ゼロトラストアーキテクチャにおける ブラウザフィンガープリントを利用したアクセス制御

Access control using browser fingerprints in zero trust architecture

高木祥一・ネットワーク分科会・情報セキュリティ大学院大学

In recent years, the zero-trust model has attracted a lot of attention, but there is no specific technology to realize the zero-trust architecture. However, there is no specific technology for realizing the zero-trust architecture. ″Access to individual enterprise resources is granted on a per-session basis.″ is one of the concepts of the zero-trust model, and it is necessary to evaluate the trustworthiness of frequent accessors. Therefore, we focused on browser fingerprints, which are known to be easy to identify the access source. In this paper, we propose a method of access control using browser fingerprints, because it can be inferred that a user continues to use the same environment when the browser fingerprints are continuously the same.

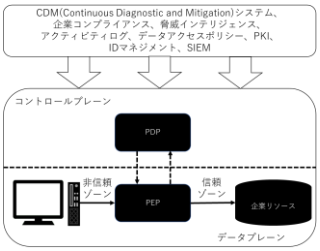
1. 背景

近年，ゼロトラストに注目が集まっているが，実装方法については特に定められていない．
「企業リソースへのアクセスは，セッション単位で付与する」はゼロトラストの考え方の1つであり，頻繁なアクセス元の信頼性評価が求められている．ユーザ操作が必要な認証を頻繁に実施するとユーザビリティ低下が予想されるため，アクセス元の識別がしやすいことで知られているブラウザフィンガープリントを利用してアクセス制御を行う手法の提案を行った．

2. ゼロトラスト

- ゼロトラスト：各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体
- ゼロトラストアーキテクチャ(ZTA)：ゼロトラストの概念を利用したサイバーセキュリティ計画

ZTAアーキテクチャは右図のようになるがPEP/PDPでどのような制御を行うかはZTAを構築する組織に委ねられている

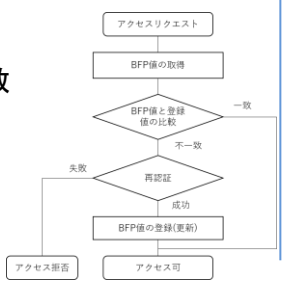


3. 提案手法

- Webサイトとアクセス元の間でブラウザフィンガープリントの値（BFP値）の検証を実施
  - リクエストと共にBFP値を送信
  - 検証済のリクエストのみをWebサイトへ転送

提案手法の工夫点

- 偽装値を送られないように乱数を用いたチャレンジレスポンス方式の導入
- BFP値は同じ値であり続ける保証がないため更新可能な検証フローの導入



4. 実装と評価

- 提案手法を実装したWebサイトを構築し，以下の不正アクセスを検知できることを示した
  - クレデンシャルスタッフィング
  - Cookieハイジャック

BFP値が異なるためアクセス不可

- 頻繁なBFP値の変化は再認証の発生に繋がるため，特定環境のBFP値の継続取得実験を実施

	端末1			端末2		
	Firefox	Chrome	Edge	Firefox	Chrome	Edge
2021/4/23	f1_1	c1_1	e1_1	f2_1	c2_1	e2_1
2021/4/30	f1_1	c1_2	e1_2	f2_1	c2_2	e2_2
2021/5/7	f1_1	c1_2	e1_3	f2_1	c2_2	e2_3
2021/5/14	f1_1	c1_3	e1_4	f2_1	c2_3	e2_4
2021/5/21	f1_1	c1_3	e1_5	f2_1	c2_3	e2_5
2021/5/28	f1_1	c1_4	e1_6	f2_1	c2_4	e2_6
2021/6/4	f1_2	c1_4	e1_7	f2_2	c2_4	e2_7
2021/6/11	f1_2	c1_5	e1_7	f2_2	c2_5	e2_7

変化頻度はブラウザ毎に異なるも，ブラウザの更新が主な起因であることが分かった

5. まとめと今後の課題

- ブラウザフィンガープリントを利用してアクセス制御を行う手法を提案
- BFP値が同じになりやすい環境における不正アクセス検知に向けたBFP値要素の追加検討や提案手法へのロジック追加が必要