未知のセキュリティ脆弱性発見ツール

FFR Raven

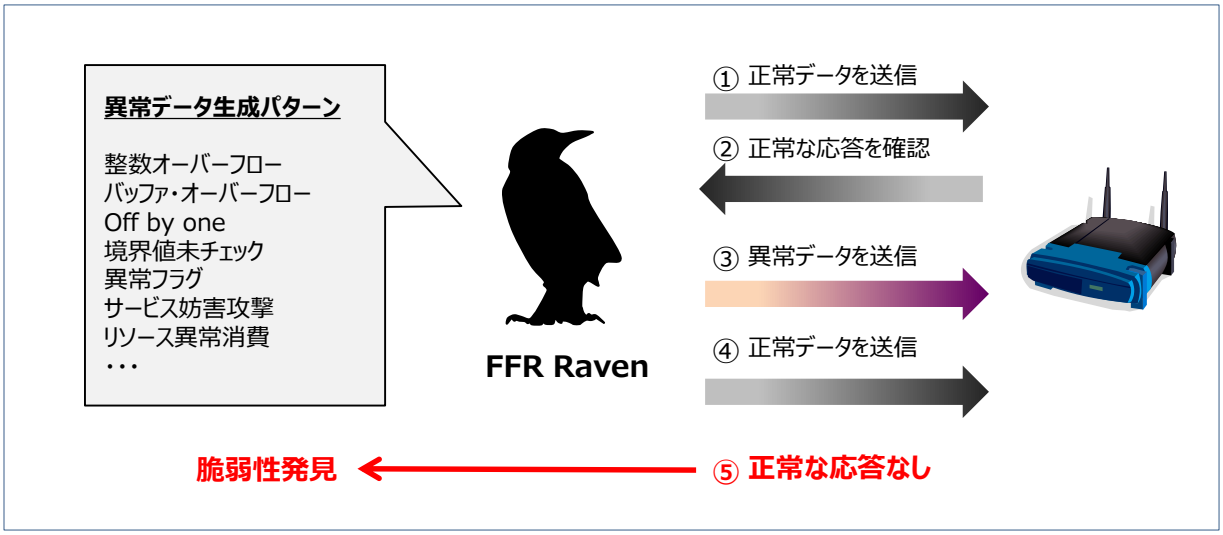
Product Security Testing Suite

簡単操作で高性能FuzzingTestを実現

ネットワーク組み込み機器を検査し、未知のセキュリティ脆弱性を発見

近年、ネットワーク組み込み機器の脆弱性報告や攻撃が急増しています。組み込み機器は、インターネットが成熟期に入った段階で急速にネット化が進んだ経緯もあり、古典的なセキュリティ脆弱性を持つ機器が数多く存在しています。開発ベンダーのセキュリティ対策は十分ではなく、多くのインシデントを経て安全性が向上したWindowsやUNIXの経験が生かされていないケースが多いのが現状です。

FFR Ravenは、未知のリモートセキュリティ脆弱性発見に特化したツールです。
セキュリティ脆弱性を誘発する可能性がある異常なパケットの組み合わせを自動生成して対象機器に送信する事で、対象の異常をモニタリングする「FuzzingTest」を実施。
当テストにて、バッファオーバーフロー、整数オーバーフロー、フォーマットストリング、off-by-one、読み込み境界未チェック、異常リソース消費、サービス妨害など、多数の致命的な脆弱性を発見する事が可能です。



脆弱性スキャンとFuzzing Testの違い

現在、製品テストで行われている脆弱性スキャンは、既知の脆弱性をカバーする対策が取られているかどうか（OS/Firmwareアップデート等）を確認するための手法。

「Fuzzing Test」では、対象機器に対し、不具合が起こり得る異常パケットを自動生成・送信する事により、未知の脆弱性を発見し、開発段階での随時対策を可能とします。

FFR Ravenの洗練された機能

FFR Raven
Product Security Testing Suite

簡単操作で高品質のセキュリティ・テストを実現

使用方法は、対象機器のIPと検査するプロトコルを選択し、自動実行させるだけ。簡単な操作でセキュリティ・エキスパートのテスト実施内容を再現します。

利用者に優しいインタフェース

インストールが容易であり、また、日本語のユーザーインターフェイスと詳細かつ丁寧なマニュアルを完備。
付属のWord形式のレポートテンプレートが、顧客や開発者への検査レポート作成を容易にします。

充実のR&D・サポート体制

100を超える世界クラスのセキュリティ脆弱性発見・対策技術研究の実績を背景とした、完全国産・フルスクラッチツール。

随時、検査項目の追加や、脆弱性研究のエキスパートによるサポートを行います。

卓越した脆弱性検出能力

当ツールにて検査を行ったところ、90%以上の製品に何らかの脆弱性を発見(*)。
高い脆弱性検出能力を誇ります。

電気錠システム、家庭用ブロードバンドルーター、IP電話アダプタ他、スイッチやモバイル機器、テレビなど多数の機器における脆弱性を検出。

*当社調べ：約20種類の製品について検査

軽快な動作でモバイルPCにも対応

200万もの検査パターンを2.5時間で高速に実施。低CPU負荷、低リソース消費のため低スペックPCやウルトラ・モバイルPCでも動作可能です。

広範囲のプロトコル検査をサポート（今後も随時追加予定）
※IPv6ファジング、Webクライアントファジング（HTML,Javascript,CSS,GIF,JPEG,SWF）にも対応

TCP/IP Option Fuzzing、IP Option Fuzzing (TCP)、IP Option Fuzzing (UDP)、IP Option Fuzzing (ICMP ECHO REQUEST)、ICMP Option Fuzzing (ICMP UNREACH HOST)、TCP Header Fuzzing、UDP Header Fuzzing、SYN Flood DoS、Land Attack DoS、Ether X-DoS、Ether Fuzzing、ARP DoS、ARP Fuzzing、ICMP Ping of Death、ICMP Fuzzing、HTTP（POST/GET/etc) Fuzzing、DHCP Option Fuzzing、FTP Use/Pass Fuzzing、FTP Command Fuzzing、Telnet Account Fuzzing、Telnet Terminal Fuzzing、UPnP Fuzzing、SNMP Community Fuzzing、SNMP Encoding Fuzzing、TFTP Name Fuzzing、TFTP Type Fuzzing、SIP Fuzzing

動作環境

環境	CPU　：Intel Pentium 4 1.6GHz以上のプロセッサ メモリ　：1GB以上を推奨 HDD　：16GB以上を推奨 NIC　：10/100-BASE-T/TX以上のLANカード
OS (32bit)	Windows 7　：Home Premium, Professional, Ultimate Windows 8.1　：Pro, Enterprise
OS (64bit)	Windows 7　：Home Premium, Professional, Ultimate Windows 8.1　：Pro, Enterprise

※Symantec Endpoint Protectionが有効になっている環境では、HTTP fuzzingは競合が発生し正常に動作しません。最悪windowsがクラッシュする危険性があります。

製品・サービスについてのお問い合わせは

株式会社ＦＦＲＩ

〒150-0013
東京都渋谷区恵比寿1-18-18　東急不動産恵比寿ビル4階
TEL：03-6277-1811 E-mail：sales@ffri.jp
本製品に関する情報はインターネットでもご覧いただけます。

http://www.ffri.jp/

2016年01月現在

Ver 2.00.06