Universidade Federal do Pampa
Emilio Roberto Reginaldo Tubino

Um Estudo Acerca das Fraudes na Comunicação por Campo de Proximidade

Alegrete
2016

Emilio Roberto Reginaldo Tubino

Um Estudo Acerca das Fraudes na Comunicação por Campo de Proximidade

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Juliano Fontoura Kazienko, Dr.

Alegrete

2016

Emilio Roberto Reginaldo Tubino

Um Estudo Acerca das Fraudes na Comunicação por Campo de Proximidade

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Trabalho de Conclusão de Curso defendido e aprovado em 23 de Junho de 2016. Banca examinadora:

Prof. Juliano Foutoura Kazienko, Dr.
Orientador

Prof. Igor Cancela Melnik, Dr.
UNIPAMPA

Prof. Fabiano Tondello Castoldi, Me.
UNIPAMPA

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais) .

T53e Tubino, Emilio Roberto R.
Um Estudo Acerca das Fraudes na Comunicação por Campo de Proximidade / Emilio Roberto R. Tubino.
73 p.

Trabalho de Conclusão de Curso(Graduação)-- Universidade Federal do Pampa, CIÊNCIA DA COMPUTAÇÃO, 2016.
"Orientação: Juliano F. Kazienko".

1. Comunicação por Campo de Proximidade. 2. NFC. 3. Segurança. 4. RFID. I. Título.

Resumo

Dentre as tecnologias de comunicação sem fio, a Comunicação por Campo de Proximidade, do inglês, *Near Field Communication* (NFC) tem recentemente atraído o interesse tanto da comunidade científica quanto da indústria, além de possuir grande aceitação por parte dos usuários. Tais fatores tornam o NFC uma tecnologia de comunicação promissora. Entretanto, mesmo com a grande popularização, tal tecnologia ainda possui questões de segurança em aberto que devem ser tratadas. Principalmente por ser uma tecnologia aplicada muitas vezes na área de pagamentos eletrônicos, área que constantemente sofre com fraudes tecnológicas. Assim, este trabalho de conclusão de curso tem por objetivo identificar fraudes no âmbito da tecnologia NFC, propondo contramedidas que serão analisadas através de estudos de caso.

Palavras-chave: NFC, Comunicação por Campo de Proximidade, Vulnerabilidades, Contramedidas.

Abstract

Among the wireless communication technologies, the Near Field Communication (NFC) has recently attracted the interest of both the scientific community and industry. In addition, such technology has gotten high user acceptance. These factors make NFC a promising communication technology. Although the wide popularity, the technology has security issues that should be carefully addressed. It is important to point out that the NFC is applied on areas as electronic payments and medicine which demand by security services. Hence, this work aims to identify frauds related to the NFC technology, proposing countermeasures that will be analyzed through study cases.

Key-words: NFC, Near Field Communication, Vulnerabilities, Countermeasures.

Lista de ilustrações

Lista de tabelas

Lista de siglas

BD Banco de Dados

CF *Chunk Flag*

CMAC *Cypher-based Message Authentication Code*

DES *Data Encryption Standard*

DoS *Denial of service,* Negação de Serviço

ES Elemento Seguro

GPS Sistema de Posicionamento Global

HMAC *Hash Message Authentication Code*

IL *ID Length Present*

IoT *Internet of Things,* Internet das Coisas

MAC *Message Authentication Code,* Código de Autenticação de Mensagem

MB *Message Begin*

ME *Message End*

NDEF *NFC Data Exchange Format*

NFC *Near Field Communication,* Comunicação por Campo de Proximidade

QR *Quick Response Code*

RFID *Radio Frequecy Identification,* Identificação por Radiofrequência

RSA Assinatura digital Rivest, Shamir e Adelman

RSSF Rede de Sensores Sem Fio

RTD *Record Type Definition*

SR *Short Record*

TCC Trabalho de Conclusão de Curso

TNF *Type Name Format*

URI *Unique Resource Identifier*

WPAN *Wireless Personal Area Network,* Rede Sem Fio de Área Pessoal

Sumário

1 Introdução

Avanços tecnológicos na miniaturização de dispositivos, como na computação móvel e em sistemas distribuídos, contribuem para a integração e proliferação de dispositivos computacionais. Tais avanços viabilizam a computação de forma ubíqua e pervasiva, tornando possível a presença da tecnologia em todo o lugar e em objetos do nosso cotidiano (ATZORI; IERA; MORABITO, 2010), remetendo, assim, diretamente a um importante paradigma da computação, a Internet das coisas, do inglês, *Internet of Things* (IoT). A IoT é basicamente formada pela conexão e interação entre os objetos que cercam o usuário (ATZORI; IERA; MORABITO, 2010), sendo composta por tecnologias como a (i) Identificação por Radiofrequência, do inglês, *Radio Frequency Identification* (RFID), (ii) Redes Sensores sem fio (RSSF) e a (iii) Comunicação por Campo de Proximidade, do inglês, *Near Field Communication* (NFC).

Considerada um dos pilares da IoT, a tecnologia RFID é comumente utilizada para controle de estoque, identificação de objetos e controle de acesso, com diversas áreas de aplicação como na agricultura, controle industrial, serviços de segurança e na área pessoal e militar. Dependendo das aplicações, subconjuntos desta tecnologia são criados e adaptados para atender melhor as especificações necessárias para determinadas aplicações, como no caso da tecnologia NFC.

A tecnologia NFC, foi desenvolvida em 2002 com base na tecnologia RFID, tendo um alcance máximo de comunicação de aproximadamente 10 cm e operando na frequência de 13,56 MHz. Tal tecnologia é comumente utilizada em sistemas de pagamento, identificação pessoal e identificação de objetos, podendo ser encontrada em *smartphones*, *notebooks* e etiquetas NFC (COSKUN; OZDENIZCI; OK, 2013) (WANT, 2011). Comparada a tecnologias semelhantes como o *Bluetooth*, o NFC possui um pareamento mais rápido e uma área de alcance menor, resultando em uma configuração mais rápida e uma comunicação mais segura. A tecnologia NFC possui também uma maior confiabilidade e sustentabilidade comparada aos os códigos *Quick Response* (QR), pelo fato de serem reaproveitáveis e menos propensas a erros de leituras (WANT, 2011).

Tal tecnologia tem atraído o interesse tanto da comunidade científica quanto da indústria (BORGIA, 2014)(ATZORI; IERA; MORABITO, 2010)(ILIE-ZUDOR et al., 2011). Calcula-se que 50% dos telefones produzidos a partir de 2015 tenham NFC habilitado, e que 150 bilhões de dólares serão originados em transações realizadas a partir de dispositivos NFC (NFCFORUM, 2015). Estimando-se também, que, mais de 603 milhões de *smartphones* habilitados NFC sejam comercializados em 2018 (NFCWORLD, 2015). Tal tecnologia é utilizada aqui no Brasil na recarga do bilhete de ônibus, na cidade de

São Paulo, através do uso do *smartphone* para recarga dos créditos em um terminal NFC (RFIDJORNALBRASIL, 2015).

Apesar da tecnologia NFC já ser utilizada em diversos ambientes, ainda trata-se de uma tecnologia relativamente nova, e que ainda necessita de aprimoramentos em âmbito da segurança (CHEN; LIN; YANG, 2014) (SPRUIT; WESTER, 2013). Mesmo com seu curto alcance do sinal, o que dificulta a recepção do sinal por atacantes, o NFC ainda é suscetível a ataques como *Denial of Service* (DoS), retransmissão de dados, personificação de dispositivos, entre outros (HASELSTEINER; BREITFUSS, 2006) (CHATTHA, 2014) (CHEN; LIN; YANG, 2014). A tecnologia 2.2 possui métodos de segurança que solucionam diversas vulnerabilidades existentes, entretanto, tais métodos muitas vezes não podem ser aplicados na tecnologia NFC, em virtude das diferenças físicas e operacionais entre elas, principalmente em relação as etiquetas NFC. As etiquetas NFC normalmente possuem menor capacidade computacional que alguns tipos de etiquetas RFID (LEHTONEN et al., 2009), que são capazes de gerar resumos de mensagens *Hash's* e gerar números aleatórios, auxiliando no desenvolvimento de mecanismos de segurança como o sugerido pelos autores do trabalho (DIMITRIOU, 2005). Métodos mais complexos de segurança necessitam de dispositivos com um poder de processamento maior como *smartphones* e leitores, para ser aplicados neste tipo de etiquetas NFC. Desse modo, existe a necessidade do desenvolvimento de novos tipos de mecanismos de segurança que se adéquem a suas limitações.

Pelo fato da tecnologia NFC ter uma grande utilização em áreas médicas e de pagamentos eletrônicos (WANT, 2011) (RFIDJORNALBRASIL, 2015) (NFCFORUM, 2015) (NFCWORLD, 2015), sendo essa última constantemente fraudada em meios tecnológicos, como as apresentadas na Seção 2.4.2, pretende-se desenvolver aqui mecanismos de segurança que visem mitigar ou eliminar vulnerabilidades de segurança encontradas ao decorrer do TCC na tecnologia NFC. Assim, será abordado aqui um estudo de tal tecnologia, suas vulnerabilidades e fraudes existentes em âmbito da segurança.

1.1 Objetivo Geral

Este TCC de curso tem por objetivo estudar e identificar fraudes existentes na Comunicação por Campo de Proximidade, que serão avaliadas através de estudos de caso, apresentando ataques e propostas de contramedidas.

1.2 Objetivos Específicos

- Estudar a tecnologia NFC;
- Estudar propriedades e mecanismos de segurança;

- Revisar a literatura com relação as fraudes envolvendo a tecnologia NFC;
- Identificar fraudes no âmbito da tecnologia NFC;
- Avaliar, através de estudos de caso, tais fraudes propondo contramedidas para as mesmas.

1.3 Organização deste Trabalho

O desenvolvimento deste trabalho de conclusão de curso é organizado de forma a introduzir o leitor a tecnologia NFC. A partir do Capítulo 2, o ambiente que cerca tal tecnologia é apresentado, assim como suas características e aplicações. O Capítulo 3 apresenta ao leitor os trabalhos relacionados ao apresentado aqui, em âmbito da segurança. Com isto, propostas de mecanismos de segurança foram desenvolvidos e apresentados no Capítulo 4 a fim de mitigar ou eliminar as vulnerabilidades presentes na tecnologia NFC. Por fim, o Capítulo 5 apresenta as considerações finais do trabalho desenvolvido e objetivos para trabalhos futuros.

2 Fundamentação Teórica

O capítulo de Fundamentação Teórica tem por objetivo introduzir o leitor ao âmbito da tecnologia NFC. Apresentando a Internet das Coisas, Seção 2.1, e a tecnologia RFID, Seção 2.2, este capítulo descreve também as tecnologias semelhantes e suas áreas de aplicação, assim como suas características físicas e computacionais, Seção 2.3. Por fim, o leitor é introduzido ao âmbito da segurança da informação na Seção 2.4, abordando suas propriedades, fraudes e mecanismos de segurança existentes.

2.1 Internet das Coisas

O termo computação ubíqua e pervasiva é geralmente aplicado ao entranhamento da tecnologia e sua disponibilidade no dia a dia do usuário, este termo é normalmente encontrado em pequenos dispositivos de uso cotidiano, como Sistema de Posicionamento Global (GPS), celulares, geladeiras e relógios, abrindo espaço para um importante paradigma da computação, a IoT.

A IoT é o termo dado para a conexão entre tais dispositivos, que ao interagirem e criam uma rede de conexões entre si. Os exemplos de interações entre itens da IoT mais comuns são o de geladeiras inteligentes que interagem com o *smartphone* do usuário, comunicando a ele a falta de algum alimento, ou então, a interação de *smartphones* com *smartwacths* (relógio inteligente), para isso o *smartphone* comunica-se com o *smartwatch* fazendo com que ele efetue alguma ação de aviso como luz, som ou vibração, para alertar o usuário sobre eventos. Para isso, a IoT utiliza a tecnologia RFID, que realizada a troca de mensagens através de antenas de rádio, com o receptor e emissor do sinal operando na mesma frequência (WANT, 2006).

2.2 Identificação por Radiofrequência

Considerada um fator crucial para a existência da IoT (KHOO, 2011), a tecnologia RFID é comumente utilizada na identificação de itens, controle de ambientes e comunicação de dispositivos. A RFID tem sua gradativa adoção justificada por sua facilidade de uso, praticidade, custo e desempenho (ROBERTS, 2006), sendo aplicada em diversas áreas como na agricultura, transporte, rastreamento de cargas e identificação de produtos (ILIE-ZUDOR et al., 2011).

De forma geral, a tecnologia RFID é composta por dispositivos ativos e passivos. Dispositivos como terminais RFID e GPS são considerados ativos por possuírem energia

própria e alimentarem energeticamente dispositivos passivos como etiquetas RFID, através das ondas de radiofrequência geradas por sua comunicação (COSKUN; OZDENIZCI; OK, 2013). É importante ressaltar que nem todas as etiquetas RFID são passivas. Etiquetas ativas são utilizadas junto a fontes de energias, normalmente mais caras, robustas e capazes de realizar operações mais complexas que as etiquetas passivas (WANT, 2006).

Diversos padrões da tecnologia RFID são criados e adaptados dependendo das necessidades de cada aplicação. É o caso da tecnologia NFC, que possui um campo de comunicação reduzido em relação a outros padrões dessa tecnologia, sendo aplicada principalmente na área de identificação de itens e pagamentos eletrônicos (WANT, 2011).

2.3 Comunicação por Campo de Proximidade

A tecnologia NFC foi desenvolvida em 2002 pelas empresas *Philips e Sony*, e padronizada em 2004 pelo *NFC-Forum*, um consórcio global composto por empresas como *Philips, Sony, LG, Motorola, Visa, MasterCard, PayPal, Google, Microsoft, Intel*, entre outras (NFCFORUM, 2015). Sua comunicação é realizada por indução magnética através de ondas de rádio na frequência de 13,56 MHz e um alcance máximo de comunicação de 10 cm, operando em uma configuração *half-duplex*(WANT, 2011). Possui uma fácil utilização, rápido pareamento e um baixo custo monetário e energético (COSKUN; OZDENIZCI; OK, 2013).

O NFC pode ser classificado como uma tecnologia pertencente às Redes Sem Fio de Área Pessoal, do inglês, *Wireless Personal Area Network* (WPAN) (TUBINO; QUINCOZES; KAZIENKO, 2015a), assim como as tecnologias *Bluetooth* e *Zigbee* (COSKUN; OZDENIZCI; OK, 2013). A Tabela 1 apresenta uma comparação entre as tecnologias de comunicação de dados discutidas nesta seção.

A tecnologia *Bluetooth* foi desenvolvida em 1998, tendo seu desenvolvimento dirigido pelo *Bluetooth Special Interest Group*. Com o objetivo de ser uma solução de conectividade de curto alcance para dispositivos portáteis de uso pessoal. Esta tecnologia opera em uma frequência de 2,4 GHz, possui uma distância de comunicação de até 100 metros, e alto consumo energético (COSKUN; OZDENIZCI; OK, 2013). O *Bluetooth* é utilizado na área automotiva, em celulares, sistemas de saúde, entre outras.

A tecnologia *ZigBee* foi desenvolvida em 1998 e padronizada em 2003 pela *ZigBee Alliance*, uma aliança aberta sem fins lucrativos. Tal tecnologia opera em uma frequência de 2,4 GHz, com um alcance de aproximadamente de 10 à 100 metros, podendo atingir distâncias maiores na ausência de obstáculos entre os dispositivos que se comunicam. Possui um consumo de energia moderado, sendo mais apropriado para dispositivos que possuem severas restrições quanto ao consumo energético (COSKUN; OZDENIZCI; OK, 2013). Esta tecnologia permite a formação de uma Rede de Sensores Sem Fio (RSSF).

Tabela 1 – Comparação das tecnologias

Parâmetros	NFC	Bluetooth	Zigbee
Alcance	4 - 10 cm	10 - 100 m	10 - 100 m
Veloc. de Transferência	0,02 - 0,4 Mbps	0,8 - 2,1 Mbps	0,02 - 0,2 Mbps
Custo de Hardware	Baixo	Baixo	Baixo
Consumo de Energia	Baixo	Alto	Médio
Frequência de atuação	13,56 MHz	2,4 GHz	2.4 GHz
Segurança	Alta	Baixa	Baixa
Usabilidade	Fácil	Moderada	Fácil
Tempo p/ estabelecer conexão	Aprox. 1 s	Aprox. 6 s	Aprox. 0,5 s

Baseado em (COSKUN; OZDENIZCI; OK, 2013).

2.3.1 Aplicações

As tenologias citadas na tabela 1 não podem ser comparadas entre si sem haver um ambiente de aplicação desejado. Isso significa que a aplicação determinará qual tecnologia é a melhor para o seu objetivo. Como exemplos, as RSSFs são implantadas com o intuito de monitoramento e controle de ambiente, como em aplicações de detecção de fumaça/incêndio em uma floresta ou prédio, ou monitoramento do nível de poluição dos oceanos. Tal tecnologia é capaz de suportar milhares de sensores em uma única rede (BORGIA, 2014) (ATZORI; IERA; MORABITO, 2010) (COSKUN; OZDENIZCI; OK, 2013).

Podemos dizer que tecnologias RFID são mais indicadas para a comunicação e identificação. Entretanto, a tecnologia NFC, mesmo sendo um padrão da tecnologia RFID, não pode ser utilizada em algumas dessas aplicações, como as de controle de ambiente. Tal impossibilidade é causada por conta de sua curta área de comunicação. Neste caso, sistemas antifurto, por exemplo, não identificariam a saída de itens não autorizados do ambiente, caso passassem a uma distância maior que 10 cm dos terminais detectores. Por outro lado, esta característica possibilita uma melhor utilização para aplicações onde o curto alcance da comunicação é desejada. Proporcionando assim uma maior segurança na comunicação dos dispositivos NFC e dificultando a interceptação dos dados transmitidos (WANT, 2011) (COSKUN; OZDENIZCI; OK, 2013). Algumas aplicações que já estão utilizando a tecnologia NFC ou possuem propostas para seu uso são:

- Pagamento eletrônico e Bilhetagem: A tecnologia NFC é utilizada para o pagamento de passagens metrô e ônibus. No Brasil, na cidade de São Paulo, foram disponibilizados aplicativos de recarga do bilhete único através da tecnologia NFC (RFIDJORNALBRASIL, 2015). No Japão, usuários do metrô são cobrados através de *smartphones* habilitados NFC (WANT, 2011).

  No comércio em geral, com o apoio de empresas de telefonia e operadoras de cartões de crédito, a comunicação NFC tem sido aplicada em substituição ao uso de cartões

para o pagamento eletrônico;

- Saúde: O gerenciamento de sistemas de saúde é outra grande área de aplicação. Tal tecnologia pode ser utilizada para o controle de medicamentos ministrados a pacientes. Como no atendimento domiciliar a pacientes idosos, trazendo maior comodidade a eles (IGLESIAS et al., 2009);

- Controle de acesso: Trata-se do controle de acesso a ambientes físicos em geral. Neste caso, o usuário utiliza seu dispositivo NFC, seja uma etiqueta ou um *smartphone*, para acessar determinado ambiente, autenticando-se perante um dispositivo leitor. Além do dispositivo em si (algo que o usuário possui), outro fator de autenticação auxiliar pode ser utilizado, como uma senha, a fim de reforçar o processo de autenticação. Um exemplo consiste no uso de uma etiqueta como chave de acesso à casa de um usuário em uma aplicação de "fechadura eletrônica" (AL-OFEISHAT; MOHAMMAD, 2012);

- Educação: Na área de educação, o leque de aplicações possíveis é vasto. A tecnologia pode ser utilizada no cadastramento e controle em eventos culturais em instituições de ensino, como palestras e sessões de teatro (RFIDJORNALBRASIL, 2015), e identificação do patrimônio de algumas escolas e universidades. Sendo utilizada na gestão e controle de bibliotecas, otimizando processos de retirada e devolução de livros.

  Outra aplicação é o ensino de línguas estrangeiras para crianças, com etiquetas NFC fixadas aos objetos que ao serem aproximados de um leitor, exibe em um monitor o nome do objeto já traduzido para a língua estudada, contribuindo para o processo ensino-aprendizagem. No trabalho apresentado por (COSKUN; OZDENIZCI; OK, 2013), é citado o uso da tecnologia NFC aliada ao *Moodle*, que consiste em um sistema de apoio a aprendizagem, habilitando o uso de jogos no processo de ensino e aprendizagem.

2.3.2 Arquitetura NFC e Modos de Operação

No momento em que as duas antenas da tecnologia NFC são postas juntas, uma pequena carga eletromagnética é gerada, esse processo é chamado de acoplamento indutivo. Através dessa carga, o dispositivo de comunicação é energizado, permitindo assim que dados sejam transferidos através das ondas de radiofrequência (STMicroelectronics, 2015). Tal tecnologia possui dispositivos ativos e passivos. Os dispositivos ativos desta tecnologia são compostos por *smartphones* e leitores NFC, e os dispositivos passivos compostos por etiquetas NFC. A comunicação entre os dispositivos só é possível caso ao menos um dos dois dispositivos for ativo. Assim a comunicação entre dispositivos NFC só ocorre entre dois dispositivos ativos, ou um ativo e outro passivo. Tal comportamento ativo ou

passivo impacta diretamente no modo de operação/comunicação entre dois dispositivos NFC.

O primeiro modo de operação é o de (i) Leitura/Escrita. Neste modo, o dispositivo móvel ativo pode ler e modificar os dados contidos no dispositivo passivo, ou seja, a etiqueta. No modo (ii) Ponto-a-Ponto, um dispositivo ativo estabelece comunicação *half-duplex* com outro dispositivo ativo a fim de trocar dados, cartões de visita e imagens, etc. E por fim o modo (iii) Emulação de Cartão, nesse modo um *smartphone*, emula um *smartcard* podendo ser usado como um cartão de crédito em aplicações de pagamento eletrônico (WANT, 2011) (COSKUN; OZDENIZCI; OK, 2013). Nesse modo, o *smartphone* interage com o Elemento Seguro (ES), presente no microchip NFC. O ES consiste em uma plataforma dinâmica capaz de hospedar aplicações e armazenar dados confidenciais, como credenciais do usuário (COSKUN; OZDENIZCI; OK, 2013) (CHATTHA, 2014). Tais modos devem ser utilizados de acordo com o tipo de aplicação e dispositivo a ser utilizado.

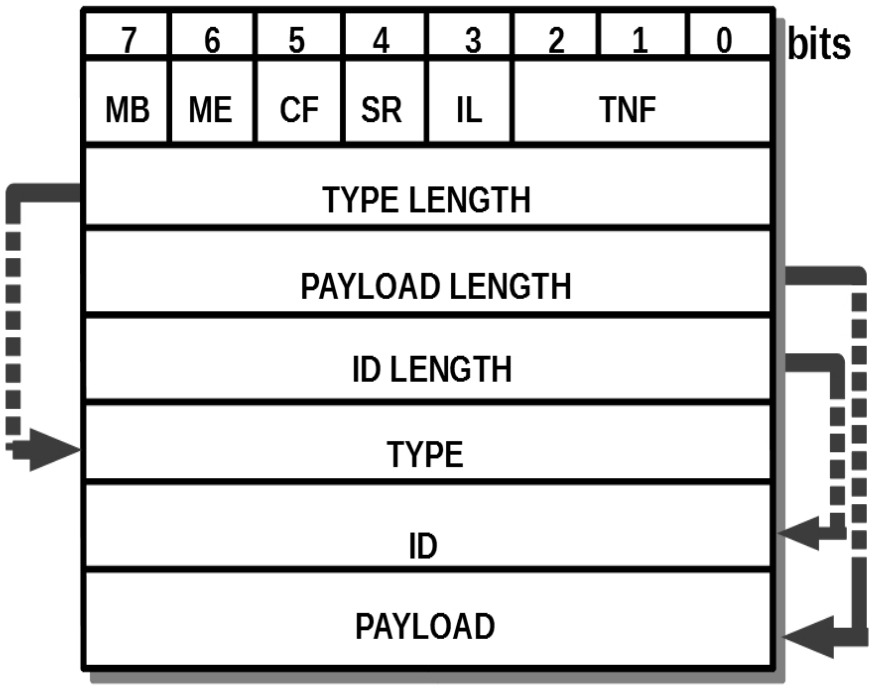
2.3.2.1 Formato de Mensagem

O *NFC Data Exchange Format* (NDEF) é um dos principais formatos para troca de mensagens da tecnologia NFC, no modo de operação Leitura/Escrita. Uma mensagem NDEF pode conter um número ilimitado de registros NDEF‘s. Cada registro contém tamanho, tipo, dentre outros parâmetros. O *Type Name Format* (TNF) consiste em um campo de 3 bits que descreve a estrutura do tipo de registro armazenado no campo. *Type* descreve o tipo de carga útil. O campo de *Payload* contém a carga útil da mensagem NDEF.

De forma geral, alguns campos (flags) do registro NDEF ajudam no controle e delimitação da mensagem, como pode ser observado na Figura 1. O primeiro é o *Message Begin* (MB), responsável por identificar o primeiro registro da mensagem. O *Message End* (ME) marca o último registro. O *Chunk Flag* (CF) indica se a carga útil do registro é continuada no próximo registro. O *Short Record* (SR) possibilita o uso de registros mais compactos, ou seja, menores em tamanho. Já o *ID Length Present* (IL) indica se o campo *ID Length* (comprimento em bytes do campo ID) está presente no cabeçalho em um único octeto (COSKUN; OZDENIZCI; OK, 2013)(HASELSTEINER; BREITFUSS, 2006).

Embora o tipo de informação enviada através do registro NDEF seja extensível, o conjunto mínimo de *Record Type Definition* (RTD) foi especificado, propiciando uma maneira eficiente para definir os formatos de registros para novas aplicações. O tipo *Signature*, especificado pelo RTD, define um formato para assinatura de um conjunto de registros NDEF, incluindo o algoritmo de assinatura utilizado e tipos de certificados digitais utilizados. Com isso, tal campo visa facilitar a operação e integração com uma infraestrutura de chaves públicas (WANT, 2011) (NFCFORUM, 2015). Já o tipo *Unique*

Figura 1 – Estrutura do Registro NDEF



Referência: Baseado em (COSKUN; OZDENIZCI; OK, 2013)

Resource Identifier (URI) identifica um registro. Assim, uma aplicação, ao receber um registro NDEF com o cabeçalho URI definido, poderá optar por passá-lo automaticamente a outra aplicação, como, por exemplo, um *"Http://www."*. Nesse caso, o navegador *WEB* será aberto. Outro tipo é o *SmartPoster*, que define como colocar *URLs*, *fSMSs* ou número de telefone em uma etiqueta NFC. O tipo *Text* é a forma mais simples, além de fornecer uma maneira eficiente de armazenar cadeias de texto em vários idiomas (WANT, 2011) (NFCFORUM, 2015).

2.3.2.2 Tipos de Etiquetas

De acordo com o (NFCFORUM, 2015), as etiquetas NFC são categorizadas em 4 tipos de acordo com suas características. Basicamente, a principal diferença entre os tipos apontada pelo (NFCFORUM, 2015) são as capacidades de armazenamento. As etiquetas do Tipo 1 possuem capacidade de armazenamento que varia entre 96 *bytes* a 2 *kbytes*. As etiquetas do Tipo 2 possui a capacidade de armazenamento que varia entre 48 *bytes* a 2 *kbytes*. Já as etiquetas do Tipo 3 possuem capacidade de armazenamento variada, mas teoricamente é limitada a 1 *Mbyte*. Por fim, as etiquetas do Tipo 4 possuem a capacidade de armazenamento de 32 *kbytes*.

As etiquetas do tipo 1 2 e 4 são baseadas na ISO (14443 ISO, 2008), que especifica as funcionalidades das etiquetas, características físicas e protocolos de comunicação. Já a etiqueta do tipo 3 é especificada pelo Padrão da Indústria Japonesa, do inglês, Japonese Industrial Standard (JIS) (NFCFORUM, 2015). Todos os tipos possuem a capacidade de leitura e escrita, podendo ser posta no modo apenas leitura.

2.4 Segurança da Informação

A segurança da informação diz respeito a segurança sobre os dados armazenados e compartilhados em sistemas computacionais. Tais dados muitas vezes são confidências e não devem ser acessados sem a devida permissão. Vale lembrar que a comunicação de tais dados também fazem parte de tal fundamento, partindo do princípio em que todo o caminho das informações deve ser seguro. Assim, a segurança deve ser aplicada desde a origem até destino da informação.

Algumas ameaças que ferem os princípios de segurança são: Interrupção, transporte da informação da fonte ao destino é de alguma forma interrompido. Interceptação, a informação é interceptada, mas não barrada no trasporte entre a fonte e o destino. Modificação, a informação após ser enviada pela fonte é interceptada, modificada e reenviada para o destino, que só receberá o conteúdo modificado. Fabricação, a informação é originada de uma fonte ilegítima e recebida pelo destino sem que a ilegitimidade da fonte e da informação sejam percebidas(STALLINGS, 2010).

2.4.1 Propriedades de Segurança em Âmbito da Tecnologia NFC

No âmbito da tecnologia NFC, quatro propriedades de segurança devem ser contempladas afim manter o fundamento da segurança de informação. Primeiramente, a confidencialidade das comunicações é uma propriedade de segurança de extrema importância, uma vez que os dados transmitidos podem ser sigilosos. O meio sem fio é utilizado para a comunicação dos dados no NFC. Logo, a interceptação de dados que são transmitidos são mais facilmente capturados por dispositivos atacantes. A fim de prover confidencialidade a informação, as mensagens transmitidas devem ser cifradas, para evitar que elas sejam lidas por atacantes, e assim, apenas os dispositivos legítimos terão acesso aos dados. Este método assegura que mesmo que a comunicação seja interceptada, o atacante não consegua compreender os dados (HASELSTEINER; BREITFUSS, 2006).

A segunda propriedade consiste na autenticidade das partes. Apesar da área de cobertura reduzida no NFC dificultar a interação entre dispositivos legítimos e dispositivos camuflados, tal ameaça ainda é presente. Assim, torna-se importante autenticar mutuamente os dispositivos envolvidos na comunicação, a fim de evitar a troca de mensagens com dispositivos atacantes e, consequentemente, o furto de informações pessoais,

como senhas, dados bancários, etc. Para (CHEN; LIN; YANG, 2014), é necessário utilizar chaves criptográficas para que dispositivos autentiquem um ao outro, impedindo assim a personificação de dispositivos. Vários trabalhos reforçam a necessidade de autenticidade das partes no NFC (ZHUANG; ZHANG; GENG, 2014) (TIMALSINA; BHUSAL; MOH, 2012).

A terceira propriedade consiste na integridade e procedência do conteúdo. É possível que um dispositivo transmita um conteúdo malicioso ou adulterado via NFC. Por exemplo, a leitura de informações oriundas de uma etiqueta anexada a um "pôster inteligente", que poderia provocar a inserção de códigos maliciosos ou mesmo ajudar o atacante a obter vantagens do sistema. Desse modo, torna-se necessário que dispositivos NFC tenham um mecanismo de defesa que impeça o recebimento, ou que permita a detecção de conteúdo malicioso (HAMEED et al., 2014) (CHATTHA, 2014) (CHEN; LIN; YANG, 2014).

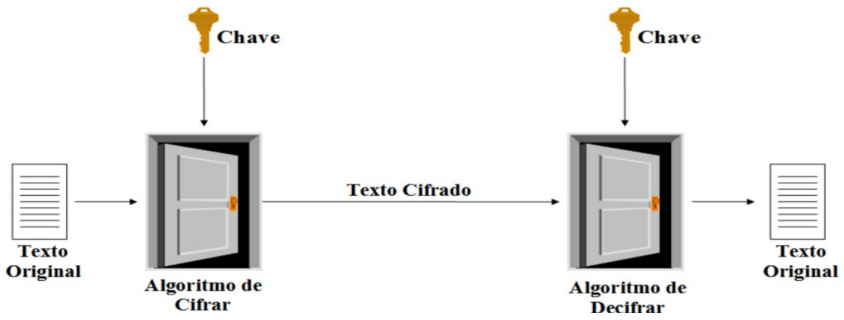
A última propriedade de segurança diz respeito à legitimidade, ou ainda, a originalidade do dispositivo. Na tecnologia NFC, a clonagem de etiquetas é um problema relevante devido principalmente à facilidade de leitura de dados de uma etiqueta, inclusive seu número serial. Por isso, em muitas aplicações envolvendo a tecnologia NFC, a clonagem permite acesso irrestrito a objetos ou ambientes. Um exemplo que pode ser citado consiste na clonagem de uma etiqueta NFC que é utilizada como chave de acesso a portas eletrônicas, permitindo que o atacante a utilize para ter acesso à sua residência (CHEN; LIN; YANG, 2014) (SAEED; WALTER, 2012).

2.4.2 Fraudes na Tecnologia NFC

Para o Dicionário Aurélio (FERREIRA, 2014) fraude é "Falsificação. Adulteração. Ação praticada de má-fé.", podendo ser aplicada também no contexto tecnológico. Fraudes no âmbito da tecnologia da informação estão cada vez mais presentes nos dias atuais. Atualmente tais fraudes estão sendo exercidas em caixas bancários (NOTÍCIAS, 2015b), através de dispositivos conhecidos como "chupa-cabra", por exemplo, que são instalados em terminais a fim de extrair dados dos usuários e clonar cartões bancários.

Terminais de pagamento também são adulteradas para transmitir as informações dos cartões aos atacantes via comunicação *Bluetooth* (NOTÍCIAS, 2015c), fraudes que trazem enormes prejuízos aos usuários de cartões de crédito (NOTÍCIAS, 2015a). Tais fraudes trazem riscos a tecnologia NFC, visto que esta tecnologia já é aplicada para sistemas de pagamentos (RFIDJORNALBRASIL, 2015) (WANT, 2011). Assim, contramedidas devem ser adotadas no âmbito da tecnologia NFC, a qual apresenta vulnerabilidades de segurança, (CHEN; LIN; YANG, 2014) (SPRUIT; WESTER, 2013) (CHATTHA, 2014).

Figura 2 – Criptografia Simétrica



Referência: Baseado em (STALLINGS, 2010).

2.4.3 Mecanismos de Segurança

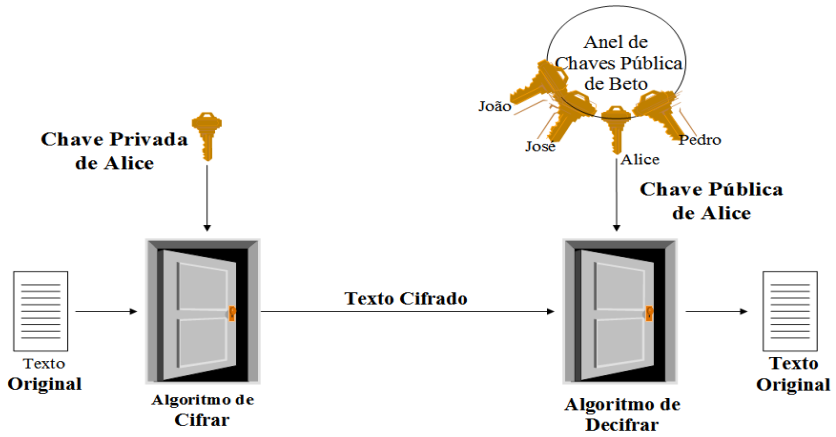
Para se obter um maior sigilo nas informações armazenadas e compartilhadas entre dispositivos, técnicas de segurança são utilizadas para trazer confiabilidade à tais informações. Com a aplicação de tais técnicas é possível mitigar ou eliminar ameaças a segurança citadas anteriormente.

2.4.3.1 Criptografia

A criptografia é aplicada para se obter autenticidade e sigilo em mensagens. No âmbito da computação, a criptografia é aplicada na comunicação de dados, sendo uma forma de garantir a confidencialidade e autenticidade do conteúdo da mensagem. Este método consiste no compartilhamento de uma chave entre os dispositivos da comunicação, utilizada para cifrar e descifrar as mensagens compartilhadas. As chaves utilizadas na comunicação podem ser aplicadas de duas formas: Simetricamente e Assimetricamente. O modo simétrico conta com apenas uma chave para cifrar e decifrar uma mensagem, nesse modo a chave é conhecida por todos os dispositivos que fazem parte da comunicação, como pode ser observado na Figura 2.

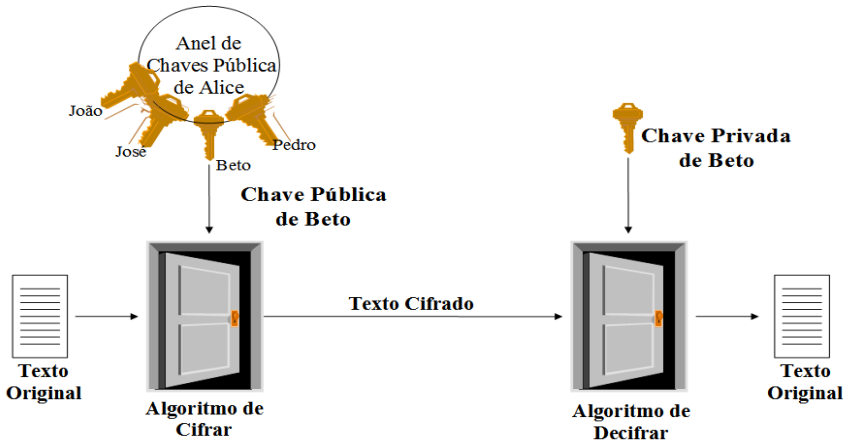
Já no modo Assimétrico, Figura 3, um dispositivo emissor utiliza sua chave privada para cifrar a mensagem, e esta mensagem só poderá ser decifrada pela chave pública do emissor, que será distribuída para os demais dispositivos (STALLINGS, 2010). Este método possibilita a autenticidade das partes, onde, apenas a chave pública do emissor consiga decifrá-la. O modo Assimétrico também pode ser utilizado para garantir a confidencialidade da mensagem Figura 4, nesse modo, o emissor envia a mensagem cifrada com a chave pública do receptor. Assim apenas o receptor terá a chave para decifrar a mensagem recebida. Entre as duas formas de criptografia, a Assimétrica é a mais segura mas também a mais custosa, visto que é necessária a criação de duas chaves para o funcionamento do mecanismo. Assim os dois dispositivos devem ter conhecimentos das duas

Figura 3 – Criptografia Assimétrica com Autenticidade do Emissor



Referência: (STALLINGS, 2010).

Figura 4 – Criptografia Assimétrica com Sigilo ao Destinatário



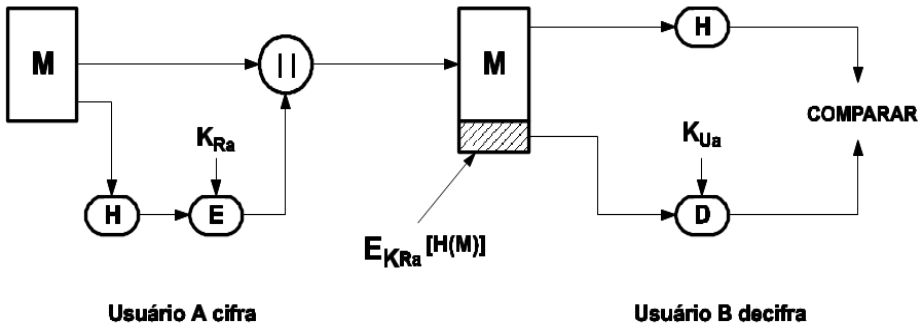
Referência: (STALLINGS, 2010).

chaves, ou de todas as chaves pertencentes aos dispositivos da rede de comunicação.

2.4.3.2 Resumo de Mensagem

Um Resumo de Mensagem, ou *Hash*, é uma função criptográfica que realiza o mapeamento dos dados de uma mensagem gerando um resumo. Basicamente, quando um resumo é aplicado sobre uma mensagem, ele gera uma sequência de saída de tamanho fixo. Esta sequência deve ser única, ou seja, ao alterar a mensagem não se deve alcançar o

Figura 5 – Assinatura Digital: Abordagem RSA



Referência: (STALLINGS, 2010).

mesmo resultado (STALLINGS, 2010). A *Hash* é unidirecional, sendo assim, a engenharia reversa não é aplicada, não sendo possível chegar a mensagem a partir do resultado do *Hash*. Existem vários algoritmos da função *Hash* como o *MD2, MD4, MD5 e SHA-1* (STALLINGS, 2010). Tal função é utilizada normalmente como um mecanismo da Assinatura Digital.

2.4.3.3 Assinatura Digital

A assinatura digital é um mecanismo que permite que um emissor anexe um código na mensagem que o autentique perante outro usuário. Na abordagem Assinatura digital Rivest, Shamir e Adelman (RSA), apresentada na Figura 5, um dispositivo ao criar uma mensagem para envio, realiza uma função *Hash* com sua chave privada sobre a mensagem e anexa o resultado junto a mensagem original (STALLINGS, 2010). Um dispositivo ao ler esta mensagem, utiliza a chave publica do signatário para realizar um novo *Hash* sobre a mensagem recebida. Assim, quando os dois *Hash's* comparados são iguais, a mensagem é autêntica e inalterada, constatando assim sua integridade. Tal afirmação é possível pelo fato de que, caso um único bit for alterado, o *Hash* resultante será diferente do original. Os certificados de assinatura são obtidos de autoridades de certificados de terceiro. Na tecnologia NFC estes certificados são regidos pelo *NFC fórum Signature RTD Certificate Policy*.

2.4.3.4 Código de Autenticação de Mensagem

O Código de Autenticação de Mensagem, do inglês, *Message Authentication Code* (MAC), é uma técnica de autenticação que envolve o uso de uma chave secreta para gerar um pequeno bloco de dados de tamanho fixo, o qual é anexado à mensagem original. Tal método é utilizado para verificar a autenticidade e integridade de uma mensagem (STALLINGS, 2010). Este mecanismo utiliza criptografia simétrica, utilizando a mesma chave para cifrar e decifrar o código. Assim, o emissor da mensagem realiza uma função MAC sobre o texto, e a envia junto ao texto para o destinatário. O destinatário então executa a função com a mesma chave sobre o texto recebido e compara os dois resultados, se caso os dois códigos forem iguais, a autenticidade do emissor é constatada, pois apenas ele teria a chave para reproduzir tal código. Tal método é conhecido como *Cypher-based Message Authentication Code* (CMAC).

Este mecanismo também pode utilizar a função *hash* para gerar um resumo a ser comparado pelo destinatário. Neste caso, o emissor realiza um *hash* sobre o texto e um segredo compartilhado. Assim, a mensagem com o código MAC correspondente são enviados ao destinatário. O destinatário, por sua vez, gera um novo código MAC computando um novo *hash* a partir da mensagem e do segredo compartilhado. Por fim, os dois MAC's são comparados, e se ambos forem iguais, a mensagem é dada como autêntica. Tal método é conhecido como *Hash Message Authentication Code* (HMAC).

Já a confidencialidade da mensagem é garantida caso a mensagem seja cifrada antes do envio. Neste caso há a necessidade de uma dupla de chaves simétricas. Desse modo, o emissor antes de enviar o texto junto ao código MAC ou *hash*, cifra a mensagem com a chave. O emissor ao receber a mensagem, utiliza a chave simétrica para decifrar e ter acesso ao texto e ao código MAC ou *hash*, dependendo do caso. Com isto a confidencialidade dos dados é garantida, pois apenas o emissor e destinatário terão acesso à chave de cifragem.

3 Trabalhos Relacionados

Este capítulo apresenta um levantamento teórico dos trabalhos relacionados a tecnologia NFC no âmbito da segurança. Tais trabalhos realizam um levantamento sobre fraudes existentes relacionadas a tecnologia NFC e rfid. Na Seção 3.1, serão apresentados os trabalhos relacionados aos ataques de clonagem de dispositivos e etiquetas. A Seção 3.2, apresenta os trabalhos relacionados aos ataques de adulteração de dados. Na Seção 3.3, são apresentados os trabalhos relacionados ao ataque de retransmissão de dados, que adicionalmente sugere a possibilidade da união do ataque de clonagem com o de retransmissão de dados. Por fim a Seção 3.4, apresenta os ataques relacionados a autenticação de dispositivos. Após cada trabalho ser apresentado, comentários sobre suas propostas de segurança são discutidas e, caso possua, suas limitações são apontadas. Tais limitações estarão relacionadas a aplicação das propostas de contramedidas na tecnologia NFC presentes no Capítulo 4.

3.1 Clonagem de Dispositivos

No trabalho apresentado por (SPRUIT; WESTER, 2013), os autores realizam um levantamento acerca das ameaças e contramedidas no âmbito da tecnologia RFID. Relacionado ao ataque da clonagem, a contramedida proposta consiste no método *Public Key Re-Encryption*, que está baseado no envio de dados cifrados pela etiqueta, impedindo que o atacante consiga clonar seu serial para simulá-la posteriormente. Entretanto, esse método não permite sua aplicação em etiquetas capazes somente de realizar operações de leitura e gravação de dados, que são mais populares em razão de seu custo, devido à incapacidade de realizar computações como a cifragem de dados.

Um protocolo proposto para combater a clonagem de etiquetas RFID é apresentado pelo autor (ABAWAJY, 2009). Como tal protocolo requer a realização operações mais complexas para fins de autenticação pela etiqueta, somente é possível naquelas que possuem capacidade de processamento. A opção pela adoção de tal tipo de etiqueta pode encarecer a implantação de um sistema de controle através da tecnologia RFID, como em uma aplicação de controle de estoque.

No trabalho (DIMITRIOU, 2005), o autor propõe um esquema de autenticação entre terminal e etiqueta RFID seguro contra ataques de replicação, personificação e clonagem. Neste esquema a etiqueta deve se autenticar perante o leitor, sendo necessário executar operações mais complexas como o resumo criptográfico (*hash*) e geração de *nonce*. Assim, este mecanismo necessita de etiquetas mais inteligentes, que disponibilizem operações mais complexas do que apenas leitura/escrita como as etiquetas abordas neste

estudo.

Outro trabalho que propõe um mecanismo de segurança, a fim de evitar o ataque de clonagem, é o apresentado pelos autores (KOSCHER et al., 2009). Neste trabalho, os autores propõem a identificação das etiquetas via serial, onde através da leitura da etiqueta pode-se identificar se a etiqueta pertence ao sistema. Este serial só será visível para o sistema via código de autenticação, para assim, o serial estar disponível para leitura com o comando *ACCESS*. Tal comando está disponível em alumas etiqueta RFID, e possibilita a leitura do serial através do código de autenticação correto.

O comando *ACCESS* evitaria que atacantes realizassem a clonagem de etiquetas, mesmo que seja possível copiar os dados armazenados nela, não será possível que a ilegítima se autentique perante o terminal. Isto acontece pelo fato de que as etiquetas RFID e NFC, como de praxe, são identificadas por seu serial. Uma vez que a etiqueta que está tentando se autenticar não tenha seu serial reconhecido pelo terminal, será tratada como ilegítima, ou não pertencente ao sistema. Assim as etiquetas estariam seguras contra tal ataque. Vale ressaltar, que não é encontrado tal comando em etiquetas NFC, nem mesmo na literatura, não sendo possível aplicar tal mecanismo em etiquetas NFC.

Já o trabalho apresentado pelos autores (LEHTONEN et al., 2009) aborda um mecanismo de detecção do ataque da clonagem em etiquetas que permitem apenas operações de leitura e escrita. Em razão de tais características, computações mais complexas não podem ser realizadas, como a computação de um *hash* ou mesmo a geração de números aleatórios. Os autores propõem um mecanismo de autenticação baseado em um segredo compartilhado, nesse mecanismo o terminal e a etiqueta compartilham um mesmo valor gerado randomicamente. Tal valor é atualizado a cada leitura, sendo o novo valor armazenado em um terminal e na etiqueta. Com esse valor, um ataque de clonagem pode ser detectado após o uso das duas etiquetas: uma delas legítima e outra ilegítima (clonada), a qual poderá acessar o sistema. Isso ocorre pelo fato do terminal não conseguir distinguir uma etiqueta clonada de uma legítima. Assim, a detecção da clonagem só ocorre quando duas etiquetas com o mesmo serial tentam acessar o sistema com o valor de autenticação randômico diferente do armazenado no terminal.

Entretanto, apesar de o trabalho de (LEHTONEN et al., 2009) citar ataques de negação de serviço, o mecanismo proposto pelos autores não resolve o problema da negação de serviço, (DoS), ocasionado pela clonagem de etiquetas. No DoS, o objetivo principal é inviabilizar o acesso ao serviço, ou seja, causar a negação de serviço a uma etiqueta legítima que se autentica perante um dado terminal. Desse modo, através da clonagem e uso de etiquetas clonadas, se impede que etiquetas legítimas tenham acesso ao sistema o que configura o ataque de negação de serviço.

3.2 Adulteração de Dados

O trabalho apresentado pelos autores (MADLMAYR et al., 2008) apresentam o ataque DoS em etiquetas NFC, ataque resultante de uma modificação mais intensa dos dados armazenados, como um problema a ser tratado, sugerindo a necessidade da existência de um mecanismo que controle o a função Leitura/Escrita, para evitar que usuários não autorizados utilizem tal função na etiqueta. Já o trabalho (CHEN; LIN; YANG, 2014) apresenta o ataque DoS em dispositivos como *Smartphones*, nesse ataque um dispositivo sobrecarrega outro com requisições de comunicação, o que encarretaria na sua incapacidade de realizar a comunicação com os demais dispositivos.

Já os autores (MADLMAYR et al., 2008), sugerem a necessidade de um mecanismo de controle de escrita e leitura em etiquetas NFC. Tal mecanismo sugerido, em teoria, evitaria ataques de adulteração e clonagem de etiquetas NFC. Onde apenas pessoas autorizadas poderiam ler e escrever nas etiquetas, evitando assim que os dados sejam manipulados por atacantes. Assim, a clonagem seria evitada com este mecanismo, pois assim como os dados da etiqueta seriam somente acessados por dispositivos autorizados, o serial da etiqueta também seria somente disponibilizado perante autenticação.

O autor do trabalho (CHEN; LIN; YANG, 2014) propõe então contramedidas para ataques como modificação e corrompimento de dados, na comunicação entre dispositivos ativos, como leitores NFC e *Smartphones*. Basicamente, ataques como inserção, modificação e corrompimento de dados são solucionados através da observação das ondas de radiofrequência da comunicação entre os dispositivos. Os autores propõem a geração de um canal seguro entre a comunicação dos dispositivos, sendo considerado por eles a melhor forma de segurança contra tais ataques.

O canal seguro apresentado por (CHATTHA, 2014) funciona, basicamente, com uma troca de mensagens sincronizada entre os dois dispositivos, enviando ao mesmo tempo bits aleatórios. Ao final, todos os bits que foram trocados ao mesmo tempo e são iguais, são descartados. O resultado do envio será então o segredo compartilhado. Isto é feito porque cada dispositivo sabe o que enviou, e sabe o que recebeu, já um atacante só terá as frequências para observar. Por exemplo, quando os dispositivos enviam ao mesmo tempo o bit 1, o que o atacante verá será a soma dos sinais, e quando for 0, verá o sinal nulo, assim ele sabe que foi enviado o bit 0 ou 1. Já quando o bit for diferente como 0 e 1, o atacante não saberá qual está enviando 0 e qual está enviando 1, confundindo a coleta de informação do atacante, baseada nas ondas de radiofrequência. Assim este segredo compartilhado pode ser utilizado como uma chave de criptografia entre os dispositivos legítimos.

Relacionado a autenticação entre terminal e etiqueta, um mecanismo é proposto pelo trabalho (SAEED; WALTER, 2012). Neste mecanismo, os autores propõem um

esquema anti-clonagem e adulteração, onde os dados armazenados nas etiquetas são assinados e através de um esquema de criptografia dentro da etiqueta são encriptados. Neste esquema a adulteração dos dados seria detectada através da assinatura digital, já a clonagem da etiqueta seria identificada através do esquema de criptografia utilizado pela etiqueta. Os autores citam que tal operação é possível dentro de alguns tipos de etiquetas NFC, sendo capaz de executar criptografias simétricas e assimétricas.

Neste mecanismo apresentado por (SAEED; WALTER, 2012), as etiquetas realizam uma operação de criptografia. Etiquetas NFC de baixo custo possibilitam apenas operação de leitura e escrita, não sendo possível realizar essa operação. É importante ressaltar que ao estudar os diversos tipos de etiquetas, até então, não foi encontrada a função de criptografia em etiquetas NFC, mesmo as do tipo 4. Onde também não se identifica tal possibilidade de criptografia realizada pelas etiquetas nos demais trabalhos encontrados.

3.3 Retransmissão de dados

A tecnologia NFC também está vulnerável aos ataques de retransmissão, do inglês, *Relay attack*. Os estudos apresentados pelos autores (CAVDAR; TOMUR, 2015) e (WANG et al., 2012) comprovam a existência de lacunas de segurança na comunicação em sistemas de controle de acesso através de dispositivos móveis. Provando, através de estudos práticos, a vulnerabilidade a este tipo de ataque. Ressaltando assim, a necessidade de um mecanismo de segurança capaz de detectar o ataque de retransmissão em tempo real.

O trabalho apresentado pelo autor (ROLAND; LANGER; SCHARINGER, 2013) ressalta a existência da vulnerabilidade da tecnologia NFC ao ataque de retransmissão, através de um estudo prático, realizado em um ambiente real de pagamento. Onde através da aplicação do ataque em tal ambiente, identificou a existência da vulnerabilidade neste sistema de pagamento. O sistema de pagamento utilizado no estudo foi o *Google Wallet*. O *Google Wallet* é um sistema de pagamento desenvolvido pela empresa *Google* em 2011, que permite que os usuários armazenem cartões de créditos em *Smartphones* e realizem pagamentos através da tecnologia NFC.

Através do estudo realizado pelo autor (ROLAND; LANGER; SCHARINGER, 2013), podemos concluir a presença real da vulnerabilidades ao ataque de retransmissão em um sistema já utilizado para aplicações de pagamento, área de aplicação constantemente vitima de fraudes 2.4.2. Ressaltando ainda mais a necessidade de evoluções em termos de segurança no âmbito da tecnologia NFC. Para assim trazer uma maior confiabilidade tal tecnologia.

Os autores do trabalho (ROLAND; LANGER; SCHARINGER, 2013) propõem

uma contramedida para a aplicação do ataque de retransmissão no sistema *Google Wallet*. Basicamente a comunicação neste sistema é iniciada pelo terminal NFC, isto deixa o *Smartphone* vulnerável a requisições de dados indesejadas. O que os autores propuseram foi bloquear o *Smartphone* para requisições através de um código de verificação inserida pelo usuário. Assim a requisição dos dados feita pelo terminal só será aceita caso o usuário digite o código de verificação previamente.

A contramedida apresentada pelos autores no trabalho (ROLAND; LANGER; SCHARINGER, 2013) possui algumas vulnerabilidades citadas por eles. Caso o *Smartphone* do usuário esteja infectado por um aplicativo malicioso, este aplicativo poderá habilitar o a comunicação NFC do *Smartphone* sem o consentimento do usuário. Podemos identificar também que a contramedida apresentada por eles é utilizável apenas em *Smartphones* NFC, e não em etiquetas, pois o bloqueio da comunicação entre etiqueta e terminal não é realizado a partir da etiqueta NFC.

O autor (HANCKE; MAYES; MARKANTONAKIS, 2009), além de estudar o ataque de retransmissão semelhante ao apresentado pelos autores (CAVDAR; TOMUR, 2015) e (WANG et al., 2012), realizam uma crítica às contramedidas existentes a este ataque. Eles também citam a existência de um mecanismo de tempo na comunicação NFC especificada pela ISO (14443 ISO, 2008), para evitar o ataque de retransmissão. Esse mecanismo é criticado pelos autores pelo seu tempo de tolerância muito prolongado que tende a deixar uma grande margem para que um atacante realize o ataque de retransmissão.

Alguns métodos de contramedida voltadas ao ataque de retransmissão são apresentados pelo autor (SHEN et al., 2015), no âmbito da tecnologia RFID. Apresentando o protocolo de delimitação de distância, do inglês, *Distance Bounding Protocol*, que limita a distância máxima da comunicação entre etiqueta e leitor, com o uso da intensidade do sinal. Um exemplo de método utilizado neste protocolo, é o baseado em sensores de temperatura. Neste método um sensor de temperatura é adicionado aos dispositivos que no momento da comunicação compara as temperaturas do emissor e destinatário. Onde a variação de temperatura entre eles é utilizada na determinação da distância.

Outro método de limite de distância apresentado pelo autor (SHEN et al., 2015) é o que utiliza coordenadas geográficas dos dispositivos de comunicação. Onde, em cada comunicação, as coordenadas do emissor é enviada junto com a mensagem. Em ambos os casos, a intensidade do sinal recebido pelo dispositivo é comparado com a variação de temperatura do dispositivo e/ou comparado com a posição geográfica. Caso as variações de temperatura ou posição geométrica sejam diferentes do que a intensidade do sinal aparenta, resulta na detecção da possível presença do ataque de retransmissão.

A aplicação de protocolos de delimitação de distância na tecnologia NFC é bastante limitada pela capacidade de processamento das etiquetas e alguns dispositivos desta

tecnologia. Necessitando assim de dispositivos mais sofisticados e robustos, ocasionando no encarecimento da tecnologia e diminuição de sua praticidade e portabilidade. Outro fator que pode tornar essa prática redundante para a tecnologia NFC é a já existente limitação de distância de aproximadamente 10 cm máximos.

Os autores (OH et al., 2015) propõem um mecanismo de segurança para evitar a retransmissão de dados. Esse mecanismo considera que os dispositivos atacantes realizem a retransmissão através de uma rede *Wi-Fi*. Pelo fato da tecnologia NFC e a *Wi-Fi* utilizarem uma frequência de comunicação diferente uma da outra. O mecanismo proposto realiza uma interferência na comunicação *Wi-Fi*, do inglês, *Jamming*, através do envio de bits aleatórios na frequência utilizada pela tecnologia *Wi-Fi* para impedir que os dispositivos se comuniquem (MARGI et al., 2009), não interferindo na comunicação NFC. Com isso, no momento da comunicação entre a etiqueta NFC e o terminal legítimo, nenhuma comunicação que utilize a frequência da tecnologia *Wi-Fi* será realizada, evitando assim o ataque de retransmissão que utilize tal tecnologia para a retransmissão dos dados.

Apesar de a contramedida apresentada pelo autor (OH et al., 2015) parecer eficaz, ela possui algumas limitações. Primeiramente o mecanismo só se mostrará eficiente caso a tecnologia de comunicação utilizada para a retransmissão dos dados for a tecnologia *Wi-Fi*, sendo ineficiente caso a tecnologia de comunicação utilizada for a *Bluetooth* por exemplo, como apresentada pelos autores (CAVDAR; TOMUR, 2015) e (WANG et al., 2012). Esta contramedida também mostra-se ineficaz ao ataque de retransmissão que utilize um meio cabeado para a retransmissão dos dados.

Outra limitação da contramedida apresentada pelo autor (OH et al., 2015) é a interferência em qualquer comunicação *Wi-Fi*, ou seja, todos os dispositivos que estiverem utilizando esta tecnologia para comunicação, sejam eles de usuários legítimos ou atacantes, serão afetados por tal sinal de poluição. Se levarmos em consideração um ambiente que utiliza a *internet* através de uma rede *Wi-Fi*, este mecanismo causaria problemas de comunicação aos usuários do sistema central, como, por exemplo, constantes quedas da rede, ruídos e não interceptação dos dados, entre outros. Assim este mecanismo mostra-se, no mínimo, problemático para determinados ambientes de aplicação, que tendem a ser mais afetados a medida que a tecnologia NFC é utilizada. Isto ocorre pois a cada requisição de autenticação da comunicação entre terminal e etiqueta NFC, um novo sinal de poluição é gerado, causando maior impacto ao sistema de acordo com o número de autenticações necessárias em um determinado período de tempo.

Ao decorrer do estudo, cogitou-se também a possibilidade de uma união entre o ataque de clonagem e o de retransmissão. Essa união seria utilizada para burlar os mecanismos baseados em tempo e distância. O ataque de retransmissão seria utilizado para transmitir as requisições do leitor à etiqueta, que através da resposta clonaria a etiqueta em uma ilegítima próxima ao leitor. Com isso, os dados requisitados pelo leitor

estariam a pronta entrega, e o ataque não seria identificado pelo leitor. Esse união de ataques será aborda no EC 4, Seção 4.5, entretanto, é importante ressaltar que tal união dos ataques não foi encontrada na literatura.

As propostas de contramedidas para o ataque de retransmissão estão relacionadas na Tabela 2.

Tabela 2 – Tabela de Propostas de Contramedidas ao Ataque de Retransmissão

Primeiro Autor	**Tecnologia**	**Contramedida Utilizada**
Roland, M.	NFC	Senha para desbloqueio da comunicação
Hancke, G. P.	NFC	Baseada no tempo de comunicação dos dispositivos
Shen, W.	RFID	Baseada na distância entre os dispositivos
Oh, S.	NFC	Interferência do sinal da tecnologia de retransmissão

3.4 Autenticação de Dispositivos

Outro mecanismo de segurança é proposto pelos autores do trabalho (CEIPIDOR et al., 2012) com o objetivo de melhorar o protocolo de segurança utilizado para pagamentos eletrônicos conhecido como *Europay, Mastercard e VISA* (EMV). O EMV é um protocolo utilizado em todo mundo para realizar pagamentos eletrônicos utilizando cartões inteligentes e terminais de cartões de crédito. Um *Smartphone* também poder ser utilizado para realizar pagamentos utilizando o EMV, através da tecnologia NFC. E pelo fato de um *Smartphone* conter maiores recursos computacionais que os cartões inteligentes, abre caminho para atacantes executarem outros ataques (CEIPIDOR et al., 2012). Um dos ataques possibilitados pelo uso da tecnologia NFC citados pelos autores é a captura dos dados transmitidos através da RFID. Logo a interceptação dos dados possibilita ataques de personificação e adulteração.

Pelo fato de que no protocolo EMV o terminal de cartões realiza a autenticação do dispositivo mas o dispositivo não autenticar o terminal, os autores do trabalho (CEIPIDOR et al., 2012) propõem então um mecanismo de autenticação mútua entre os dispositivos, para assim evitar que, através dos ataques de personificação e adulteração, um atacante realize fraudes no sistema. O protocolo apresentado pelos autores utiliza um *Smartphone* NFC e um terminal leitor de cartões, que realizam a autenticações entre eles. Basicamente, no protocolo sugerido pelos autores o terminal ao realizar a requisição de dados envia um número randômico para o *Smartphone*, o *Smartphone* então envia os dados e o randômico recebido cifrados com sua chave privada e reenvia a mensagem com um novo randômico. O leitor ao receber estes a mensagem a decifra com a chave pública e caso esteja tudo correto, gera um novo randômico e cifra com sua chave privada o novo randômico e a mensagem recebida. Estes passos se repetem até que todas as informações necessárias sejam recebidas.

O protocolo apresentado pelos autores do trabalho (CEIPIDOR et al., 2012) mostra-se seguro no momento da autenticação mútua, mas seu excesso de informações trocadas no momento da autenticação pode trazer complicações no decorrer da comunicação. Pois toda informação relacionada ao protocolo de autenticação é reenviada diversas vezes, ou seja, caso haja 100 comunicações de autenticação entre dois dispositivos, os valores randômicos iniciais serão repassados 100 vezes, e serão gerados mais 99 valores que serão retransmitidos a cada autenticação. Logo, ao final da comunicação serão transmitidos 100 números randômicos, o que pode trazer lentidão ao sistema, pois eles são cifrados novamente a cada envio, assim o tempo para realizar tal operação ira aumentar a cada randômico gerado.

Já em relação a confidencialidade das mensagens trocadas entre dispositivos ativos, um mecanismo de segurança é proposto pelos autores do trabalho (LI; ZHAO; XUE, 2013). Os dispositivos utilizados no mecanismo são dois *Smartphones* com NFC integrado. O mecanismo é responsável por encriptar as mensagens antes de serem transmitidas. A chave de criptografia é gerada ao mesmo tempo nos dois dispositivos a partir de um padrão de movimento realizado com o deslize do dedo do usuário na tela de cada um dos *Smartphone*. Tal movimento é feito simultaneamente em cada uma das telas e deve ser igual nos dois dispositivos. Através deste movimento uma chave criptográfica é gerada para cifrar e decifrar as mensagens.

O mecanismo apresentado em (LI; ZHAO; XUE, 2013) é considerado seguro pelos autores na comunicação dos dados pelo fato de que a chave de criptografia não ser transmitida pelas ondas de radiofrequência. Dificultando assim aos atacantes a coleta da chave de encriptação devido a chave ser gerada de forma separada em cada dispositivo. É importante ressaltar que tal mecanismo só é possível em *Smartphones* ou outros dispositivos NFC que possibilitam o uso de uma tela sensível ao toque. Assim etiquetas e leitores NFC mais comuns não poderiam utilizar tal técnica de geração de chave. A utilização deste método também diminui a praticidade da comunicação NFC, necessitando assim de um pareamento antes da comunicação.

Em relação a segurança na leitura de etiquetas, o trabalho (HAMEED et al., 2014) sugere um esquema de segurança contra conteúdo malicioso. Neste tipo de ataque, uma *URL* é inserida em etiquetas, onde um *Smartphone* ao ler esta etiqueta, é direcionado para um *link* malicioso. Tal *link* pode conter um *download* de aplicativos prejudiciais, por exemplo. Sendo assim, a contramedida propostas pelos autores, é utilizar um sistema intermediário que armazene uma tabela com os sites conhecidos. Assim estes sites são adicionados a listas, *white list* (lista branca) e *black list* (lista negra). Outra lista que também é utilizada, é a lista de reputação, nela o site é classificado quanto a confiança dos usuários, e seus votos. Através desta lista, o sistema intermediário confronta as *URL* lidas, e verifica a confiabilidade da mesma. Assim, caso a *URL* lida direcione o usuário a

um site que não esteja na lista branca, o usuário então é notificado (alertado).

Entre as fraudes apresentadas aqui presentes na literatura, estão presentes as que ferem os princípios da confidencialidade, autenticidade e integridade. Como exemplo estão os ataques de personificação (através da clonagem e roubo de dados), negação de serviço, adulteração e retransmissão no âmbito da tecnologia NFC e RFID. Os trabalhos presentes nesta revisão de literatura estão relacionados na Tabela 3, com seus respectivos temas abordados neste capítulo.

Tabela 3 – Tabela de Trabalhos Relacionados

Primeiro autor	**Referência**	**Tecn.**	**Tema abordado**
Marco Spruit	(SPRUIT; WESTER, 2013)	RFID	Clonagem
Jemal Abawajy	(ABAWAJY, 2009)	RFID	Clonagem
Tassos Dimitrious	(DIMITRIOU, 2005)	RFID	Clonagem
Karl Koscher	(KOSCHER et al., 2009)	RFID	Clonagem
Mikko Lehtonen	(LEHTONEN et al., 2009)	NFC	Clonagem
Cheng Chen	(CHEN; LIN; YANG, 2014)	NFC	Adulteração
Naveed Chattha	(CHATTHA, 2014)	NFC	Adulteração
Gerald Madlmayr	(MADLMAYR et al., 2008)	NFC	Adulteração
Muhammad Saeed	(SAEED; WALTER, 2012)	NFC	Adulteração
Ugo Ceipidor	(CEIPIDOR et al., 2012)	NFC	Personificação
Shahul Hameed	(HAMEED et al., 2014)	NFC	Conteúdo Malicioso
Lingjun Li	(LI; ZHAO; XUE, 2013)	NFC	Confidencialidade
Derya Cavdar	(CAVDAR; TOMUR, 2015)	NFC	Retransmissão
Zhou Wang	(WANG et al., 2012)	NFC	Retransmissão
SungTaek Oh	(OH et al., 2015)	NFC	Retransmissão
Weiwei Shen	(SHEN et al., 2015)	RFID	Retransmissão
Michael Roland	(ROLAND; LANGER; SCHARINGER, 2013)	NFC	Retransmissão
Gerhard Hancke	(HANCKE; MAYES; MARKANTONAKIS, 2009)	NFC	Retransmissão

4 Estudos de Caso

Visto que a tecnologia NFC ainda possui vulnerabilidades de segurança, será proposto neste capítulo diversos mecanismos de segurança contra fraudes existentes no âmbito dessa tecnologia, desenvolvidos com os materiais apresentados na Seção 4.1. Assim, na Seção 4.2 será apresentado um estudo de caso com foco da detecção de etiquetas NFC clonadas. Já a Seção 4.3 apresenta um estudo de caso com foco da adulteração de dados em etiquetas NFC. Na Seção 4.4 será abordado um estudo acerca do ataque de retransmissão, com objetivo de detectar tal ataque. Adicionalmente a Seção 4.5 apresenta um estudo sobre o ataque de clonagem de dados unido ao ataque de retransmissão, com o objetivo de evitar que tal união de ataques burle o mecanismo desenvolvido na seção anterior. Por último a Seção 4.6 trata de um estudo acerca da personificação de dispositivos através de dados roubados dos dispositivos legítimos.

Tais Seções apresentam o ataque e as vulnerabilidades que possibilitam sua aplicação. Adicionalmente, ao fim de cada estudo de caso, são apresentados os resultados obtidos com as contramedidas propostas a estas vulnerabilidades.

4.1 Materiais Utilizados

Nesta Subseção serão apresentados os materiais utilizados ao longo das avaliações dos mecanismos propostos nos estudos de caso. Os materiais foram subdivididos em *Hardwares* e *Softwares*, para melhor organização do texto e entendimento do leitor. Entre os materiais utilizados aqui, alguns foram utilizados também no trabalho (TUBINO; QUINCOZES; KAZIENKO, 2015a), que estão presentes na Figura 6, a qual adicionalmente contém as etiquetas do tipo 1 (5) e tipo 2 (4)(2).

4.1.1 Hardware

Os *Hardwares* utilizados nos mecanismos foram um *notebook* Sony Vaio modelo *svf15213cbw* com NFC integrado, um *notebook LG*x modelo *A530*. Um leitor NFC modelo *ACR 122U* (6) com conexão *USB*. Também foram utilizados *Smartphone Samsung E7* e *Smartphone Sony Xperia M* (1), ambos com NFC integrado. E por fim etiquetas NFC do modelo *MIFARE DESfireEV1* tipo 4 (3), com a capacidade de armazenamento de 4.094 *Bytes*.

Figura 6 – Materiais

Referência: (TUBINO; QUINCOZES; KAZIENKO, 2015a).

4.1.2 Software

Os protótipos apresentados nos estudos de caso foram desenvolvidos no sistema operacional *Windowns 10*. As funcionalidades envolvendo o leitor *ACR 122U* foram desenvolvidas no ambiente de programação(IDE) *Eclispe* na linguagem de programação *Java*. Já envolvendo os *Smartphones* NFC, utilizou-se o ambiente de programação (IDE) *Android Studio* na linguagem *Java* para *Android*, sistema operacional presente nos *Smartphones* utilizados aqui.

4.2 Estudo de caso 1: Detecção de etiquetas clonadas

4.2.1 Vulnerabilidade

Um dos grandes desafios da tecnologia NFC consiste na detecção e invalidação de etiquetas clonadas nas quais disponibilizam apenas operações de leitura e escrita de dados sem a capacidade de realizar processamentos adicionais. Assim toda a informação da etiqueta legítima pode ser lida por qualquer dispositivo. Isto possibilita a um atacante, realizar a leitura da etiqueta e copiar todo o conteúdo para uma etiqueta ilegítima. Tal fator torna esta vulnerabilidade difícil de ser resolvida e ainda requer soluções apropriadas (CHEN; LIN; YANG, 2014) (LEHTONEN et al., 2009) (SPRUIT; WESTER, 2013)

(KHOO, 2011). Assim, o mecanismo proposto aqui tem por objetivo detectar e invalidar de forma simples e eficiente etiquetas clonadas (ilegítimas) em um sistema baseado na tecnologia NFC. O mecanismo proposto é destinado a etiquetas que possuem operações de leitura e escrita apenas, pois tais etiquetas são largamente utilizadas devido ao seu baixo custo.

4.2.2 Ataque

O ataque da clonagem consiste na cópia dos dados de uma etiqueta (legítima) e posterior gravação desses dados em outras etiquetas (ilegítima). Com isso, o atacante, possuidor de uma etiqueta clonada pode obter vantagem indevida, identificando-se como terceiros, acessando ambientes, etc. (NELSON; QIAO; CARPENTER, 2013) (CHEN; LIN; YANG, 2014). Suponha um ambiente que possui controle de acesso que utiliza a etiqueta NFC como "chave" permitindo a abertura de uma fechadura NFC que dá acesso à residência de uma pessoa ou ambiente de trabalho, um atacante ao realizar o ataque da clonagem da etiqueta, terá a etiqueta ilegítima aceita pelo terminal. Isso porque os dados da etiqueta ilegítima serão os mesmos da legítima.

4.2.3 Contramedida

Para tanto, o sistema em que o mecanismo é aplicado possui terminais NFC responsáveis pela leitura/escrita e autenticação das etiquetas. Estes terminais estão conectados a um Banco de Dados (BD) responsável pelo armazenamento das informações contidas nas etiquetas. Cada etiqueta deste sistema armazena seu número serial, dados do usuário e um contador de leituras $cont_e$, onde toda a vez que é autenticada em um terminal do sistema, seu contador é incrementado. O valor deste contador é atualizado tanto na etiqueta ($cont_e$) quanto no BD ($cont_e$), sincronizando assim todos os terminais do sistema. Este contador $cont_e$, será armazenado na etiqueta de modo cifrado $E_K(cont_e)$, utilizando uma chave simétrica K, conforme mostrado na Figura 7. Tal cifragem é necessária para que um atacante não tenha conhecimento do valor de $cont_e$.

Um terminal, ao realizar a leitura dos dados da etiqueta, decifra o contador $cont_e$ com a chave K da seguinte forma $D_K(E_K(cont_e))$. Em seguida, através da busca pelo serial da etiqueta no BD, o terminal resgata o valor de $cont_t$, e confere se $cont_e = cont_t$. Se tais contadores forem iguais, o terminal incrementa os contadores, $cont_t = cont_t + 1$ e $cont_e = cont_e + 1$. Em seguida, cifra $cont_e$ através da operação $E_K(cont_e)$ gravando o novo valor de $cont_e$ na etiqueta e atualizado o valor de $cont_t$ no banco de dados, conforme ilustrado na Figura 8.

À medida que um atacante clona uma etiqueta e a usa junto ao terminal pela primeira vez, tal etiqueta é aceita. Como explicado anteriormente, o contador será decifrado,

Figura 7 – Cadastro da Etiqueta.

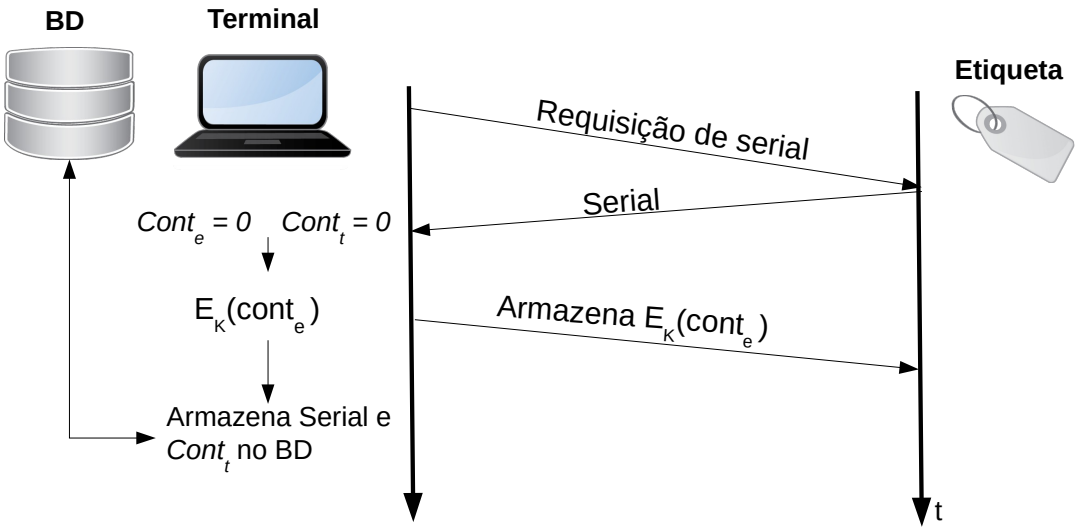
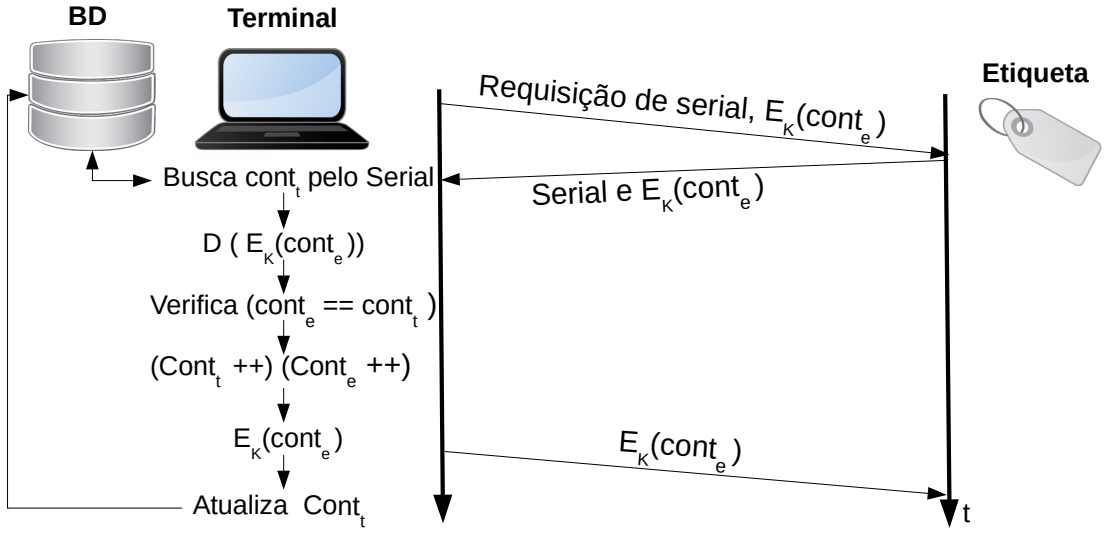


Figura 8 – Uso da etiqueta.



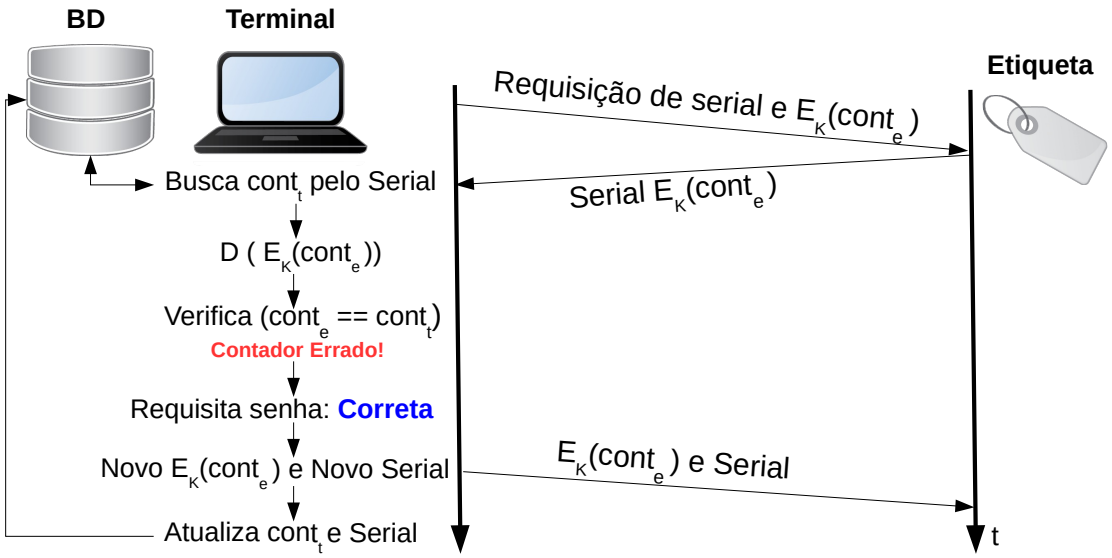
incrementado e gravado de forma cifrada na etiqueta clonada, sem que o terminal perceba que a etiqueta em questão não é legítima. Neste ponto, nem o terminal nem o usuário que contém a etiqueta legítima sabem da transação envolvendo a etiqueta clonada. A detecção da clonagem acontece quando o usuário da etiqueta legítima utiliza o terminal novamente, uma vez que o terminal detecta que $cont_t \neq cont_e$.

4.2.3.1 Versão 1 do Mecanismo Proposto: Com Uso de Senhas

Conforme o ambiente no qual o mecanismo for utilizado, duas versões do mecanismo são propostas. A Figura 9 ilustra a solução envolvendo o uso de senhas. Nesta versão, um terminal ao identificar uma etiqueta como clonada, ou seja $cont_e \neq cont_t$,

requisita uma senha previamente cadastrada pelo usuário legítimo da etiqueta. Tal senha é utilizada para fins de autenticação, sendo armazenada no BD. Ao inserir sua senha, o usuário terá o serial de sua etiqueta alterado e atualizado no BD, fazendo com que a etiqueta clonada não seja mais válida em nenhum terminal. É importante destacar que o uso de uma senha permite que o usuário não sofra uma negação de serviço, ou seja, DoS. Desse modo, o usuário autêntico poderá continuar utilizando o sistema. Nesse caso, há a possibilidade do usuário utilizar a etiqueta legítima antes do atacante, fazendo com que o atacante ao utilizar a etiqueta ilegítima não possuirá o contador correto. Esta solução apropriada para ambientes que possibilitam o uso de terminais com senha, como, por exemplo, estabelecimentos comerciais, mercados, restaurantes e cafeterias.

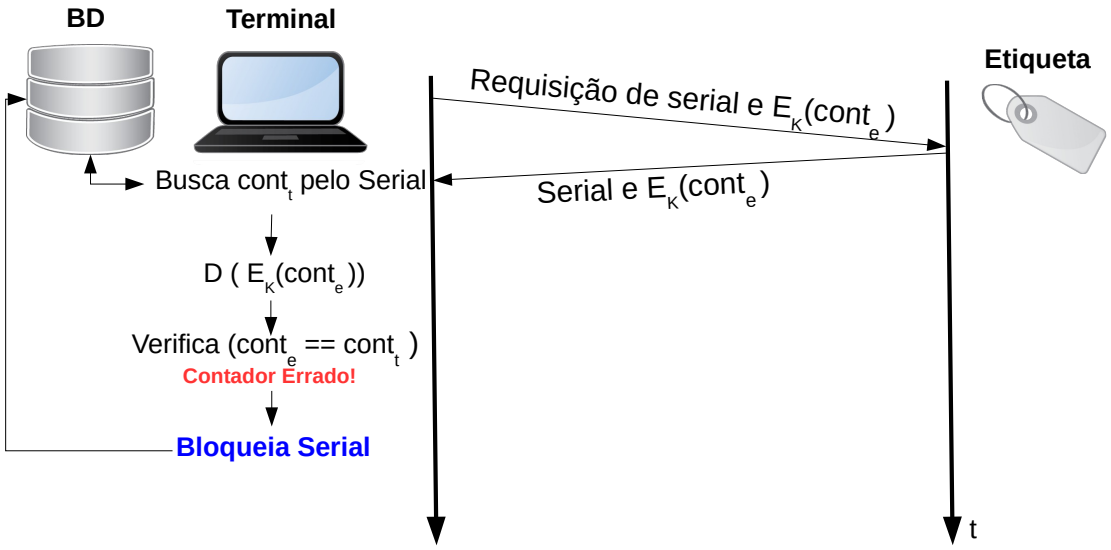
Figura 9 – Solução para sistemas com senha.



4.2.3.2 Versão 2 do Mecanismo Proposto: Sem Uso de Senhas

Já para ambientes que não possibilitam o uso de senhas, como no controle de mercadorias ou mesmo o controle de gado via etiqueta NFC, a segunda versão mostrada na Figura 10 é mais apropriada. Nesta versão, uma etiqueta ao ser identificada como clonada, ou seja, $cont_e \neq cont_t$, terá seu serial bloqueado no BD. Assim, tanto a etiqueta legítima quanto a ilegítima são invalidadas no banco de dados. É importante observar que se deve cadastrar novamente os dados em uma etiqueta para a mercadoria ou usuário legítimo. Como o serviço de identificação é negado, esse método está sujeito ao ataque de DoS. Vale lembrar que o foco do método proposto é retirar a etiqueta clonada de circulação para evitar maiores prejuízos ao usuário.

Figura 10 – Solução para sistemas sem senha.



4.2.4 Avaliação

O mecanismo apresentado aqui foi implementado e avaliado no trabalho publicado (TUBINO; QUINCOZES; KAZIENKO, 2016), onde, para fins experimentais, utilizou-se o *Data Encryption Standard* (DES) como algoritmo de cifragem. Entretanto qualquer cifra simétrica poderia ser utilizada. Basicamente, o mecanismo proposto conta com a cifragem e decifragem do contador $cont_e$ gravado na etiqueta e no BD.

O protótipo construído permitiu verificar que o sistema é funcional. O tempo médio para a execução do mecanismo na Versão 1 com uso de senha é de 7 ms, desconsiderando o tempo que o usuário leva para digitar a senha. Já o tempo médio para execução do mecanismo na Versão 2 sem senha é 5 ms. Além disso, um terceiro cenário sem mecanismo, isto é, sem qualquer controle anti-clonagem foi utilizado. Nesse cenário, o tempo médio para a comunicação entre leitor e etiqueta foi de 2 ms. A avaliação experimental revelou a funcionalidade do mecanismo proposto e uma baixa sobrecarga de tempo em relação a não aplicação do mecanismo, conforme o terceiro cenário considerado. É importante destacar que o mecanismo proposto não leva em consideração falhas de comunicação, visto que o contador só será incrementado após a confirmação da escrita de $cont_e$ na etiqueta.

Adicionalmente, quando o tempo demandado para autenticação em (LEHTONEN et al., 2009) de 864 ms, dos quais 101 ms é demandado somente para autenticação, ou seja, verificação do segredo compartilhado é comparado ao o mecanismo proposto neste TCC, a sobrecarga em termos de tempo de execução é de 94 ms levando em consideração a Versão 1 (7 ms), que requer procedimentos adicionais para autenticação. Alguns fatores que poderiam causar tal sobrecarga de tempo são apontadas pelos próprios autores: (i)

baixa eficiência do algoritmo de autenticação e (ii) diferença de *hardware* de autenticação. De forma geral, um fator que pode influenciar na diferença de tempos total dos mecanismos consiste na diferença de padrões de RFID. Também em comparação ao trabalho (LEHTONEN et al., 2009), o ataque DoS foi evitado na primeira versão do mecanismo proposto aqui através do uso da senha, Seção 4.2.3.1, que evita a negação de serviço ao usuário legítimo.

É importante ressaltar que, embora o método permita uma interação do atacante com o terminal, ele se mostrou eficaz em detectar a clonagem de uma etiqueta e invalidá-la. Comparando à detecção da clonagem de cartões de crédito, que em geral fica por conta do próprio usuário, o mesmo pode perceber a fraude somente depois de várias compras realizadas pelo atacante. Adicionalmente, o método proposto aqui é simples uma vez que requer a troca de poucas mensagens, além de o terminal usar criptografia simétrica, de menor custo computacional quando comparado à criptografia assimétrica. Atualmente, evitar a clonagem de etiquetas é um desafio.

4.3 Estudo de Caso 2: Detecção a adulteração de etiquetas NFC

4.3.1 Vulnerabilidade

Etiquetas NFC são normalmente capazes de realizar apenas operações de leitura e escrita. Particularmente, tal tipo de etiqueta é abordado neste trabalho pelo fato de possuir menor custo sendo comumente encontradas na área comercial. O fato das etiquetas possuírem apenas operações leitura e escrita as torna mais vulneráveis a ataques de adulteração. Tais etiquetas não possuem controle de escrita, como "somente leitura", ou o uso de senhas para a alteração dos dados disponíveis em etiquetas com um preço mais elevado e menos populares.

4.3.2 Ataque

Ao contrário do ataque da clonagem, o ataque de Adulteração de conteúdo utiliza uma etiqueta legítima, ou seja, uma etiqueta pertencente ao ambiente, ou usuário legítimo, para realizar um ataque (NELSON; QIAO; CARPENTER, 2013) (CHEN; LIN; YANG, 2014). Tal etiqueta tem seus dados adulterados pelo atacante, obtendo dois possíveis resultados. O primeiro seria alterar informações da etiqueta com o objetivo de obter vantagem com isto. Neste caso um atacante pode adulterar o preço de uma mercadoria, possibilitando que ele pague um preço menor que original. Outro resultado seria prover a negação de serviço. Levando em consideração a aplicação anterior, uma etiqueta que é utilizada como chave para abertura de fechaduras NFC, pode ter seus dados adulterados para impossibilitar a autenticação do usuário legítimo perante a fechadura, causando DoS.

4.3.3 Contramedida

O mecanismo proposto tem por objetivo detectar ataques de adulteração de dados e a inserção de etiquetas falsas (ilegítimas) em etiquetas que possibilitam apenas operações de leitura e escrita. Este mecanismo possui três agentes principais: (i) o terminal de leitura do sistema, que é responsável por cadastrar as etiquetas; (ii) o terminal de leitura do usuário/cliente, responsável por ler e autenticar os dados das etiquetas e (iii) as próprias etiquetas. Para fins de validação do mecanismo proposto, é abordado um cenário de uma loja de produtos eletrônicos. Tal mecanismo foi implementado e avaliado no trabalho (TUBINO; QUINCOZES; KAZIENKO, 2015b).

Nesse sistema, todos os produtos possuem uma etiqueta NFC com seus dados técnicos e preço gravados nela, cada etiqueta é previamente cadastrada através de um leitor NFC. Assim, dados como o número serial da etiqueta são armazenados em um banco de dados. Os usuários do sistema (clientes) poderão utilizar seu *Smartphone*, habilitado NFC para consultar informações e preços dos produtos do estabelecimento. Tal *Smartphone* deve estar atualizado com o software da loja previamente disponibilizado.

O esquema de autenticação é baseado na abordagem para obtenção de assinatura digital *Rivest, Shamir e Adelman* (RSA) (STALLINGS, 2010), utilizando chaves assimétricas. O terminal recebe os dados que serão armazenados na etiqueta, como representado na Figura 11, realiza um resumo criptográfico (*hash*) da mensagem M, *hash*(M), e através da chave privada, E_KR, cifra afim de computar a assinatura digital da mensagem $\sigma = E_KR(hash(M))$. M consiste nos dados armazenados na etiqueta como preço e dados técnicos de um produto. Assim, são gravados na etiqueta M e a assinatura σ.

Na Figura 12, pode-se observar o processo de autenticação dos dados da etiqueta pelo dispositivo de um usuário. Através da chave pública do terminal, E_KP, previamente distribuída entre os usuários do sistema, o *hash* contido na etiqueta é decifrado através da operação $D_KP(\sigma)$, e um novo *hash* da mensagem recebida é gerado, *hash*'(M). Tais resumos são comparados: $hash'(M) = D_KP(\sigma)$. Se forem iguais, a mensagem é aceita como integra e autêntica, finalizando assim o processo de autenticação.

4.3.4 Avaliação

Preliminarmente, o protótipo construído permitiu verificar que o sistema é funcional. Para testar o sistema, 5 etiquetas foram usadas das quais 3 foram adulteradas. Nos três casos, ocorreu a detecção da fraude. O tempo médio de execução do protocolo de autenticação dos dados na etiqueta é de 3 ms. Tal sobrecarga de tempo é baixa comparada a um sistema sem autenticação, que demandou 2 ms. É importante ressaltar que o mecanismo não evita a adulteração dos dados, mas, ainda assim, permite a detecção do ataque da adulteração, protegendo os usuários das etiquetas contra tal tipo de ataque.

Figura 11 – Cadastro da Etiqueta.

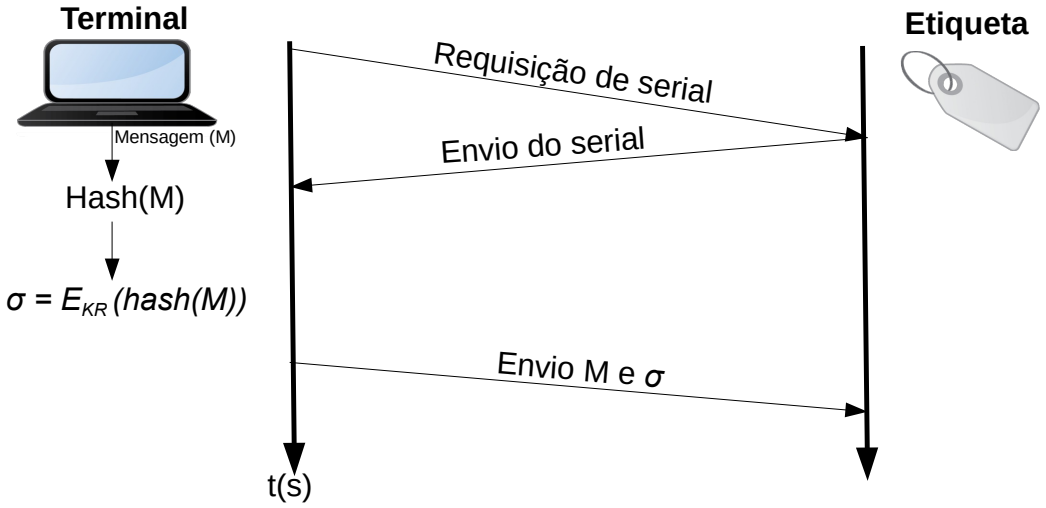
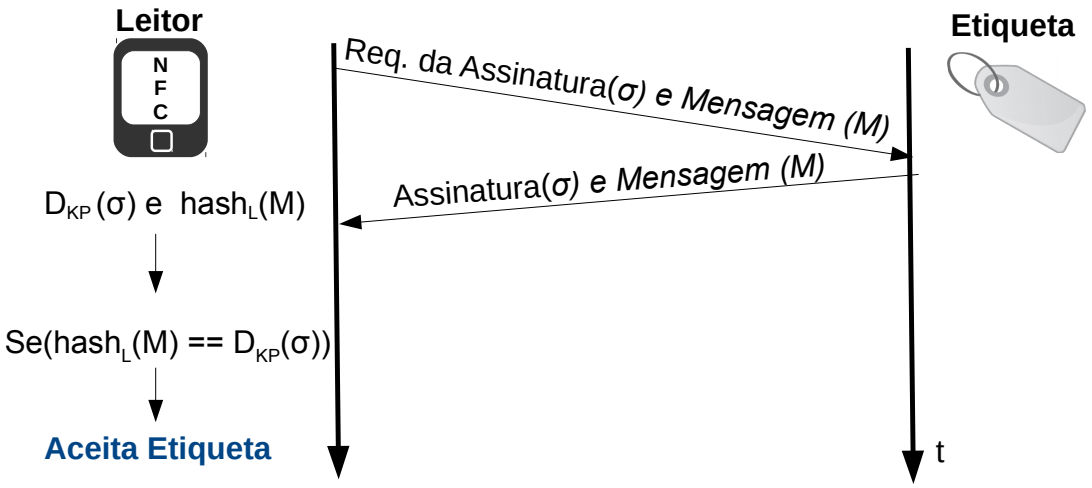


Figura 12 – Autenticação da Etiqueta.



Neste caso, conclui-se que o mecanismo proposto é capaz detectar a adulteração dos dados das etiquetas e detectar etiquetas falsas (ilegítimas), dispensando processamento nas etiquetas. Desse modo o sistema é mantido livre de fraudes provenientes do ataque de adulteração às etiquetas da tecnologia NFC.

4.4 Estudo de Caso 3: Detectando o ataque de retransmissão de dados em dispositivos NFC

4.4.1 Vulnerabilidade

As comunicações geradas entres dispositivos NFC utilizam ondas de radiofrequência para o transporte dos dados. Ou seja, os dados transportados entre dois dispositivos são passíveis de interceptação, por um dispositivo operando na mesma frequência da transmissão e dentro da área de cobertura. Tais dados, ao serem recebidos por um dispositivo atacante, podem ser retransmitidos para os demais dispositivos que não fazem parte de tal comunicação, mesmo na presença de mecanismos de autenticação mútua entre os dispositivos legítimos. A retransmissão dos dados pode ser feita utilizando outras tecnologias de comunicação, como a tecnologia *Bluetooth*, amplamente conhecida e utilizada.

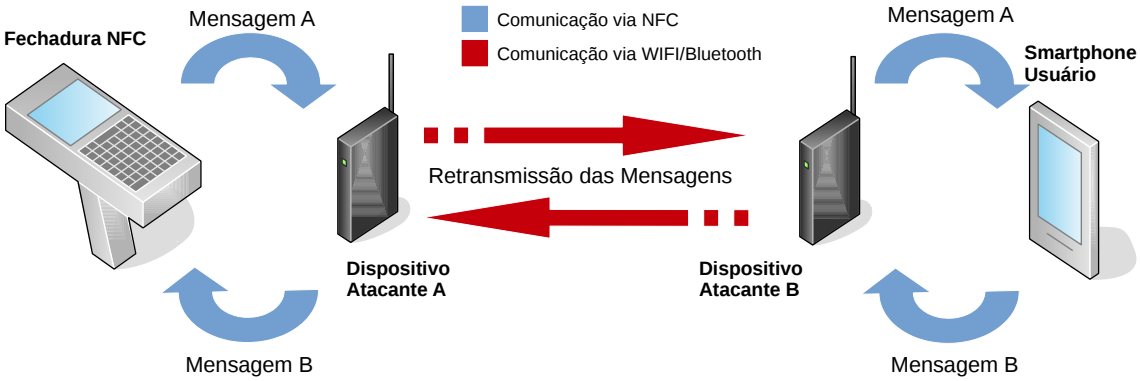
4.4.2 Ataque

O ataque de retransmissão, pode ser utilizado para fraudar uma transmissão NFC, criando uma espécie de ponte de comunicação entre dois dispositivos e camuflando a distância entre eles. Sendo possível iniciar uma comunicação não desejada pelos usuários legítimos entre seus dispositivos legítimos.

A comunicação NFC utiliza uma distância máxima de aproximadamente 10 cm de distância, como visto anteriormente, por motivos de segurança. Esta medida de segurança pode ser burlada utilizando esse tipo de ataque. Onde um dispositivo atacante A comunica-se com um terminal via NFC, que transmite sua comunicação via *Bluetooth* para o dispositivo atacante B que, por fim, retransmite a mensagem para o dispositivo legítimo (*Smartphone*) via NFC novamente, como pode ser visto na Figura 13. Assim, os dados enviados pelo terminal são exatamente os mesmos recebidos pelo dispositivo legítimo com o uso do ataque de retransmissão. Desta forma um atacante pode realizar a comunicação entre os dispositivos a uma distância de até 100 m, conforme a tecnologia *Bluetooth*. Assim um atacante pode fraudar a presença de um dispositivo em um ambiente, por exemplo em sistemas em que um funcionário utiliza um crachá NFC para bater seu ponto em um terminal NFC.

Utilizando esse ataque, um atacante pode também realizar uma comunicação entre dois dispositivos NFC sem o consentimento do usuário do dispositivo. Na tecnologia NFC a comunicação ocorre de maneira intencional, dada pela curta distância de comunicação entre os dispositivos. Ou seja, na prática, a comunicação entre os dispositivos só ocorrerá caso esta seja a intenção do usuário. Desse modo, um atacante pode forçar a comunicação entre dois dispositivos que estão distantes um do outro para realizar comunicações indesejadas. Neste contexto, um possível cenário de ataque consiste naqueles que utilizam

Figura 13 – Ataque de Repasse.



Referência: Baseado em (WANG et al., 2012).

fechaduras NFC. Neste caso um atacante pode aproveitar-se da distração do usuário legítimo e realizar o ataque de retransmissão para abrir uma fechadura distante do mesmo, sem seu consentimento.

É importante ressaltar que a presença do canal de comunicação criado pelo atacante não é visível para os dispositivos legítimos. Logo, a "ponte"criada entre o dispositivo atacante A e B não são visíveis na comunicação. Assim, apenas os dispositivos legítimos são visíveis na rede de comunicação.

4.4.3 Contramedida

O mecanismo proposto aqui tem por objetivo detectar o ataque de retransmissão de dados. Considerando um ambiente de acesso controlado por uma fechadura NFC, um terminal NFC é responsável pela autenticação dos dispositivos e etiquetas NFC, que serão as chaves de acesso. Este mecanismo de segurança baseia-se na comparação de tempo de resposta de uma comunicação para a detecção do ataque de retransmissão.

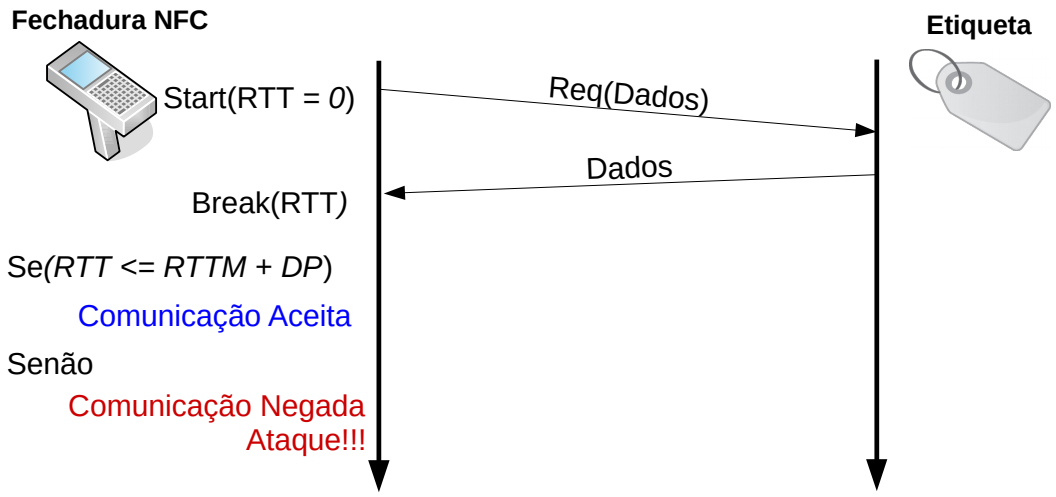
Neste sistema, o terminal requisita os dados de autenticação ao dispositivo, disparando um contador de tempo de resposta, do inglês, *Round Trip Time* (RTT), que é automaticamente encerrado após o recebimento da resposta vinda do dispositivo. Onde o tempo de comunicação médio da etiqueta, $RTTm$, é conhecido pelo terminal.

Por fim, o sistema compara o valor resultante do tempo de resposta, RTT, com o tempo médio de comunicação, $RTTm$. Caso o RTT esteja dentro do Desvio Padrão (DP)[1], aceitável esta comunicação é dada como livre de retransmissão. Caso o valor seja superior ao DP aceitável esta comunicação é dada como resultante do ataque de

[1] Medida mais comum da dispersão estatística. Demonstra o quanto de variação ou dispersão existe em relação à média, ou valor esperado.

retransmissão. Esse procedimento pode ser visualizado na Figura 14.

Figura 14 – Verificação do ataque de retransmissão.



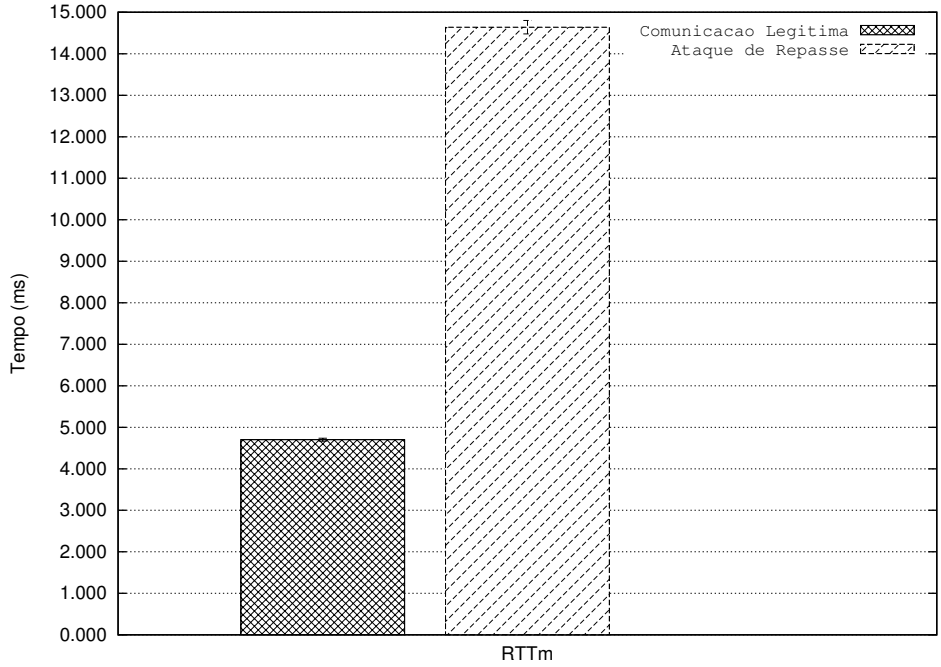
4.4.4 Avaliação

Para avaliar o mecanismo de segurança contra o ataque de retransmissão, implementou-se um sistema de comunicação entre um terminal e uma etiqueta NFC, baseado em um cenário de autenticação de etiquetas para abertura de fechaduras eletrônicas. Posteriormente, implementou-se o ataque de retransmissão semelhante ao apresentado pelos autores (CAVDAR; TOMUR, 2015) e (WANG et al., 2012). Para tanto, utilizou-se dois *smartphones* atacante, A e B, para realizarem a retransmissão dos dados via *Bluetooth*, sendo que A comunica-se com o leitor autêntico e B comunica-se com a etiqueta autêntica.

Assim os tempos médios, $RTTm$, da comunicação legítima entre leitor e etiqueta, e o tempo de ataque de retransmissão foram coletados a partir de 1000 testes de comunicação e apresentados no gráfico esboçado na Figura 15. Em tal figura, obteve-se um tempo médio de comunicação do leitor NFC e da etiqueta de $4,70ms$ com um desvio padrão de $0,571ms$, e um tempo médio de ataque de $14,64ms$ com um desvio padrão de $2,081ms$. Essa figura tem por objetivo demonstrar estatisticamente que o tempo de comunicação pode ser utilizado para detectar o ataque de retransmissão, sendo possível observar a não intersecção do intervalo de confiança entre os tempos médios de comunicação, gerado com um nível de confiança de 95%.

Com a intenção de testar de forma prática o mecanismo de segurança, realizou-se 1000 comunicações legítimas com o intuito de verificar a eficácia do mecanismo ao verificar autenticidade de uma comunicação sem a presença do ataque de retransmissão. Posteriormente aplicou-se o ataque de retransmissão 1000 vezes no sistema, onde os tempos dos ataques foram comparados com o desvio padrão da comunicação legítima. Como

Figura 15 – Comparação do tempo necessário para as comunicações legítimas e as providas do ataque de retransmissão.



resultado em todos os 1000 testes da comunicação legítima não houve a ocorrência de falsos positivos, ou seja, identificar uma comunicação legítima como ataque de retransmissão ($\neg Positivo = Negativo$), sendo todas aceitas pelo sistema. Já nos 1000 testes de ataques de retransmissão houve 100% de identificação do ataque de retransmissão, e todas as comunicações providas desse ataque foram recusadas.

É importante ressaltar que o tempo médio de comunicação entre a etiqueta legítima e o leitor NFC é coletado para que o sistema tenha conhecimento do tempo necessário para que uma comunicação legítima ocorra. Através do uso do desvio padrão dos tempos coletados, é possível encontra um tempo de tolerância mais otimizado para a comunicação legítima. Portanto, ao contrário do método já existente e criticado pelo autor (HANCKE; MAYES; MARKANTONAKIS, 2009), este mecanismo utiliza o tempo necessário para que uma comunicação não seja identificada como falso positivo, sem que permita a presença do ataque de retransmissão, ou seja, evitando também falsos negativos ($\neg Negativo = Positivo$). Este mecanismo mostra-se mais otimizado e eficiente do que o já existente na tecnologia NFC citado pelos autores (HANCKE; MAYES; MARKANTONAKIS, 2009).

Por fim, os resultados encontrados mostram que este mecanismo de segurança é eficaz contra este ataque. Onde o tempo de ataque, até mesmo em seu melhor caso de $8,10ms$, continua sendo recusado. Sendo possível então, detectar e evitar um ataque de retransmissão que siga este modelo de ataque apresentado pelos autores (CAVDAR; TOMUR, 2015) e (WANG et al., 2012), através do uso do tempo de comunicação entre os dispositivos, conforme demonstrado estatisticamente na Figura 15.

4.5 Estudo de Caso 4: Detectando o ataque de retransmissão de dados unido ao ataque de clonagem em dispositivos NFC

4.5.1 Vulnerabilidade

Conforme as vulnerabilidades apresentadas na Seção 4.2, o ataque de clonagem realiza o roubo de dados de uma etiqueta legítima e os armazena em uma etiqueta ilegítima. Tal ataque pode ser utilizado junto ao ataque de repassar, onde, os dados capturados da etiqueta legítima são transmitidos para um segundo dispositivo ilegítimo, conforme apresentado na Seção 4.4. Assim um atacante ao capturar os dados de uma etiqueta legítima repassa a um segundo dispositivo que então utiliza tais dados para cloná-la em um dispositivo atacante.

Com isto um atacante poderia burlar o mecanismo de segurança apresentado na Seção 4.4. Isto é possível pelo fato de que o tempo de retransmissão dos dados via *Bluetooth* e leitura da etiqueta legítima não serão contabilizados na comunicação entre o leitor legítimo. Causando então uma drástica redução no tempo do ataque de retransmissão, resultando na não identificação do ataque de retransmissão.

4.5.2 Ataque

O ataque estudado aqui utiliza dois ataques já estudados anteriormente, sendo eles o ataque da clonagem, Seção 4.2, e o ataque de retransmissão, Seção 4.4. Primeiramente, o atacante realiza o ataque de clonagem para capturar os dados da etiqueta legítima utilizando um dispositivo B. Ao contrário do ataque de clonagem, os dados capturados não são armazenados em uma etiqueta, e sim repassados para um dispositivo B. Este dispositivo então armazena os dados na memória e inicia a comunicação com o leitor legítimo. Posteriormente, o leitor legítimo realiza a requisição dos dados a etiqueta, que é então emulada pelo dispositivo A. Onde o dispositivo A possui todos os dados da etiqueta armazenados, enviando diretamente ao leitor, conforme a Figura 16.

4.5.3 Contramedida

A contramedida proposta aqui tem por objetivo evitar o ataque de retransmissão com o uso do mecanismo de segurança apresentado na Seção 4.4, que utiliza o tempo de comunicação para detecção do ataque de retransmissão. Contudo este mecanismo sozinho não é suficiente para evitar o ataque de retransmissão unido ao ataque de clonagem. Assim, este mecanismo será modificado baseado em etiquetas que possuem um sistema interno que limita a leitura de seus dados através de chaves de segurança. Ou seja, estas etiquetas só permitem a leitura de seus dados caso a chave informada seja a correta. Tais etiquetas são apresentadas felo fabricante (NXP Semiconductors, 2015). É importante

Figura 16 – Identificação do ataque de retransmissão na comunicação.

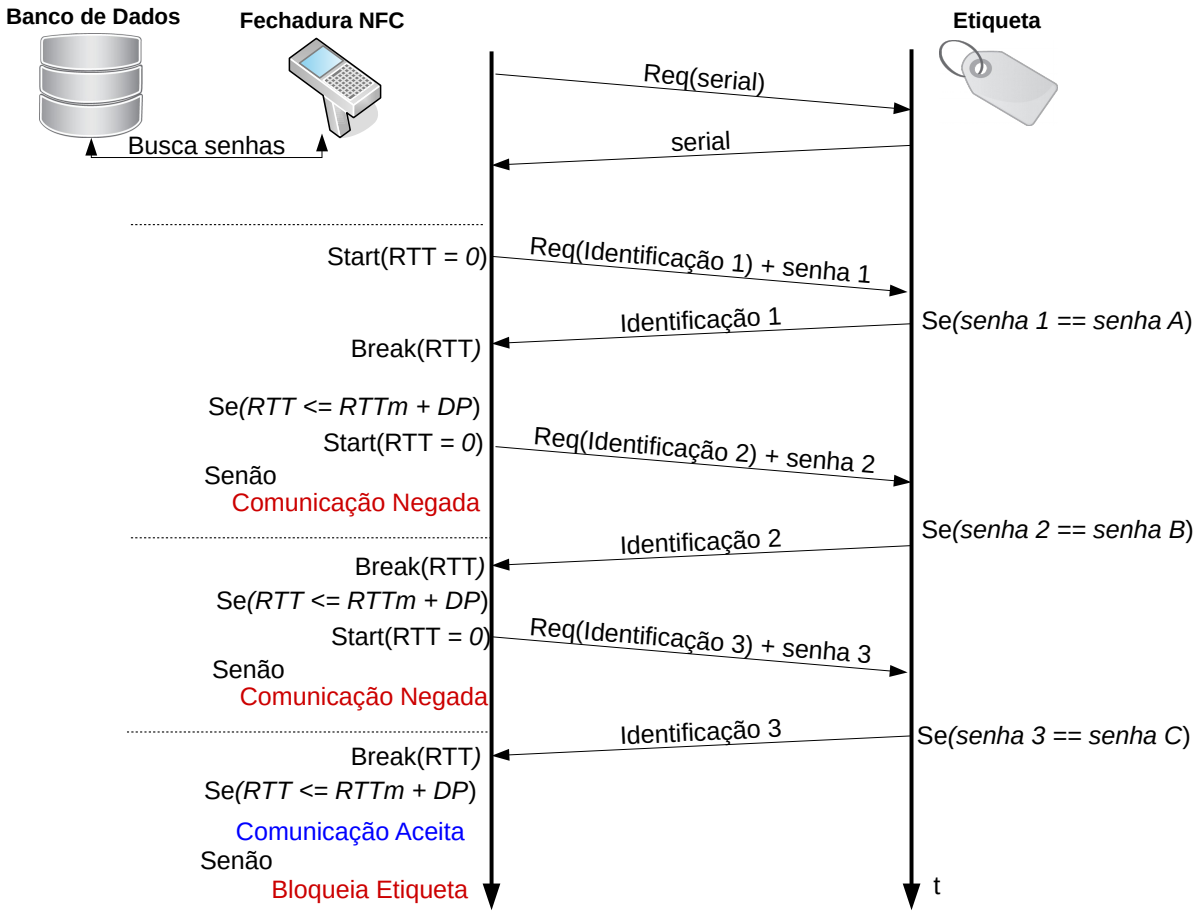
destacar que tal funcionalidade não é encontrada nas especificações do (NFCFORUM, 2015), mesmo que esta etiqueta siga as especificações relacionadas ao tipo 2 de etiquetas.

No mecanismo proposto aqui, a etiqueta legítima possuirá 4 tipos de dados armazenados, (i)serial, (ii) identificação 1, (iii) identificação 2, (iv) identificação 3, sendo os 3 últimos restritos através do uso de 3 diferentes senhas. Tal funcionalidade está de acordo com as especificações do fabricante (NXP Semiconductors, 2015).

Primeiramente o leitor legítimo requisitará o serial da etiqueta, para assim resgatar as 3 senhas de acesso no banco de dados. Assim o leitor requisita o primeiro dado de identificação utilizando a primeira senha iniciando o tempo de transmissão. O novo RTT é comparado com o $RTTm + DP$, caso seja menor o leitor requisita o segundo dado de identificação utilizando a segunda senha, e compara o novo RTT resultante com $RTTm + DP$, onde caso seja menor, o leitor requisita o terceiro dado de identificação utilizando a terceira senha. Por fim,, caso o novo RTT seja menor que $RTTm + DP$, a comunicação é dada como livre do ataque de retransmissão. Nas duas primeiras requisições, caso o RTT seja maior que o $RTTm + DP$, esta comunicação é dada como provida de um ataque de retransmissão. Já para a ultima requisição, caso o novo RTT seja maior que o $RTTm + DP$, esta etiqueta é bloqueada. Tais passos podem ser observados na Figura 17.

Estas requisições com senhas impedem que o atacante consiga capturar todos os dados da etiqueta legítima em um primeiro momento, havendo assim a necessidade utilizar o ataque de retransmissão para retransmitir a senha de segurança para capturar os dados de identificação da etiqueta e repassá-los novamente para o leitor. Enquanto a requisição dos dois primeiros dados de identificação providas de um ataque de retransmissão apenas são apenas recusadas, a terceira comunicação identificada como ataque de retransmissão ocasiona no bloqueio da etiqueta. Isto é necessário pois o mecanismo identifica a captura

Figura 17 – Identificação do ataque de retransmissão na comunicação.



das senhas de acesso aos dados de identificação por força bruta, ou seja, o atacante utiliza o ataque de retransmissão para capturar os dados de identificação mesmo ao ser detectado. Neste caso os dados são clonados através das senhas transmitidas pelo terminal legítimo no momento da requisição dos dados a etiqueta.

4.5.4 Avaliação

Para a detecção do ataque de retransmissão utilizou-se os resultados obtidos na Seção 4.4. Estes resultados são decorrentes dos testes de segurança realizados para a identificação do ataque de retransmissão, onde obteve-se resultados que garantiram eficiência na identificação de tal ataque.

Até o final deste trabalho não foi possível adquirir a etiqueta *NTAG216*, a qual possui a funcionalidade de controlar a leitura dos dados perante uma senha de acesso (NXP Semiconductors, 2015). Desse modo, não foi possível realizar a avaliação do mecanismo de forma prática através desta etiqueta. Entretanto, como a identificação do ataque de retransmissão foi garantida na Seção 4.4, restou apenas verificar se a união do mecanismo

baseado em tempo com a funcionalidade de bloqueio de leitura presente na etiqueta *NTAG216*, é suficiente para identificar o ataque de retransmissão unido ao ataque de clonagem.

Um atacante ao unir o ataque de retransmissão ao ataque da clonagem consegue burlar o mecanismo de segurança apresentado na Seção 4.4. Isto acontece pois esse mecanismo detecta a presença do ataque de retransmissão ao perceber um tempo de comunicação maior do que o esperado por uma comunicação legítima. O aumento do tempo de comunicação é causado pela necessidade de um atacante ter que repassar a requisição de dados do leitor legítimo a um segundo dispositivo atacante que deve comunicar-se com a etiqueta legítima e assim repassar os dados de volta ao leitor legítimo. Por outro lado o atacante ao utilizar o ataque da clonagem poderá adiantar o processo de retransmissão dos dados, ou seja, o atacante poderá capturar todos os dados da etiqueta e cloná-los em um dispositivo atacante, que por sua vez, comunica-se diretamente com o leitor legítimo sem que haja a necessidade de realizar a retransmissão dos dados da etiqueta no meio da comunicação com o leitor legítimo.

Para evitar que o atacante utilize o ataque da clonagem para reduzir o tempo de ataque burlando então o mecanismo proposto na Seção 4.4, deve-se forçar o atacante a realizar o ataque de retransmissão no meio da comunicação com o leitor legítimo, ou seja, deve-se assegurar que o atacante necessite realizar a comunicação com a etiqueta legítima enquanto tenta autenticar-se perante o leitor legítimo. Para isso, deve-se evitar que um atacante consiga clonar todos os dados da etiqueta legítima para que o leitor legítimo requisite dados da etiqueta que o atacante não tenha clonado, ocasionando assim, a necessidade do atacante de comunicar-se com a etiqueta legítima.

Através do controle de leitura através de senhas presentes nas etiquetas *NTAG216* (NXP Semiconductors, 2015), é possível evitar que o atacante clone todos os dados das etiquetas legítimas caso não possua a senha para leitura. Logo, o protocolo desenvolvido aqui utiliza três diferentes senhas para a leitura dos três diferentes dados de identificação. Assim, o atacante é forçado a realizar o ataque de retransmissão para realizar a retransmissão dos dados das etiquetas, já que não possui todas as senhas para a leitura dos dados de identificação para realizar o ataque de clonagem. É importante ressaltar que mesmo as senhas de leitura sendo enviadas pelo leitor legítimo e capturadas pelo atacante no momento da retransmissão dos dados, esta comunicação ainda será dada como provida de um ataque de retransmissão e será recusada.

Um atacante ao realizar a captura da primeira senha, mesmo sua comunicação sendo recusada, é capaz de clonar os dados da etiqueta legítima e assim comunicar-se novamente com o leitor legítimo. Neste caso a requisição do primeiro dado de identificação, que já estará clonado no dispositivo atacante, será imediatamente fornecido sem a necessidade da retransmissão, que é aceita pelo dispositivo legítimo por conter um

tempo de transmissão aceitável, Seção 4.4. Logo, será possível então realizar a captura da segunda senha no momento da requisição feita pelo leitor legítimo à etiqueta legítima para requisitar o segundo dado de identificação. Novamente o ataque de retransmissão será identificado e barrado pelo leitor legítimo, mas a segunda senha enviada pelo leitor legítimo é então utilizada para realizar a captura do segundo dado de identificação da etiqueta. Assim o atacante realiza a clonagem do segundo dado de identificação da etiqueta, e comunica-se com o terminal legítimo utilizando os dois primeiros dados de identificação clonados ao decorrer do ataque.

Por fim, resta apenas ao atacante realizar mais uma vez o ataque para assim possuir os três dados de identificação clonados no dispositivo atacante, que através desta clonagem será possível comunicar-se com o leitor legítimo sem que haja sobrecarga de tempo causada pela etapa da retransmissão. Para evitar isto, no momento da requisição do terceiro dado de identificação, esta etiqueta é então bloqueada no sistema

Levando em consideração os resultados da Seção 4.4, obteve-se 100% de eficiência na identificação do ataque de retransmissão. É possível afirmar que todos os ataques de retransmissão serão identificados pelo leitor legítimo, baseado no tempo médio de ataque de $14,64ms$ e no tempo da comunicação legítima de $4,70ms$, obtidos de acordo com a etiqueta *MIFARE DESfireEV1* tipo 4 utilizada na avaliação da Seção 4.4, na qual o tempo de ataque é maior do que a margem de erro aceitável. Sendo assim, no momento da retransmissão do terceiro dado de identificação, a etiqueta será bloqueada inutilizando os resultados obtidos pelo atacante através desse ataque, que é composto de três etapas (retransmissões com clonagem). Tal ataque leva em média um tempo total estimado de aproximadamente $42ms$.

Portanto o ataque de retransmissão unido ao ataque de clonagem, teoricamente, seria ineficaz perante o mecanismo desenvolvido aqui. Nessa avaliação, utilizou-se os resultados obtidos no mecanismo apresentado na Seção 4.4 baseado no entendimento da funcionalidade de bloqueio de leitura de dados presente nas etiquetas *NTAG216* (NXP Semiconductors, 2015). Logo, tal mecanismo só funcionaria em etiquetas com tal funcionalidade, não sendo possível sua aplicação nas etiquetas adotadas até agora.

4.6 Estudo de Caso 5: Mecanismo de segurança contra a personificação de dispositivos

4.6.1 Vulnerabilidade

Diversos tipos de ataques já foram descritos neste trabalhos, e entre eles estão os que utilizam o roubo de dados para a personificação de usuários ou dispositivos. Conforme a Subseção 2.4.2, ataques como “Chupa-Cabras” e adulteração de máquinas de cartões

utilizam dados roubados dos usuários para trazer prejuízos ao sistema em geral. Os dispositivos utilizados nestes ataques já possuem os protocolos utilizados no sistema. Dessa forma, os dados armazenados nos cartões são facilmente interpretados, podendo ser utilizados posteriormente. Havendo a necessidade de invalidar tais dados.

Visto que a tecnologia NFC também é utilizada na área de pagamentos, Seção 2.3.1, este tipo de fraude é estudada aqui com o objetivo de prover melhor segurança a tecnologia NFC em relação ao roubo de dados.

4.6.2 Ataque

Partiremos basicamente dos dois tipos de ataques citados anteriormente, neles os atacantes podem utilizar dispositivos construídos para o roubo dos dados (i), como o "chupa-cabra", ou realizar a adulteração de terminais autênticos para realizar o roubo de dados (ii). No primeiro caso, o atacante insere um terminal falso, ilegítimo, no lugar do verdadeiro, legítimo, onde o terminal colocado pelo atacante não é detectado pelo dispositivo legítimo e nem usuário do sistema. Assim, o dispositivo legítimo comunica-se com o terminal inserido pelo atacante, que realiza o roubo dos dados sem que o usuário perceba. Neste caso o terminal ilegítimo inserido pelo atacante deve conhecer todos os protocolos utilizados pelo sistema.

No segundo caso, o atacante realiza a adulteração de um terminal legítimo, como por exemplos, um terminal de pagamento de cartão de crédito. Neste ataque o terminal adulterado armazena os dados dos dispositivos legítimos. Em ambos os casos, os dados são então recuperados pelo atacante, sendo comumente utilizada para isto, a comunicação *Bluetooth*, não havendo a necessidade e um novo contado do atacante com o terminal ilegítimo inserido.

4.6.3 Contramedida

O objetivo deste mecanismo proposto é inutilizar os dados roubados através destes ataques em ambientes NFC. Para isto, serão utilizados um terminal NFC que realiza a autenticação dos dispositivos do sistema, um BD e um *Smartphone* NFC, responsável pela autenticação do usuário. O mecanismo utilizará o método de assinatura digital com chaves assimétricas na abordagem *Rivest, Shamir e Adelman* (RSA) (STALLINGS, 2010). Neste mecanismo o dispositivo NFC possui os dados de autenticação, são eles: nome do usuário, serial do dispositivo e um contador, $cont_d$, o qual sempre incrementado de forma randômica. O terminal NFC realizará a busca no BD, através do serial, recuperando chave pública do dispositivo a ser autenticado.

O incremento randômico será utilizado para evitar que um terminal adulterado utilize um contador roubado para a autenticação. Em outras palavras, isto é necessário

pois um terminal adulterado que recebe o contador de um dispositivo com o valor 75, já incrementado de forma sequencial, pode evitar o incremento do contador no BD e autenticar-se com esse contador correto e já assinado, onde o valor 75 será o esperado pelo terminal autêntico.

No momento da autenticação, representada pela Figura 18, o terminal gera um número randômico, $randX$ e envia ao dispositivo a ser autenticado. O dispositivo então realiza o incremento do contador, $cont_d = +randX$. Em seguida realiza um resumo criptográfico sobre os dados a serem enviado (M) (nome de usuário e serial do dispositivo) e o contador, através da sua chave privada, $\sigma = E_K R(hash(M|cont_d))$. Adicionalmente, o dispositivo gera um novo número randômico, $randY$, que é enviado junto de σ e M.

O terminal ao receber a mensagem, utiliza a chave pública do dispositivo, KP, armazenada no BD para realizar um novo *hash'* através da operação $hash'(M|cont_d)$. Assim, o *hash'* é comparado com o *hash* recebido na mensagem: $hash'(M|\sigma) == D_K P(\sigma)$. Se forem iguais, o contador do terminal é incrementado com o número randômico gerado anteriormente, $cont_t = +randX$, e comparado ao recebido do dispositivo, pela operação $cont_t == cont_d$. Se forem iguais, o contador é atualizado no BD, e os dados recebidos são constatados como providos de um dispositivo autêntico.

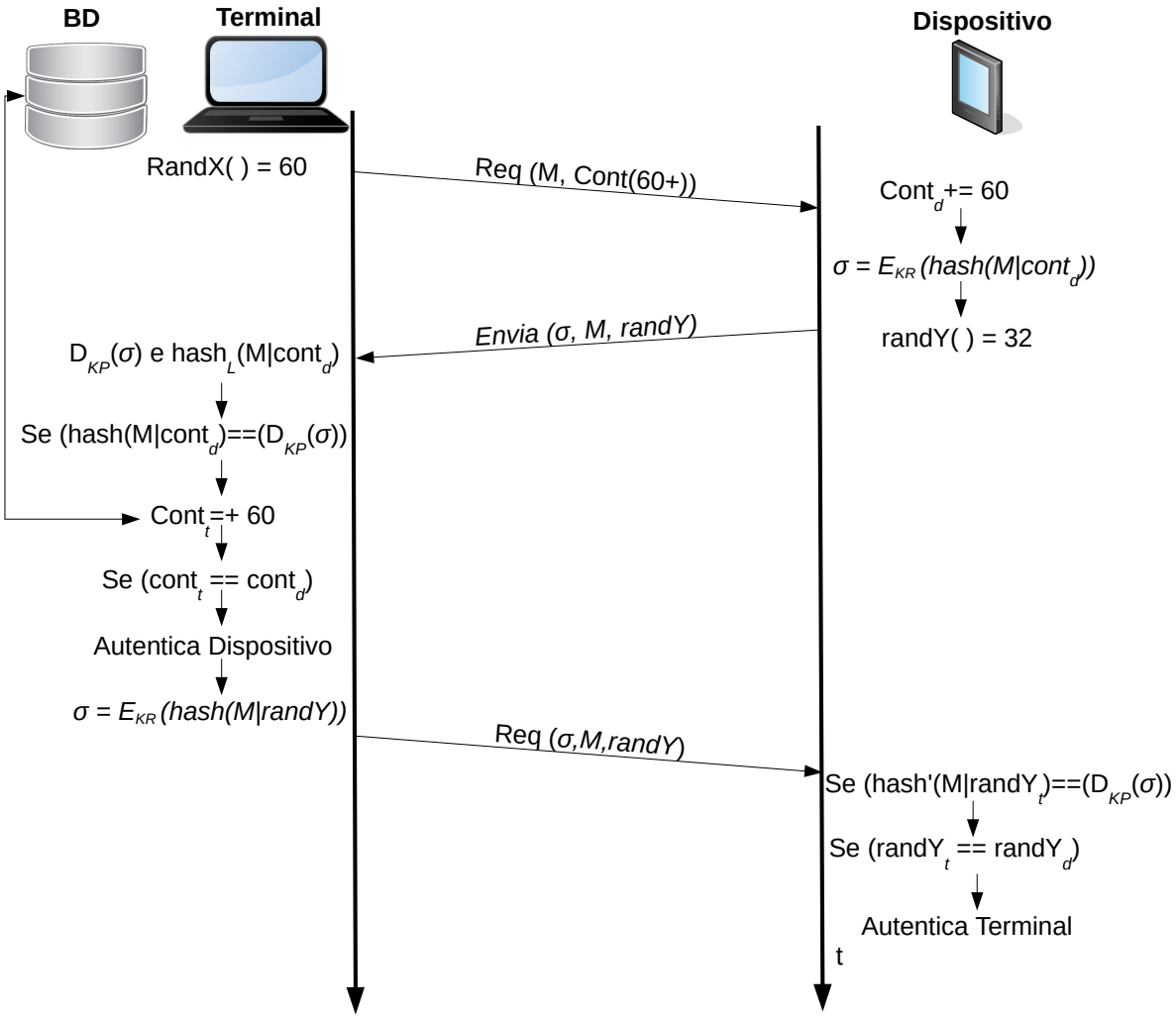
Por fim, o leitor ao constatar a autenticidade do dispositivo, realiza um resumo criptográfico sobre M e o número randômico enviado pelo dispositivo, $randY$, utilizando sua chave privada, $\sigma = E_K R(hash(M|randY))$. O dispositivo ao receber σ, realiza um novo *hash'* da mensagem recebida através da operação $hash'(M|randY)$, e compara com o *hash* recebido na mensagem: $hash'(M|\sigma) == D_K P(\sigma)$. Se forem iguais, o dispositivo compara o $randY$ recebido pelo terminal com o $randY$ gerado anteriormente pelo dispositivo, $randY_t == randY_d$. Se forem iguais, o leitor é autenticado, finalizando assim a etapa de autenticação dos dispositivos.

4.6.4 Avaliação

Primeiramente um sistema de comunicação e autenticação de dados entre dois *Smartphones* foi desenvolvido. Este sistema tem por objetivo fazer com que cada *Smartphones* se autentica perante o outro. Em seguida realizou-se 100 comunicações entre os dispositivos, onde em cada autenticação uma nova verificação da autenticidade do dispositivo emissor dos dados era verificada. Por fim, realizou-se a comunicação entre um dispositivo legítimo e um dispositivo personificado, que enviada dados roubados de outro dispositivo legítimo para autenticar-se perante o outro.

Como resultado todas as comunicações realizadas entre os dispositivos legítimos foram autenticadas, e todos os dispositivos que tentaram se autenticar utilizando dados roubados foram recusados. Através do uso do mecanismo proposto aqui, coletou-se um

Figura 18 – Autenticando origem dos dados.



tempo de $7ms$ para a autenticação dos dados, resultando em um baixo aumento de tempo em comparação a comunicação sem o mecanismo de autenticação, que necessitava de $5ms$ para comunicar-se com o leitor. Logo, pela baixa sobrecarga no tempo de comunicação entre os dispositivos legítimos e a identificação do ataque, podemos afirmar que o mecanismo é eficiente e pode ser aplicada contra ataques de personificação. Este mecanismo também não gera uma sobrecarga de conteúdo a ser cifrado para comunicações mais longas, como descrito na Seção 3.4 no trabalho (CEIPIDOR et al., 2012).

5 Conclusão

Apesar da tecnologia NFC ser promissora e estar sendo utilizada em diversas áreas de aplicações, ainda possui vulnerabilidades de segurança. O trabalho apresentado aqui teve por objetivo realizar um estudo sobre as fraudes envolvendo a tecnologia NFC, propondo novas contramedidas para os ataques de clonagem, adulteração de dados, personificação de dispositivos e retransmissão de dados, sendo avaliadas através de estudos de caso no Capítulo 4.

Como resultado do estudo realizado aqui, foi possível propor diversos mecanismos de segurança. O primeiro deles, o mecanismo de segurança contra a clonagem, realiza a detecção de etiquetas clonadas, mostrando-se mais eficiente que o apresentado em (LEHTONEN et al., 2009). Também em relação ao mecanismo apresentado em (LEHTONEN et al., 2009), o proposto aqui não é vulnerável ao ataque DoS, conforme a versão apresentada na Subseção 4.2.3.1, e possibilita a obtenção do histórico do atacante. O segundo deles é capaz de detectar a adulteração de etiquetas e a inserção de etiquetas não pertencentes ao ambiente, sem sobrecargas de tempo na autenticação das etiquetas.

Na Seção 4.4 o mecanismo de segurança desenvolvido foi capaz de detectar o ataque de retransmissão, sem a necessidade de ferramentas adicionais como GPS e medidor de temperatura como apresentado pelo trabalho (SHEN et al., 2015). Também nãi necessita realizar a interferência nas comunicações presentes no ambiente de aplicação da tecnologia, como o mecanismo apresentado em(OH et al., 2015). O mecanismo proposto mostrou-se também mais eficiente do que o já existente na tecnologia NFC, sem presença de falsos positivos e falsos negativos por possuir um tempo mais otimizado para cada etiqueta do sistema (HANCKE; MAYES; MARKANTONAKIS, 2009).

Adicionalmente, na Seção 4.5 desenvolveu-se um mecanismo de contramedida para o ataque do retransmissão unido ao ataque da clonagem. Para a avaliação desse mecanismo utilizou-se os resultados encontrados na Seção 4.4 e um diferente padrão de etiquetas que possibilitam o bloqueio de leitura por senhas. Essas etiquetas são mais caras e não tão comuns no mercado como as até então abordadas. Sua utilização foi necessária para forçar um atacante a realizar o ataque de retransmissão em meio a uma comunicação NFC, para assim detectar o ataque de retransmissão em meio a uma comunicação NFC. Por fim, foi possível também, realizar uma autenticação mútua entre dispositivos NFC sem a sobrecarga de processamento em longas trocas de informações, como no trabalho (CEIPIDOR et al., 2012).

Para trabalhos futuros, pretende-se melhorar o mecanismo proposto na Seção 4.2 para identificar o ataque da clonagem antes da utilização da etiqueta ilegítima, ou até

mesmo, evitar a clonagem de etiquetas que possibilitam apenas operações de leitura e escrita. Pretende-se também, avaliar de forma prática os estudos de caso apresentado na Seção 4.5 e adaptá-lo para etiquetas que possibilitam apenas operações de leitura e escrita. Com isso, o estudo das fraudes envolvendo a tecnologia NFC será continuado com aprimoramentos nos mecanismos já propostos e propondo novos mecanismos.

Referências

14443 ISO. *Identification cards - Contactless integrated circuit(s) cards - Proximity cards*. [S.l.], 2008. Citado 2 vezes nas páginas 27 e 37.

ABAWAJY, J. Enhancing RFID tag resistance against cloning attack. In: *Third International Conference on Network and System Security (NSS'09)*. [S.l.: s.n.], 2009. p. 18–23. Citado 2 vezes nas páginas 33 e 41.

AL-OFEISHAT, H. A.; MOHAMMAD, A. Near field communication (NFC). *International Journal of Computer Science and Network Security*, v. 12, n. 2, p. 93–99, 2012. Citado na página 24.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Computer networks*, Elsevier, v. 54, n. 15, p. 2787–2805, 2010. Citado 2 vezes nas páginas 17 e 23.

BORGIA, E. The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, Elsevier, v. 54, p. 1–31, 2014. Citado 2 vezes nas páginas 17 e 23.

CAVDAR, D.; TOMUR, E. A practical NFC relay attack on mobile devices using card emulation mode. In: *38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015*. [S.l.: s.n.], 2015. Citado 6 vezes nas páginas 36, 37, 38, 41, 54 e 55.

CEIPIDOR, U. B. et al. Kernees: a protocol for mutual authentication between nfc phones and pos terminals for secure payment transactions. In: IEEE. *9th International ISC Conference on Information Security and Cryptology (ISCISC)*. [S.l.], 2012. p. 115–120. Citado 5 vezes nas páginas 39, 40, 41, 63 e 65.

CHATTHA, N. A. NFC Vulnerabilities and defense. In: *2014 Conference on Information Assurance and Cyber Security (CIACS)*. [S.l.: s.n.], 2014. p. 35–38. Citado 5 vezes nas páginas 18, 25, 28, 35 e 41.

CHEN, C. H.; LIN, I. C.; YANG, C. C. NFC Attacks Analysis and Survey. In: *Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*. [S.l.: s.n.], 2014. p. 458–462. Citado 7 vezes nas páginas 18, 28, 35, 41, 44, 45 e 49.

COSKUN, V.; OZDENIZCI, B.; OK, K. A Survey on Near Field Communication (NFC) Technology. *Wireless Personal Communication*, Springer, v. 71, p. 2259–2294, 2013. Citado 6 vezes nas páginas 17, 22, 23, 24, 25 e 26.

DIMITRIOU, T. A lightweight RFID protocol to protect against traceability and cloning attacks. In: IEEE. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks. SecureComm 2005*. [S.l.], 2005. p. 59–66. Citado 3 vezes nas páginas 18, 33 e 41.

FERREIRA, A. B. D. H. *Dicionário Aurélio da Língua Portuguesa*. [S.l.]: Positivo, 2014. Citado na página 28.

HAMEED, S. et al. Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters. In: IEEE. *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*. [S.l.], 2014. p. 900–905. Citado 3 vezes nas páginas 28, 40 e 41.

HANCKE, G. P.; MAYES, K.; MARKANTONAKIS, K. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, Elsevier, v. 28, n. 7, p. 615–627, 2009. Citado 4 vezes nas páginas 37, 41, 55 e 65.

HASELSTEINER, E.; BREITFUSS, K. Security in near field communication (NFC). In: *Workshop on RFID security*. [S.l.: s.n.], 2006. p. 12–14. Citado 3 vezes nas páginas 18, 25 e 27.

IGLESIAS, R. et al. Experiencing NFC-based touch for home healthcare. In: ACM. *Proceedings of the 2nd international conference on pervasive technologies related to assistive environments*. [S.l.], 2009. p. 27. Citado na página 24.

ILIE-ZUDOR, E. et al. A survey of applications and requirements of unique identification systems and RFID techniques. *Computers in Industry*, Elsevier, v. 62, n. 3, p. 227–252, 2011. Citado 2 vezes nas páginas 17 e 21.

KHOO, B. RFID as an enabler of the internet of things: issues of security and privacy. In: IEEE. *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*. [S.l.], 2011. p. 709–712. Citado 2 vezes nas páginas 21 e 45.

KOSCHER, K. et al. EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. In: ACM. *Proceedings of the 16th ACM conference on Computer and communications security*. [S.l.], 2009. p. 33–42. Citado 2 vezes nas páginas 34 e 41.

LEHTONEN, M. et al. Securing RFID Systems by Detecting Tag Cloning. In: TOKUDA, H. et al. (Ed.). *7th International Conference on Pervasive Computing (Pervasive 2009)*. Nara, Japan: Springer, 2009. (Lecture Notes in Computer Science, v. 5538), p. 291–308. Citado 7 vezes nas páginas 18, 34, 41, 44, 48, 49 e 65.

LI, L.; ZHAO, X.; XUE, G. Near field authentication for smart devices. In: IEEE. *INFOCOM, 2013 Proceedings IEEE*. [S.l.], 2013. p. 375–379. Citado 2 vezes nas páginas 40 e 41.

MADLMAYR, G. et al. NFC devices: Security and privacy. In: IEEE. *Third International Conference on Availability, Reliability and Security*. [S.l.], 2008. p. 642–647. Citado 2 vezes nas páginas 35 e 41.

MARGI, C. et al. *Segurança em redes de sensores sem fio*. [S.l.]: Minicursos: IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG), 2009. 149–194 p. Citado na página 38.

NELSON, D.; QIAO, M.; CARPENTER, A. Security of the near field communication protocol: an overview. *Journal of Computing Sciences in Colleges*, Consortium for Computing Sciences in Colleges, v. 29, n. 2, p. 94–104, 2013. Citado 2 vezes nas páginas 45 e 49.

NFCFORUM. 2015. Disponível em: http://nfc-forum.org. Acessado em: 29/05/2015. Citado 7 vezes nas páginas 17, 18, 22, 25, 26, 27 e 57.

NFCWORLD. 2015. Disponível em: http://http://nfcworld.com/. Acessado em: 27/07/2015. Citado 2 vezes nas páginas 17 e 18.

NOTÍCIAS, G. *Cliente tem cartao clonado e prejuizo de quase R$ 8 mil em Aracaju*. 2015. Disponível em: http://g1.globo.com/. Acessado 2em: 06/11/2015. Citado na página 28.

NOTÍCIAS, G. *Guarda encontra "chupa-cabra"em duas maquinas em banco de Tatuí*. 2015. Disponível em: http://g1.globo.com/. Acessado em: 06/11/2015. Citado na página 28.

NOTÍCIAS, G. *Quadrilha usa bluetooth para clonar cartoes de chip e movimenta milhoes*. 2015. Disponível em: http://g1.globo.com/. Acessado em: 06/11/2015. Citado na página 28.

NXP Semiconductors. *NTAG213/215/216*. [S.l.], 2015. Citado 5 vezes nas páginas 56, 57, 58, 59 e 60.

OH, S. et al. Countermeasure of nfc relay attack with jamming. In: IEEE. *12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT)*. [S.l.], 2015. p. 1–4. Citado 3 vezes nas páginas 38, 41 e 65.

RFIDJORNALBRASIL. 2015. Disponível em: http://brasil.rfidjournal.com/. Acessado em: 27/07/2015. Citado 4 vezes nas páginas 18, 23, 24 e 28.

ROBERTS, C. M. Radio frequency identification (RFID). *Computers & Security*, Elsevier, v. 25, n. 1, p. 18–26, 2006. Citado na página 21.

ROLAND, M.; LANGER, J.; SCHARINGER, J. Applying relay attacks to google wallet. In: IEEE. *5th International Workshop on Near Field Communication (NFC)*. [S.l.], 2013. p. 1–6. Citado 3 vezes nas páginas 36, 37 e 41.

SAEED, M. Q.; WALTER, C. D. Off-line NFC Tag Authentication. In: *IEEE International Conference for Internet Technology And Secured Transactions*. [S.l.: s.n.], 2012. p. 730–735. Citado 4 vezes nas páginas 28, 35, 36 e 41.

SHEN, W. et al. Research on Defense Technology of Relay Attacks in RFID Systems. *015 International Conference on Computer Science and Intelligent Communication (CSIC 2015)*, June 2015. ISSN 2352-538x. Citado 3 vezes nas páginas 37, 41 e 65.

SPRUIT, M.; WESTER, W. *RFID Security and Privacy: Threats and Countermeasures*. [S.l.], 2013. Citado 5 vezes nas páginas 18, 28, 33, 41 e 44.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. [S.l.]: Prentice Hall, 2010. Citado 7 vezes nas páginas 27, 29, 30, 31, 32, 50 e 61.

STMicroelectronics. *Technical Note: NFC Guide, TN1216*. [S.l.], 2015. Citado na página 24.

TIMALSINA, S. K.; BHUSAL, R.; MOH, S. NFC and its application to mobile payment: Overview and comparison. In: IEEE. *8th International Conference on Information Science and Digital Content Technology (ICIDT)*. [S.l.], 2012. v. 1, p. 203–206. Citado na página 28.

TUBINO, E. R.; QUINCOZES, S. E.; KAZIENKO, J. F. *Comunicação por Campo de Proximidade: Tecnologia, Aplicações e Questões de Segurança*. [S.l.]: Tendências e Técnicas em Sistemas Computacionais, 2015. 41–59 p. Citado 3 vezes nas páginas 22, 43 e 44.

TUBINO, E. R.; QUINCOZES, S. E.; KAZIENKO, J. F. Detectando a Adulteração de Dados Armazenados em Etiquetas na Comunicação por Campo de Proximidade. In: *VII Salão Internacional de Ensino, Pesquisa e Extensão*. [S.l.: s.n.], 2015. v. 7, p. 1–2. Citado na página 50.

TUBINO, E. R.; QUINCOZES, S. E.; KAZIENKO, J. F. Detecção e Invalidação de Etiquetas Clonadas na Identificação por Radiofrequência. In: *Computer on the Beach*. [S.l.: s.n.], 2016. v. 1, p. 118–125. Citado na página 48.

WANG, Z. et al. Implementation and Analysis of a Practical NFC Relay Attack Example. In: *Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012*. [S.l.: s.n.], 2012. p. 143–146. Citado 7 vezes nas páginas 36, 37, 38, 41, 53, 54 e 55.

WANT, R. An introduction to RFID technology. *Pervasive Computing, IEEE*, IEEE, v. 5, n. 1, p. 25–33, 2006. Citado 2 vezes nas páginas 21 e 22.

WANT, R. Near field communication. *IEEE Pervasive Computing*, IEEE Computer Society, v. 10, n. 3, p. 4–7, 2011. Citado 7 vezes nas páginas 17, 18, 22, 23, 25, 26 e 28.

ZHUANG, Z.-J.; ZHANG, J.; GENG, W.-D. Analysis and Optimization to an NFC Security Authentication Algorithm Based on Hash Functions. In: *2014 International Conference on Wireless Communication and Sensor Network (WCSN)*. [S.l.: s.n.], 2014. p. 240–245. Citado na página 28.