Estudo Sobre o Impacto das Vulnerabilidades de um Cartão Inteligente Sem Contato

Luiz Eduardo Mendes Matheus (UFJF), Eduardo P. Julio (UFJF),
Alex B. Vieira (UFJF), Edelberto Franco (UFJF)

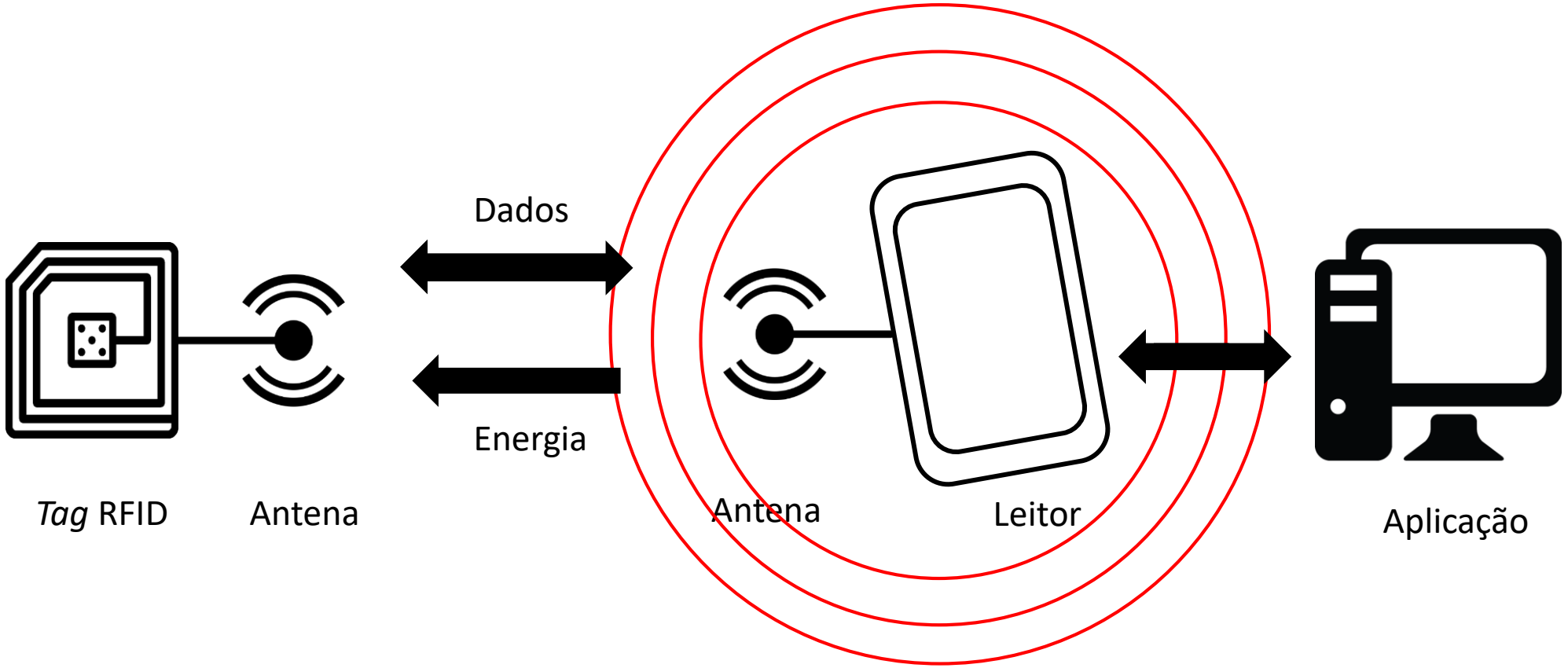
Agenda

- Introdução
- Motivação
- Estrutura do cartão
- Trabalhos relacionados
- Metodologia de ataque
- Soluções
- Contribuições

Introdução

- O que é RFID?
  - ***R****adio-****F****requency* ***Id****entification*
  - Uso de ondas de rádio para identificação e rastreamento de objetos
  - Modernização de tecnologias como código de barras
  - Dois principais componentes: *Tag* e Leitor

Introdução



Aplicações

- Controle de acesso
- Bilhetagem eletrônica
  - Metrôs
  - Ônibus
  - Estacionamento Rotativo
  - Crédito em RUs
- Rastreamento de mercadorias
- Rastreamento de gado

Problema

- Transações financeiras e controle de acesso
- Diversas empresas confiam no cartão inteligente utilizado
- Cartões com criptografia proprietária
  - Segurança através da obscuridade

Utilização de cartões inteligentes cujas vulnerabilidades foram expostas!

Justificativa

- Cartão escolhido:
  - *Mifare Classic* 1K
- Empresas que o utilizam:
  - Rio Card
  - BHTrans
  - Bilhete Único - Juiz de Fora
  - Postos de gasolina - Shell
  - Estacionamento rotativo – Juiz de Fora-MG, São Carlos-SP, Itajaí-SC, São Paulo-SP, Vila Velha-ES, ...

Justificativa – Exemplo de Impacto

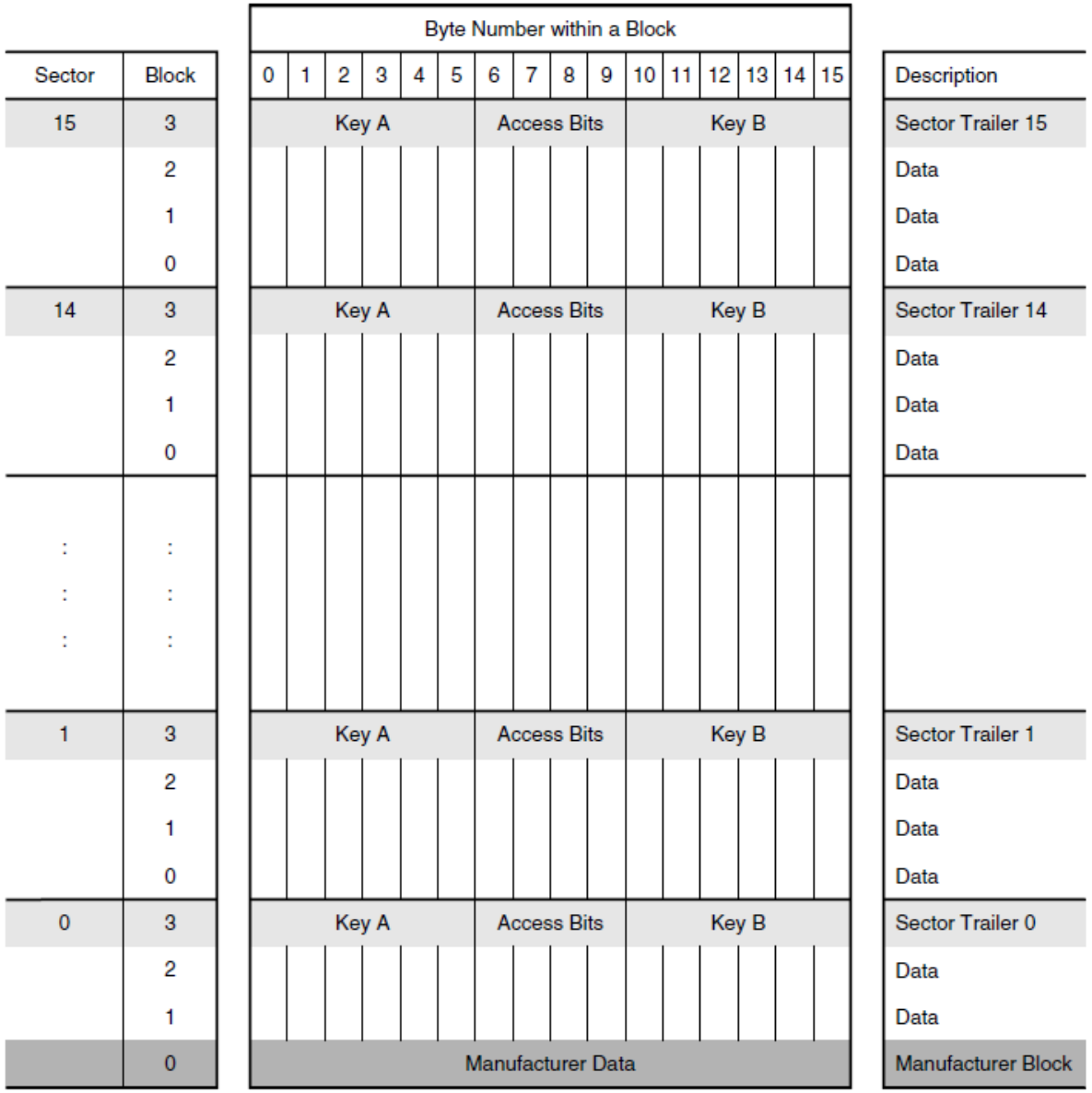
- Estacionamento rotativo – Atuação em 17 cidades brasileiras
- Juiz de Fora (aproximadamente 600 mil habitantes)
  - Mais de 2392 vagas para carros e 358 para motos
  - R$ 2,30 – 2 horas
- Considerando uma ocupação mensal de 50% das vagas disponíveis.
  - Período de 8h/dia (horário comercial) e 40h/semana (dias úteis)
  - Total: R$ 11.003,20/dia ou R$ 220.064,00/mês (20 dias úteis)
  - Considerando que 10% dos usuários realizem o ataque:

Só na cidade de Juiz de Fora!!

Prejuízo mensal próximo de R$ 20.000,00

Estrutura do cartão

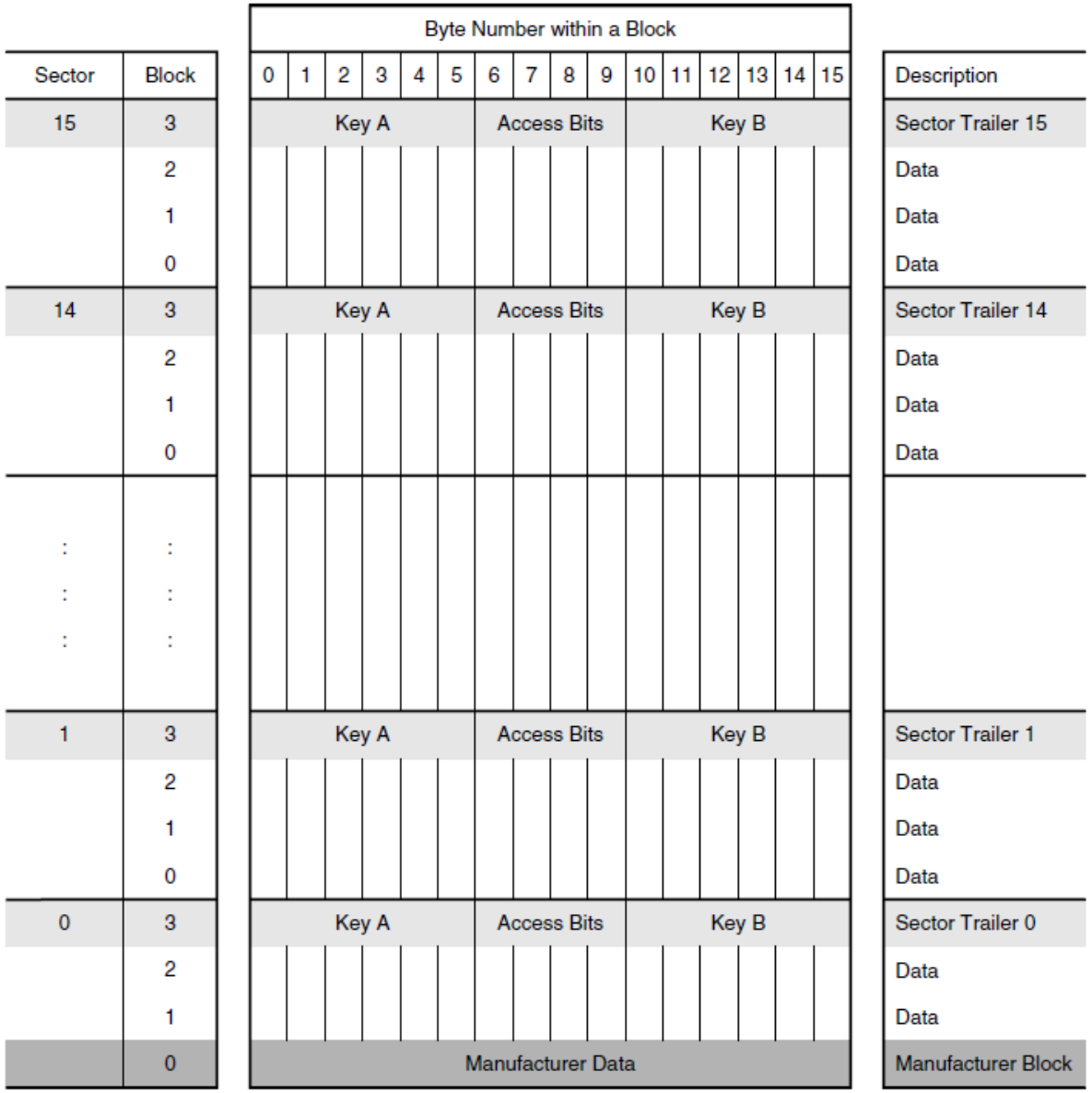
- Memória interna de 1Kb
- 16 setores
- 1 Setor – 4 blocos
- 1 bloco – 16 bytes



Sector	Block	Byte Number within a Block 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0	Manufacturer Data																Manufacturer Block

Estrutura do cartão

- Chaves são guardadas no último bloco de cada setor.
  - Chave A e B (48 bits)
  - Condições de acesso
- Bloco 0: Protegido contra escrita.
  - Contém o identificador do cartão.



Sector	Block	Byte Number within a Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Description
15	3	Key A | Access Bits | Key B	Sector Trailer 15
	2		Data
	1		Data
	0		Data
14	3	Key A | Access Bits | Key B	Sector Trailer 14
	2		Data
	1		Data
	0		Data
:	:		
:	:		
:	:		
1	3	Key A | Access Bits | Key B	Sector Trailer 1
	2		Data
	1		Data
	0		Data
0	3	Key A | Access Bits | Key B	Sector Trailer 0
	2		Data
	1		Data
	0	Manufacturer Data	Manufacturer Block

Estrutura do cartão

- Transições autorizadas de acordo com condições de acesso.
- Protocolo de autenticação mútua em três passos.
- *Crypto-1*: Criptografia proprietária.
  - Implementada em *hardware*
  - Segurança através de obscuridade

Vulnerabilidades conhecidas

- Força bruta (Nohl *et al*., 2008)
  - Utilização da placa FPGA Copacobana
  - 50 minutos para recuperar a chave de 48 bits
- **Mfcuk**: Exposição de *keystream* (Courtois *et al*., 2009)
  - Recupera uma chave do cartão, explorando as vulnerabilidades do processo de autenticação
- **Mfoc:** Autenticação aninhada (Garcia *et al*., 2009)
  - Explora a vulnerabilidade do gerador de números pseudo-aleatórios
  - Utiliza uma chave previamente conhecida
  - Recupera as demais chaves do cartão

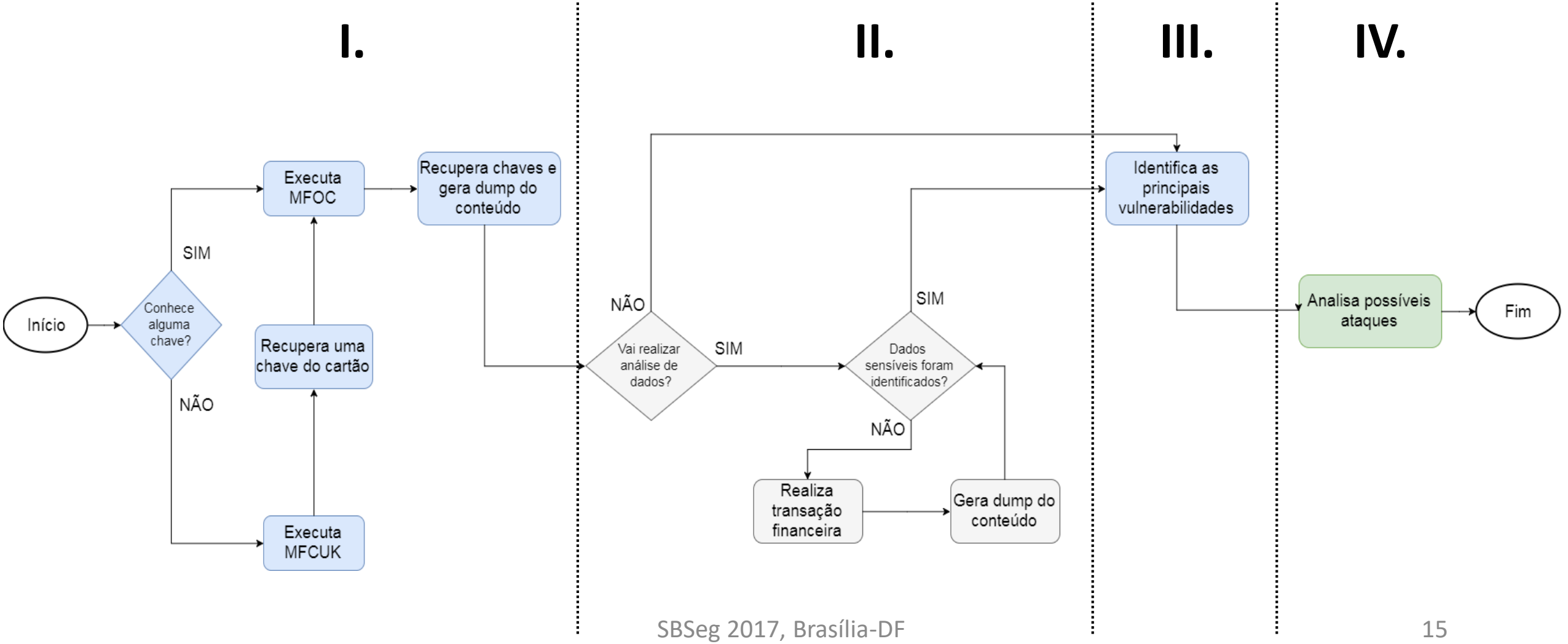
Estudo de caso

- Cenário escolhido:
  - Estacionamento rotativo
- Ferramentas:
  - Leitor NFC ACR122U
  - Raspberry Pi B+

Metodologia de ataque

I. Recuperação de chaves utilizando algoritmos **mfcuk** e **mfoc**
II. Análise de conteúdo do cartão
III. Identificação das vulnerabilidades e falhas de segurança
IV. Análise de possíveis ataques

Metodologia de ataque



I. Recuperação das chaves secretas

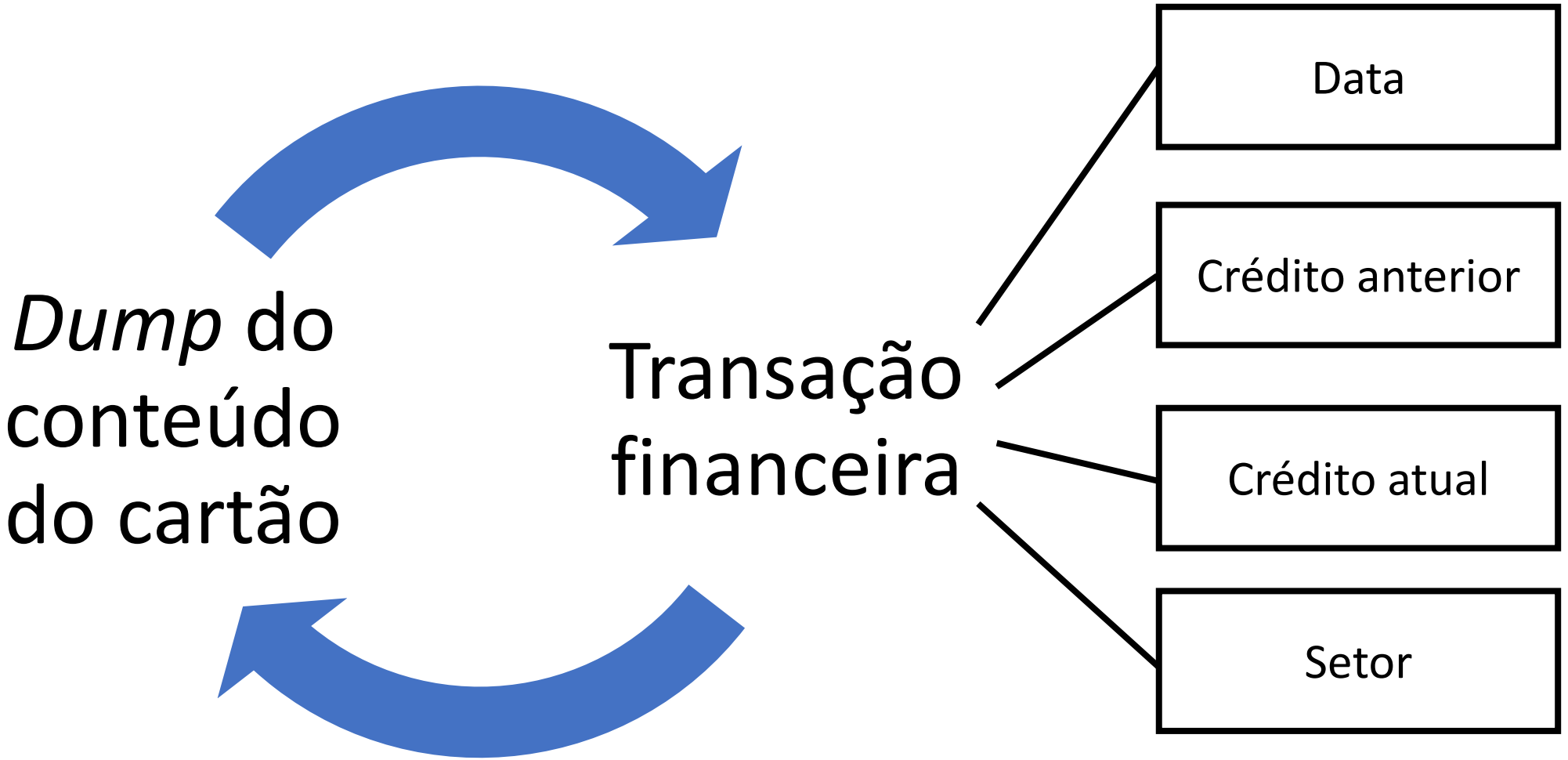
Recuperação das chaves secretas

- Execução do **mfoc**
- Dois setores com chaves personalizadas
- Dois blocos com dados preenchidos (Blocos 50 e 53)

```
55 key 5e58e13fcc4f :00  00  00  00  00  00  ff  07  80  54  92  50  7b  bf  50  79
54 key 5e58e13fcc4f :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
53 key 5e58e13fcc4f :4c  a0  10  24  f4  01  00  00  00  00  00  00  00  00  00  2d
52 key 5e58e13fcc4f :00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
51 key 5e58e13fcc4f :00  00  00  00  00  00  ff  07  80  54  92  50  7b  bf  50  79
50 key 5e58e13fcc4f :4c  a0  10  24  f4  01  00  00  00  00  00  00  00  00  00  2d
49 key 5e58e13fcc4f :02  00  00  00  00  00  00  00  00  00  00  00  00  00  00  02
48 key 5e58e13fcc4f :01  fa  c0  72  0f  e8  00  00  00  00  00  00  00  00  00  ae
```

II. Análise do conteúdo

Análise do conteúdo



Análise do conteúdo

- Localização da data de transação é registrada de forma direta
  - 10 24 = 16h36
  - 0D 26 = 13h38
  - 0D 0A = 13h10
- Dados conferem com comprovante gerado na máquina

4C	A0	10	24	F4 01	00	00	00	00	00	00	00	00	00	2D
Mês	Dia	Hora	Minuto	Crédito										Checksum

Análise do conteúdo

- Localização dos créditos foi descoberta após algumas transações.
  - R$ 9,00 = 84 03
  - R$ 7,00 = BC 02
  - R$ 5,00 = F4 01
  - R$ 3,00 = 2C 01

4C	A0	10	24	F4 01	00	00	00	00	00	00	00	00	00	2D
Mês	Dia	Hora	Minuto	Crédito										Checksum

Análise do conteúdo

- Crédito não é registrado de forma direta
  - F4 01 != 5
- Entretanto
  - 01 F4 = 500
- Crédito registrado em forma de centavos, inversamente.

4C	A0	10	24	F4 01	00	00	00	00	00	00	00	00	00	2D
Mês	Dia	Hora	Minuto	Crédito										Checksum

Análise do conteúdo

- Byte final era modificado depois de todas as transações
- Técnica de soma de verificação muito utilizada para validação de dados
- Tentativa com XOR entre todos os bytes
- 4C ⊕ A0 ⊕10 ⊕24 ⊕ F4 ⊕ 01⊕00 ... ⊕00 = 2D

4C	A0	10	24	F4	01	00	00	00	00	00	00	00	00	00	2D
Mês	Dia	Hora	Minuto	Crédito											Checksum

III. Identificação das vulnerabilidades

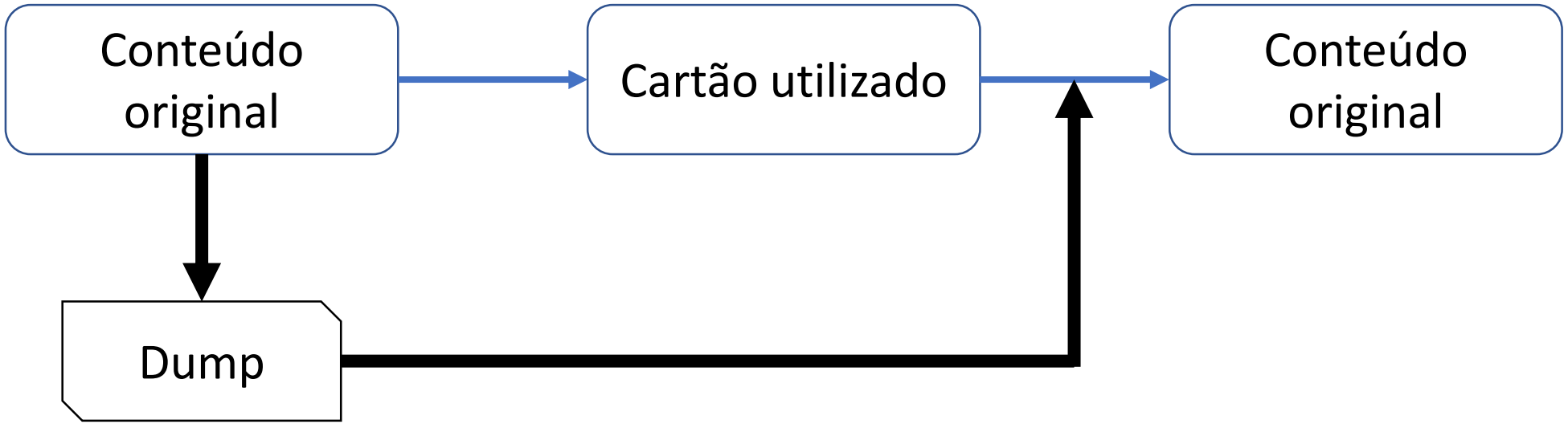
Identificação de vulnerabilidades

- Setores com chaves padrões
- Dados registrado diretamente no cartão
- Setores com chaves idênticas
- Mecanismo de validação de dados fraco
- **Sistema opera *offline***
  - Dados são guardados apenas no cartão
  - Confiança total nos mecanismos proprietários

IV. Análise dos possíveis ataques

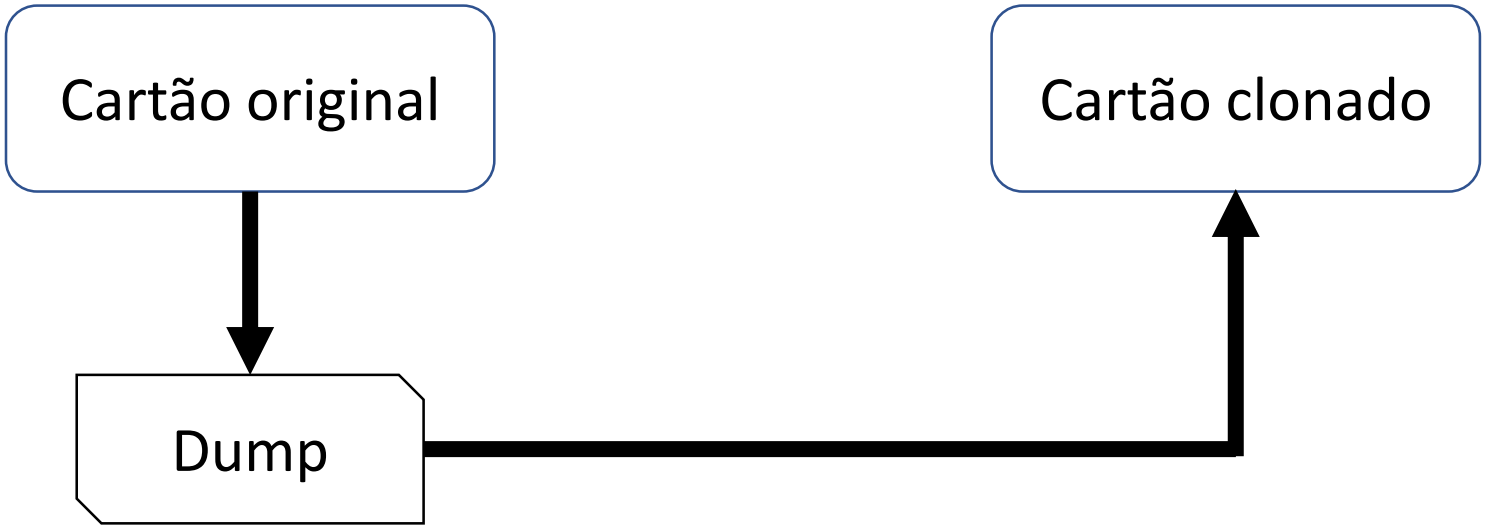
Análise de ataques

- Ataque de repetição



Análise de ataques

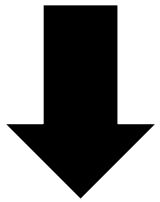
- Clonagem do cartão
- “Cartão mágico chinês”
  - Cartões *Mifare* 1k cujo bloco 0 é editável



Análise de ataques

- Adulteração de dados

4C	A0	10	24	F4 01	00	00	00	00	00	00	00	00	00	2D
Mês	Dia	Hora	Minuto	Crédito										Checksum



4C	A0	10	24	D0 07	00	00	00	00	00	00	00	00	00	0F
Mês	Dia	Hora	Minuto	Crédito										Checksum

Soluções

1. Troca do cartão inteligente utilizado
   - *Mifare DESFire*
2. Utilização de criptografia própria
3. Utilização de um sistema integrado e online
   - Todas as transações financeiras são registradas
   - Identificação única registrada
   - Associação individual (Usuário- Cartão)

Contribuições

- Estudo da tecnologia
  - Pesquisa bibliográfica
  - Estrutura do cartão
- Metodologia de ataque
  - Pode ser aplicada para qualquer sistema que utilize o cartão inteligente *Mifare Classic* 1k
  - Pode ser estendida para outras tecnologias RFID
- Análise de possíveis ataques e proposta de soluções

Trabalhos futuros

- Identificar vulnerabilidades de outros sistemas
  - Bilhetagem eletrônica
  - Controle de acesso

- Analisar e comparar outras tecnologias de cartão inteligente sem contato
  - RFID 125KHz
  - Mifare DESFire
  - Mifare Classic 4k

Estudo Sobre o Impacto das Vulnerabilidades de um Cartão Inteligente Sem Contato

Luiz Eduardo Mendes Matheus (UFJF), Eduardo P. Julio (UFJF),
Alex B. Vieira (UFJF), Edelberto Franco (UFJF)