相手認証における安全性と攻撃に関する調査

Survey on Security and attack in Identity Authentication

楊璐伊・ネットワーク分科会・情報セキュリティ大学院大学

Abstract: With the popularity of the Internet, fraud and information theft methods other than social engineering are also increasing. On the other hand, there are many attacks that attack password authentication. Therefore, password less authentication is concern. In particular, the utilization of the convenient authentication means FIDO has increased in recent years, with browsers providing the domain name of the visited website to the authenticator for the challenge-response protocol, reducing the reliance on passwords. In this study, we focus on the investigation of the security of FIDO authentication.

背景

パスワード攻撃やフィッシング 攻撃などの増加に伴い、パスワード認証を安全に 使用することが難しくなっており、これらの攻撃　に防ぐため、パスワードレス認証の仕組みが注目されている。一部の実装に対して、PETSのMichal[1]の発表より、FIDO2で認証器へのタイミング攻撃を行われてきた；USENIXのEnis[2]の発表より、ソーシャルエンジニアリングを通じてFIDOを別の代替手段に格下げし、リアルタイムのフィッシング攻撃を受けやすくするダウングレード攻撃を行われてきた。FIDO認証の安全性を様々な角度から検証することを目指している。

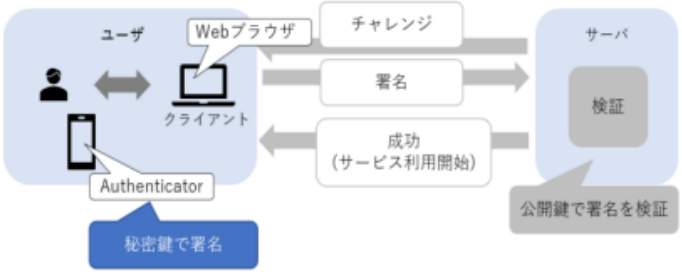
認証方式

・パスワード認証:ユーザーを「ID」と「パスワード」により認証するもので、インターネットから使われている認証方式です。複数のサービスを利用していると、異なるパスワードを使いまわしてしまい、サービスのパスワードが漏えいしたリスクがある。

・パスワードレス認証:認証器による所有要素や生体要素(指紋など身体特徴など)になる代替方法です。代表としてFIDOである。

FIDO認証

・チャレンジ(ランダムな値)と対応する電子署名を用いるレスポンス方式に基づく認証する方式。



・安全性

-サイトの間でユーザーを追跡することはできない。

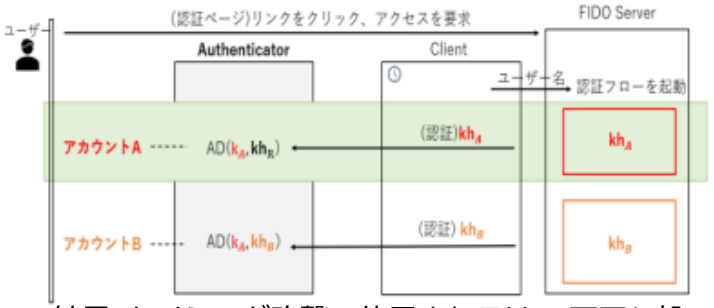
-認証器を持っているユーザーのみ秘密鍵を利用できる。

[1] Michal Kepkowski, Lucjan Hanzlik,Ian Wood, Mohamed Ali Kaafar ,How Not to Handle Keys: Timing Attacks on FIDO Authenticator Privacy. PETS Privacy Enhancing Technologies Symposium (was International Workshop of Privacy Enhancing Technologies)（2022）

[2] Ulqinaku, Enis, Hala Assal, Abdelrahman Abdou, Sonia Chiasson Srdjan Capkun "Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols" Proceedings of the 30th USENIX Security Symposium（2021）

タイミング攻撃

・クライアントと認証器を介してタイミング攻撃を実行する手法。

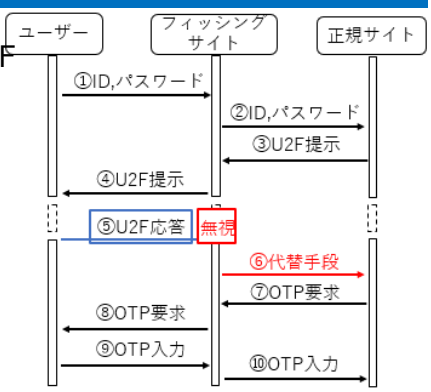


・結果:タイミング攻撃で使用されるkhの不正な処理により、khの処理時間の違いによるものである。khが復号できた場合、同一認証器で生成されたものがわかる。

ダウングレード攻撃

・フィッシング攻撃を防ぐ「FIDO　U2F認証」を、フィッシング攻撃に受けやすい「第二要素認証」に置き換える。

・実際にクレデンシャルを盗みたいわけではない。ユーザーに成りすましてアクセスできる。



今後の方針

・多角的に攻撃、防御、ユーザビリティ動向調査