

Um Mecanismo Simples e Eficiente para a Autenticação de Dispositivos na Comunicação por Campo de Proximidade

Silvio E. Quincozes¹ e Juliano F. Kazienko¹

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

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

Abstract. *Near Field Communication is a recent technology that uses radio waves at high frequency for data communication. One of the major research challenges in this area is the end point identification. In this sense, a hidden device within the legitimate devices coverage area makes possible to capture data as well as the device impersonation. This work presents a mechanism for devices authentication, aggregating relevant security properties for data exchange. The proposal is evaluated through a prototype. Low number of messages exchanged, low mechanism execution time and improvements related to other works reveal that the proposed mechanism is promising.*

Resumo. *A comunicação por campo de proximidade é uma tecnologia recente que utiliza ondas de rádio de alta frequência para a comunicação de dados. Um dos principais desafios de pesquisa nessa área consiste na identificação do ponto final. A presença de um dispositivo camuflado dentro da área de cobertura de dispositivos legítimos torna possível a captura das informações, bem como a personificação dos mesmos. Este trabalho apresenta um mecanismo que autentica os dispositivos, agregando propriedades de segurança importantes para a troca de dados. A proposta é validada através de um protótipo. O baixo número de mensagens trocadas, baixo tempo de execução do mecanismo e diferenciais em relação a outros trabalhos revelam que o mecanismo é promissor.*

1. Introdução

A tecnologia de Comunicação por Campo de Proximidade, do inglês, *Near Field Communication* (NFC), possibilita a troca de mensagens entre dispositivos, como celulares, *notebooks*, crachás, etc. Tal tecnologia de comunicação sem fio utiliza ondas de rádio de alta frequência, tradicionalmente 13,56 MHz, com um alcance máximo de dez centímetros. O NFC tem aplicações em diversos campos, como saúde, transporte e pagamentos eletrônicos. O NFC tem maior usabilidade e menor tempo de configuração, comparado a tecnologia *Bluetooth*, por exemplo [Eun et al. 2013][Coskun et al. 2013].

Um dos grandes desafios de pesquisa na área consiste no estabelecimento de segurança nas comunicações. A curta distância exigida para a troca de dados pode ser considerada uma vantagem. Desse modo, um atacante precisa estar muito próximo dos dispositivos legítimos para interceptar as mensagens trocadas, o que facilita sua detecção. No entanto, a presença de um dispositivo malicioso camuflado dentro da área de cobertura dos dispositivos legítimos pode viabilizar ataques, bem como a personificação dos dispositivos. Desta forma, o emprego de mecanismos destinados à garantia da autenticidade dos dispositivos se faz essencial.

Segundo [Miorandi et al. 2012], a comunicação segura através de radiofrequência requer soluções eficientes e de baixo custo computacional. Em muitos cenários que envolvem o uso de NFC, o consumo energético deve ser considerado, especialmente ao se utilizar dispositivos móveis. Atualmente, pontos que requerem atenção são: privacidade, autenticação de entidades, prevenção da espionagem e baixo custo energético [Alzahrani et al. 2013]. O presente trabalho tem por objetivo propor um mecanismo leve e eficiente que autentica mutuamente dispositivos NFC, agregando propriedades de segurança importantes para a troca de dados. De forma a aplicar o mecanismo proposto, foi implementado um protótipo. Nas demais seções tal mecanismo é introduzido.

2. Trabalhos Relacionados

Em [Chen et al. 2010], é proposto um mecanismo para estabelecer a autenticação de dispositivos NFC e permitir transações financeiras. Foram aproveitadas as primitivas criptográficas da tecnologia GSM, utilizando o cartão *Subscriber Identity Module* (SIM) de celulares para identificá-los. Nesse trabalho, as chaves são geradas dinamicamente a cada autenticação. Como a operadora de telefonia participa na geração da chave compartilhada, o uso do mecanismo fica limitado a dispositivos da mesma operadora.

O trabalho de [Eun et al. 2013] propõe um método de privacidade condicional para proteger a privacidade do usuário usando pseudônimos. Essa proposta exige um terceiro confiável para a solicitação de um conjunto de pseudônimos. Com essa renovação o problema de rastreabilidade é controlado. Porém, essa abordagem requer aparelhos equipados com *Secure Element* (SE), o que inviabiliza o uso seguro dos demais dispositivos, como etiquetas NFC, por exemplo. Além disso, existe um custo computacional adicional para a solicitação de novos pseudônimos. Segundo os autores, um conjunto de 1000 pseudônimos exigiria um espaço de 146,484 Kbytes em memória.

3. O Mecanismo Proposto

Suponha que dois dispositivos A e B necessitam se comunicar de forma segura através do modo de operação *Peer-To-Peer* [Coskun et al. 2013]. O dispositivo A possui identidade pública ID_A , como um terminal para compra de passagens, por exemplo. O dispositivo B é um aparelho pessoal, como um telefone celular, por exemplo, conforme ilustrado na Figura 1(a). Logo B deve ter sua identidade ID_B preservada. Nesse caso, A possui uma lista de chaves $L_A \leftarrow \{K_{[i]}, K_{[i+1]} \dots\}$. Cada chave representa um dispositivo conhecido. O dispositivo B possui outra lista de chaves $L_B \leftarrow \{K_{[ID_A]}, K_{[ID_C]} \dots\}$, onde cada registro possui referência ao ID de um dispositivo conhecido. Dessa forma, quando A envia ID_A , B deve procurar por $K_{[ID_A]}$ como chave para a autenticação. Na primeira comunicação $K_{[ID_A]}$ não existirá. Nesse caso, B atribui para o *bit* β de associação: $\beta \leftarrow 0$. Assim, ao receber a mensagem, A sabe que é preciso que seja definida e compartilhada uma nova chave. Para tal, a sugestão aqui proposta é o uso de um Número de Identificação Pessoal (PIN). O PIN deve ser gerado aleatoriamente e exibido na tela do dispositivo B , conforme $P1$ na Figura 1(b). Em seguida, tal PIN é mostrado ao operador do dispositivo A , que atualiza o sistema para o cálculo de K , conforme $P2$ na Figura 1(b).

Inicialmente, ao detectar a presença de um dispositivo próximo, A envia uma mensagem $M_1 \leftarrow \{ID_A, n_1\}$ em texto plano, onde n_1 é um *nonce*. O dispositivo B faz uma busca por $K_{[ID_A]}$ ($P1$, Figura 1(b)). Se $K_{[ID_A]} \neq \emptyset$, então $\beta \leftarrow 1$. Senão,

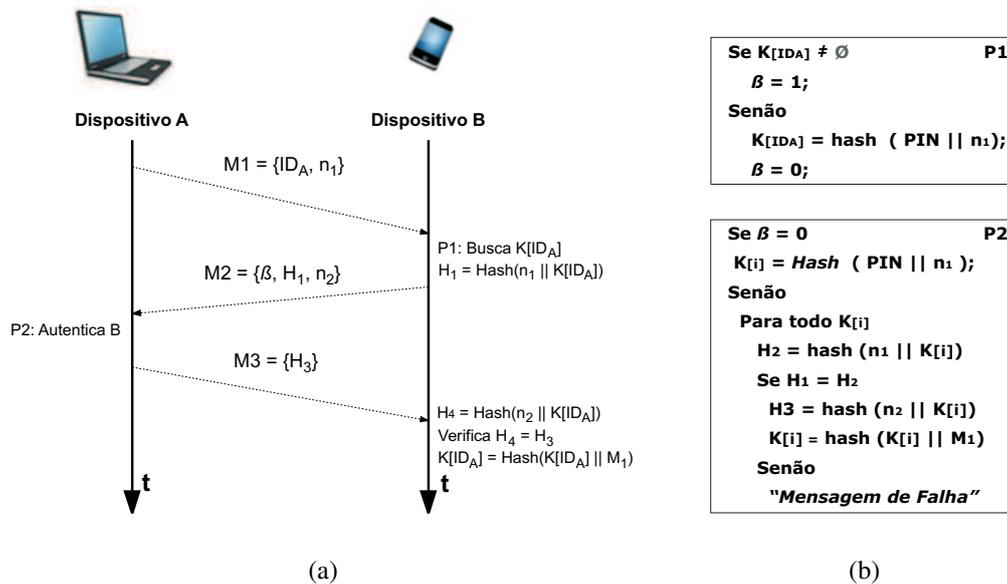


Figura 1. A Figura (a) ilustra as mensagens trocadas. A Figura (b) detalha os algoritmos utilizados no mecanismo proposto.

$\beta \leftarrow 0$ e um PIN é gerado para definição de $K_{[ID_A]} \leftarrow Hash(PIN || n_1)$. É calculado $H_1 \leftarrow Hash(n_1 || K_{[ID_A]})$ e gerado outro *nonce* n_2 . Em seguida B emite $M_2 \leftarrow \{\beta, H_1, n_2\}$. Quando $\beta = 0$ (P2, Figura 1(b)), insere-se $K_{[i]} \leftarrow Hash(PIN || n_1)$ na lista. Para tal, é necessário que o usuário digite em A , o PIN gerado e exibido por B . Quando $\beta = 1$, o dispositivo A computa $H_2 \leftarrow Hash(n_1 || K_{[i]})$ e verifica se $H_1 = H_2$. Isso se repete para todo índice i dos registros da lista L_A até que seja satisfeita a igualdade, onde B é considerado autêntico. Se a igualdade não for satisfeita, ocorre então uma falha na autenticação de B e o processo é interrompido. Por fim, A calcula $H_3 \leftarrow Hash(n_2 || K_{[i]})$, atualiza $K_{[i]} \leftarrow Hash(K_{[i]} || M_1)$ e envia $M_3 \leftarrow \{H_3\}$. O dispositivo B computa $H_4 \leftarrow Hash(n_2 || K_{[ID_A]})$ e verifica se $H_3 = H_4$. Se a igualdade for satisfeita, A é autenticado e ocorre a atualização de $K_{[ID_A]} \leftarrow Hash(K_{[ID_A]} || M_1)$.

4. Resultados Preliminares e Trabalhos Futuros

A fim de validar o mecanismo da Figura 1(a), um protótipo foi implementado. Para tal, utilizou-se um telefone celular da marca Sony modelo Xperia M, com o sistema operacional Android 4.2 instalado, e um notebook da marca Sony Vaio, modelo *svf15213cbw*, com sistema operacional Windows 8. O estabelecimento da comunicação entre tais dispositivos está calcada no modo de operação entre dispositivos NFC denominado *Peer-to-Peer* [Coskun et al. 2013]. A programação do protótipo se deu nas linguagens Java e C Sharp, respectivamente. Para computar os resumos foi utilizado o *Message-Digest algorithm 5* (MD5), entretanto qualquer algoritmo *hash* poderia ser utilizado. O tamanho total do executável instalado é de 1,25 Mbytes no celular e 25 Kbytes no notebook. O tempo médio total para a execução do mecanismo proposto é de 253 ms.

Visto que a descoberta de K implica no comprometimento da autenticidade de quaisquer dos dispositivos, o mecanismo proposto efetua a renovação dinâmica de chaves a cada autenticação. Dessa forma, mesmo que um atacante descubra K anterior, ela não

servirá para a próxima autenticação. Tal processo é independente de terceiro confiável. Além disso, o usuário do celular consegue provar sua autenticidade sem expor sua identidade, mantendo assim a privacidade e evitando o rastreamento. Devido ao baixo número de mensagens trocadas, o mecanismo se torna eficiente do ponto de vista do consumo energético. A Tabela 1 compara trabalhos existentes com o mecanismo proposto aqui.

Tabela 1. Propriedades dos Mecanismos.

	[Eun et al. 2013]	[Chen et al. 2010]	Mecanismo Proposto
<i>Privacidade do Usuário</i>	Em Risco	Parcial	Satisfatória
<i>Terceiro Confiável</i>	Dependente	Dependente	Independente
<i>Simplicidade</i>	Complexo	Médio	Simples
<i>Espaço de Armazenamento</i>	Demasiado	Pouco	Pouco
<i>Autenticação Mútua</i>	Possui	Possui	Possui
<i>Dependência de SE</i>	Dependente	Dependente	Independente
<i>Renovação de Chaves</i>	Razoável	Razoável	Aceitável

Observa-se que a renovação de chaves é um ponto que requer melhorias. O uso de um terceiro confiável é uma alternativa, entretanto deve ser considerada a possibilidade da indisponibilidade do mesmo. O mecanismo proposto independe de terceiro confiável. Porém, se um atacante descobrir K e escutar as mensagens trocadas no processo de autenticação, ele é capaz de computar o novo K . Uma solução para tal problema consiste no uso de um PIN gerado em um dos dispositivos e digitado pelo usuário no outro dispositivo. É importante destacar que a geração do PIN deve acontecer sempre que houver autenticação, o que pode ser inconveniente do ponto de vista do usuário.

Como trabalhos futuros, pretende-se aplicar o mecanismo em um ambiente hospitalar. Desse modo, um médico poderia de forma rápida e segura recuperar dados de pacientes como seus prontuários médicos através de dispositivos móveis. Adicionalmente, deseja-se utilizar etiquetas NFC junto aos leitos dos pacientes, adequando o mecanismo proposto a tais dispositivos. Nesse cenário, a autenticação, privacidade, integridade e confidencialidade são propriedades que devem ser garantidas [Alzahrani et al. 2013].

Referências

- Alzahrani, A., Alqhtani, A., Elmiligi, H., Gebali, F., and Yasein, M. S. (2013). NFC security analysis and vulnerabilities in healthcare applications. In *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, pages 302–305. IEEE.
- Chen, W., Hancke, G., Mayes, K., Lien, Y., and Chiu, J.-H. (2010). NFC mobile transactions and authentication based on GSM network. In *Second IEEE International Workshop on Near Field Communication (NFC)*, pages 83–89. IEEE.
- Coskun, V., Ozdenizci, B., and Ok, K. (2013). A Survey on Near Field Communication NFC Technology. *Wireless Personal Communications*, 71:2259–2294.
- Eun, H., Lee, H., and Oh, H. (2013). Conditional privacy preserving security protocol for NFC applications. *IEEE Transactions on Consumer Electronics*, 59(1):153–160.
- Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497–1516.