UNIVERSIDADE FEDERAL DE SÃO CARLOS

DEPARTAMENTO DE COMPUTAÇÃO

SEGURANÇA CIBERNÉTICA

DOCENTE RESPONSÁVEL: Paulo Matias

Bruno Nieri Nunes - 820590
Gustavo Kim Alcantara - 820763
Guilherme Bartoletti Oliveira - 821881
Lucas Mantovani - 794040
Maykon dos Santos Gonçalves - 821653
Pietro Bernardo Dutra Scaglione - 824375
Tiago de Paula Evangelista - 824369
Vinícius Marto da Veiga - 821252

SÃO CARLOS – SP
2025

Write-Up: Captura RF

1) Introdução

✔ O que é RF e captura de sinais

A radiofrequência (RF) corresponde ao conjunto de sinais eletromagnéticos transmitidos pelo ar em determinadas faixas do espectro, permitindo a comunicação sem fio entre dispositivos. Por serem transmitidos de forma aberta e propagarem-se em todas as direções, as comunicações por RF estão naturalmente expostas à captura de RF (captura de radiofrequência), que refere-se ao processo pelo qual um receptor, circuito ou sistema eletrônico se conecta, detecta ou extrai informações úteis de um sinal de radiofrequência recebido.

✔ Onde RF aparece no cotidiano

No cotidiano, lidamos com RF em diversas situações: ao usar um controle de portão eletrônico, ao destravar o carro com uma chave automotiva sem fio, ao conectar dispositivos via Bluetooth ou ao utilizar sistemas por aproximação baseados em NFC, como cartões contactless.

✔ Por que segurança em RF é importante

A segurança em RF tornou-se um tema essencial porque muitos dispositivos utilizam protocolos simples, sem criptografia, sem autenticação ou com códigos fixos que podem ser facilmente copiados, como é o caso de grande parte dos controles de portão, especialmente os mais antigos. Isso possibilita ataques como captura passiva (sniffing), reprodução de sinais (replay attacks), clonagem de dispositivos e até falsificação ativa de comandos (spoofing). Em sistemas desprotegidos, basta gravar um único sinal para reproduzir o comportamento original, comprometendo totalmente a confidencialidade e a autenticidade da comunicação.

✔ Objetivo do desafio

O objetivo do desafio é, portanto, compreender o comportamento de um sinal RF, demonstrar como a captura seria realizada na prática, analisar o arquivo fornecido e discutir ataques possíveis e mitigações aplicáveis no contexto da segurança cibernética de hardware.

---

2) Metodologia

Nesta etapa, o foco foi analisar o único sinal de radiofrequência (RF) do conjunto disponibilizado, identificado como controle1.wav, com o objetivo de identificar bursts presentes na transmissão e obter um padrão de sequência e duração. Para isso, foram utilizados dois softwares principais: Universal Radio Hacker (URH) e Audacity.

2.1. Ferramentas Utilizadas

Universal Radio Hacker (URH)

O URH foi utilizado para:

- carregar o arquivo de sinal RF;
- visualizar a representação I/Q;
- identificar bursts ao longo da transmissão;
- obter strings de bits associadas a cada burst;
- medir a duração de cada burst.

Audacity

O Audacity foi utilizado de forma complementar para:

- visualizar o waveform do sinal;
- observar a separação temporal entre bursts;
- confirmar visualmente a presença de picos e intervalos.

2.2. Procedimento de Análise

O processo foi dividido em etapas sequenciais:

1) Carregamento do sinal

O arquivo controle1.wav foi aberto diretamente no URH, através do menu File → Open File.
O programa reconheceu automaticamente o sinal como RF e exibiu a forma de onda.

2) Identificação de bursts

Na aba Interpretation, foi possível observar vários picos bem definidos ao longo da transmissão.
Cada pico foi selecionado individualmente com o mouse, destacando a região correspondente ao burst.

Para cada burst, o URH apresentou:

- uma string de bits (`010`, `010000`, etc.)
- uma estimativa de duração

Essas informações foram registradas manualmente conforme apareciam.

3) Medição complementar no Audacity

O mesmo arquivo foi carregado no Audacity para:

- confirmar a separação visual entre bursts;
- medir o tempo aproximado de duração em nanosegundos;
- verificar a consistência dos resultados.

Os dois softwares apresentaram resultados compatíveis, fortalecendo a interpretação.

2.3. Resultados Obtidos

Durante a análise, foram identificados 18 bursts distintos. Cada burst apresentou:

- uma string de bits associada
- uma duração aproximada

Duas categorias principais ficaram claras:

Tipo de burst	**String**	**Duração**
Curto	010	~6 ns
Longo	010000	~12 ns

Os bursts se repetem ao longo da transmissão formando uma sequência alternada:

- `[010, 010, 010, 010, 010000, 010000, 010000, ...]`

Essa repetição indica um padrão de transmissão estruturado, consistente com o comportamento esperado de um dispositivo de controle ou sinal digital simples.

2.4. Considerações

A análise mostrou que:

- O sinal não é aleatório;
- Existem apenas duas durações distintas para bursts;
- O comprimento temporal parece estar sendo usado como codificação.

Isso fornece informações suficientes para as próximas etapas do grupo, onde os colegas podem:

- comparar padrões entre sinais,
- buscar significado dos bits,
- ou inferir o protocolo utilizado.

---

3) Captura do Sinal

Como o foco do trabalho é analisar sinais de radiofrequência e compreender suas vulnerabilidades, nesta seção descrevemos como ocorreria o processo de captura de um sinal RF em um cenário real, mesmo que a captura prática não tenha sido realizada pelo grupo. A intenção é apresentar o procedimento técnico normalmente utilizado para registrar transmissões de dispositivos simples, como controles remotos operando na faixa de 433 MHz.

3.1 Processo Teórico de Captura

A captura de um sinal RF consiste em registrar a transmissão emitida por um dispositivo e convertê-la em um formato analisável. Em um ambiente prático, isso é feito com um equipamento de recepção (como um SDR) configurado para monitorar a frequência utilizada pelo transmissor. Assim, quando o dispositivo envia um comando, o receptor registra a energia transmitida naquele instante.

O objetivo é obter um arquivo bruto contendo o padrão temporal dos bursts transmitidos, que posteriormente pode ser estudado em ferramentas como o Universal Radio Hacker (URH).

3.2 Observação do Waterfall e Identificação do Pico

Em uma captura real, o primeiro passo seria observar o espectro em tempo real para verificar quando ocorre a transmissão. Isso é feito através do waterfall, que exibe a intensidade do sinal ao longo do tempo.
Sempre que o dispositivo emite um comando, surge:

- um pico de energia na faixa de frequência monitorada,
- seguido por múltiplos bursts curtos e longos, característicos de modulações simples como OOK/ASK.

Esses picos permitem confirmar visualmente que a transmissão está ativa e pronta para ser registrada.

3.3. Frequência Dominante do Sinal (Análise do Arquivo WAV)

Como o grupo trabalhou com um arquivo já disponibilizado em formato .wav, a análise realizada não reflete diretamente a frequência de radiofrequência original utilizada pelo dispositivo, mas sim a frequência dominante presente na forma de onda digitalizada.
Ao carregar o arquivo no software de análise, foi possível identificar que a frequência dominante do sinal presente no arquivo controle1.wav é aproximadamente 1166,7 Hz.
Como o arquivo já se encontra convertido em áudio, não é possível inferir a frequência de RF original (como 315, 433 ou 915 MHz). Assim, trabalhamos exclusivamente com o comportamento do sinal dentro do espaço amostral do arquivo fornecido.

3.4. Etapas da Captura

Para a captura, é necessário equipamentos capazes de obter RF, como um RLT-SDR, SDRPlay,Airspy e outros.

Caso o procedimento fosse realizado na prática, os seguintes passos seriam executados:

- Ajuste da Frequência: Sintonizar o receptor em 433,92 MHz, com largura de banda suficiente para capturar o espectro do sinal transmitido.
- Ajuste de Amplitude e Ruído: Regular os níveis de ganho para evitar saturação, reduzir ruído de fundo e garantir que os bursts apareçam bem definidos.
- Gravação do Sinal: Ao pressionar o botão do transmissor, o receptor registraria a transmissão em um arquivo bruto (.iq) ou convertido para áudio (.wav). Esse arquivo contém a estrutura temporal do sinal, necessária para a etapa seguinte de análise.

3.5. Evidências na Prática (representadas teoricamente)

Se o procedimento tivesse sido conduzido, seriam coletados:

- prints do waterfall mostrando o pico na transmissão;
- imagens da forma de onda contendo os bursts;
- visualizações do sinal sendo registrado;
- metadados da captura, como timestamp e frequência central.

No contexto deste trabalho, tais evidências são discutidas apenas de forma descritiva, representando o que ocorreria durante uma captura típica de RF.

---

4) Análise do Sinal

Com base na metodologia descrita e no processamento do arquivo controle1.wav utilizando as ferramentas Universal Radio Hacker (URH) e Audacity, realizamos a análise técnica do sinal interceptado. O processo foi dividido em inspeção da forma de onda, segmentação temporal e decodificação lógica.

4.1. Inspeção da Forma de Onda (Waveform)

A primeira etapa da análise consistiu na visualização do sinal no domínio do tempo. Ao carregar o arquivo no Audacity e no URH, identificou-se que o sinal não é contínuo, mas sim composto por "pacotes" de energia bem definidos, separados por intervalos de silêncio (ausência de portadora).

A análise visual confirmou que a modulação utilizada opera no princípio de "presença e ausência" de sinal, comportamento característico de modulações de amplitude do tipo OOK (*On-Off Keying*) ou ASK (*Amplitude Shift Keying*), amplamente utilizadas em controles de portões e dispositivos ISM (Industrial, Scientific, and Medical) de baixo custo.

4.2. Segmentação e Padrões Temporais

Através da ferramenta de análise automática do URH, o sinal foi segmentado em 18 *bursts* (pulsos de transmissão) distintos. A inspeção da duração desses pulsos revelou a existência de apenas dois comprimentos de onda predominantes, indicando uma codificação binária baseada em largura de pulso (PWM - *Pulse Width Modulation*):

- **Burst Curto:** Associado à sequência lógica de bits 010, com duração aproximada de 6 unidades de tempo.
- **Burst Longo:** Associado à sequência lógica de bits 010000, com duração aproximada de 12 unidades de tempo.

Essa consistência temporal (onde o pulso longo tem aproximadamente o dobro da duração do curto) reforça a tese de que o tempo de transmissão está sendo utilizado para diferenciar bits (0 e 1) ou símbolos do protocolo.

4.3. Decodificação e Lógica do Protocolo

Após a extração dos bits brutos de cada *burst*, observou-se a estrutura dos dados transmitidos. O sinal apresentou um padrão repetitivo e estruturado:[010, 010, 010, 010, 010000, 010000, 010000, ...]

A análise desta sequência permitiu concluir que:

1. **Ausência de Aleatoriedade:** O sinal não apresenta variações, contadores ou "sais" (*salts*) criptográficos entre as repetições.
2. **Protocolo de Código Fixo:** A repetição exata da mesma sequência de *bursts* (curtos e longos) confirma que o dispositivo transmissor utiliza um protocolo de *Fixed Code*.

4.4. Conclusão da Análise

A análise do sinal controle1.wav demonstrou que a transmissão carrega a informação de comando de forma estática, sem camadas de ofuscação ou criptografia dinâmica. O transmissor envia repetidamente a mesma sequência de pulsos (representados pelas strings 010 e 010000) enquanto o botão permanece pressionado.

Técnicamente, isso significa que a captura realizada contém toda a informação necessária para a replicação do comando. Uma vez que o padrão lógico e a temporização dos pulsos foram extraídos com sucesso, o sinal pode ser reconstruído e retransmitido por um atacante (ataque de *Replay*), conforme detalhado na seção de Vulnerabilidades a seguir.

---

5) Vulnerabilidades Encontradas

A partir da análise do sinal realizada, conseguimos obter algumas informações que permitiriam um ataque:

- Ausência de criptografia no sinal;
    - Em sistemas seguros, o sinal transmitido deveria ser o resultado de uma operação matemática complexa entre a informação original e uma chave secreta. Quando não há criptografia, o que é transmitido é a informação bruta.
    - Isso viola diretamente dois pilares da Segurança da Informação: **Confidencialidade** (qualquer um pode ler) e **Autenticidade** (não há como provar quem enviou).
    - Ataques:
        - A. Sniffing / Eavesdropping (Interceptação Passiva): Como o meio de transmissão é o ar (broadcast), o sinal se propaga em todas as direções. Sem criptografia, um atacante pode apenas "escutar" e interpretar os dados.
        - Replay Attack
        - Signal Spoofing: Este é mais sofisticado que o Replay. Se o sinal não é criptografado, o atacante pode realizar engenharia reversa do protocolo e criar comandos novos que nunca foram capturados.
        - **Como funciona:** Suponha que o sinal para "Ligar Luz" seja `1010` e "Desligar Luz" seja `1111`. Mesmo que o atacante só tenha capturado o sinal de "Ligar", ele pode deduzir ou testar o sinal de "Desligar" e gerá-lo via software (como no GNU Radio ou URH).

- Código do sinal é fixo (claro, usamos somente um sinal, mas a ideia é emular um dispositivo simples que não use rolling code);
    - Em sistemas de Código Fixo, o transmissor envia exatamente a mesma sequência de bits toda vez que o botão é pressionado. Não há variação, contador, timestamp ou "sal" (salt) na transmissão. É o equivalente digital a uma chave de metal física: a forma da chave nunca muda.
    - Ataques:
        - Clonagem de Dispositivo
        - Ataque de Força Bruta:

          Muitos sistemas de código fixo antigos utilizam configurações manuais (como *DIP Switches* de 8 ou 10 pinos) para definir o código.

          - **Como funciona:** O espaço de chaves (keyspace) é muito pequeno (ex: 28=256 possibilidades ou 210=1024). Um atacante pode usar um script (ex: no Arduino ou Flipper Zero) para testar todas as combinações possíveis em questão de segundos ou minutos até o portão abrir.
        - Replay Attack:

Temos duas vulnerabilidades principais que possibilitam o replay attack. A ideia da exploração será, então, encontrar qual é esse código fixo para que possa ser possível reproduzi-lo posteriormente. Para isso, será necessário conhecer a frequência do sinal.

É importante fazer algumas considerações: dispositivos atuais costumam usar a técnica de rolling code ou hopping code - ou seja, o código transmitido por eles não é sempre o mesmo - e, dessa forma, não haveria uma das vulnerabilidades importantes para usar esse ataque simples.

Tendo a frequência do sinal, o que será feito pelo replay attack é reproduzir o que foi captado sem ter a necessidade de entendê-lo, e dado um receptor que - aparentemente - não possui requisição de autenticação, utilizando a frequência correta de transmissão, ele deve receber o comando malicioso sem empecilhos.

Pelos mesmos motivos, também se torna possível o spoofing: neste caso, o atacante não só reproduz um sinal antigo, mas forja um novo sinal que imita o transmissor legítimo,

fazendo-se passar por ele e podendo emitir comandos diferentes daqueles previamente capturados.

---

6) Demonstration / PoC

Infelizmente, não temos o equipamento certo para testar nada

✔ Evidência de que o sinal pode ser reproduzido

✔ mostrar o comando sendo repetido

✔ resultado prático:

- **luz ligada**
- **campainha tocada**
- **log mostrando resposta**
- **Abrir porta de carro com replay bufferizado**

reenvio do mesmo sinal produziu o mesmo comportamento, em teoria

---

7) Mitigações e Boas Práticas

As mitigações e boas práticas focadas em RF visam tornar esses sinais capturados inúteis para o atacante, ou garantir que o sistema não aceita comandos não autorizados.

1. Criptografia Forte

A criptografia é a fundação da segurança em comunicações RF. Seu objetivo é tornar os dados (o payload) ilegíveis, mesmo que o sinal seja interceptado.

Princípio: Utilizar algoritmos robustos (como AES) para embaralhar a informação antes da transmissão.

Exemplos:

Wi-Fi: Adotar WPA3 (ou WPA2 com 802.11w para proteger quadros de gerenciamento) em vez de protocolos mais antigos e quebráveis, como WEP.

Rádios Digitais: Usar rádios bidirecionais que oferecem criptografia digital para embaralhar as comunicações de voz e dados, impedindo a escuta.

Boas Práticas: Garantir que o firmware dos dispositivos (roteadores, IoT, etc.) esteja sempre atualizado para suportar os protocolos de criptografia mais recentes e corrigir vulnerabilidades.

2. Rolling Code (Código Rolante)

O rolling code é uma mitigação crucial contra ataques de repetição (replay attacks) em dispositivos de acesso, como portões de garagem e sistemas de alarme.

Funcionamento: Em vez de transmitir um código de acesso fixo (que pode ser capturado e retransmitido), o controle remoto e o receptor usam um algoritmo sincronizado para gerar um código único e diferente a cada acionamento.

Vantagem: Se um atacante capturar um código, ele será inútil na próxima tentativa, pois o código válido já terá "rolado" para o próximo na sequência. Se o receptor não receber os códigos na ordem esperada, ele rejeita o comando, protegendo contra clonagem.

3. Autenticação e Autorização

A autenticação garante que apenas dispositivos confiáveis possam se comunicar ou enviar comandos.

Protocolos: Implementar protocolos de comunicação que exigem um processo de handshake seguro e verificação de credenciais antes de permitir a transmissão de dados.

Limitação de Acesso: Em ambientes corporativos, limitar o acesso físico e lógico aos rádios e pontos de acesso apenas a pessoal autorizado, implementando mecanismos de autenticação de usuário no próprio equipamento (se disponível).

4. Detectar Repetições (Anti-Replay) e Limitar Retransmissões

Esta técnica visa especificamente anular o ataque de repetição, muitas vezes em conjunto com o rolling code.

Detectar Repetições: Os sistemas (como o receptor do portão) devem manter um registro dos códigos mais recentes válidos. Se um código capturado for retransmitido, o sistema o reconhece como um código antigo (ou fora da sequência esperada) e o rejeita.

Limitar Retransmissões: Configurar o receptor para aceitar comandos de um único dispositivo/código em um intervalo de tempo limitado. Se receber o mesmo código (ou códigos muito próximos na sequência) repetidamente em segundos, o sistema deve bloquear temporariamente o dispositivo, o que ajuda a frustrar ataques de força bruta ou repetição rápida.

5. Outras Técnicas Importantes

Otimização de Potência: Reduzir a potência de transmissão de RF (quando possível) para que o sinal não se estenda desnecessariamente para fora da área de cobertura pretendida, diminuindo a chance de interceptação a longa distância.

Frequência e Canal: Em redes Wi-Fi, escolher canais menos congestionados e adotar bandas de frequência menos comuns (como 5 GHz) pode reduzir a interferência e o foco de ataque em ambientes urbanos.

Monitoramento Ativo: Usar analisadores de espectro ou software de monitoramento de rede para identificar e alertar sobre transmissões anômalas, Access Points não autorizados ("rogue APs") ou atividades de sniffing na rede.

---

8) Conclusões

✔ importância para segurança do mundo real

A segurança em RF é essencial porque muitos dispositivos cotidianos (como controles de portão, alarmes de baixo custo e algumas chaves automotivas antigas) utilizam protocolos simples sem criptografia ou autenticação robusta.

- Ameaça de Replay Attack: A demonstração da vulnerabilidade ao código fixo mostra que um atacante pode facilmente capturar o sinal transmitido no ar (sniffing) e, em seguida, reproduzi-lo com um transmissor para obter o mesmo efeito (ex: abrir um portão ou desativar um alarme).
- Violação de Confidencialidade e Autenticidade: A ausência de criptografia e a codificação estática violam diretamente os pilares de Confidencialidade (qualquer um pode ler o comando) e Autenticidade (não há como provar a origem do comando).
- Recomendação de Mitigações: O estudo enfatiza que a segurança em RF depende da implementação de Criptografia Forte e, principalmente, do Rolling Code (Código Rolante) , que muda o código a cada transmissão, tornando os sinais capturados inúteis para futuros ataques

✔ limitações do experimento

Embora o experimento prático de *Replay Attack* não tenha sido realizado por falta de equipamento específico, a análise teórica e técnica do sinal fornecido comprovou que o dispositivo, se real, seria altamente vulnerável.

O trabalho ressalta a importância da Segurança Cibernética em Hardware, uma vez que muitos dispositivos cotidianos, como controles de portão e chaves automotivas antigas, ainda utilizam protocolos simples e desprotegidos. A captura de RF, o *Sniffing* e o *Replay Attack* são ameaças reais que podem comprometer a segurança física e patrimonial se as mitigações (como o *Rolling Code* e a criptografia) não forem implementadas.