The following abstract is a submission to the Workshop on Improving Trust in the Online Marketplace. It proposes defenses against an adversary who has been able to spoof an SSL/TLS server certificate, and thus belongs to an emerging technology space that could be called "Defense in Depth" (against server certificate spoofing).

Emerging Technology Space: Defense in Depth
Title: Defenses against Spoofed SSL/TLS Server Certificates
Authors: Francisco Corella and Karen P. Lewison

--- Body of abstract ---

A spoofed server certificate is a maliciously procured certificate that binds the public key of an attacker to the domain name of a target web site or a homographic or similar name. If trusted by the user's browser, it may allow the attacker to spoof the target site or mount a man-in-the-middle attack. New protocols have been proposed to mitigate the risk of certificate spoofing, but adoption will take time and risk may remain. Therefore defenses against certificate spoofing are needed today and may remain useful in the future.

We propose a cumulative series of defenses that result in increasingly stronger security postures against an attacker who has spoofed the certificate of a site that maintains user accounts:

1. After a TLS connection is established, instead of sending a password, the user authenticates by signing a challenge with a private key associated with a public key registered with the site. This prevents password phishing, but not site spoofing or man-in-the-middle attacks.

2. The challenge includes the server certificate used in the TLS handshake, in addition to a server nonce. This prevents man-in-the-middle attacks, but not site spoofing.

3. After successful client authentication, the server authenticates to the user by showing an image and a sentence. This prevents site spoofing besides man-in-the-middle attacks. (Compare to SiteKey, which allows site spoofing by a man-in-the-middle.)

4. The key pair is regenerated from a PIN and a protocredential. An attacker who captures the user's computing device cannot mount an offline guessing attack against the PIN if the site keeps the public key confidential, because all PINs yield well-formed key pairs.

5. Privacy-preserving biometric techonology supplies a third authentication factor as input to key pair regeneration.

--- End of body of abstract ---