Um Estudo Acerca das Fraudes na Comunicação por Campo de Proximidade

Emilio R. R. Tubino e Juliano F. Kazienko

[1]Curso de Ciência da Computação - Universidade Federal do Pampa (UNIPAMPA)
Prédio A1 – CEP 97.546-550 – Alegrete – RS – Brasil

emiliotubino@alunos.unipampa.edu.br, kazienko@unipampa.edu.br

Abstract. *The Near Field Communication (NFC) has recently attracted the interest of the scientific community, industry, and users. It makes the NFC a promising communication technology. However, for its advance there are issues that need to be addressed. This work aims to study the frauds regarding to the NFC technology, specially ones related to the data modification, tag cloning, and data relay. Hence, we accomplish three study cases identifying vulnerabilities, attacks, and countermeasures. In addition, the proposed countermeasure in each study case is evaluated in order to demonstrate its efficiency.*

Resumo. *A Comunicação por Campo de Proximidade, do inglês, Near Field Communication (NFC) tem recentemente atraído o interesse da comunidade científica, da indústria e usuários, tornando-se uma tecnologia de comunicação promissora. Contudo, apesar de gradativa popularização, tal tecnologia ainda possui questões de segurança em aberto que devem ser tratadas. Este trabalho tem por objetivo estudar as fraudes no âmbito da tecnologia NFC, especialmente envolvendo a adulteração, a clonagem e a retransmissão. Para tanto, são realizados três estudos de caso nos quais se identificam vulnerabilidade, ataque e contramedida. Adicionalmente, a contramedida proposta através de cada estudo de caso é avaliada a fim de demonstrar sua efetividade.*

1. Introdução

A tecnologia de Identificação por Radiofrequência, do inglês, *Radio Frequency Identification* (RFID), realiza sua comunicação através de ondas de radiofrequência entre dispositivos. Essa tecnologia é comumente utilizada na identificação de itens, controle de ambientes e comunicação de dispositivos. Diversos padrões da tecnologia RFID são criados e adaptados dependendo das necessidades de cada aplicação. Esse é o caso da tecnologia de Comunicação por Campo de Proximidade, do inglês, *Near Field Communication* (NFC), que possui um campo de comunicação reduzido a uma distância máxima entre os dispositivos de aproximadamente 10 cm e opera em uma frequência de 13,56 MHz [Want 2011] [Coskun et al. 2013]. Suas aplicações consistem no controle de acesso em fechaduras eletrônicas, identificação de objetos através de etiquetas NFC, na área de pagamentos eletrônicos e bilhetagem de ônibus e metro, no Japão, Europa e Brasil [RFIDJournalBrasil 2015].

Apesar da tecnologia NFC já ser utilizada para diversas aplicações, ainda trata-se de uma tecnologia relativamente nova, possuindo vulnerabilidades que permitem ataques como os de adulteração de dados, clonagem e retransmissão [Chen et al. 2014]

[Madlmayr et al. 2008] [Hancke et al. 2009] [Roland et al. 2013] [Oh et al. 2015], necessitando assim, de aprimoramentos no âmbito da segurança [Chen et al. 2014] [Chattha 2014]. A necessidade de resolver as vulnerabilidades presentes nessa tecnologia torna-se ainda mais evidente por ser comumente aplicada, por exemplo, a área médica e de pagamentos eletrônicos, tendo sido essa última, alvo constante de fraudes.

Relacionado às vulnerabilidades citadas anteriormente, a tecnologia RFID já possui mecanismo de segurança que evitam e/ou mitigam os ataques citados anteriormente. Entretanto, muitos dos mecanismos existentes e aplicados na tecnologia RFID não são adequados à tecnologia NFC, mesmo sendo essa última um subconjunto da tecnologia RFID. Isso ocorre pela diferença entre protocolos e dispositivos presentes na tecnologia NFC, como o caso da comunicação par-a-par e dispositivos como os *smartphones* que estão presentes apenas na tecnologia NFC. Logo, os mecanismos de segurança existentes na tecnologia RFID requerem adaptação, ou, novos mecanismos devem ser desenvolvidos baseados nas características do NFC.

Neste trabalho, é realizado um estudo sobre fraudes existentes na tecnologia NFC. Desse modo, realiza-se, através de estudos de caso, a identificação de vulnerabilidades, ataques e contramedidas. Particularmente, trata-se através de tais estudos de caso os ataques de adulteração de dados, clonagem de etiquetas e retransmissão de dados. Adicionalmente, as contramedidas propostas são avaliadas a fim de demonstrar sua efetividade. Na Seção 2, são discutidos os trabalhos relacionados. A Seção 3 apresenta os estudos de caso desenvolvidos. Por fim, na Seção 4, são tecidas as considerações finais.

2. Trabalhos Relacionados

Os trabalhos apresentados pelos autores [Chen et al. 2014] e [Madlmayr et al. 2008] realizam um estudo acerca das fraudes aplicáveis na tecnologia NFC. Tais trabalhos apresentam o ataque de negação de serviço, do inglês, *Denial of Service* (DoS), em etiquetas NFC como um problema a ser tratado, sugerindo a necessidade um mecanismo de controle da função de leitura e escrita na etiqueta a fim de evitar que usuários não autorizados adulterem os dados armazenados nela. Tais trabalhos citam o ataque de adulteração de dados como um problema em aberto.

O trabalho apresentado pelos autores [Hameed et al. 2014] apresenta um mecanismo de segurança contra conteúdos maliciosos armazenados em etiquetas NFC, baseado em lista branca (*white list*) e lista negra (*black list*). Através dessas listas, o mecanismo intermediário confronta a *URL* lida, e verifica a confiabilidade da mesma. Neste tipo de ataque, uma *URL* pode ser inserida em um etiqueta para que um *smartphone* ao ler o conteúdo, seja direcionado para um *link* malicioso, como *link's* para *download* de aplicativos prejudiciais ou sites de empresas concorrentes a proprietária da etiqueta. Esse mecanismo apresenta vulnerabilidades como *URL's* não cadastradas na lista, e a necessidade do *smartphone* estar sempre atualizado com as listas, havendo assim o risco do conteúdo armazenado na etiqueta ser acessada pelo usuário pelo fato de não poder verificar sua confiabilidade.

No trabalho apresentado por [Spruit and Wester 2013], os autores propõem um mecanismo de segurança contra o ataque da clonagem no âmbito da tecnologia RFID. 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. Entretanto, esse método não permite sua aplicação em etiquetas capazes somente de realizar operações de leitura e escrita de dados, devido à incapacidade de realizar computações como a cifragem de dados.

O trabalho apresentado por [Lehtonen et al. 2009] aborda um mecanismo de detecção do ataque da clonagem em etiquetas que permitem apenas operações de leitura e escrita. Esse mecanismo é baseado em um número randômico compartilhado entre o terminal e a etiqueta. Com a comparação do valor randômico da etiqueta e terminal, verifica-se a sincronia entre os valores para a detecção da adulteração. A detecção da clonagem só ocorre quando duas etiquetas com o mesmo serial tentam acessar o sistema, assim a primeira a acessar o sistema dessincroniza o valor de autenticação randômico armazenado no terminal em relação a outra etiqueta.

Entretanto, apesar de o trabalho de [Lehtonen et al. 2009] citar ataques DoS, o mecanismo proposto pelos autores não resolve esta vulnerabilidade ocasionada pela clonagem das etiquetas. Nesse ataque, o objetivo principal é inviabilizar o acesso ao serviço a um usuário que tente autenticar-se perante um terminal utilizando a etiqueta legítima. Por utilizar números randômicos, este mecanismo também não possibilita a obtenção do histórico do atacante, não sendo possível verificar quais foram as utilizações da etiqueta clonada (ilegítima) e quais suas ações.

Outro ataque ao qual a tecnologia NFC está vulnerável consiste no ataque de retransmissão, ou do inglês, *Relay Attack*. Os autores [Hancke et al. 2009], além de estudar o ataque de retransmissão e realizarem uma crítica às contramedidas existentes a este ataque, também citam a existência de um mecanismo de tempo na comunicação NFC especificada pela ISO [14443 ISO 2008] para evitar o ataque de retransmissão. De acordo com os autores, seu tempo de tolerância muito prolongado tende a deixar uma grande margem para que um atacante realize o ataque de retransmissão.

O trabalho apresentado pelos autores [Ranganathan et al. 2015] propõem um mecanismo de segurança contra o ataque de retransmissão baseado na distância entre os dispositivos. Esse mecanismo utiliza o sinal de comunicação para detectar a distância entre os dispositivos, verificando a intensidade e ruído do sinal recebido através do uso de um osciloscópio. Com a comparação do sinal recebido e o sinal legítimo conhecido, é possível identificar a diferença entre os ruídos e intensidade do sinal recebido caso ele tenha sido gerado de um ataque de retransmissão. Esse mecanismo tem um custo mais elevado pois necessitar de *hardwares* mais robustos, não sendo viável utilizá-lo para o uso pessoal da tecnologia NFC, como em dispositivos *smartphones*.

Pelo fato da tecnologia NFC e a *Wi-fi* utilizarem uma frequência de comunicação diferente uma da outra, o trabalho de [Oh et al. 2015] propõe um mecanismo de segurança para evitar o ataque da retransmissão através da interferência do canal de comunicação, do inglês, *Jamming*, utilizado pela tecnologia *Wi-Fi*, não interferindo na comunicação NFC. Entretanto, o mecanismo apresentando em [Oh et al. 2015] se mostra ineficiente caso a tecnologia de comunicação utilizada para o ataque for diferente da *Wi-Fi* ou utilize um meio cabeado para a retransmissão dos dados. Outra limitação dessa contramedida é a interferência em qualquer comunicação *Wi-Fi*. Assim, todos os dispositivos que estiverem utilizando tal tecnologia, sejam legítimos ou atacantes, serão afetados por tal interferência.

3. Estudos de Caso

Esta seção apresenta três estudos de caso relacionados aos ataques de adulteração de dados, clonagem de etiquetas e retransmissão de dados, apresentando propostas de contramedidas avaliadas ao final de cada estudo. Para fins de experimentação e avaliação, foram utilizados: um *notebook Sony vaio* modelo *svf15213cbw* com NFC integrado, um *notebook LG* modelo *A530* e um leitor NFC modelo *ACR 122U* com conexão *USB*. Também foram utilizados um *Smartphone Samsung E7* e *Smartphone Sony Xperia M*, ambos com NFC integrado. Por fim foram utilizadas etiquetas NFC do modelo *MIFARE DESfireEV1* tipo 4, com a capacidade de armazenamento de 4.094 *Bytes*. Entretanto, qualquer tipo de etiqueta NFC poderia ser utilizada, principalmente modelos mais baratos com processamento limitado, uma vez que as propostas foram projetadas para tais etiquetas.

3.1. Estudo de Caso 1 (EC1): Detecção a adulteração de etiquetas NFC

As etiquetas NFC mais comumente utilizadas são as capazes de realizar apenas operações de leitura e escrita. Tais etiquetas são mais vulneráveis a ataques de adulteração por não possuir um controle de escrita que evite que dispositivos não autorizados realizem a adulteração dos dados armazenados. O ataque de adulteração utiliza uma etiqueta legítima, ou seja, uma etiqueta pertencente ao ambiente para causar prejuízos ao sistema [Chen et al. 2014]. Através desse ataque, um atacante pode modificar os dados contidos em uma etiqueta legítima, alterando preços de uma mercadoria e suas características, trazendo assim, vantagens ao atacante e prejuízos ao sistema ao qual essa etiqueta pertence. É possível também que um atacante modifique uma etiqueta legítima e adicione conteúdos maliciosos ou de empresas concorrentes, dependendo da aplicação.

Portanto, a contramedida proposta aqui tem por objetivo detectar ataques de adulteração de dados em etiquetas que possibilitam apenas operações de leitura e escrita. Particularmente, tal tipo de etiqueta é abordado neste trabalho pelo fato de possuir menor custo monetário e ser comumente encontradas na área comercial. Para fins de validação do mecanismo de contramedida desenvolvido, é abordado aqui um cenário de uma loja de produtos eletrônicos. Nesse sistema, todos os produtos possuem uma etiqueta NFC com seus dados técnicos e preço gravados nela, sendo cada etiqueta previamente cadastrada através de um leitor NFC, com seus dados, como o número serial da etiqueta armazenados em um banco de dados (BD). Para consultar informações e preços dos produtos do estabelecimento, os usuários do sistema (clientes) utilizam seu *Smartphone* com NFC habilitado, que deve estar atualizado com o software da loja previamente disponibilizado.

O esquema de autenticação é baseado na abordagem de obtenção de assinatura digital *Rivest, Shamir e Adelman* (RSA) [Stallings 2010], através de chaves assimétricas. Nesse sistema o terminal recebe os dados que serão armazenados na etiqueta, realiza um resumo criptográfico (*hash*) da mensagem M, $hash(M)$, e através da chave privada, E_{KR}, à cifra a fim de computar a assinatura digital da mensagem $\sigma = E_{KR}(hash(M))$, sendo que 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. O dispositivo leitor ao comunicar-se com a etiqueta, recebe a mensagem e a assinatura armazenados nela, que através da chave pública do terminal, E_{KP}, previamente distribuída entre os usuários do sistema, decifra o *hash* contido na etiqueta, $D_{KP}(\sigma)$, e gera um novo *hash* da mensagem recebida, $hash'(M)$. 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.

3.1.1. Avaliação

Preliminarmente, o protótipo construído permitiu verificar que o sistema é funcional. Para testar o sistema, 5 etiquetas foram utilizadas, das quais 3 foram adulteradas. Nos três casos, a detecção da adulteração foi efetuada. O tempo médio de execução do protocolo de autenticação dos dados na etiqueta é de 3 ms. Tal tempo de execução é baixo comparado a um sistema sem autenticação, que demandou 2 ms para a leitura da etiqueta.

É importante ressaltar que o mecanismo proposto aqui não evita a adulteração dos dados, entretanto, ainda permite a detecção do ataque da adulteração, protegendo os usuários das etiquetas contra tal ataque. Nesse mecanismo é possível também detectar a inserção de etiquetas falsas (ilegítimas), pelo fato de que os atacantes não possuem a chave privada para a assinatura dos dados armazenados nas etiquetas.

3.2. Estudo de Caso 2 (EC2): Detecção de etiquetas clonadas

Um dos grandes desafios da tecnologia NFC consiste na detecção e invalidação de etiquetas clonadas que possibilitam apenas operações de leitura e escrita de dados. Nessas etiquetas, toda a informação armazenada pode ser lida por qualquer dispositivo [Chen et al. 2014] [Lehtonen et al. 2009], sendo essa a vulnerabilidade que possibilita a um atacante a leitura e cópia de todo o conteúdo para uma etiqueta ilegítima, requerendo tratamento apropriado.

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 terceiro, acessando ambientes, etc. [Chen et al. 2014]. Em um ambiente de controle de acesso que utiliza uma etiqueta NFC como "chave" de abertura de uma fechadura NFC, é possível que um atacante clone a etiqueta, e com isso, possa acessar um ambiente restrito. Considerando o acesso a um sistema de informação mediante a apresentação de uma etiqueta, o acesso indevido não será percebido, pois os dados da etiqueta ilegítima serão os mesmos da legítima.

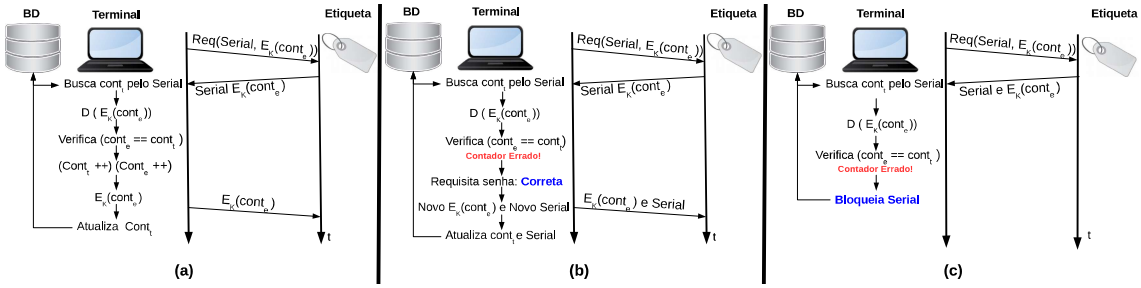
Assim, é proposto aqui como contramedida um mecanismo de detecção e invalidação de etiquetas clonadas (ilegítimas) que permitem apenas operações de leitura e escrita com o uso terminais NFC responsáveis pela detecção do ataque. Esses terminais estão conectados a um BD responsável pelo armazenamento das informações contidas nas etiquetas, como seu número serial, dados do usuário e um contador de leituras $cont_e$. Tal contador é incrementado a cada autenticação e atualizado no BD ($cont_e$) e armazenado na etiqueta de modo cifrado, $E_K(cont_e)$, utilizando uma chave simétrica K. 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 1(a). A detecção da clonagem acontece quando o usuário da etiqueta legítima utiliza o terminal novamente, uma vez que o terminal detecta que $cont_t \neq cont_e$.

Conforme o ambiente no qual o mecanismo for utilizado, duas versões do mecanismo são propostas. A Figura 1(b) ilustra a Versão 1, que envolve o uso de senhas. Nessa 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 e fica 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 (ilegítima) 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. Assim, 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 1. (a) Mecanismo de detecção de etiquetas clonadas, (b) versão com senha e (c) versão sem senha.



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 Versão 2 mostrada na Figura 1(c) 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, sendo necessário 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.

3.2.1. Avaliação

Para fins experimentais, utilizou-se o *Data Encryption Standard* (DES) como algoritmo de cifragem. Entretanto, qualquer cifra simétrica poderia ser utilizada. 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 de 5 ms. A avaliação experimental revelou a funcionalidade do mecanismo proposto e uma baixa sobrecarga de tempo em relação a não aplicação do mecanismo, que possui um tempo médio de 2 ms para comunicação. Esse mecanismo mostra-se mas eficiente visto que o tempo demandado para autenticação em [Lehtonen et al. 2009] de 864 ms. Adicionalmente, o mecanismo proposto aqui abrange uma maior variedade de cenários, sendo capaz de evitar prejuízos causados pelo ataque DoS na Versão 1 do mecanismo, que faz uso de senha. Entretanto, a Versão 2, idealizada para cenários que não possibilitam o uso de senha, ainda admite esse ataque.

É importante ressaltar que, embora o método permita uma interação do atacante com o terminal, ele se mostrou eficaz em detectar a clonagem e invalidar uma etiqueta. Comparando à detecção da clonagem de cartões de crédito, que em geral fica por conta do próprio usuário, o mecanismo proposto aqui detecta a clonagem da etiqueta na sua próxima utilização posterior a da etiqueta clonada. Nesse mecanismo é possível identificar os danos causados pelo atacante utilizando o histórico obtido através da comparação entre o contador da etiqueta legitima e armazenado no BD. 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.

3.3. Estudo de Caso 3 (EC 3): Detectando o ataque de retransmissão de dados

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, sendo essa uma vulnerabilidade que implica na possibilidade de que os dados ao serem recebidos por um dispositivo atacante, possam 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. Na prática, a comunicação entre os dispositivos só ocorrerá caso esta seja a intenção do usuário, dado pela sua curta distância de comunicação. Com essa forma de ataque, um atacante pode forçar a comunicação entre dois dispositivos que estão distantes um do outro para realizar comunicações indesejadas, aproveitando-se da distração do usuário legítimo.

O ataque de retransmissão, do inglês, *Relay Attack*, pode ser utilizado para fraudar uma transmissão NFC, criando uma "ponte" de comunicação entre dois dispositivos camuflando a distância entre eles. Nesse caso, 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. 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 maior, fraudando a presença de um dispositivo em um ambiente.

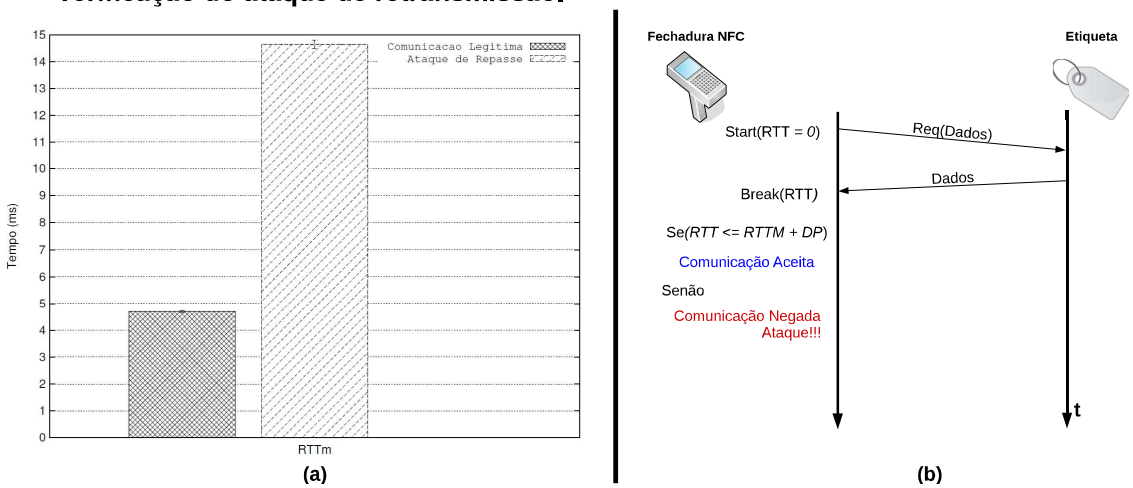
A contramedida proposta aqui tem por objetivo detectar o ataque de retransmissão de dados. Para isso, baseia-se em um ambiente de acesso controlado por uma fechadura NFC. Nesse mecanismo um terminal NFC é responsável pela autenticação dos dispositivos e etiquetas NFC, que serão as chaves de acesso. Esse mecanismo de segurança baseia-se na comparação de tempo de resposta de uma comunicação para a detecção do ataque

de retransmissão. Para isso, 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. Tal 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, $RTTm$, como apresentado na Figura 2(b). Caso o RTT esteja dentro do Desvio Padrão (DP) 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 retransmissão.

3.3.1. 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 and Tomur 2015] e [Wang et al. 2012], utilizando dois *Smartphones* atacante, A e B, para realizarem a retransmissão dos dados via *Bluetooth*. Onde 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 na Figura 2(a). O 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 que o tempo de comunicação pode ser utilizado para detectar o ataque de retransmissão. Apresenta-se um nível de confiança de 95%.

Figura 2. A Parte (a) ilustra a comparação do tempo entre comunicações legítimas e ataques de retransmissão. A Parte (b) apresenta o protocolo de verificação do ataque de retransmissão.



Com a intenção de testar o mecanismo de segurança de forma prática, realizou-se 1000 comunicações legítimas e 1000 ataques de retransmissão. Como resultado, em todos

os testes da comunicação legítima não houve a ocorrência de falsos positivos, ou seja, identificar uma comunicação legítima como ataque de retransmissão, sendo todas aceitas pelo sistema. Já nos testes de ataques de retransmissão houve 100% de identificação do ataque, onde todas as comunicações retransmitidas pelo atacante 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. Desse modo, através do uso do desvio padrão dos tempos coletados, é possível encontrar um tempo de tolerância mais adequado para a comunicação legítima. Portanto, ao contrário do método já existente e criticado pelo autor [Hancke et al. 2009], esse 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.

Por fim, os resultados experimentais apresentados mostram que esse mecanismo de segurança é eficaz contra esse ataque. É importante observar que 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 and Tomur 2015] e [Wang et al. 2012], através do uso do tempo de comunicação entre dispositivos, conforme mostrado na Figura 2.

A união do ataque de clonagem e retransmissão poderia burlar o mecanismo de tempo. Nessa união, o ataque da clonagem seria utilizado para prover os dados mais rapidamente ao leitor, realizando a clonagem da etiqueta legítima dos dados recebidos através do ataque de retransmissão. Assim, o dispositivo ilegítimo, por possuir os dados da etiqueta legítima a pronta entrega, seria aceito por não possuir um tempo elevado de comunicação. Um mecanismo de contramedida foi desenvolvido para evitar que a união dos ataques burle a contramedida baseada em tempo. Para isso, é necessário realizar bloqueio de leitura das etiquetas, para assim forçar o atacante a realizar o ataque de retransmissão para a captura dos dados. Entretanto, até o presente momento não foi possível avaliar tal contramedida de forma prática.

4. Conclusão e Trabalhos Futuros

Através do estudo realizado sobre fraudes na tecnologia NFC, foi possível identificar a existência de vulnerabilidades e propor mecanismos de contramedida. Tais mecanismos foram desenvolvidos e avaliados através de estudos de caso, resultando na identificação da adulteração de dados, com uma baixa sobrecarga de tempo.

Foi possível também detectar o ataque da clonagem de forma mais eficiente que o apresentado pelo autor [Lehtonen et al. 2009], evitando o ataque de DoS e possibilitando a obtenção do histórico de uso do sistema pelo atacante através da etiqueta clonada. Entretanto, não foi possível evitar o ataque de clonagem, porém foram diminuídos os danos causados por esse ataque ao identificar o uso da etiqueta clonada após o uso da legítima.

Outro ataque que foi estudado consiste na retransmissão de dados. O estudo permitiu identificar e evitar tal ataque de uma forma mais adequada que o mecanismo de temporização existente na tecnologia NFC [14443 ISO 2008] e discutido por [Hancke et al. 2009]. Adicionalmente, o mecanismo de combate a retransmissão proposto no Estudo de Caso 3 não necessita de *hardwares* adicionais, diferentemente do que

se propõe no trabalho desenvolvido pelos autores [Ranganathan et al. 2015].

Para trabalhos futuros, objetiva-se evoluir as contramedidas desenvolvidas aqui, como no caso do EC 2, visando a identificação de uma etiqueta clonada de forma prévia, ou até mesmo evitando a clonagem de uma etiqueta de baixo custo. Também objetiva-se avaliar o mecanismo contra a união dos ataques de clonagem e retransmissão.

Agradecimentos

Trabalho Conclusão de Curso e Iniciação Científica executados com apoio financeiro da Universidade Federal do Pampa, recursos do Edital n. 08/2015 - Programa de Bolsas de Iniciação à Pesquisa (PBIP).

Referências

14443 ISO (2008). Identification cards - Contactless integrated circuit(s) cards - Proximity cards. Technical Report ISO/IEC JTC1/SC17 Número 1363, International Standard ISO/IEC.

Cavdar, D. and Tomur, E. (2015). 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*.

Chattha, N. A. (2014). NFC Vulnerabilities and defense. In *2014 Conference on Information Assurance and Cyber Security (CIACS)*, pages 35–38.

Chen, C. H., Lin, I. C., and Yang, C. C. (2014). NFC Attacks Analysis and Survey. In *Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 458–462.

Coskun, V., Ozdenizci, B., and Ok, K. (2013). A Survey on Near Field Communication (NFC) Technology. *Wireless Personal Communication*, 71:2259–2294.

Hameed, S., Hameed, B., Hussain, S. A., and Khalid, W. (2014). Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters. In *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 900–905. IEEE.

Hancke, G. P., Mayes, K., and Markantonakis, K. (2009). Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627.

Lehtonen, M., Ostojic, D., Ilic, A., and Michahelles, F. (2009). Securing RFID Systems by Detecting Tag Cloning. In Tokuda, H., Beigl, M., Friday, A., Brush, A. J. B., and Tobe, Y., editors, *7th International Conference on Pervasive Computing (Pervasive 2009)*, pages 291–308, Nara, Japan. Springer.

Madlmayr, G., Langer, J., Kantner, C., and Scharinger, J. (2008). NFC devices: Security and privacy. In *Third International Conference on Availability, Reliability and Security*, pages 642–647. IEEE.

Oh, S., Doo, T., Ko, T., Kwak, J., and Hong, M. (2015). Countermeasure of nfc relay attack with jamming. In *12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT)*, pages 1–4. IEEE.

Ranganathan, A., Danev, B., and Capkun, S. (2015). Proximity verification for contactless access control and authentication systems. In *31st Annual Computer Security Applications Conference (ACSAC)*, pages 271–280. ACM.

RFIDJournalBrasil (2015). RFID Journal Brasil Website. Disponível em: http://brasil.rfidjournal.com/. Acessado em: 27/07/2015.

Roland, M., Langer, J., and Scharinger, J. (2013). Applying relay attacks to google wallet. In *5th International Workshop on Near Field Communication (NFC)*, pages 1–6. IEEE.

Spruit, M. and Wester, W. (2013). RFID Security and Privacy: Threats and Countermeasures. Technical report, Department of Information and Computing Sciences Utrecht University, Netherlands - Technical Report UU-CS- 2013-001.

Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. Prentice Hall.

Wang, Z., Xu, Z., Xin, W., and Chen, Z. (2012). Implementation and Analysis of a Practical NFC Relay Attack Example. In *Second International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012*, pages 143–146.

Want, R. (2011). Near field communication. *IEEE Pervasive Computing*, 10(3):4–7.

