HMDを利用したパターン認証に対するショルダーサーフィン攻撃の実証

Demonstration of shoulder surfing attack against pattern authentication using HMD

大木圭介・ネットワーク分科会・情報セキュリティ大学院大学

Virtual Reality (VR) is a rapidly advancing technology in recent years. On the other hand, the challenges in using VR systems securely have not been fully explored. In particular, user authentication using a Head Mounted Display (HMD) may be subject to shoulder surfing attacks. In this paper, we survey research on the security of pattern authentication using HMDs. As a result, we found that the security of pattern authentication using HMDs has not been sufficiently verified. Therefore, we conducted a demonstration of a shoulder surfing attack, in which the authentication behavior was recorded against pattern authentication using HMDs, and patterns were identified by an object detection and tracking algorithm.

1. 背景と目的(ざっくり)

- HMD（Head Mounted Display）が普及してきている
- パターン認証はショルダーサーフィン攻撃に対して弱そう

⇒攻撃システムを作って実証！

2. HMDのユーザ認証は安全？

ユーザ認証の使い道は？

HMDのロック解除・アプリのアクセス制御・
アカウントログイン・決済時の本人確認

認証情報が
漏れた場合…

クレカの不正利用・メタバース上でのなりすましetc..

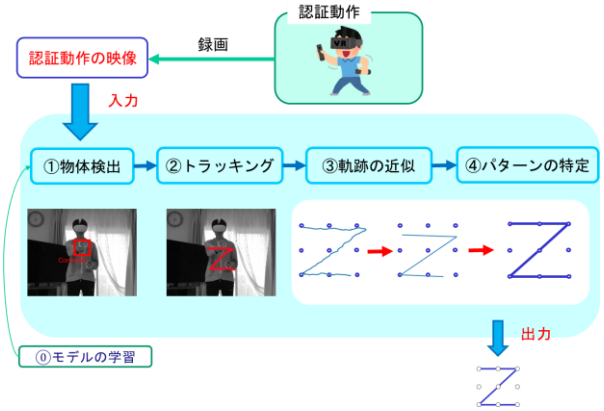
HMDのユーザ認証の特徴

①単純な認証情報を選択しがち

②周囲の人間・物体の変化に気づきづらい

⇒ショルダーサーフィン攻撃に弱いのでは？？

3. 攻撃システムのなかみ



4. 実証結果

○約36%の確率で推測に成功！

○推測の精度に関わる要因としては、認証動作の個人による癖の差が大きそう

×推測の精度を左右する要素が多すぎて、特定が難しい

5. 今後の研究

- パターン認証以外に適用できる？
- 不確定要素を減らした実証