Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20260501025
Volume 5, Issue1 (January-April 2026), PP: 180-182.
www.indjcst.com
ISSN No: 2583-5300

Neutralizing RAT-Assisted Passkey Hijacking via the Visual Password System (VPS)

Aniket Chandramohan Deshpande
Independent Researcher, B.E Electronics and Telecommunications, Post Graduate in Marketing, Pune, Maharashtra, India.

***To Cite this Article**: Aniket Chandramohan Deshpande "Neutralizing RAT-Assisted Passkey Hijacking via the Visual Password System (VPS)", Indian Journal of Computer Science and Technology, Volume 05, Issue 01 (January-April 2026), PP: 180-182.*

Abstract: *As the cyber security industry transitions to Passkeys (FIDO2/WebAuthn), a critical vulnerability has emerged in cloud-synced recovery flows. Current implementations rely on a static Device PIN for synchronization. Our research identifies the "Sync-Infiltrator" exploit, where an attacker uses a Remote Access Trojan (RAT) to capture this PIN, allowing them to bypass hardware-binding and clone a victim's identity onto an attacker-controlled device.The proposed Visual Password System (VPS) is a dynamic authentication protocol that shifts the "Root of Trust" to the user's cognitive space. By utilizing a high-entropy pool of say 54 unique graphical assets, a private mental margin, and hidden "Locker Key" positions, the user ensures that no reusable data is ever typed or displayed. The system effectively neutralizes Phishing and RATs through Proactive Credential Rotation and Visual Masking. This paper introduces the Visual Password System (VPS), a cognitive authentication protocol designed to eliminate reusable secrets and resist RAT-based credential harvesting.*

Key Words: *Passkey Security; RAT Mitigation; Cognitive Authentication; Visual Passwords; FIDO2*

I. INTRODUCTION

Modern authentication relies on "Something You Have" (a device). However, for recovery, these are backed up by "Something You Know" (a PIN) and synced via the cloud. An attacker using a Phishing + RAT combination can monitor the user's screen and record the device PIN as it is entered, intercept account credentials via phishing, and exfiltrate the "Master Keychain" from the cloud to their own device. Finally, they can persist by using the RAT to delete security alerts from the victim's email, completing a total account takeover without the victim's knowledge.

Threat Model: The attacker is assumed to have full remote access to the victim device through a Remote Access Trojan (RAT). The attacker can observe screen activity, capture keyboard input, and attempt credential replay attacks. However, the attacker does not have access to the user's internal cognitive secrets such as the mental margin or locker key positions used in the VPS protocol.

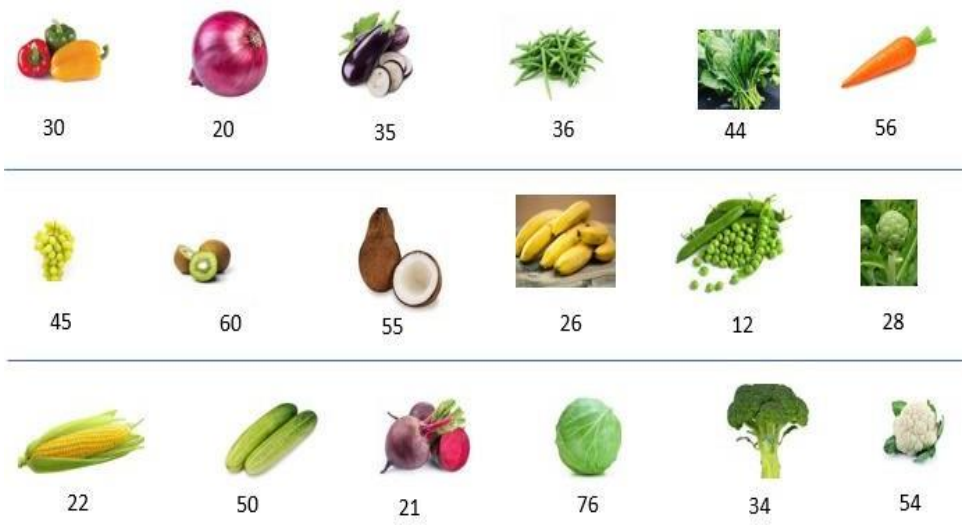
II.MATERIAL AND METHODS

This research proposes the Visual Password System (VPS) to replace static inputs with a dynamic mental challenge. The protocol utilizes a corpus of say 54 unique graphical items (vegetables and fruits).

Procedure methodology
The authentication workflow consists of the following phases:

1. **Secret Selection:** During signup, the user selects four items (e.g., Onion, Potato, Apple, Tomato) and a Mental Margin (e.g., 5).
2. **Randomized Challenge:** During login, only one secret item appears among randomized decoys. Each item is assigned a random session-value.
3. **Mental Calculation:** If "Onion" appears with the value 20, the user mentally adds their margin (5) to get 25.
4. **Positional Entry:** The user enters 2 in secret position A and 5 in secret position D. All other fields (B, C, E, etc.) are filled with decoy noise random numbers. Positions A and D are also selected at signup.

Example:
Login Attempt first screen: User attention will be captured by Onion as it is one of his secret items.



Login Process: Mental Math
Users will see value 20 mentioned beside Onion. Now the user will add his mental margin which is 5.
So, the result will become 5 + 20 which is 25. User will do this mentally.

Login Attempt: Second Screen
User has chosen A and D as is locker key password during sign up. He has to input the result 25 in the places A and D as 2 and 5 as shown in the below table.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
2	3	5	5	9	6	7	2	0	3	2	6	9	7	5

ARCHITECHTURE DIAGRAM

———— REGISTRATION PROCESS ————

[User Registration]
→
[Select Secret Items]
→
[Choose Mental Margin]
→
[Choose Locker Key Positions]

———— LOGIN PROCESS ————
→
[Randomized Grid Displayed]
→
[User Identifies Secret Item]
→
[Mental Calculation]
→
[Enter Digits in Secret Positions]
→
[Server Verification]
→
[Authentication Success]

III.RESULT

The Visual Password System (VPS) incorporates multiple defensive layers designed to prevent attackers from deducing user secrets even in the presence of device compromise:

1. Proactive Credential Rotation (PCR)

VPS enforces periodic secret renewal to prevent statistical inference attacks. If an attacker attempts to observe multiple login sessions to infer the user's private logic, VPS limits the observation window by forcing credential rotation after a predefined number of authentications (e.g., 400 sessions). This threshold is intentionally set below the estimated number of samples required to deduce the user's mental margin or positional keys, thereby preventing accumulation of sufficient data for inference.

2. Visual Masking (Blank-Screen Protocol)

During sensitive authentication phases, VPS employs visual masking overlays designed to disrupt screen- capture and RAT-based observation. These overlays interfere with automated screen-scraping techniques, ensuring that even if malware is present on the device, the attacker cannot reliably determine which graphical items were selected or which values were entered.

3. Zero-Knowledge Input

The core secrets of VPS — the mental margin and locker key positions — exist only within the user's cognition. No reusable secret is stored on the device or transmitted over the network. As a result, even full device compromise does not expose credentials that can be replayed or reused by an attacker.

IV.DISCUSSION

The Visual Password System represents a shift from static knowledge to active cognition. It provides a scalable Login-as-a-Service (LaaS) model for banking, crypto-wallets, and enterprise security. This model remains robust even when the device hardware is fully compromised by malware, as the real logic exists only in the user's mind.

V.CONCLUSION

The VPS effectively neutralizes the "Sync-Infiltrator" exploit by ensuring no reusable data is ever typed or displayed. It provides a robust authentication framework for high-security environments. The Visual Password System represents a shift from static knowledge to active cognition. It provides a scalable Login-as-a-Service (LaaS) model for banking, crypto-wallets, and enterprise security that remains robust even when the device hardware is fully compromised by malware.

Intellectual Property Notice: The Visual Password System (VPS), including the 54-item graphical pool, mental margin logic, and positional locker key protocol described in this paper, is the subject of a pending provisional patent application filed by the author. All rights are reserved.

Conflict of Interest: The author declares no competing financial interests or institutional conflicts that influenced this research.

REFERENCES

1. FIDO Alliance. (2024). FIDO2: WebAuthn & CTAP Security Analysis.
2. Yadav, A., & Seamons, K. (2024). Security Analysis of Local Attacks Against FIDO2. NDSS Symposium.
3. Verizon. (2025). Data Breach Investigations Report (DBIR).
4. IBM Security. (2025). Cost of a Data Breach Report 2025.
5. Guan, L., et al. (2022). Formal Analysis of FIDO2 Protocols: Synced Passkey Weaknesses. ACM CCS.