無線通信工学十徳ナイフ RFRaptor

SecHack365

学習駆動コース 今岡ゼミ
08Si 岩橋涼介

#Rust #無線 #SDR #OffensiveSecurity

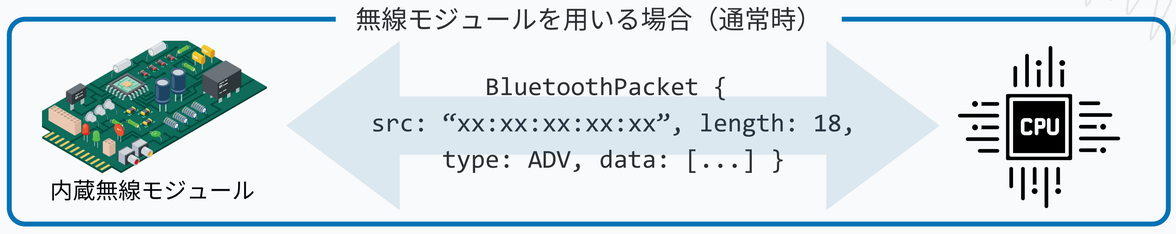
1. RFRaptor を一言で...

SDRを用いた脆弱性診断ツール

written in Rust!

2. SDRとは？

SDR（Software Defined Radio）とは**何でもできる無線機**です。周波数の指定や変調方式、送信するビット列をソフトウェアで指定でき、Wi-Fi・Bluetoothなど任意の無線機の代わりとして用いることができます。



3. 診断対象について

無線機の<u>**ファームウェア**</u>や<u>**デバイスドライバ・無線を用いたアプリケーション**</u>など、幅広いレイヤを対象に無線通信のブラックボックステストを行います。

SDRの「任意の無線機の代わりとして用いることができる」という性質を利用することで、**全ての無線規格のテストを行うことができます**。

また、電波レベルで任意のデータを送信することができるため、無線モジュールが許していない「壊れたパケット」を送ることもできます。

壊れたパケットの例

```
Packet {
  length: 6,
  bytes: [1, 2, 3],
}
```
長さが不正

```
Packet {
  ..data,
  checksum: 0x000,
}
```
チェックサムが不正

```
Packet {
  length: 100
  bytes: [1, ..., 100]
}
```
規格外の長さのパケット

4. RFRaptorってどんなツール？

無線モジュールや、無線を使ったソフトウェアの**開発・デバッグ・脆弱性診断**ツールです。自作プロトコルを含む全ての無線規格を対象に、統一された直感的なUIでデバイスの発見・盗聴などの操作をリアルタイムで行うことができます。

また、RFRaptorは**能動的な診断**も行うことができます。診断用のエクスプロイトデータベースが内蔵されており、発見したデバイスに対して偵察や診断といった操作を可能にします。

SDRを使うから一台のハードウェアだけでWi-FiやBluetoothを使えて、全部同じUIで盗聴や診断を行うことができるんだね！

でも新しいプロトコルの対応が大変そうだなぁ

5. なぜRFRaptorが必要なの？

SDRは非常に強力なハードウェアですが、無線規格に適合させて使用するためには、ソフトウェアによる適切な信号処理が必要です。しかし、単純な実装では処理が間に合わず、liquid-dspなど最適化されたライブラリを用いてもなおリアルタイム処理ができないという致命的な課題がありました。

RFRaptorでは、信号の整数化・SIMD命令の活用・メモリレイアウトの最適化などの高度なパフォーマンスチューニングを通じてリアルタイム処理に必要な性能を達成しました。これらのライブラリを活用することで、右の例のようにシンプルなコードでBluetoothのリアルタイム処理が可能となります。

```
let packet = burst
    .catcher(s)                          信号レベルがHiのときを検知
    .ok_or(ProcessFailKind::Catcher)?;

let demodulated =                        FSK復調器
    fsk.demodulate(packet).map_err(ProcessFailKind::Demod)?;

let byte_packet =                        ビット列へ変換(whiteningなど)
    crate::bitops::fsk_to_packet(demodulated, freq as usize)?;

let bt =                                 プロトコル・スタックへ入力
    crate::bluetooth::Bluetooth::from_bytes(byte_packet, freq as usize)?;
```

Bluetooth受信の例

6. RFRaptorの特徴

拡張性

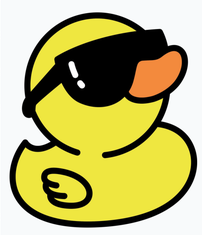
作成した高速信号処理ライブラリは汎用性が高く、それを用いて独自プロトコルの設計・開発が可能です。また、作成したプロトコルは**Traitの実装**という形で簡単に本体に取り込むことができます。

セキュリティ

本体に診断機能を搭載することで、GNU RadioやURHよりもスムーズに脆弱性診断が可能です。最新のPoCやエクスプロイトを取り込み、ボタン一つで手軽に試すことができます。

UI

デモ画面ではTUIにviキーバインドと、Hacker FriendlyなUIを目指しました。対応したプロトコル全てに対して同じUIを提供することで、同じ操作感で解析や診断を行うことができます。



実は、RFRaptor自体もMITライセンスで公開されてるよ！

新しいプロトコルへの拡張やエクスプロイトを簡単に追加できちゃう上に、他のツールとの連携もできて、更にMITライセンスで公開されてるなんて、全部が**オープン**なんだね！

7. 誰向けのツール？

- 無線を含む機器のベンダーには、デバッグツールとして
- 無線に関する脆弱性診断士には、診断ツールとして
- 教育関係者には、無線通信の実装を含む実践的な教材として

8. これらからのRFRaptor

プロトコルは拡張可能ですが、現状対応しているのはBluetoothのみで、実行可能な診断も用意した脆弱性に対してだけとなっています。そこで、プロトコルの拡充とエクスプロイト収集のためRFRaptorを中心としたコミュニティの醸成を計画しています！

9. まとめ

高速な信号処理ライブラリとそのUIをRustで作成しました。

IoTによって通信規格が多様化する中、SDRによって統一的にあらゆるプロトコルのデバッグ・脆弱性診断を行うことができます。

様々な用途が考えられるため、応用の幅を広げつつ対応プロトコル増加やエクスプロイトの収集をしていく予定です。

この場をお借りしまして、この一年間にわたり大変お世話になりましたSecHack365事務局の皆様、トレーナーの皆様、アシスタントの皆様、そしてともに切磋琢磨してまいりましたトレーニーの皆様に、心より深く感謝申し上げます。
とりわけ、今岡トレーナーと工藤アシスタントにおかれましては、多くのご指導を賜り、誠にありがとうございました。

GitHub repository link and QR
https://github.com/Iwancof/RFRaptor

外部発表 コンピュータセキュリティシンポジウム(CSS2024)
SDRを用いた無線脆弱性診断プラットフォーム 岩橋 涼介

RFRAPTOR