様々なプロトコルに対応！

ゼロデイアタックの原因となる通信プロトコルの欠陥や脆弱性を発見する！！
IoTデバイス開発時のセキュリティ対策に必須な検査ツール！

PEACH FUZZER

Peach Fuzzer

ファジングテストソリューションのリーダである**Peach Fuzzer 合同会社（アメリカ）**が開発した**Peach Fuzzer**は、様々なITデバイスに潜む脆弱性をファジングテストと呼ばれるテスト手法によって発見し、ゼロデイ攻撃のリスクを最小限に抑えます。
IoT（Internet of Things）時代の幕開けと共に多種多様なITデバイスがインターネットに接続される一方、ITデバイスに対するセキュリティ対策の不備が指摘されています。

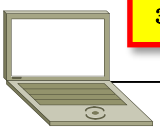
ITデバイス開発時（製品リリース前）に**Peach Fuzzer**でテストする事により、短時間で内在する脆弱性を発見・修正し、製品リリース後に起こり得るITデバイスの脆弱性に起因する重大なセキュリティ問題のリスクを回避する事が可能です。
Peach Fuzzerは、**IoTを含むITデバイス開発**において、**簡単**で**確実**に実施できるセキュリティ対策の為の強力なツールです！

【ファジングテストとは？】

・意図しない、或いは不正な通信パケットをテスト対象のデバイスへ送信し、デバイスがフリーズしたり、通信不能に陥ったりしないか監視し、検査する手法。
・Peach Fuzzerは、彼らが長年蓄積している経験と知識を駆使し、数千・数万に上る膨大なファジングパターンをプロトコル毎にプロファイル化し、効率的にファジングテストできる様、開発されています。

テストイメージ

1、ターゲットのIPアドレス・MACアドレスを設定してテスト開始
2、指定ポートへ、ファズデータ（不正・予期しないデータ）を生成
3、ICMP、TCP監視、Syslog等で通信を監視



Ethernet (10/100/1000Base-T)

Peach Fuzzer Platform

1、膨大な量のファズデータ（不正・予期しないデータ）をターゲットデバイスへ送信し、クラッシュしたり不安定になったりしないかをテストする。
2、テスト中に起こったイベントは、テストログに保存される。
3、テストログを参照して、脆弱性の特定とその修正を行う。

様々なプロトコルに対するテストが可能です！！

- **IPv4**：・ICMP ・IGMP ・ARP ・TCP ・UDP
- **IPv6**：・ICMP ・TCP ・UDP ・MLD
- **Network Discovery**：・DHCP ・DHCPv6 ・LLDP ・CDP
- **Network Service**：・FTP ・NTP ・Telnet ・POP3 ・SSH-FTP
- **Healthcare**：・DICOM /HL7（ネットワーク / ファイル）
- **Network Switching**：・Ethernet ・VXLAN・LACP ・IEEE 802.1Q ・ERPS
- **STORAGE**：・NFSv3 ・NFSv4 ・PORTMAP ・CIFS
- **Web**：・HTTP ・SSL/TLS1.2
- **Individual**：・CAB ・IPSECv6 ・LDAP ・Wi-Fi ・ZIP
- **SCADA**：・MODBUS (Serial / TCP)・DNP3 ・BACnet
- **Network Management**：・SNMPv2 ・SNMPv3
- **IoT**：・CoAP DTLS New!

様々なファイルフォーマットに対するテストが可能です！！

- **IMAGE**：・AVI ・BMP ・GIF ・ICO ・JPEG2000 ・JPEG ・PNG

Peach Fuzzerは、下記の要件に最適です！！

- IoTデバイスに対し、セキュリティ検査をしたい。
- 顧客から、開発したITデバイスのセキュリティ検査を求められている。
- 開発したITデバイスに対し、どの様なセキュリティ検査を行うべきか分からない。
- ITデバイスやシステムに対するデバックに多大な時間と労力を費やしている。

Peach Fuzzerは、下記の導入メリットがあります！！

- 製品リリース前に各種プロトコルの脆弱性を潰し、最小限に抑える事で、リリース後の重大なセキュリティ問題を回避可能です。
- 膨大な時間と労力を費やしていた脆弱性検査（バグ取り）を、簡単且つ短時間で実施可能です。
- 開発する全てのITデバイスに対し一定のセキュリティ堅牢性を担保でき、統一したセキュリティ検査基準を確保できます。
- 幅広いプロトコルをカバーしているので、複数のツールを保有する必要がありません。

Peach Fuzzerは、新しいプロトコルを続々カバーします！！

【2016年第1四半期にサポート予定のプロトコル】
【IPv6】NDP 【Network Service】DNS 【Storage】MOUNT, SUNRPC 【Network Management】SNMPTRAP, BOOTP
【Network Switching】STP, RSTP, ERPS (G.8032), MSTP

システム要件

【OS】Windows：XP以降,各種Window Server Microsoft.NET v4 runtime, WireShark
Linux：Ubuntu/Debian Linux, Redhat Enterprise Linux (RHEL and CentOS), SUSE Enterprise Linux (SLES)
OS X：mono Microsoft.NET runtime, CrashWrangler and Xcode

CORNET TECHNOLOGY
日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2 〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp

Rev E (042017)

Peach Fuzzer　vs　商用ファザー

ファジングテストは、安全且つ信頼性の高いソフトウェア及びハードウェアの開発に不可欠です。
ファジングテストは、サイバー攻撃を受ける前にゼロデイの欠陥を明らかにします。
それぞれのニーズに合ったファジングツールを選択する事が非常に重要と考えます。

ファジングツール検討の為の5つのポイント

PEACH FUZZER

VS

他社商用ファザー

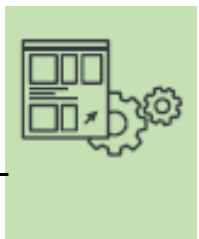
（1）拡張性

完全なセキュリティテストプラットフォーム
Peach Fuzzerの伸展性、拡張性及び複数のユースケースは、包括的なプラットフォームとして定義されます。ファジング対象のネットワークプロトコル、ファイル形式、デバイス、カーネルは顧客のニーズに合わせて進化します。

限定的なセキュリティテストツール
他社製品は、伸展性も拡張性もありません。主にネットワークプロトコルに対してしかユースケースを持ちません。
他社製品は顧客のニーズに合わせて拡張することはできません。

（2）テストケースの制限

無制限のテストケース、最大限のカバレッジ
Peach Fuzzerは、総合的なファジングエンジンを含みます。動的にユニークなテストセットを新しく生成します。
PeachFuzzerは本物の無制限ファジングツールです。



ファジングエンジン無きファジングツール
他社製品はファジングエンジンを持ちません。多額のライセンス費用は、事前生成されたテストケースの限定セットです。限定されたテストケースで十分にバグを見つけられますか？

（3）独自プロトコルの制限

独自プロトコルのファジング
Peach Fuzzerは、コンポーネント、SDK及びソースコードテンプレートをモデル化し、フル拡張可能なフレームワークを使用して独自プロトコルのファジングを支援します。

事前定義で立ち往生
独自プロトコルをテストする場合、他社製品は、伸展性・拡張性の無さで立ち往生します。

（4）問題箇所の特定

高度なモニタリングにより正確な結果を得る
Peach Fuzzerは、問題検知機能・データコレクタ機能・環境マネージャの3つの高度なモニタ機能を持っています。これらにより、より多くのバグの発見と正確な結果を得る事が可能です。

初歩的なモニタリングによるバグの見逃し
脆弱性の特定と修正は非常に難しい作業です。初歩的なモニタリングでは、脆弱性の特定を見逃す可能性があります。

（5）柔軟性

柔軟な操作
Peach Fuzzerの新しいフルグラフィックユーザインターフェイスとウィザード形式のコンフィギュレータ、堅牢なヘルプレポジトリは簡単で柔軟性に富んでいます。

古いソリューション
サイバー攻撃は日々進化しています。
限定されたテストケースとユースケース、古いインターフェイスでは、十分なテスト結果を得る事はできません。

CORNET TECHNOLOGY 日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2　〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp