Uma Abordagem sobre Segurança em Sistemas RFID

Rogéria Oliani[1], Alexandre César R. da Silva[1], Tércio Alberto dos Santos Filho[2]

[1]Departamento de Engenharia Elétrica – Universidade Estadual Paulista (UNESP)
Ilha Solteira – SP – Brasil

[2]Departamento de Ciência da Computação - Universidade Federal de Goiás (UFG)
Catalão – GO - Brasil

rooliani@gmail.com, acrsilva@dee.feis.unesp.br, tercioas@gmail.com

Abstract. *Radio Frequency Identification (RFID) is a generic term for technologies that use radio waves to automatically identify people or objects, through the use of tags and readers. The diversity of applications that can be given to this technology are extensive. Thus, demand careful consideration in relation to security issues, which can range from loss of privacy, the large financial losses. This paper presents a study to RFID, with its main features and applications, as well as address issues of security, describing various types of attacks and countermeasures.*

Resumo. *Identificação por Rádio Frequência (RFID - Radio Frequency Identification) é um termo utilizado para tecnologias que utilizam a Rádio Frequência para identificação de objetos ou pessoas, através do uso de tags (etiquetas) e leitores. A diversidade de aplicações que podem ser dadas a essa tecnologia é extensa. Com isso, demanda uma análise cuidadosa em relação a questões de segurança, que podem abranger desde a perda da privacidade, a grandes prejuízos financeiros. Neste artigo apresenta-se um estudo ao RFID, com suas principais características e aplicações; bem como aborda questões de segurança, descrevendo diversos tipos de ataques e contramedidas.*

1. Introdução

Identificação por radiofrequência (RFID - *Radio Frequency Identification*) é um termo genérico para tecnologias que utilizam ondas de rádio para identificar automaticamente pessoas ou objetos. Um sistema RFID possui dois componentes básicos: Tag RFID, ou Etiqueta RFID, e Leitor RFID, ou Interrogador. A tag RFID, basicamente, possui um microchip ligado a uma antena, os quais são acondicionados em uma embalagem (encapsulamento) apropriada ao objeto ou pessoa a que se destina identificar (cartão de crédito, chave de veículo, prego para identificação de árvores ou paletes, etiquetas de vestuários, dentre outros). O Leitor RFID é um dispositivo utilizado para se comunicar com as tags através da emissão de ondas de rádio. Em relação a sua fonte de energia, as tags podem ser divididas em 3 tipos [RFID Journal Brasil 2013]:

1. Passiva: Não possui fonte de energia. A energia necessária ao seu funcionamento é recebida do leitor através dos sinais emitidos por este. Em virtude desta característica, são mais baratas e têm uma maior duração em comparação as tags ativas. Contudo, possuem capacidade computacional e memória limitada.

2. Semi-passiva ou semi-ativa: possuem bateria interna, porém utiliza a energia fornecida pelos leitores para transmitir o sinal a estes, como ocorre com as tags passivas. Neste caso, a bateria fornece energia ao seu microchip, permitindo que este tenha uma maior capacidade de processamento.
3. Ativas: possuem fonte de energia interna, o que possibilita o envio de sinais de transmissão de dados ao leitor, bem como alimentar circuitos mais complexos e sensores. Este tipo de tag possui um valor comercial mais alto, e um tempo de vida menor em comparação as tags passivas.

Outra forma de classificação das tags é dada pela frequência do sinal de transmissão de dados. Estas podem atuar em [Finkenzeller 2010]:

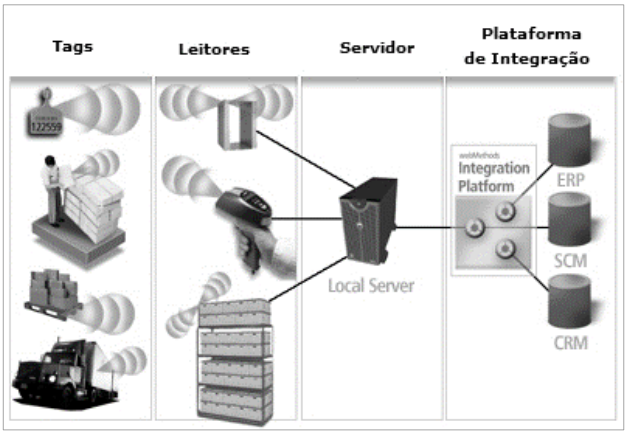
1. Baixa Frequência (LF – *Low Frequency*): atuam em uma frequência de 30 a 300 kHz, e possuem uma transferência de dados lenta, bem como um pequeno alcance de leitura (até 1 metro);
2. Alta Frequência (HF – *High Frequency*): a frequência encontra-se em uma faixa de 3 a 30 MHz. Elas geralmente podem ser lidas até 1 metro de distância, e possuem transmissão de dados mais rápida que as tags de baixa frequência, contudo, consomem mais energia do que estas.
3. Ultra Alta Frequência (UHF – *Ultra High Frequency*): atuam em uma faixa de frequência de 300 MHz a 3 GHz, e tipicamente operam entre 866 e 960 MHz. Tags UHF possuem taxas de transferência mais altas e maior alcance do que as tags de alta e baixa frequência. No entanto, as ondas de rádio, nesta frequência, não passam por itens com alto teor de água. Em comparação às tags de baixa frequência, as tags UHF são mais caras e utilizam mais energia.
4. Microwave: atuam em frequência acima de 3 GHz. Tags Microwave têm taxas de transferência muito altas e podem ser lidas a longas distâncias, contudo, elas usam uma grande quantidade de energia e são mais caras em comparação as demais.

Para armazenar e fazer o controle das informações que são lidas das tags pelos leitores, temos os servidores. Os servidores são computadores que armazenam o banco de dados das tags, e efetuam a comunicação com os leitores RFID através de uma rede (padrão IEEE 802.11, IEEE 802.15.4, dentre outros) ou, simplesmente, através de uma porta USB. As tags podem conter diversas informações, ou apenas um número de identificação (ID). Através do ID o servidor pode identificar a tag e obter as informações relacionadas a esta. Estas informações podem ser utilizadas pelas organizações para efetuar o controle de folha de pagamento, produção, inventário, controle de processos em linha de produção, análise de perfil, tendências, dentre inúmeras outras.

Na Figura 1, apresenta-se o esquema de um sistema RFID. Neste, a leitura dos dados de diversos tipos de tags – que identificam animais, caixas, paletes e caminhões – são realizadas por diferentes leitores; sendo o modelo de cada leitor adequado ao tipo de tag que deseja efetuar a leitura. Os dados são enviados a um servidor local, no qual encontram-se armazenadas as informações referentes a cada item identificado com a tag. As informações localizadas no servidor local são utilizadas em uma plataforma integrada com o Sistema Integrado de Gestão Empresarial (ERP - *Enterprise Resource Planning*), Gestão de Relacionamento com o Cliente (CRM - *Customer Relationship Management*) e Gestão da Cadeia Logística (SCM - *Supply Chain Management*). Desta forma, as

informações das tags lidas, podem ser obtidas em tempo real por toda a cadeia, podendo chegar até o cliente.

Figura 1 – Esquema de um sistema RFID.



Fonte: [RFIDBr 2008], adaptada pelo autor.

Há uma grande diversidade de sistemas que são implementados utilizando RFID, os quais se estendem pela cadeia de suprimentos, pedágios, transporte público, dentro outros. Os prejuízos financeiros e à privacidade, que a falta de segurança neste sistemas podem trazer, motiva o estudo e implementação de diversas técnicas e equipamentos que auxiliem na proteção destes.

Neste artigo apresenta-se alguns padrões RFID utilizados, exemplos de aplicações, bem como aborda questões relacionadas à segurança, descrevendo diversos tipos de ataques e contramedidas. Este artigo está organizado da seguinte forma: Na Sessão 2, serão apresentados alguns padrões utilizados na tecnologia RFID. Na Sessão 3, serão apresentadas diferentes tipos de aplicação da tecnologia RFID. Na Sessão 4, é aborda a questão da segurança e da privacidade em sistemas RFID, e apresenta diversos tipos de ataques, bem como contramedidas que podem ser utilizadas. Na Sessão 5, serão apresentadas as conclusões.

2. Padrões

Para que seja realizada a comunicação entre tags, leitores e servidor RFID é necessário a utilização de protocolos, os quais definem as regras de como esta será realizada. Estas regras definem, dentro outras questões, quais sinais são reconhecidos, como a comunicação é realizada, qual o significado dos dados recebidos das tags, quais dispositivos podem transmitir a cada tempo (resolvendo problemas de colisão). Assim, é importante a padronização destas regras, para que sistemas e equipamentos diversos sejam compatíveis, diminuindo o custo destes e facilitando sua implantação e disseminação. Neste âmbito, duas organizações se destacam: ISO (*International Standards Organization*) e a EPC Global. A ISO é uma união mundial de instituições nacionais de normalização, tais como DIN (Alemanha) e ANSI (EUA) e contribui com inúmeros comitês e grupos de trabalho para o desenvolvimento de padrões de RFID [Finkenzeller 2010]. Dentre os padrões ISO podemos citar os de baixa frequência, utilizado no rastreamento de animais (ISO 11784, ISO 11785, ISO 14223), os de alta frequência utilizados em cartões inteligentes (ISO 10536, ISO 14443, ISO 15693) e os da série ISO 18000, utilizados no gerenciamento de itens, os quais atuam em diferentes

frequências. A EPC Global é uma organização sem fins lucrativos que visa a padronização do RFID através do Código Eletrônico de Produto (EPC - *Electronic Product Code*) e da EPC *Network*. O EPC é um meio para identificar de forma única paletes, caixas ou itens. Uma tag EPC não carrega informações pessoais. Todas as informações sobre o objeto com a tag EPC é administrada exclusivamente no EPCglobal Network. O EPCglobal *Network* é uma tecnologia, a qual permite a parceiros comerciais documentar e determinar a localização de bens individuais na cadeia de abastecimento, se possível em tempo real [Finkenzeller 2010]. Dentre os padrões EPC podemos citar o *Class* 0, *Class* 1 e o *Class* 1 *Gen* 2; sendo este último reconhecido pela ISO como padrão internacional (ISO 18000-6C).

3. Aplicações

Existe um grande número de sistemas que são implementados utilizando RFID. A diversidade de aplicações se estende pela cadeia de suprimento, agricultura, identificação de animais, controle de acesso, transporte público, pedágios, dentre outros.

A identificação por rádio frequência nas cadeias de suprimentos permite rastrear todo o processo produtivo, materiais utilizados na fabricação, inspeção, faturamento, distribuição, até chegar ao revendedor ou mesmo consumidor final. Na fábrica de automóveis da Volkswagen, na Eslováquia, seus veículos montados nas estações de serviços finais e processos de inspeção na unidade de Bratislava, são rastreados utilizando um sistema de localização em tempo real. A solução que emprega tecnologia RFID com o uso de tags ativas, permite que a empresa localize os veículos estacionados e identifique quando um carro entra ou sai de cada um dos vários processos, o que torna possível melhorar a eficiência dos estágios de produção final [Swedberg 2012].

No Brasil, o Departamento Nacional de Trânsito (Denatran) está em processo de implantação do SINIAV (Sistema Nacional de Identificação Automática de Veículos), o qual tem por objetivo aperfeiçoar a gestão do tráfego e a fiscalização de veículos, através do rastreamento destes utilizando tecnologia RFID [Perin 2013]. O projeto do Denatran determina a adoção obrigatória da tecnologia de identificação por radiofrequência em toda a frota brasileira de veículos, estimada atualmente em 85 milhões de unidades. Os primeiros testes começaram em outubro de 2012, utilizando placas convencionais associadas as tags RFID. Em seguida foram testados os sistemas de monitoramento de veículos emplacados com tags semi-ativas, chamadas PIVEs (Placas de Identificação veicular). Em virtude da evolução do padrão EPC Gen2 v2, considera-se no futuro o uso de tags passivas, que reduziriam os custos das PIVEs, porque não exigem emprego de baterias e são mais simples [Perin 2014].

A diversidade de aplicações do RFID, e a importância destas para as organizações que as implantam, tornam necessário que se dê atenção a segurança destes sistemas.

4. Segurança e privacidade

A segurança dos sistemas que utilizam RFID engloba questões relacionadas a proteção dos dados contidos nas tags e disponibilidade dos serviços ao qual se destina a identificação fornecida por estas. Além do número de identificação, as tags podem armazenar outros dados relacionados a “quem” ou a “o que” ela se destina identificar. Estes dados podem comprometer a segurança dos processos envolvidos, bem como comprometer a privacidade das pessoas que a utilizam.

A questão da privacidade em sistemas RFID incluem o vazamento de informações contidas nas tags, bem como o rastreamentos destas. As tags podem responder aos interrogadores sem o conhecimento de quem as esta portando ou de seus proprietários. Quando o número de identificação da tag é relacionada a dados pessoais, o problema se torna maior; pois permite, por exemplo, que um comerciante trace o perfil do consumidor utilizando rede de leitores tanto dentro, quanto fora do estabelecimento comercial. No Brasil, a privacidade tem sido discutida com relação a implantação do Sistema Nacional de Identificação Automática de Veículos (SINIAV). A Ordem dos Advogados do Brasil questiona o fato do sistema permitir conhecer a exata localização do veículo de uma pessoa, ferindo, assim, o direito constitucional à garantia de privacidade dos cidadãos [Leitão 2012].

Como visto, a privacidade para ser ferida não precisa necessariamente que o sistema de RFID sofra um ataque, pois a própria entidade que disponibilizou a tag para o usuário pode utilizar-se do conhecimento das informações contidas nesta, para interesses próprio.

4.1. Ataques

Os sistemas RFID são suscetíveis a ataques como todos os sistemas que envolvem transmissão e armazenamento de dados. Os objetivos de cada ataque podem ser muito diferentes; sendo, assim, é importante identificar os potenciais alvos para compreender os possíveis ataques. A seguir são apresentados alguns tipos de ataque que sistemas RFID podem sofrer:

1. *Eavesdropping* (espionagem): é um ataque passivo no qual um atacante escuta a comunicação entre a tag e o leitor [Boli, Simplot-Ryl e Stojmenovic 2010]. Um exemplo deste tipo de ataque é a obtenção de dados de um cartão de crédito, como: nome do proprietário, número do cartão, data de expiração, tipo de cartão; através da captura das transmissões realizadas entre um leitor de cartão de crédito e um cartão de crédito RFID. Os dados obtidos neste tipo de ataque podem ser utilizados em ataques mais complexos, como: *Replay* e *Tracking*.
2. *Man in the middle*: O atacante se posiciona em um local intermediário entre o leitor e a tag que se encontra fora do alcance de leitura do mesmo. Assim, interrompe o caminho de comunicação, e manipula as informações que serão transmitidas tanto para o leitor, como para a tag, engando os dois componentes [Bienert e Schalk 2013].
3. *Tracking*: O rastreamento utiliza dados contidos nas tags para identificar a presença destas em um determinado ambiente físico, sem a autorização de quem a porta ou de seu proprietário [Boli, Simplot-Ryl e Stojmenovic 2010]. Desta forma é possível identificar a trajetória do objeto ou da pessoa a ela associada. Mesmo que em uma tag esteja armazenado apenas seu número de identificação, seria possível em uma compra, por exemplo, a loja estabelecer em seu banco de dados um vínculo entre o número de identificação da tag e o cliente que adquiriu o produto no qual a tag se encontra. Desta forma, seria possível identificar a presença do cliente na loja, quando ele voltasse portando o objeto anteriormente adquirido.
4. *Replay*: neste tipo de ataque os dados transmitidos entre a tag e o leitor são capturados e, posteriormente, reutilizados de forma a forjar uma nova comunicação [Bienert e Schalk 2013].

5. *Cloning*: Os dados de uma tag válida são capturados pelo leitor do atacante e, posteriormente, escritos em uma outra tag (clone) [Finkenzeller 2010]. Desta forma a tag clonada se comportará como a original perante o leitor.
6. *Spoofing*: o invasor simula uma identidade diferente da que ele tem, no caso, ele simula uma tag válida, e assim, pode fazer uso de todos os privilégios que aquela tag proporciona. A diferença entre este tipo de ataque e o *Cloning* é que neste último há uma reprodução física de uma tag original, enquanto no ataque *Spoofing* é utilizado um equipamento eletrônico para emular ou imitar a tag original [Tehranipoor e Wang 2012].
7. *Denial of Service* (DoS): Os ataques de negação de serviço têm o objetivo de impedir que usuários legítimos consigam utilizar o sistema. Ataques DoS podem ser realizados, por exemplo, utilizando dispositivos que emitam sinais de ruído na faixa de frequência utilizada pela rede RFID, reduzindo a taxa de transferência e, consequentemente, emperrando o sistema [Xiao, Gibbons e Lebrun 2009]. Um outro exemplo seria a utilização não autorizada do comando *KILL*, desta forma as tags deixariam de responder aos leitores [Tehranipoor e Wang 2012].

Alguns ataques, em um primeiro momento, podem parecer não trazer prejuízos, como é o caso do *Eavesdropping*, contudo, servem como base para outros mais complexos (*Replay*, *Tracking*). As consequências geradas pelos diversos tipos de ataques podem atingir diferentes níveis de prejuízo financeiro, ou até mesmo relativos a privacidade de indivíduos, como podem ocorrer com o *Tracking*. Ataques como *Cloning* e *Spoofing* podem permitir acesso a áreas não autorizadas de empresas e residências, no caso destas utilizarem fechaduras com tecnologia RFID, bem como qualquer outro tipo de privilégio que se poderia ter com uma tag original.

A seguir, apresenta-se algumas contramedidas que podem ser utilizadas de forma a inibir diferentes tipos de ataques.

4.2. Contramedidas

Ataques ao sistema RFID podem causar grandes prejuízos financeiros as empresas que o utilizam, bem como a usuários finais, neste último caso, podendo atingir também a privacidade destes. Assim, faz-se necessário que contramedidas sejam tomadas para evitar ataques RFID. Dentre as várias contramedidas, podemos citar:

1. RSA *Blocker Tags*: é um produto desenvolvido pelos cientistas do laboratório RSA em conjunto com o Professor Ronald Rivest para a proteção da privacidade de consumidores. O RSA *Blocker Tag* cria uma região física a sua volta, a qual impede que os leitores de RFID singularizem as tags que se encontram nesta região [Juels, Rivest e Szydlo 2003].
2. *Kill Command*: é uma forma de proteger a privacidade dos consumidores enviando um comando para matar a tag, não sendo mais possível que esta seja lida por qualquer leitor RFID [Xiao, Gibbons e Lebrun 2009], [López 2008]. Desta forma, pode ser dada ao consumidor, por exemplo, a oportunidade de matar a tag antes de sair de uma loja, evitando o seu rastreamento.
3. Gaiola de Faraday: baseado na Gaiola de Faraday, é uma forma de bloquear as frequências de rádio utilizando um isolamento, o qual impede que os sinais do interior do objeto que possui esse isolamento alcance o seu exterior e vice-versa. Este isolamento pode ser simplesmente feito com folhas de metal, ou até mesmo, ser adquirido no mercado objetos como carteiras, bolsas, porta cartão, dentre

outros, confeccionados com material próprio para esta função. Contudo, este mesmo tipo de isolamento, poderia ser utilizado, por exemplo, para efetuar furtos de produtos em lojas, inibindo a leitura das tags dos produtos.

4. Criptografia: pesquisadores têm propostos várias versões de criptografias para serem utilizadas em sistemas RFID [López 2008], [Sun e Zhong 2012], [Noman, Rahman e Adams 2011], [Sharaf 2012], [Dong, Zhan e Wei 2013]. Criptografias podem ajudar a proteger o sistema contra diversos tipos de ataque, como: *Man in the middle* [Xiao, Gibbons e Lebrun 2009], *Cloning* [López 2008], *DoS* [Dong, Zhan e Wei 2013], dentre outros. O grande desafio têm sido a criação de criptografias leves o bastante para serem utilizadas em tags de baixo custo, eis que estas possuem capacidade computacional limitada (armazenamento, circuitos e consumo de energia) [López 2008].
5. *RFID Guardian*: é um dispositivo portátil alimentado por bateria que atua como um mediador das intereações entre os leitores e tags RFID. O Guardião RFID contém recursos de um leitor de RFID e de emulação de tag, os quais lhe permitem auditar e controlar as atividades de RFID [Cengage Learning 2010].

As contramedidas voltadas ao sistema RFID são aplicadas de acordo com o objeto ou pessoa que se deseja identificar. O nível de segurança e quanto se deseja investir financeiramente nesta, vai depender do valor do objeto a que se destina, e das informações que são armazenadas na tag ou aquelas a que esta permite o acesso no sistema. Assim, há contramedidas que podem ser utilizadas tanto por organizações, quanto por usuários finais, como é o caso das carteiras baseada na Gaiola de Faraday.

Dentre as contramedidas destacam-se as criptografias, em virtude destas ajudarem a proteger o sistema de diversos tipos de ataques. Justificando, assim, o grande empenho tido por diversos pesquisadores no estudo destas.

5. Conclusão

A diversidade de aplicações que são implementadas utilizando sistemas RFID vêm aumentando em todo o mundo. Ampliando, assim, o interesse de pesquisadores na busca de soluções para problemas de segurança, com o estudos de novas criptografias, principalmente, voltadas a aplicação em tags de baixo custo, as quais são as mais utilizadas. Há no mercado a oferta de diversos tipos de tags, com diferentes preços, criptografias, frequências, e outras características; devendo serem estas escolhidas de acordo com a sua aplicação, levando em consideração o custo x benefício. Tags ativas possibilitam a implementação de uma maior segurança, em virtude de sua capacidade computacional ser melhor em relação as passivas. Contudo, seu custo é mais alto, podendo representar uma parcela significante do custo de produção de produtos de baixo valor comercial.

Bibliografia

Bienert, R.; Schalk, G. H. RFID - MIFARE and Contactless Smartcards in Application. United Kingdom: BV, Elektor International Media, 2013.

Boli, M.; Simplot-Ryl, D.; Stojmenovic, I. RFID SYSTEMS - RESEARCH TRENDS AND CHALLENGES. United Kingdom: John Wiley & Sons, 2010.

Cengage Learning. RFID Hacking. In: _____ Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems. New York: [s.n.], 2010.

Dong, Q.; Zhan, ; Wei, L. A SHA-3 Based RFID Mutual Authentication Protocol and Its Implementation. 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC), 5-8 ago. 2013. 1 - 5.

Finkenzeller, K. RFID Handbook. United Kingdom: Wiley, v. 3, 2010.

Juels, A.; Rivest, L.; Szydlo, M. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. 10th ACM conference on Computer and communications security. New York: [s.n.]. 2003.

Leitão, T. Sistema de identificação de veículos divide opiniões de especialistas, 03 outubro 2012. Disponivel em: <http://agenciabrasil.ebc.com.br/noticia/2012-10-03/sistema-de-identificacao-de-veiculos-divide-opinioes-de-especialistas>.

López, P. P. Lightweight cryptography in radio frequency identification (RFID) systems. Ph.D. THESIS, Universidad Carlos III de Madrid, Leganés,Espanha, 04 nov. 2008. Disponivel em: <http://e-archivo.uc3m.es/handle/10016/5093>.

Noman, A. N. M.; Rahman, S. M. ; Adams,. Improving Security and Usability of Low Cost RFID Tags. Ninth Annual International Conference on Privacy, 2011.

Perin, E. Ceitec inicia produção em volume do chip para o Siniav. RFID Journal Brasil, 18 novembro 2013. Disponivel em: <http://brasil.rfidjournal.com/noticias/vision ?11193/1>. Acesso em: 25 nov. 2013.

Perin, E. Siniav pode ser implantado em breve. RFID Journal Brasil, 06 fevereiro 2014. Disponivel em: <http://brasil.rfidjournal.com/noticias/vision?11415/1>. Acesso em: 27 fev. 2014.

RFID Journal Brasil. RFID Journal Brasil, 2013. Disponivel em: <http://brasil.rfidjournal.com>. Acesso em: 19 nov. 2013.

RFIDBr. Funcionamento RFID. RFIDBr, 28 novembro 2008. Disponivel em: <http: //www.rfidbr.com.br/index.php/funcionamento-rfid.html>. Acesso em: 01 mar. 2014.

Sharaf, M. RFID Mutual Authentication and Secret Update Protocol for Low-cost Tags. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 25-27 jun. 2012. 71 - 77.

Sun, D.-Z.; Zhong, J.-D. A Hash-Based RFID Security Protocolfor Strong Privacy Protection. IEEE Transactions on Consumer Electronics, v. 58, n. 4, p. 1246-1252, 2012.

Swedberg, C. Volkswagen ganha eficiência no processo de acabamento de carros. RFID Journal Brasil, 18 junho 2012. Disponivel em: <http://brasil.rfidjournal.com/estudos-de-caso/vision?9626>. Acesso em: 25 fev. 2014.

Tehranipoor, M.; Wang, C. Security for RFID Tags. In: _____ Introduction to Hardware Security and Trust. New York: Springer, 2012. p. 283-302.

Xiao, Q.; Gibbons, T.; Lebrun, H. RFID Technology, Security Vulnerabilities, and Countermeasures. Supply Chain the Way to Flat Organisation, Publisher-Intech, p. 357-382, jan. 2009.