SecHack365

SSH with Passkeys

～Passkeysを利用したセキュアなSSHログイン認証の実現～

↑ソースコードこちらから！

学習駆動コース
社会実装ゼミ　大井 智弘

1. SSHって何？

遠隔のサーバーにログインして、コマンドを実行したり、ファイルの操作や通信の転送を行うためのプロトコル。

☆ログインに関して2つの認証方式がある
- 「パスワード認証方式」

簡単だけどパスワード漏洩のリスクあり
- 「公開鍵認証方式」

セキュリティは高いけど、設定が面倒なのと秘密鍵を紛失したらアクセスできなくなる

2. Passkeyって何？

FIDO(ファイド)によって策定されたパスワードレスな新しい認証方式。従来のパスワードのように文字列を覚える必要がなく、指紋認証や顔認証といった生体認証(内部的には公開鍵)を利用することで、より安全かつ簡単にログインできるようになる。

特徴	パスワード	Passkeys
認証方法	文字列を入力	生体認証またはPINコード
セキュリティ	漏洩のリスクが高い	漏洩のリスクが低い
利便性	文字列を覚える必要がある	生体認証で簡単
フィッシング対策	フィッシングに弱い	フィッシングに強い

めちゃめちゃ簡単に言うと、パソコンやスマホ本体がログインキーになるイメージ。

3. 現在の問題点

公開鍵認証自体はセキュアなのに、鍵の保存場所が ~/.ssh/ でユーザー本人なら見ることができるので、悪意のあるアプリケーションに容易に読み取られてしまう。
→特に開発用端末では管理権限でアプリを動かすことも多いのでリスク大
サプライチェーン(開発端末を狙うのも含む)の弱点を利用した攻撃も年々増加しており、IPAの情報セキュリティ10大脅威 2025では2位になっている。
→開発端末が侵害されたときも被害を食い止める必要がある

4. SecHackでの軌跡

7月　第二回イベント（東京）

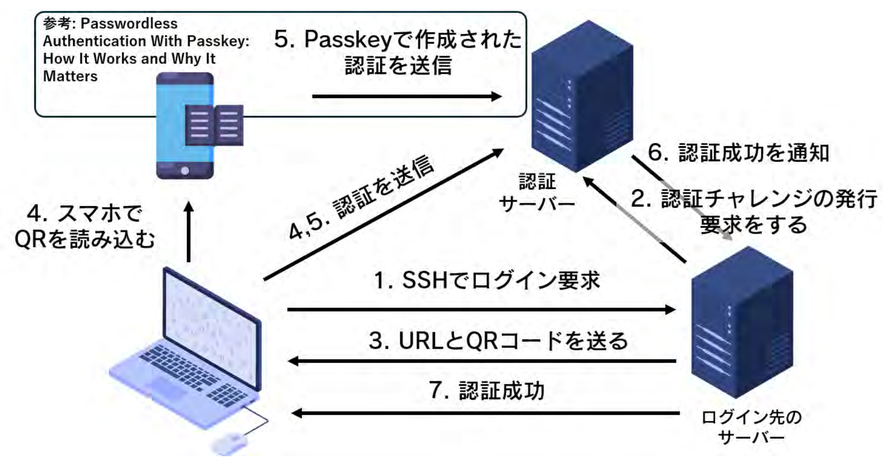
8月　ここでテーマを思いついた

9月　第三回イベント（広島）
↑とりあえず動くものを展示（セキュリティガン無視）

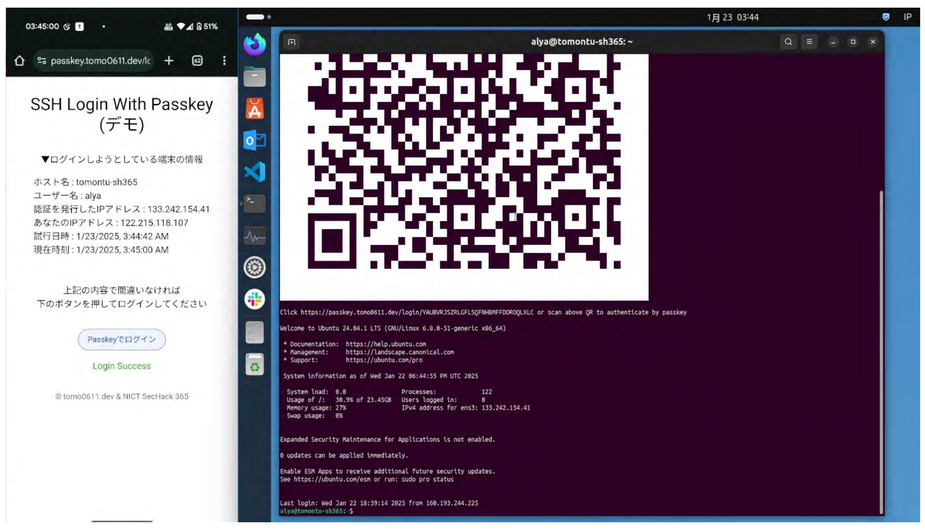
11月　第四回イベント（大阪）
↑広島で頂いた助言の技術を調査し、簡単に実装

1月　作品動画提出
↑実際に動くものを作成

5. システム構成図



6. こんな感じで動きます！



7. 今後の展望

- アカウントや組織管理、ログ周りの強化
- 企業向けのSSO (OIDCやSAML)の対応
- 認証サーバーのSaaSでの提供
- 【課題】認証サーバーの正当性の確認

NICT National Institute of Information and Communications Technology

SecHack365に関わった全ての方々へ感謝を申し上げます