Individual Submission
Internet-Draft
Intended status: Informational
Expires: 7 May 2026

D. Brown

3 November 2025

Phishing-Resistant Phone Number Attestation for MFA
draft-brown-spice-phishing-resist-attestation-00

Abstract

This draft introduces a phishing-resistant phone number attestation mechanism for multi-factor authentication (MFA). Conceptually similar to WebAuthn, it uses origin-bound cryptographic challenges to ensure that users only attest ownership of their phone numbers to legitimate relying parties. The protocol leverages network-operator-issued verifiable credentials (VCs) that cryptographically bind phone number ownership to a user’s device. Applications present origin-scoped challenges that users sign using their VC, ensuring secure, domain-specific authentication and mitigating replay, relay, and phishing attacks- without relying on SMS-based one-time passwords (OTPs).

Table of Contents

Introduction

Multi-factor authentication (MFA) is considered a best practice for preserving application security. In organizational authentication settings, secure MFA implementations (e.g., FIDO) can be implemented on the basis of a pre-established trust relationship (e.g., possession of a trusted device, authenticator, etc). However, end-user applications generally lack this pre-established trust relationship, and must instead bootstrap MFA using a user's email or phone number.

One of the most widely-adopted methods to implement phone-based MFA is SMS-based one time passwords (OTPs). This method is convenient and widely-adopted, but is vulnerable to various phishing attacks and domain spoofing. For example, a threat actor can create a fake login or password reset screen (domain spoofing) to trick a user into initiating an MFA request. The attacker intercepts the legitimate OTP sent to the user's device and uses it to gain access to the user's account.

These vectors are enabled because two attestations fail to happen:

1. The user has no cryptographic guarantee that the application requesting their OTP is the legitimate application. Without strong origin binding consistent with WebAuthn origin semantics (i.e., RP ID/origin verification), a malicious intermediary can convincingly impersonate the real application during enrollment or 2FA verification.

2. The application has no cryptographic proof that an OTP is being sent to, and returned from, the legitimate second factor device under the user's control. SMS delivery provides no assurance of endpoint identity.

This document proposes a mechanism to mitigate the risk of domain spoofing/SMS-phishing via an extension of [I-D.song-spice-telecom-usecases].

Proposed Mechanism

1. As described in [I-D.song-spice-telecom-usecases], the network operator (i.e. mobile carrier) provides a verifiable credential (VC) to the user. This VC is a cryptographically signed document that attests to the user's phone number ownership, as well as identity attributes of the user, and is stored securely on their device.

2. An application seeking to authenticate the user generates a unique cryptographic challenge and presents this to the user. The cryptographic challenge is bound to the relying party using WebAuthn-like origin semantics (i.e., RP ID/origin), limiting the usefulness of relayed or replayed material against other domains.

   * A mobile device might recognize and respond to the challenge (in a WebAuthn-like mechanism).

   * A desktop device might present the challenge as a QR code readable by a mobile device (such a QR flow would need to be cross-device-bound, e.g., by echoing a short code tied to the requesting desktop session), or use delegated credentials to recognize and respond directly.

3. The user signs the challenge and submits the assertion out-of-band over TLS to a pre-registered endpoint for the RP derived from the verified RP identity (e.g., https://<rp_id>/.well-known/phone-attest).

4. The application verifies the assertion by validating the VC chain from trusted network operators and then evaluating the RP binding and signature as appropriate for the application.

Implementations are encouraged to bind proofs to the requesting HTTP session (e.g., include a session-scoped nonce) so that successful verification upgrades the same session that initiated the challenge.

Benefits of Proposed Mechanism

* If the application receives a cryptographic proof by the above method, the application can be assured that (i) the user completed the challenge while viewing a page hosted by the backend (per origin checks aligned with WebAuthn semantics), and (ii) the user is in possession of a specific phone number:

  - Origin-bound challenges, when verified against the RP ID/origin and bound to the requesting session, mitigate real-time relay (adversary-in-the-middle) and similar phishing flows by making the assertion specific to the legitimate application context.

  - The signed proof, generated using the verifiable credential issued by the network operator, demonstrates that the device submitting the proof has cryptographic custody of the phone number.

  - Cryptographic signatures ensure integrity of the challenge and assertion; interception does not enable undetected modification.

* Depending on the set of attestations made by the network operator and the trust relationship between the application and the network operator, the application may additionally be able to verify other attributes of the user, such as their name, address, etc.

Summary of Changes

This draft does not supplant or modify any existing document.

Security Considerations

This Internet-Draft is intended to motivate changes proposed in draft-ietf-spice-sd-cwt-04 and draft-song-spice-telecom-usecases-00. A full evaluation of security considerations of this change is necessary and appropriate should these changes be promulgated into an implementable proposal. Number assignment and lifecycle considerations (e.g., SIM swap and recycling) rely on carrier-issued attestations that should be considered when utilizing the proposed mechanisms.

IANA Considerations

This draft makes no request of the IANA.

Informative References

[I-D.song-spice-telecom-usecases]
Song, Y., Li, L., Wang, D., and F. Liu, "SPICE Use Cases in Telecom Network", 3 March 2025, <https://datatracker.ietf.org/doc/draft-song-spice-telecom-usecases/>.

[I-D.ietf-spice-use-cases]
Zundel, B. and M. Prorock, "Use Cases for SPICE", 7 July 2025, <https://datatracker.ietf.org/doc/draft-ietf-spice-use-cases/>.

Author’s Address

Derek Brown
Email: mail@derektbrown.com