

JavaScriptを用いた端末特徴量抽出による Web リソースへのアクセス制御手法の提案

Proposal of Access Control of Web Resources by Extracting Device Feature Using JavaScript

西丸真生・マネジメント分科会・情報セキュリティ大学院大学

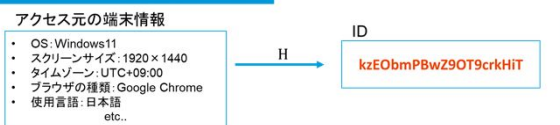
目的

端末に一元的な管理ツールを導入することなく、セキュリティ上の脆弱性が存在する端末からのアクセスを拒否することを目的とする。Webブラウザを介して取得するユーザ端末の特徴量を用いたアクセス制御手法の提案する。

ブラウザフィンガープリント (BFP)

BFPは、ユーザのブラウザを介して、収集する特徴量をハッシュ化し、固有の端末識別情報を生成する技術である。特徴量の抽出に、HTTPヘッダーやJavaScriptが用いられる。本研究では、このJavaScriptを用いて特徴量を抽出する。

フィンガープリント値生成イメージ



特徴量の要件

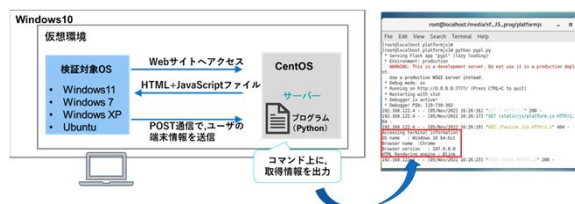
総務省のガイドラインにおける脆弱性管理の観点で、以下の特徴量を抽出する必要があると仮定した。本研究では、ソフトウェアについてはWebブラウザを検証の対象とした。

- OS の名称
- OS のバージョン
- ソフトウェアの名称
- ソフトウェアのバージョン



検証実験

アクセス元の脆弱性管理の観点で抽出する必要のある特徴量について、異なる環境における抽出の可否や正確性について検証を行った。



検証実験の結果と考察

特徴量抽出の可否

一部を除いて、OS、ブラウザ、レンダリングエンジン情報をWebサーバー側で取得することができた。

取得値と実際の値の比較

Windows10のEdge及びInternet Explorerブラウザでアクセスした場合はおおむね正確な値が取得できた。実際の値と取得値が、部分一致や広義の意味での一致など、必ずしも一致していない場合があった。



- platform.jsの一部修正。
- User-Agentの代替となるUser-Agent Client Hints APIの利用。

提案手法

提案手法の構成図を以下に示す。Web リソースへアクセスをリクエストする端末の特徴量を抽出し、Webサーバー側で特徴量の検証を行い、その結果によってアクセス制御を行う。



提案手法の評価実験

Webリソースへのアクセス許可の条件を以下の2パターン設定し、各種 OS及びブラウザからの Web リソースへのアクセス状況について観察し、提案手法の有効性を確認した。

- 条件1: OSがWindows10以上かつEdgeブラウザからのアクセスのみ許可
- 条件2: Chromeブラウザであれば、OS問わずアクセスを許可

今後の課題

今後の課題を以下に示す。

- User-Agent の段階的削減に伴うブラウザのマイナーバージョンの抽出不可への対処
- 正規の利用者が脆弱性のある端末を利用していた場合に、脆弱性が検出されないよう、改ざんする可能性への対処手法の検討