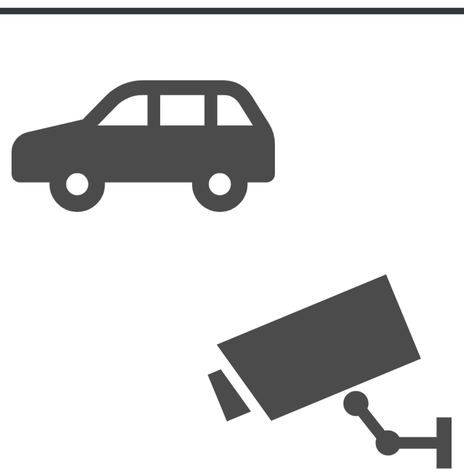
SecHack365

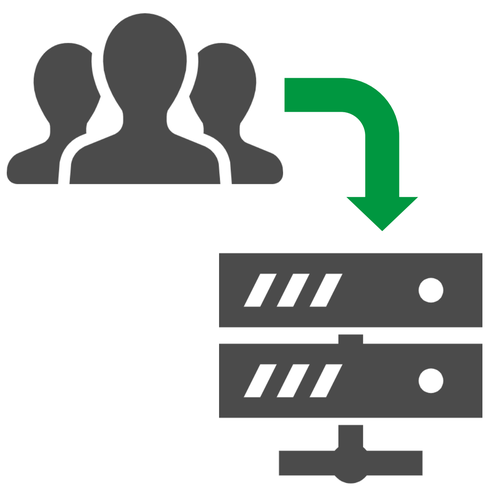
ベータテストを用いて自動チューニングを行なう アノマリ型WAFの研究

研究駆動コース　比嘉隆貴

研究背景



IoT機器



少人数で運営
しているサイト

脆弱なことが多い
➜攻撃対象になりやすい

Webアプリケーションには WAFを設置して防御

■WAF(Web Application Firewall)とは？

- Web Applicationの脆弱性をつく攻撃から防御
- シグネチャを設定して防御を行う

問題点

- シグネチャを設定，更新しないといけない
- シグネチャ型では未知の攻撃を防ぐことが厳しい
- Webアプリケーションに合わせてチューニングが必要
- 誤検知が発生する

運用コストが高い！！

簡単に扱うようにできないかな…

考察

- アノマリ型検知を行うと未知の攻撃を防げるようにチューニングができそう
- 何かしらの方法で自動的にチューニングを行い誤検知を抑えられないか

提案手法

目的

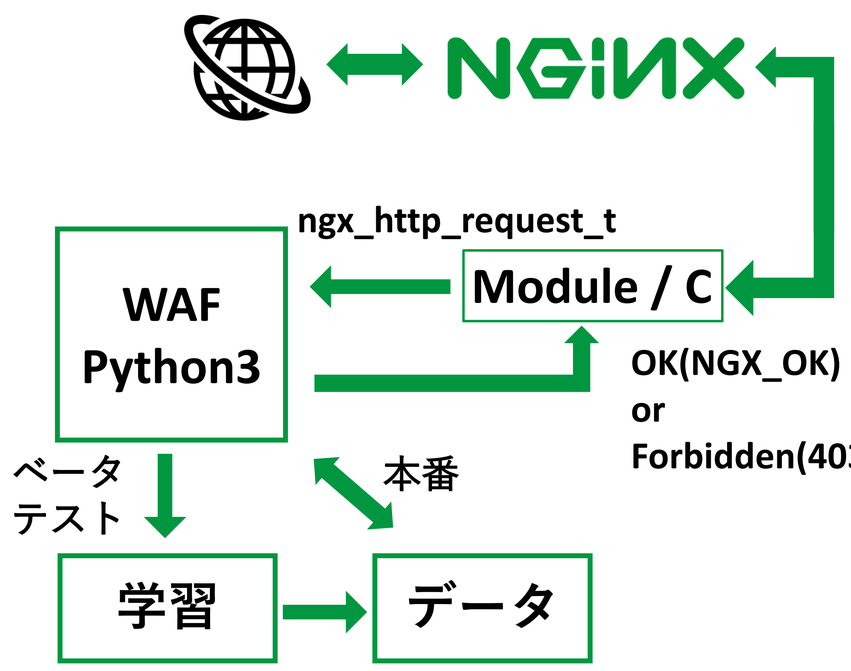
- WAFの運用コストを下げる
- 未知の攻撃を防ぐ
- 誤検知を抑える（特にFalse Positive）

アノマリ検知を行い，自動チューニングを
特徴が出そうなベータテストを用いたらどうだ！

■ベータテストとは？

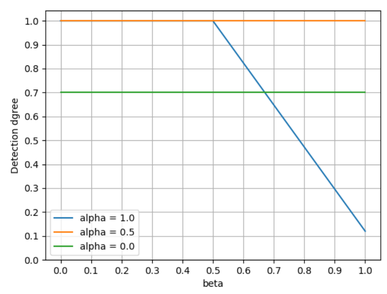
ここにおけるベータテストとは
信頼出来る人だけがリリース直前のテストサーバで
サービスを利用することです.

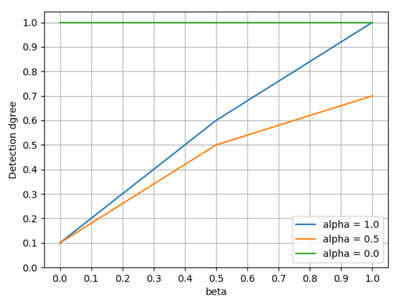
設計実装



内部ではPOSTデータのパラメタを用いて解析

結果





- ベータテストを用いない研究に比べると
  ほんの少し良い結果が得られた

今後の課題

- 簡易的なサイトでの実験であるためデータの信憑性が薄い．改善する必要がある.
- パケット長等のデータも用いて詳しく研究を行う
- ベータテストの利点をたくさん活かせるような専用のアルゴリズムの研究

NICT 国立研究開発法人 情報通信研究機構