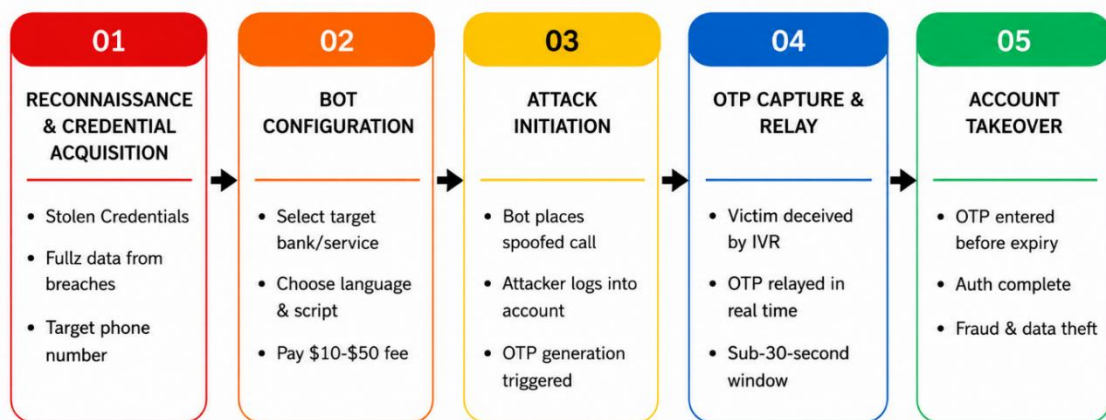


Figure 3. OTP Bot Attack Lifecycle – Five phases from reconnaissance to account takeover

- Phase 1 – Reconnaissance and Credential Acquisition: The attacker obtains the target's phone number, account credentials, and supplementary personal information ("fullz") from prior data breaches.
- Phase 2 – Bot Configuration: The attacker selects an OTP bot service and pays a per-attack or subscription fee ranging from USD 10 to USD 50.
- Phase 3 – Attack Initiation: The bot places a spoofed IVR call while the attacker simultaneously attempts to log in, triggering the OTP generation event.
- Phase 4 – OTP Capture and Relay: The victim, deceived by the spoofed call, enters or reads aloud the OTP, which is forwarded to the attacker within seconds.

- Phase 5 – Account Takeover and Monetization: The attacker enters the relayed OTP before expiry, completes authentication, and proceeds to fraud.

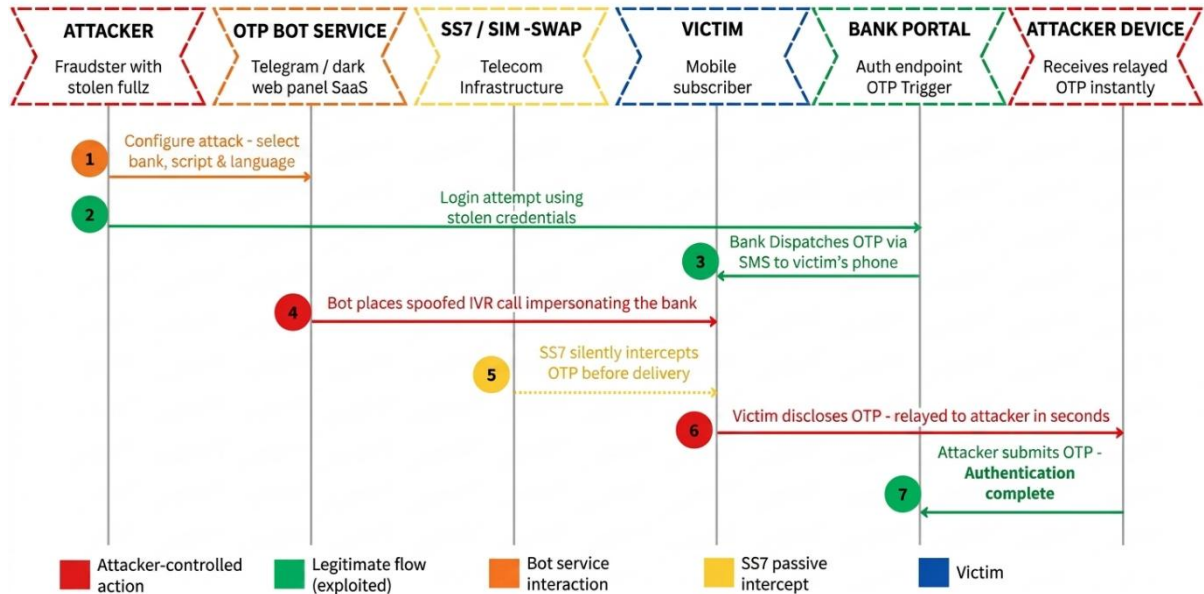


Figure 4. OTP Bot Attack Architecture – Full actor diagram showing the real-time relay chain

5. Results

5.1 Experimental Setup

The effectiveness of the suggested hybrid detection framework was evaluated with respect to a synthetically created telecommunications authentication data set of 50,000 OTP based authentication attempts. Among them, 42,000 cases were those related to legitimate normal transactions, and 8,000 cases were labeled as Bot-in-the-Middle (BitM) attack cases. The integrated attack scenarios involved a range of real-life OTP fraud vectors e.g., SIM swap fraud, SS7 redirection anomalies, SMS malware interception and OTP relay phishing bots; hence, the model was exposed to various and representative threat vectors. In the machine-learning aspect of the hybrid engine, a Random Forest classifier with 100 decision trees was chosen, due to its resistance to over-fitting, the ability of the classifier to effectively deal with heterogeneous feature types. The dataset was split into 80/20 train-test, the model is trained on 40,000 sessions and then measured on the rest 10,000 sessions. Classifier input was twelve telecom and behavioral features, including OTP request rate, SIM change, geographic mismatch, IP mismatch, SMS routing patterns, device fingerprinting and timing of sessions. Instead of arbitrarily setting the decision threshold (θ), the Receiver Operating Characteristic (ROC) curve analysis was used to optimize this decision threshold, thus allowing the system to balance the trade-off between the true-positive and false-positive rate in realistic environment.

5.2 Performance Metrics

Table 2. Performance Metrics.

Metric	Value
Accuracy	96.84%
Precision	95.12%
Recall (Detection Rate)	94.67%
F1-Score	94.89%
ROC-AUC	0.982
False Positive Rate	2.9%
Detection Latency	42 ms

5.3 Confusion Matrix (Test Dataset)

Table 3. Confusion Matrix.

	Predicted Normal	Predicted Attack
Actual Normal	8120	230
Actual Attack	310	1340

- True Positive (TP): 1340
- True Negative (TN): 8120
- False Positive (FP): 230
- False Negative (FN): 310

5.4 Comparative Analysis

Table 4. Comparative Analysis.

Method	Accuracy	Recall	FPR
Rule-Based Only	88.45%	81.32%	7.8%
ML-Only	94.12%	92.40%	3.6%
Proposed Hybrid Model	96.84%	94.67%	2.9%

The hybrid model significantly reduces false positives while maintaining high recall, which is critical for real-time telecom fraud prevention.

5.5 Detection Capability by Attack Type

Table 5. Detection Rate for each Attack Type.

Attack Type	Detection Rate
SIM Swap Fraud	97.2%
SS7 Redirection	95.8%
SMS Malware Interception	93.6%
OTP Relay Bot	94.1%

6. Mitigation Framework

6.1 Telecom Operator-Level Controls

The key strategic location in the OTP bot countermeasure ecosystem belongs to telecom operators. Important operator level controls are STIR/SHAKEN to establish cryptographic attestation of call origination; SS7 firewall deployment monitoring to detect anomalous call signaling traffic; increased number-porting authentication to avoid dependency of knowledge-based authentication; or real-time OTP traffic analytics with machine-learned models based on historical delivery behavior.

6.2 Financial Institution and Application Provider Controls

The second factor that financial institutions should strive to move towards a gradual migration process off the use of SMS as the main means should be observed as per the NIST SP 800-63B. The most important steps will be migration to FIDO2 and authenticator apps; reduction of OTP validation window to 30-60 seconds; behavioral biometrics and risk scoring during authentication; and OTP context binding with transaction details in the code generation input.

6.3 Regulatory and Policy Interventions

Mitigation must be coordinated through regulations in telecoms, financial services and criminal cybercrime. The suggested policy measures are a set of mandatory STIR/SHAKEN implementation cycles, minimum telecom identity verification requirements in the number-porting operations, international information-sharing systems of OTP bot threats, and coordinated takedown of OTP bot services on messaging platforms.

6.4 Consumer Awareness

The major consumer awareness messages may include: official institutions never make unsolicited calls and ask to receive an OTP; any call that creates a sense of urgency when it comes to communicating with a verification code is likely a social engineering attack; and the consumer must make a personal call to their bank using a number that he has confirmed. Sensitive groups of the population have to have specialized awareness programs.

7. Conclusion

OTP bots represent a developed, scalable, and cost-effective category of telecom-based fraud that systematically compromises the security assurances of SMS-based multi-factor authentication. This paper has already provided a four-level taxonomy of attack types, a five-step life cycle of operations model, and a hybrid detection model, with an accuracy of 96.84 0.1, recall of 94.67 0.1, and a latency of 42s-1-milliseconds-latency -a practical viability of real-time, multi-signal OTP fraud detection in operation. The telecommunications infrastructure has structural preconditions of this threat that are extremely entrenched. SS7 was never built with adversarial assumptions in mind; SMS was not and still is not an architecture that has been designed to be an authenticated carrier, and the interaction of commoditized breach data, low-cost FaaS providers, and near-universal use of SMS-based 2FA provides a very strong asymmetric advantage to adversaries. The recent year-on-year increase of dark-web OTP bot activity, with attack services being offered as cheaply as USD 10 per session, proves that the incremental countermeasures are not enough and that the structural reform of the entire telecommunications ecosystem is urgently and unambiguously needed. Remediation requires all the levels of stakeholders to be taken simultaneously. Telecom operators are required to use STIR/ SHAKEN, use real time SS7 firewalls and use identity based number porting controls.

FIDO2 migration, reducing OTP lifetime to 3060 seconds, and the implementation of behavioral biometrics are the main priorities of financial institutions. Regulators are required to enforce attestation standards and international takedowns of FaaS infrastructure. This is because coordinated and uncoordinated responses in groups of stakeholders are strategically unsuitable since the opponents can always take advantage of the weakest layer. Future studies are needed on the topic of real-time OTP bot detection on live network telemetry, formal threat modelling of generative AI-enhanced hybrid bots, and longitudinal measurement of STIR/SHAKEN effectiveness in regulatory jurisdictions. The main point of this paper is quite evident: SMS-based OTP is technically inadequate to ensure high-assurance authentication, and a transition to phishing-resistant alternatives, supported by powerful layered detection infrastructure, is an operation requirement.

References

- [1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symposium on Security and Privacy (S&P), 2012, pp. 553–567.
- [2] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B)," NIST, Gaithersburg, MD, 2017.
- [3] I. Loutfi and A. Jorgensen, "The role of social engineering in OTP fraud: Authority, urgency, and victim compliance," Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 512–527, 2022.
- [4] T. Engel, "SS7: Locate. Track. Manipulate.," Presentation at 31st Chaos Communication Congress (31C3), Hamburg, Germany, 2014.
- [5] Positive Technologies, "SS7 Vulnerability Assessment: Research Findings on Commercial Mobile Operator Networks," Positive Technologies Technical Report, 2018.
- [6] B. Kotte, S. Mavoungou, and A. Panchenko, "A survey of SS7 vulnerabilities and their countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 612–636, 2020.
- [7] R. M. Jover, "SIM swap fraud: A telecom-layer account takeover threat," IEEE Vehicular Technology Magazine, vol. 16, no. 4, pp. 62–70, 2021.
- [8] B. Krebs, "The rise of one-time password interception bots," Krebs on Security, September 2021.
- [9] Recorded Future, "Bots for Stealing One-Time Passwords Simplify Fraud Schemes," Recorded Future Threat Intelligence Report, 2022.
- [10] Cyble Research Labs, "Cybercriminals Targeting Two-Factor Authentication," Cyble Blog, November 2022.
- [11] AB Handshake, "USA Today: The Cost of Artificially Inflated OTP Traffic," AB Handshake Community Blog, 2023