

CAPTURA DE RF

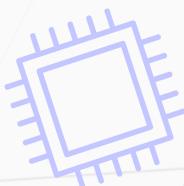
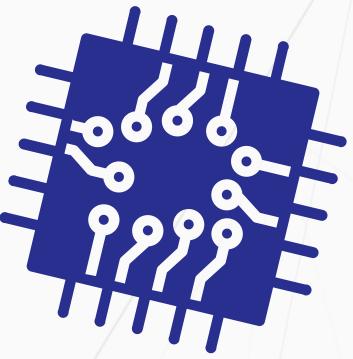
Segurança Cibernética - Universidade federal de São
Carlos - Departamento de Computação

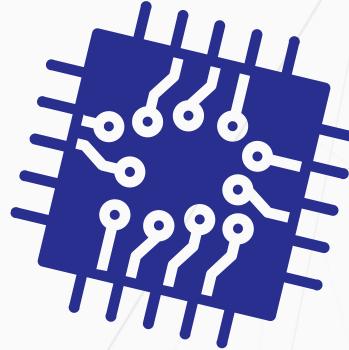


Bruno Nieri Nunes - 820590
Gustavo Kim Alcantara - 820763
Guilherme Bartoletti Oliveira - 821881
Lucas Mantovani - 794040
Maykon dos Santos Gonçalves - 821653
Pietro Bernardo Dutra Scaglione - 824375
Tiago de Paula Evangelista - 824369
Vinícius Marto da Veiga - 821252



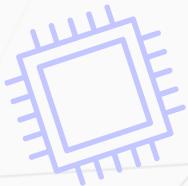
INTRODUÇÃO





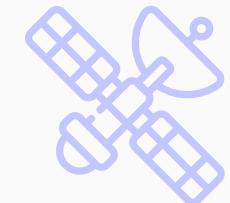
- **O que é RF e captura de sinais:**

Radiofrequência (RF) são sinais eletromagnéticos eletromagnéticos que se propagam pelo ar e permitem a comunicação sem fio entre dispositivos. Como esses sinais viajam de forma aberta e em todas as direções, ficam naturalmente expostos à interceptação. A captura de RF consiste justamente em receber e analisar esses sinais para detectar ou extrair informações transmitidas.



- **Onde RF aparece 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**

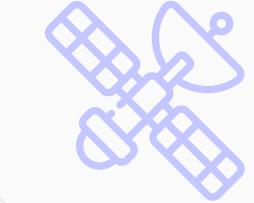
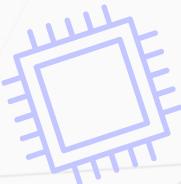
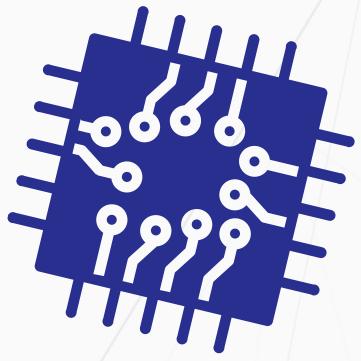
A segurança em RF tornou-se um tema essencial porque muitos dispositivos utilizam protocolos simples, sem criptografia, sem autenticação ou com códigos fixos que podem ser facilmente copiados, como é o caso de grande parte dos controles de portão, especialmente os mais antigos. Isso possibilita ataques 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.



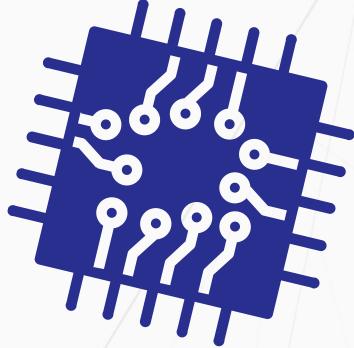
- **Objetivo do desafio**

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.

METODOLOGIA

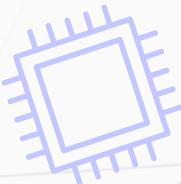


METODOLOGIA



OBJETIVOS:

- Analisar o sinal RF controle1.wav
- Identificar bursts
- Medir strings e duração

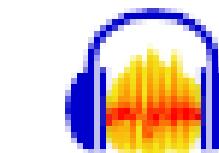


FERRAMENTAS ESCOLHIDAS:

- URH (Universal Radio Hacker)
 - visualizar o sinal
 - selecionar bursts
 - extrair strings e duração
- Audacity
 - confirmar waveform e tempos

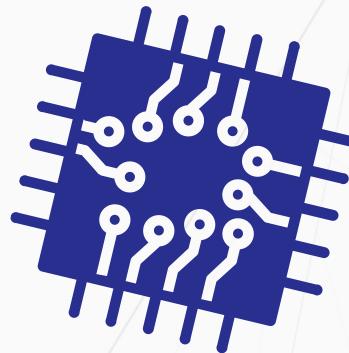


Universal Radio Hacker



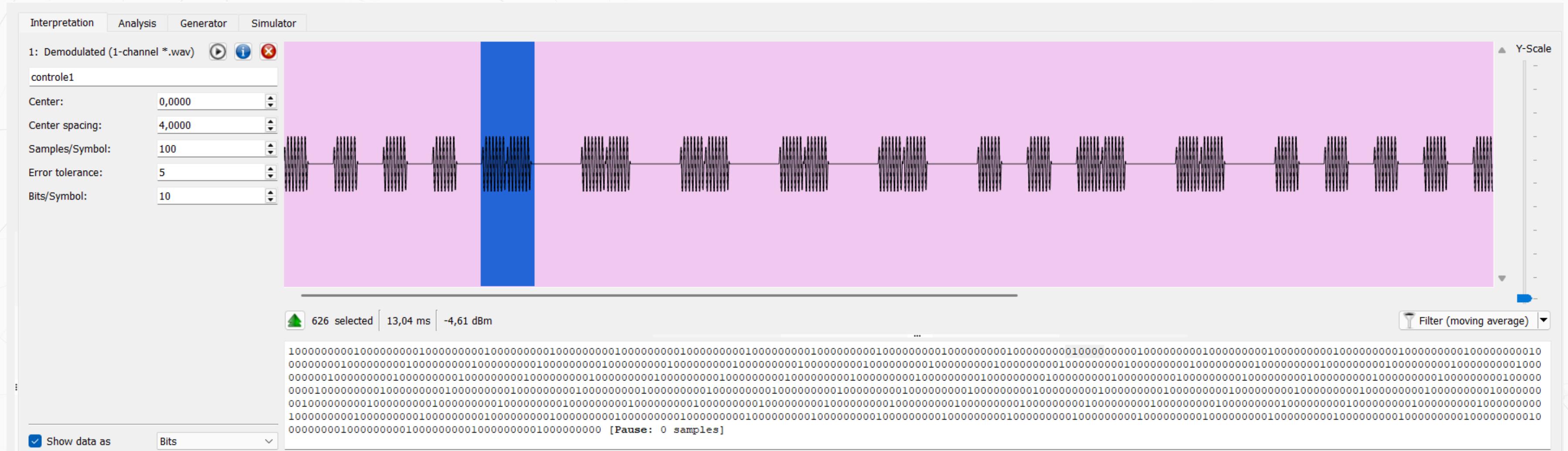
Audacity





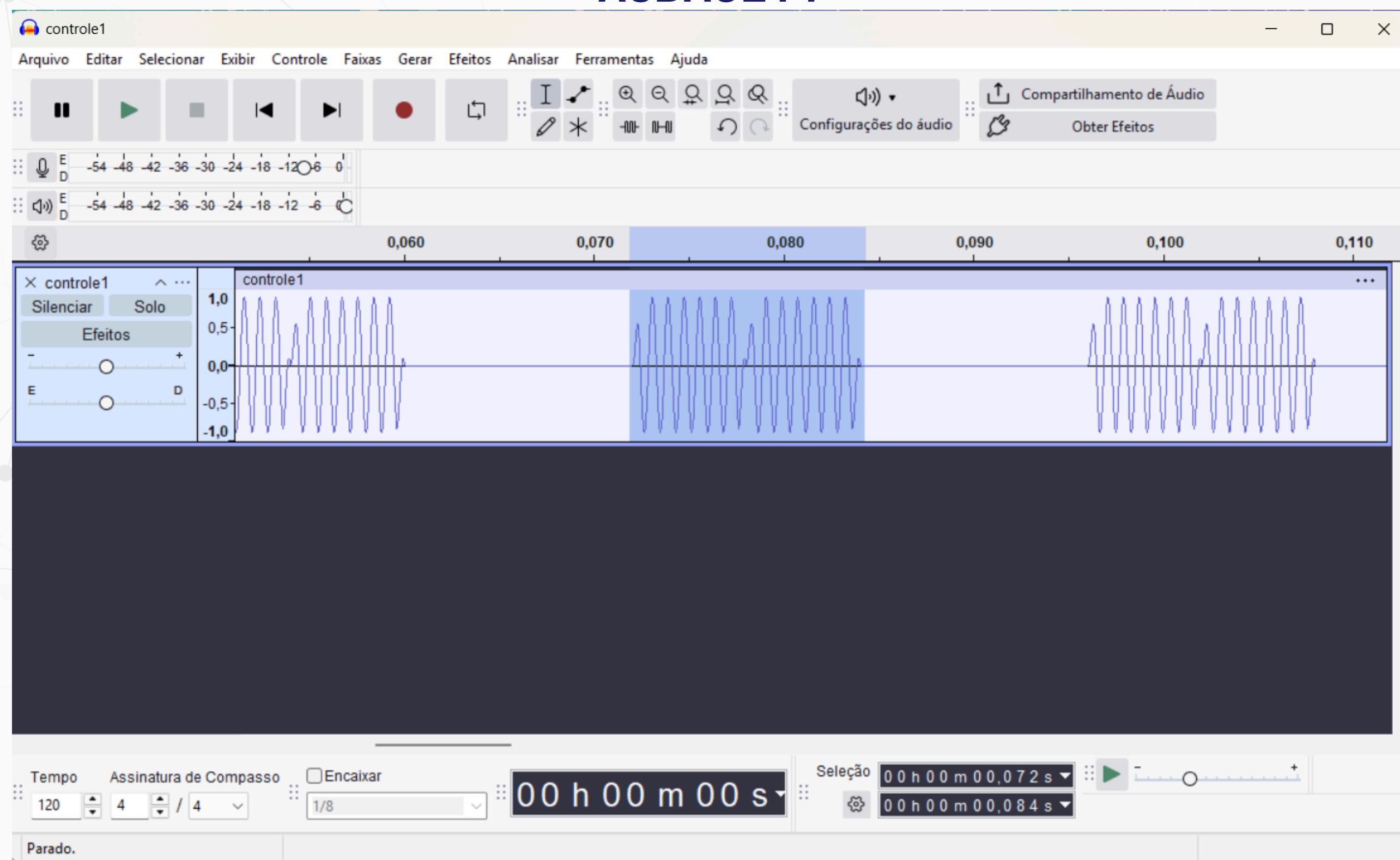
METODOLOGIA

UNIVERSAL RADIO HACKER



METODOLOGIA

AUDACITY



METODOLOGIA

PASSOS REALIZADOS:

- Passos realizados:
- Abrir controle1.wav no URH
- Selecionar bursts individualmente
- Registrar:
- string de bits
- duração aproximada
- Confirmar tempos no Audacity

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



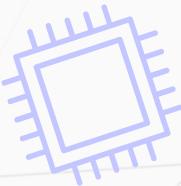
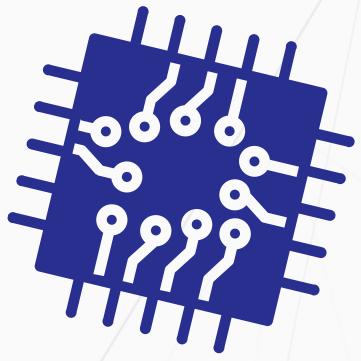
METODOLOGIA

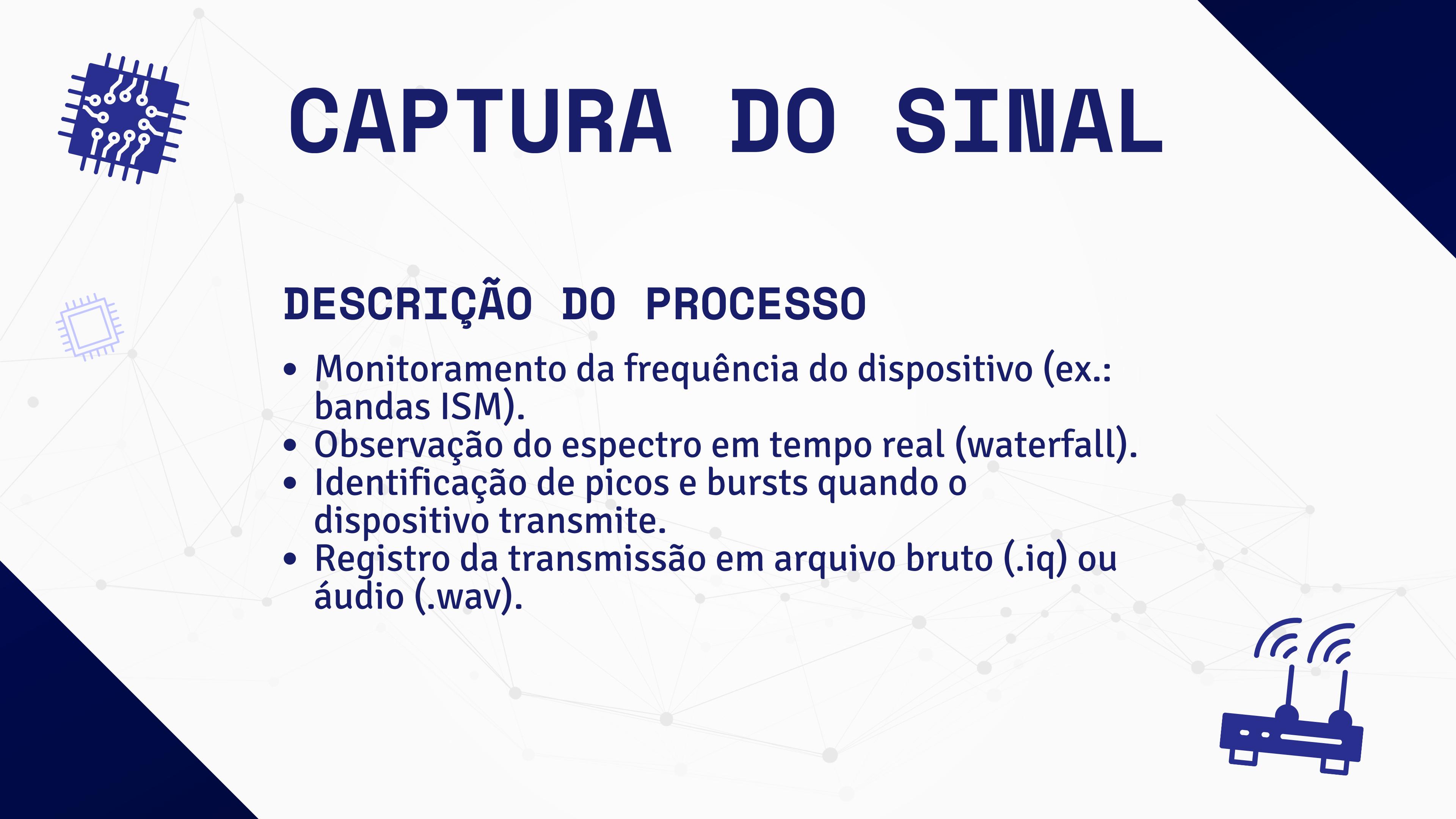
CONSIDERAÇÕES DA FASE INICIAL:

- O sinal RF não é aleatório
- Bursts possuem duas durações distintas
- A duração pode representar informação binária
- Padrão foi entregue ao grupo para comparação com outros sinais



CAPTURA DO SINAL





CAPTURA DO SINAL

DESCRIÇÃO DO PROCESSO

- Monitoramento da frequência do dispositivo (ex.: bandas ISM).
- Observação do espectro em tempo real (waterfall).
- Identificação de picos e bursts quando o dispositivo transmite.
- Registro da transmissão em arquivo bruto (.iq) ou áudio (.wav).



CAPTURA DO SINAL

ARQUIVO ANALISADO

- Sinal fornecido em formato .wav.
- Frequência escolhida: 433,92 MHz.
- Representa o sinal já convertido em áudio.

CAPTURA DO SINAL

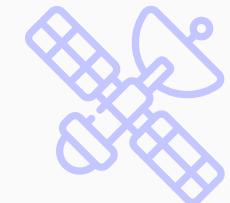
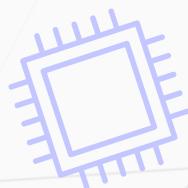
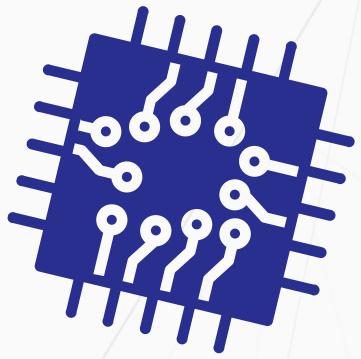
ETAPAS DE UM PROCESSO DE CAPTURA

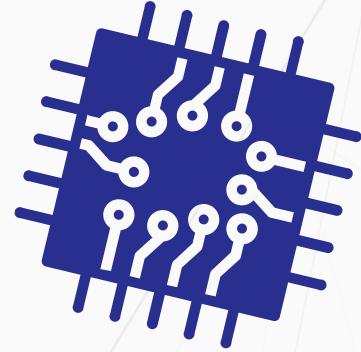
- Identificar a banda de operação
- Ajustar frequência do receptor
- Ajustar amplitude (ganho)
- Reduzir ruído
- Gravar o sinal bruto
- Analisar no URH



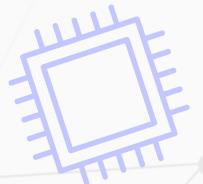
ANÁLISE DO SINAL

INSPEÇÃO, DECODIFICAÇÃO E PADRÕES





INSPEÇÃO DA FORMA DE ONDA

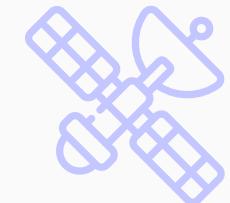


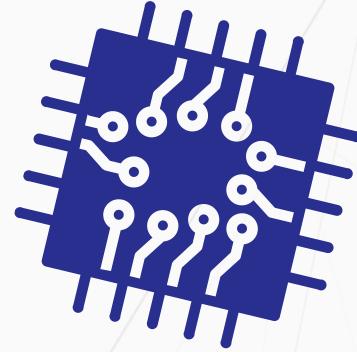
CARACTERÍSTICAS VISUAIS

NÃO CONTÍNUO: PACOTES DISCRETOS DE ENERGIA (BURSTS) SEPARADOS POR SILENCIO.

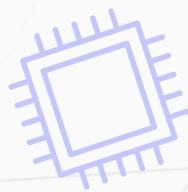
MODULAÇÃO OOK/ASK: BASEADA NA PRESENÇA (ON) E AUSÊNCIA (OFF) DA PORTADORA.

PADRÃO TÍPICO: COMUM EM DISPOSITIVOS ISM E CONTROLES DE PORTÃO DE BAIXO CUSTO (433 MHZ).



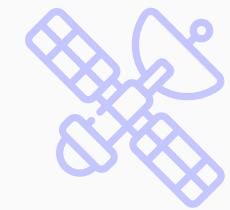


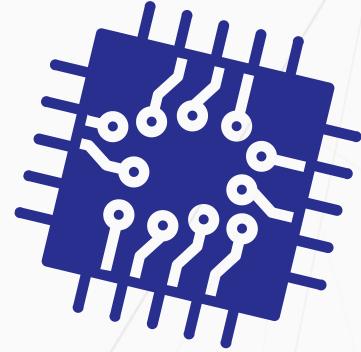
SEGMENTAÇÃO TEMPORAL



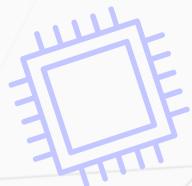
A análise automática identificou 18 bursts. Foram detectados apenas dois comprimentos de onda, indicando codificação binária (PWM).

TIPO DE BURST	BITS	DURAÇÃO	INTERPRETAÇÃO
Burst Curto	010	~6 ns	Bit '0' / Símbolo A
Burst Longo	010000	~12 ns	Bit '1' / Símbolo B
Conclusão: O pulso longo tem aprox. o dobro da duração do curto.			





LÓGICA DO PROTOCOLO



ESTRUTURA DOS DADOS

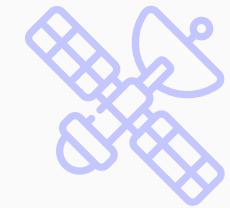
O sinal extraído apresentou a seguinte sequência repetitiva:

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

A repetição exata confirma a ausência de contadores ou variáveis dinâmicas.

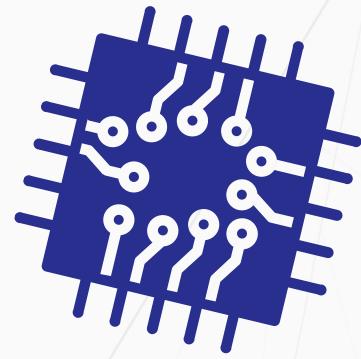
CONCLUSÕES DE SEGURANÇA

Sem Aleatoriedade:
Não há "salts" ou Rolling Code.

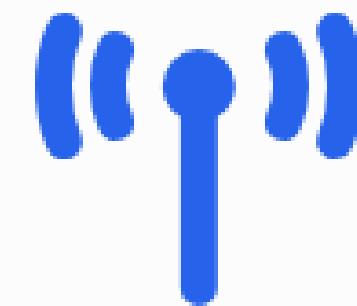


Código Fixo:
O transmissor envia sempre a mesma sequência estática.

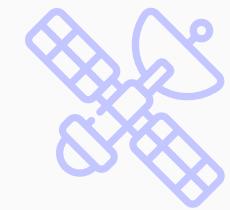


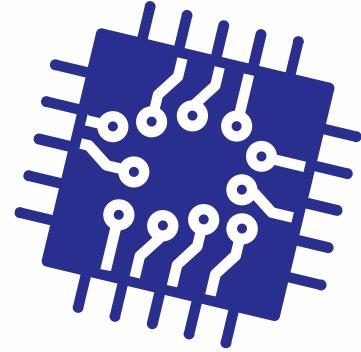


SINAL VULNERÁVEL

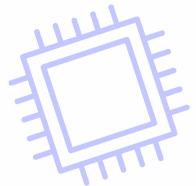


A captura contém 100% da informação necessária para replicar o comando. O sistema está suscetível a ataques de Replay simples.





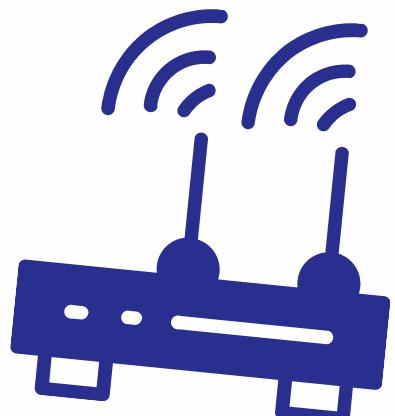
VULNERABILIDADES

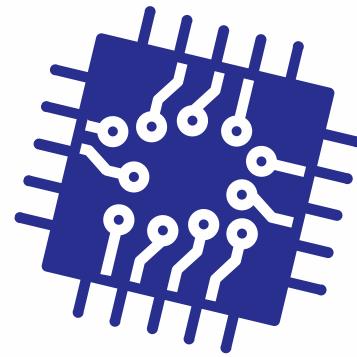


- **Sinal sem criptografia/autenticação;**
- **Código do sinal é fixo (só temos um sample, assumiremos isso).**

O que isso possibilita?

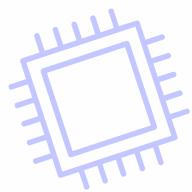
- **Replay attack: reprodução do sinal sem entendê-lo;**
- **Sniffing: interpretação passiva;**
- **Spoofing: replay mais sofisticado;**
- **Clonagem de dispositivo.**



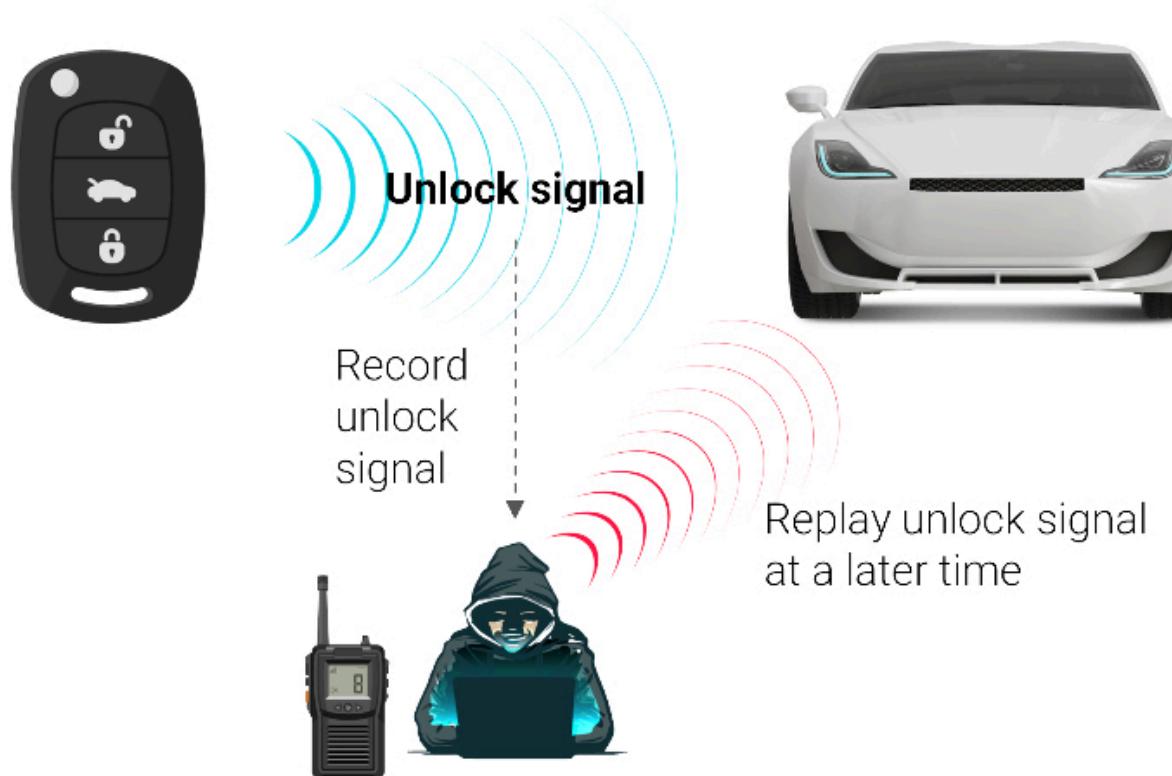


VULNERABILIDADES

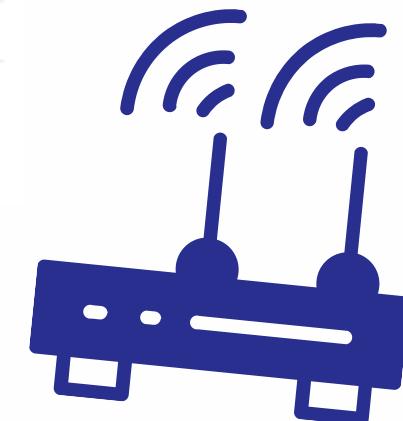
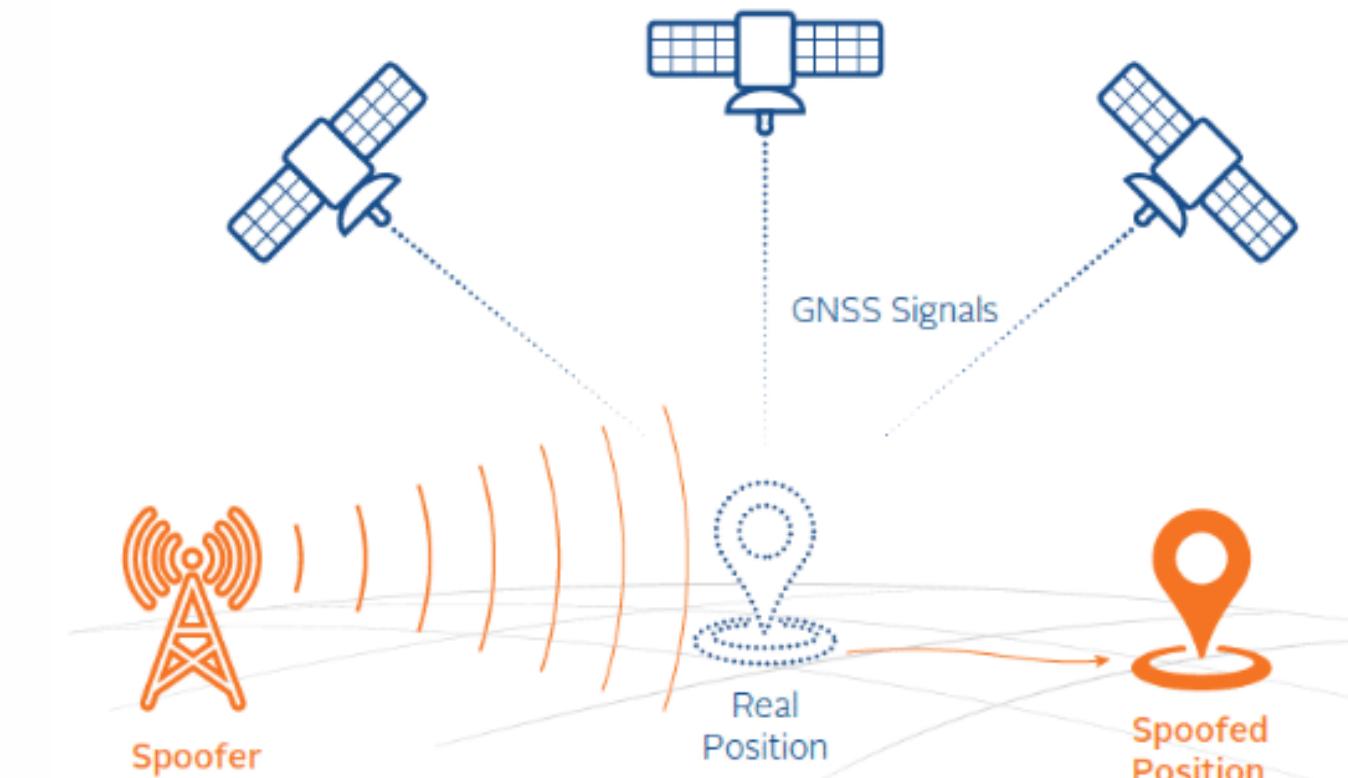
Ausência de criptografia no sinal;

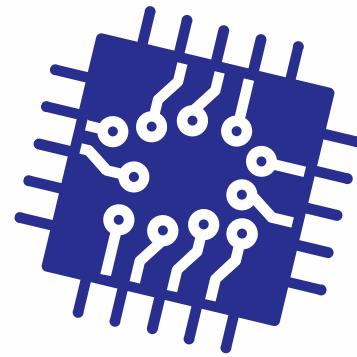


Replay Attack

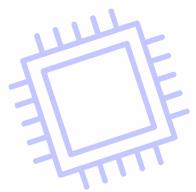


Spoofing





VULNERABILIDADES

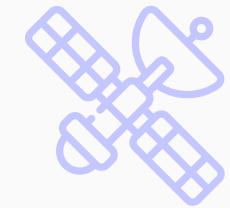
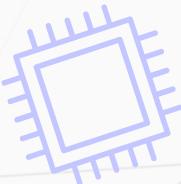
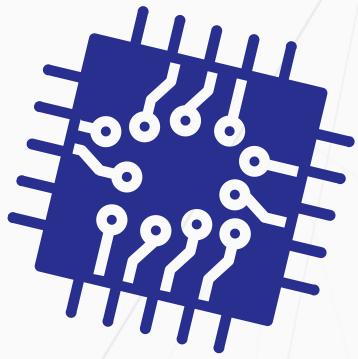


Ausência de criptografia no sinal;

Clonagem de dispositivo



MITIGAÇÕES E BOAS PRÁTICAS



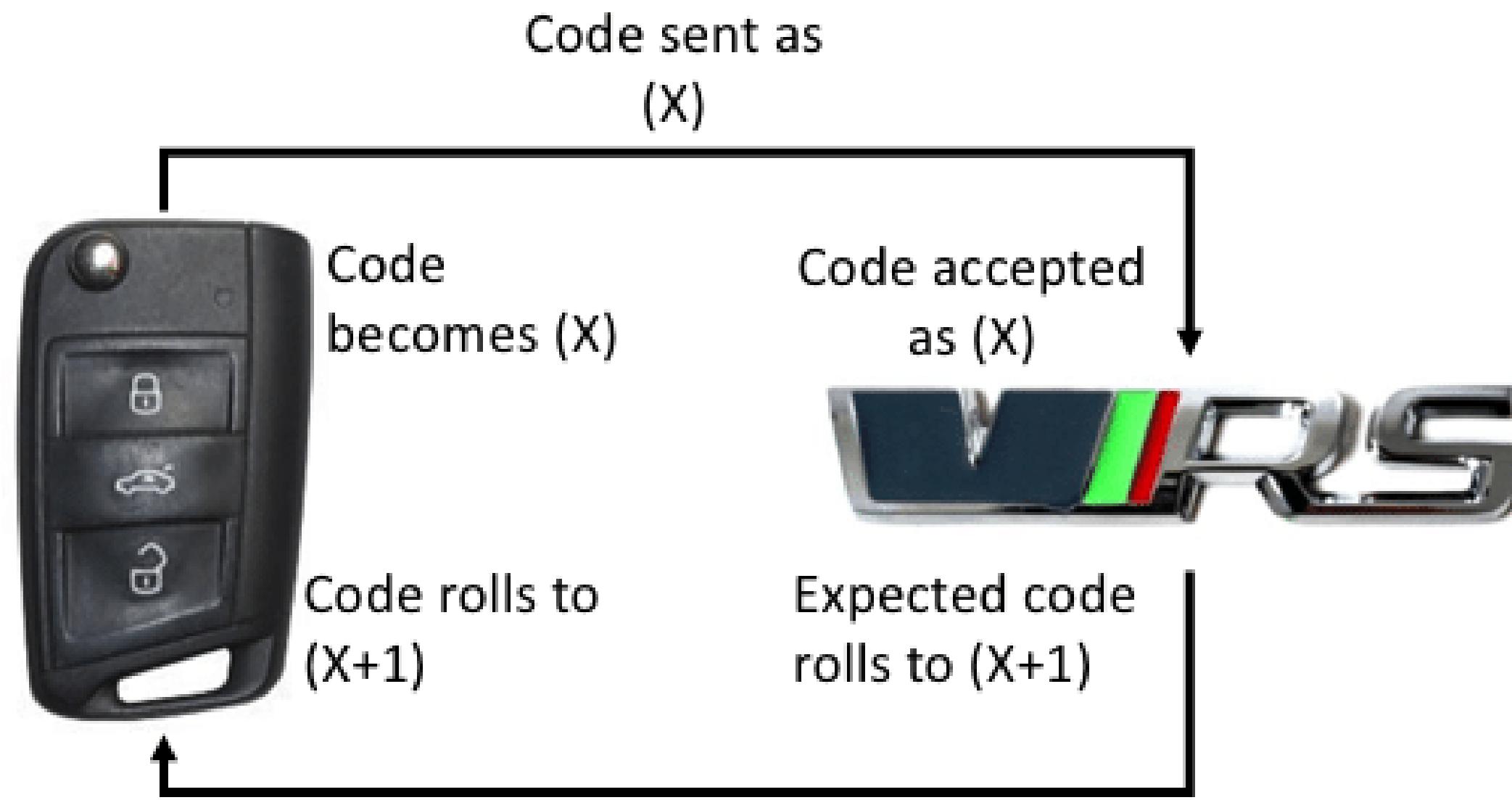
MITIGAÇÕES E BOAS PRÁTICAS

Criptografia forte



MITIGAÇÕES E BOAS PRÁTICAS

Rolling Code



MITIGAÇÕES E BOAS PRÁTICAS

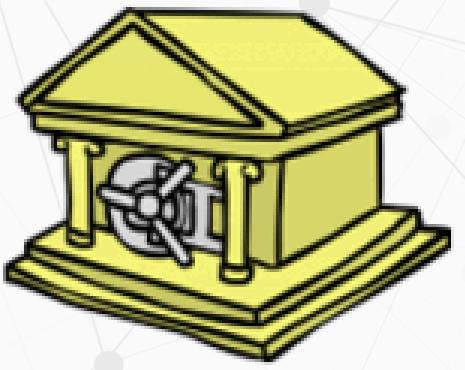
Autenticação e Autorização



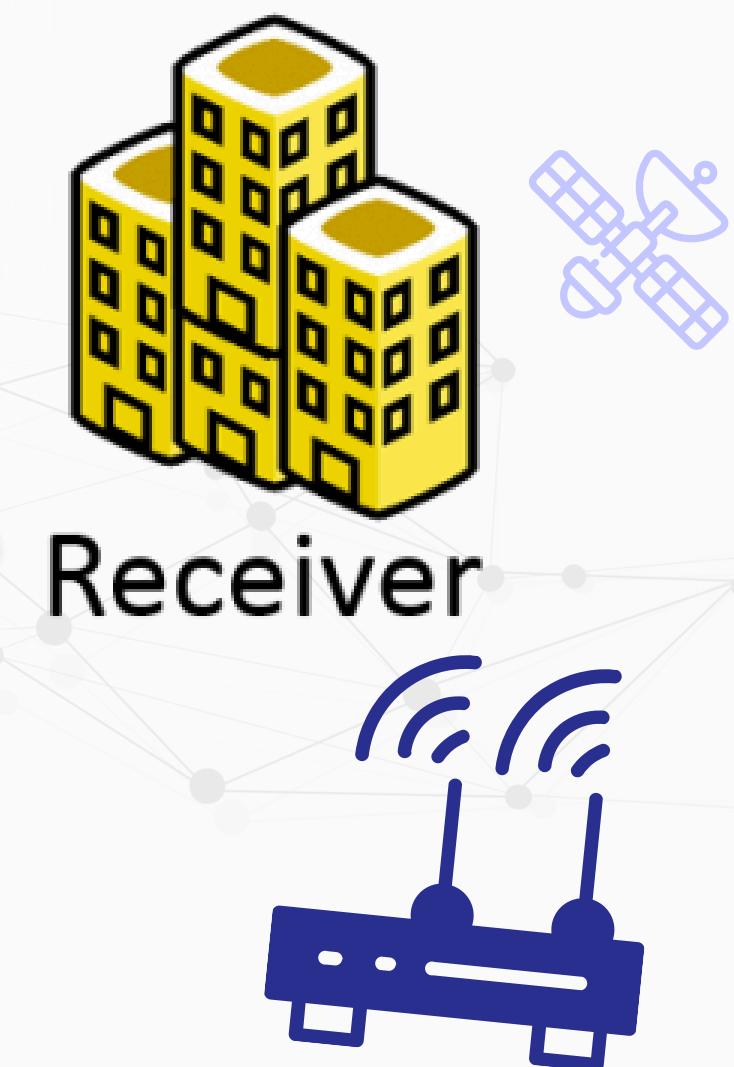
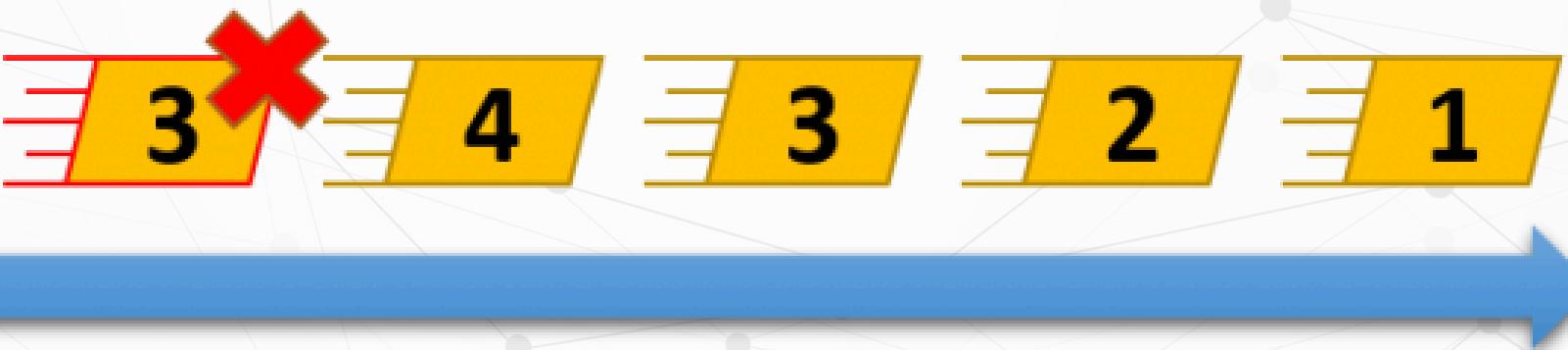
MITIGAÇÕES E BOAS PRÁTICAS

Anti - Replay

PRACTICAL NETWORKING .NET



Sender



Receiver

MITIGAÇÕES E BOAS PRÁTICAS

Outros:

- Otimização de Potência
- Frequência e Canal
- Monitoramento Ativo

LIMITAÇÕES

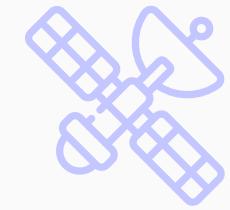
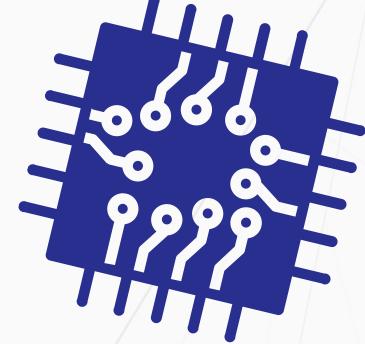
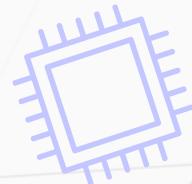
- EMBORA O EXPERIMENTO DE REPLAY ATTACK NÃO TENHA SIDO REALIZADO POR FALTA DE EQUIPAMENTO ESPECÍFICO PUDEMOS REPLICAR AS PRIMEIRAS ETAPAS DE UM **CTF DE RF**, E A ANÁLISE TEÓRICA E TÉCNICA DO SINAL FORNECIDO DEMONSTROU QUE O DISPOSITIVO, SE REAL, SERIA **ALTAMENTE VULNERÁVEL**.

IMPORTÂNCIA

- **AMEAÇA DE REPLAY ATTACK:** A DEMONSTRAÇÃO DA VULNERABILIDADE AO CÓDIGO FIXO MOSTRA QUE UM ATACANTE PODE FACILMENTE CAPTURAR O SINAL TRANSMITIDO NO AR E, EM SEGUIDA, REPRODUZIR COM UM TRANSMISSOR PARA OBTER O MESMO EFEITO (EX: ABRIR UM PORTÃO OU DESATIVAR UM ALARME).

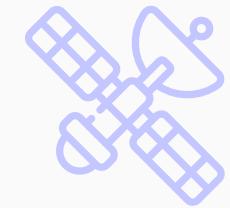
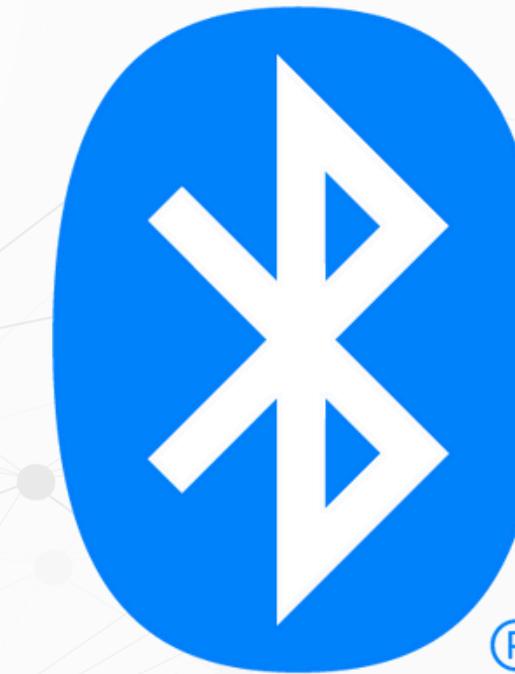
IMPORTÂNCIA

- **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).



CONCLUSÃO

- A segurança em RF é essencial porque muitos dispositivos cotidianos utilizam protocolos simples sem criptografia ou autenticação robusta.



FIM

