Detecção e Invalidação de Etiquetas Clonadas na Identificação por Radiofrequência

Emilio R. Tubino[1], **Silvio E. Quincozes**[1] **e Juliano F. Kazienko**[1]

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

{emiliotubino,silvioereno}@alunos.unipampa.edu.br,kazienko@unipampa.edu.br

Abstract. *Radio Frequency Identification (RFID) technology has been broadly used to access control and objects identification. One of the major research challenges is related to cloning detection of tags that provide just reading and writing functions, without additional processing capabilities. Currently, the detection of cloning attack demands by simple solutions due to resource limitations of such devices. This work aims at proposing of a simple and efficient mechanism for detection and invalidation of cloned tags. A prototype is presented to demonstrate the functionality of the proposed mechanism. Hence, this approach intends to increase the system's security against the cloning attack in tags with constrained resources mainly in terms of processing capacity.*

Resumo. *A tecnologia de identificação por radiofrequência, do inglês, Radio Frequency Identification (RFID), tem sido amplamente utilizada para o controle de acesso e para a identificação de objetos. Um dos grandes desafios de pesquisa envolvendo tal tecnologia consiste detecção da clonagem de etiquetas que disponibilizam apenas a função de escrita e leitura, sem realizar processamentos adicionais. Atualmente, a detecção da clonagem demanda por soluções simples devido a limitação de recursos dos dispositivos RFID. Este trabalho tem por objetivo propor um mecanismo simples e eficiente para a detecção e a invalidação de etiquetas clonadas. A funcionalidade do mecanismo proposto é demonstrada através de um protótipo. Com isso, espera–se aumentar a resistência ao ataque da clonagem de etiquetas com processamento limitado.*

1. Introdução

Nos últimos anos, a tecnologia de Identificação por Radiofrequência, do inglês, *Radio Frequency Identification* (RFID), vem sendo utilizada em diversas áreas, como na agricultura, transporte, saúde, rastreamento de cargas e identificação de produtos [Want 2006]. A facilidade de uso e sua praticidade tem contribuído para sua gradativa adoção [Roberts 2006] [Wu et al. 2006] em substituição a outros sistemas de identificação, como os códigos de barras usados para identificar mercadorias [Tanenbaum and Wetherall 2011]. De forma geral, os dispositivos RFID são divididos em: (i) ativos, que possuem alimentação energética própria, como dispositivos leitores; e (ii) passivos, que não possuem fonte de energia própria sendo energizados através das ondas de radiofrequência geradas pelos dispositivos ativos [Want 2006] [Khoo 2011] [Ahuja and Potti 2010]. Recentemente, a tecnologia de comunicação por campo de proximidade, do inglês, *Near Field Communication* (NFC), que é uma categoria do RFID, tem sido amplamente adotada [Want 2011] [Spruit and Wester 2013] [Coskun et al. 2013].

Um dos grandes desafios na área da RFID consiste em prover segurança [Roland et al. 2011] [Zuo 2012]. Em cenários em que o único fator de autenticação é uma etiqueta RFID, o ataque de clonagem de uma etiqueta pode implicar em prejuízos ao usuário legítimo. Um atacante ao clonar uma etiqueta de um usuário poderá facilmente utilizar a mesma para a realização de pagamentos eletrônicos, por exemplo, supondo que um outro fator de autenticação, como uma senha, não seja solicitado. Especialmente, a detecção e invalidação de etiquetas clonadas em etiquetas que realizam apenas operações de leitura e gravação de dados sem a capacidade de realizar processamentos adicionais é difícil de resolver e ainda requer soluções apropriadas [Chen et al. 2014] [Lehtonen et al. 2009] [Spruit and Wester 2013] [Khoo 2011] [Tubino et al. 2015].

O mecanismo proposto neste artigo tem por objetivo detectar e invalidar de forma simples e eficiente etiquetas clonadas (ilegítimas) em um sistema RFID. O mecanismo proposto é destinado a etiquetas que possuem operações de leitura e escrita apenas. Tais etiquetas são largamente utilizadas devido ao seu custo menor. Duas versões do mecanismo proposto são apresentadas: a Versão 1 está apoiada no uso de etiqueta e de senha, enquanto a Versão 2 somente no uso de etiqueta. Um protótipo, baseado no uso da tecnologia NFC, foi desenvolvido a fim de avaliar a funcionalidade e o tempo de execução do mecanismo proposto.

O restante deste trabalho está organizado como segue. Na Seção 2, são discutidos os trabalhos relacionados existentes na literatura. A Seção 3 apresenta o mecanismo proposto em duas versões: com uso de senhas e sem uso de senhas. Na Seção 4, resultados oriundos de uma avaliação experimental são apresentados. Por fim, na Seção 5, as conclusões e trabalhos futuros são apresentados.

2. Trabalhos Relacionados

Em [Spruit and Wester 2013], os autores realizam um levantamento acerca das ameaças e contramedidas no âmbito da tecnologia RFID. É importante destacar que das 13 ameaças estudadas pelos autores o ataque de clonagem está em 5º lugar no que diz respeito ao seu grau de relevância. Adicionalmente, o trabalho apresenta algumas contramedidas para o ataque de clonagem. Uma delas consiste no método *Public Key Re–Encryption*, baseado no envio de dados cifrados pelos dispositivos, impedindo que o atacante consiga identificar o serial da etiqueta e passar–se por ela com o uso de tal informação. 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 a incapacidade de realizar computações como a cifração e decifração de dados.

Um protocolo a fim de combater a clonagem de etiquetas RFID é apresentado em [Abawajy 2009]. Como tal protocolo requer a realização de processamento para fins de autenticação pela etiqueta, somente etiquetas com capacidade de processamento podem suportar a execução de tal protocolo. 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, por exemplo.

No trabalho de [Dimitriou 2005], os autores propõem 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, onde deve

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 abordadas neste estudo.

Já o trabalho de [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 tal 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, onde 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.

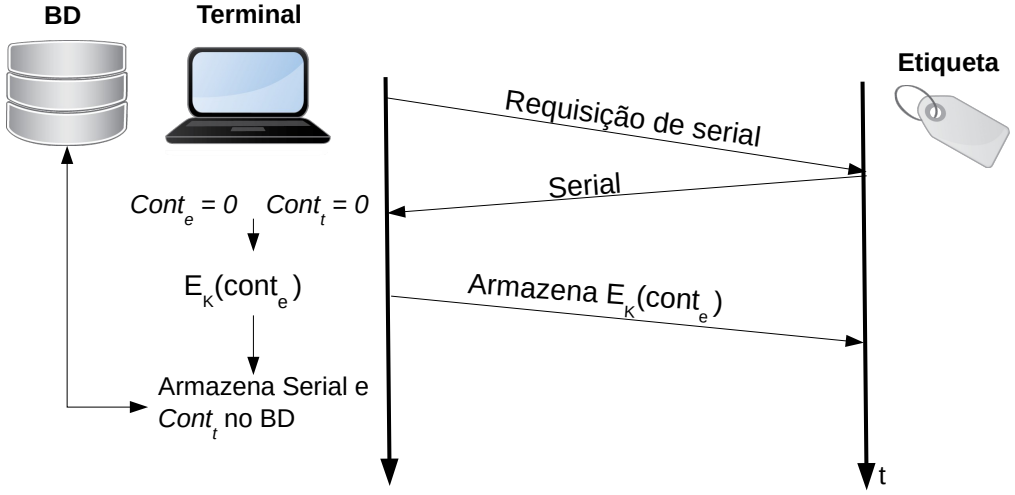
Entretanto, apesar de o trabalho de [Lehtonen et al. 2009] citar ataques de negação de serviço, o mecanismo proposto pelos autores não resolve o problema da negação de serviço, *Denial of Service* (DoS), ocasionado pela clonagem de etiquetas. No DoS, o objetivo principal é inviabilizar o acesso ao serviço, 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. O Mecanismo Proposto

O mecanismo proposto tem como objetivo retirar etiquetas RFID clonadas de circulação, evitando que tais etiquetas sejam utilizadas de forma indevida. Para tanto, o sistema em que o mecanismo é aplicado possui terminais RFID 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. Assim, 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 1. Tal cifração é necessária para que um atacante não tenha conhecimento do valor de $cont_e$.

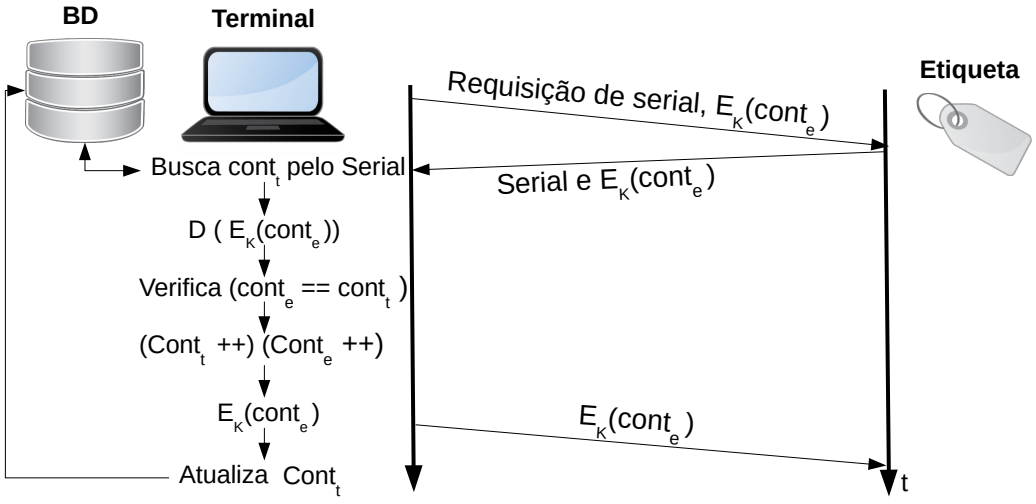
Um terminal, ao realizar a leitura dos dados da etiqueta, decifra o contador $cont_e$ com a chave K da seguinte forma $D_K(E_K(cont_e))$. Em seguida, através da busca pelo serial da etiqueta no BD, o terminal resgata o valor de $cont_t$, e confere se $cont_e = cont_t$. Se tais contadores forem iguais, 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 2.

Figura 1. Cadastro da Etiqueta.



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, 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 $cont_t \neq cont_e$.

Figura 2. Uso da etiqueta.

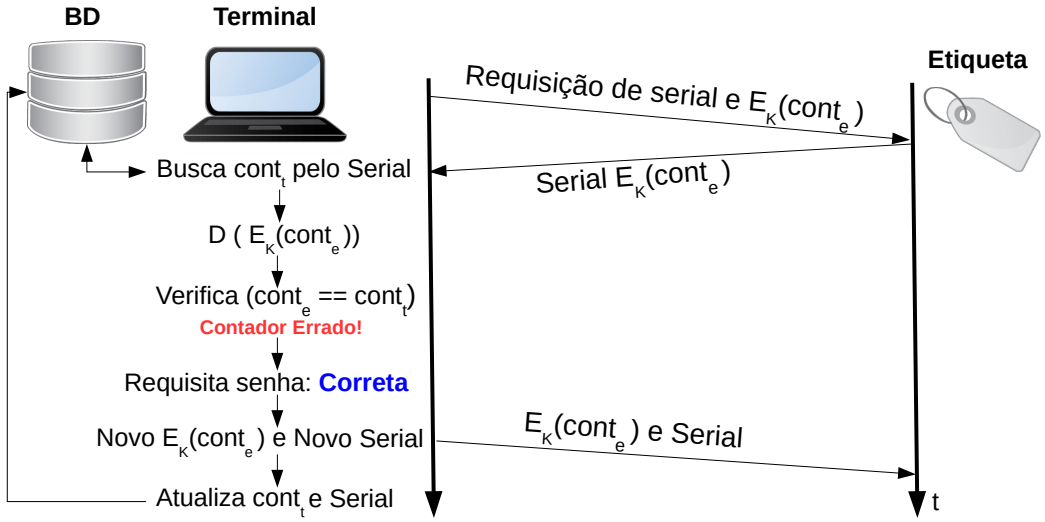


3.1. Versão 1 do Mecanismo Proposto: Com Uso de Senhas

Conforme o ambiente no qual o mecanismo for utilizado, duas versões do mecanismo são propostas. A Figura 3 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, *Denial of Service* (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, onde 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 3. Solução para sistemas com senha.



3.2. Versão 2 do Mecanismo Proposto: Sem Uso de Senhas

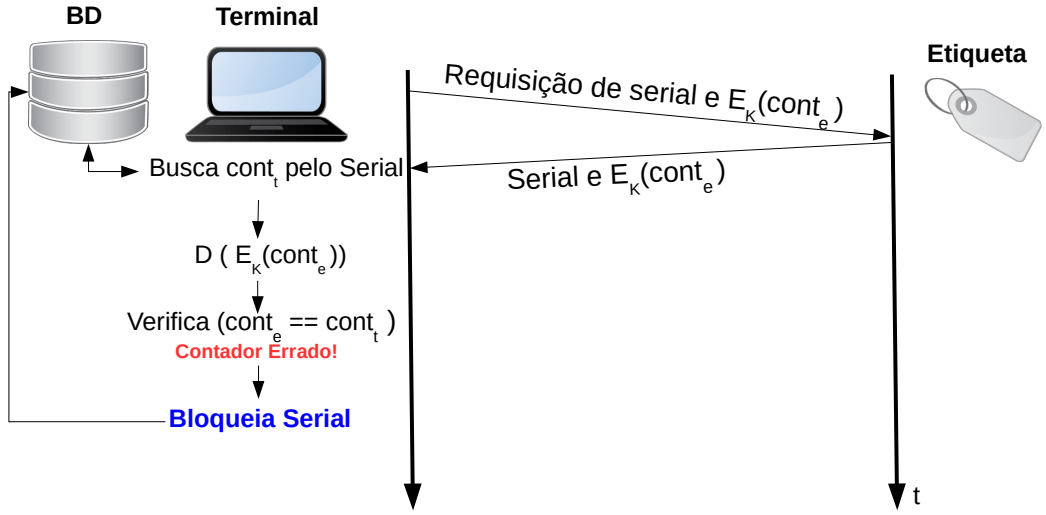
Já para ambientes que não possibilitam o uso de senhas, como no controle de mercadorias ou mesmo o controle de gado via etiqueta RFID, a segunda versão mostrada na Figura 4 é mais apropriada. Nesta versão, uma etiqueta ao ser identificada como clonada, ou seja, $cont_e \neq cont_t$, terá seu serial bloqueado 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.

4. Avaliação Experimental

Um protótipo foi implementado para avaliar do mecanismo proposto. Foi utilizado como terminal um *notebook* Sony Vaio NFC–habilitado, modelo svf15213cbw e Sistema Operacional Windows 8. Além disso, duas etiquetas MIFARE DESfireEV1, Tipo 4, com capacidade de armazenamento de 4.094 Bytes foram utilizadas.

O terminal é programado na linguagem em C *Sharp*, usando o banco de dados MySQL. Para fins experimentais, utilizou–se o *Data Encryption Standard* (DES) como

Figura 4. Solução para sistemas sem senha.



algoritmo de cifração, entretanto qualquer cifra simétrica poderia ser utilizada. Basicamente, o mecanismo proposto conta com a cifração e decifração 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. Em todos os casos, uma função de coleta de tempo foi iniciada no momento em que os dados da etiqueta eram recebidos e coletada ao final da autenticação. 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, o tempo médio de execução do mecanismo proposto em [Lehtonen et al. 2009] é de 864 ms, dos quais 101 ms é demandado somente para autenticação, ou seja, verificação do segredo compartilhado. Quando o tempo demandado para autenticação em [Lehtonen et al. 2009] é comparado ao o mecanismo proposto neste trabalho, 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. Vale reforçar que a tecnologia utilizado neste trabalho foi a comunicação por campo de proximidade (NFC), a qual possui uma maior velocidade de comunicação que outros padrões da RFID. Destaca–se ainda que a rapidez de execução do mecanismo é uma métrica importante

uma vez que, em muitos cenários de utilização da tecnologia de identificação por radiofrequência, um leitor pode interagir (ler e gravar dados) com várias etiquetas simultaneamente [Coskun et al. 2013] [Want 2006] [Want 2011].

Outro ponto importante a ser destacado em relação ao mecanismo com senha é a possibilidade da obtenção do histórico de utilização da etiqueta clonada. Este histórico é obtido no momento em que o usuário legítimo insere a senha correta no terminal, após ter sua etiqueta dada como clonada. Assim, o sistema poderá confrontar qual é o valor do contador contido na etiqueta legítima e comparar com a armazenada em seu BD, verificando quais foram as autenticações efetuadas pela etiqueta ilegítima. Em outras palavras, caso um atacante clone uma etiqueta legítima que possui um contador na posição 113 e a utilize até que o contador fique na posição 120. É possível, através da autenticação perante a senha e a comparação do contador da etiqueta legítima e contido no BD, constatar que as ultimas 7 utilizações foram feitas pelo atacante com o uso da etiqueta ilegítima. Isto é possível pelo fato do mecanismo utilizar um contador linear, ao invés do mecanismo apresentado por [Lehtonen et al. 2009], que utiliza um número randômico sem o armazenamento de histórico. Logo, tal mecanismo possibilita a aplicação de um método de controle de histórico, beneficiando diretamente ao usuário legítimo ao evitar prejuízos decorrentes ao ataque da clonagem. Onde em um cenário de pagamento, como os tradicionais cartões de crédito, a operadora de cartões poderia eximir o usuário legítimo do pagamento indevido causados por tal fraude.

5. Conclusão e Trabalhos Futuros

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 uma desafio.

Como trabalhos futuros, pretende–se (i) aprimorar o método de detecção apresentado aqui a fim de impedir interações da etiqueta clonada com o terminal e (ii) investigar formas de evitar a clonagem de etiquetas.

Agradecimentos

Trabalho executado com apoio financeiro da Universidade Federal do Pampa, recursos do Edital n. 08/2015 (PBIP) no âmbito do Projeto de Pesquisa “SEDES – Segurança e Desempenho em Computação Ubíqua e Pervasiva”.

Referências

Abawajy, J. (2009). Enhancing RFID tag resistance against cloning attack. In *Third International Conference on Network and System Security (NSS’09)*, pages 18–23.

Ahuja, S. and Potti, P. (2010). An introduction to RFID technology. *Communications and Network*, 2(3):183–186.

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 (IMIS)*, 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.

Dimitriou, T. (2005). A lightweight RFID protocol to protect against traceability and cloning attacks. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005)*, pages 59–66. IEEE.

Khoo, B. (2011). RFID as an enabler of the internet of things: issues of security and privacy. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pages 709–712. IEEE.

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)*, volume 5538 of *Lecture Notes in Computer Science*, pages 291–308, Nara, Japan. Springer.

Roberts, C. M. (2006). Radio frequency identification (RFID). *Computers & Security*, 25(1):18–26.

Roland, M., Langer, J., and Scharinger, J. (2011). Security vulnerabilities of the NDEF signature record type. In *3rd International Workshop on Near Field Communication*, pages 65–70.

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.

Tanenbaum, A. S. and Wetherall, D. (2011). *Redes de Computadores*. Pearson.

Tubino, E. R., Quincozes, S. E., and Kazienko, J. F. (2015). Comunicação por campo de proximidade: Tecnologia, aplicações e questões de segurança. *Tendências e Técnicas em Sistemas Computacionais*, vol. 1:41–59.

Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing*, 5(1):25–33.

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

Wu, N.-C., Nystrom, M., Lin, T.-R., and Yu, H.-C. (2006). Challenges to global RFID adoption. *Technovation*, 26(12):1317–1323.

Zuo, Y. (2012). Survivability experiment and attack characterization for RFID. *IEEE Transactions on Dependable and Secure Copmputing*, 9(2):289–302.