Autenticação Mútua entre Dispositivos no *Middleware* uOS

Beatriz Ribeiro, João Gondim, Ricardo Jacobi, Carla Castanho

Universidade de Brasília
Brasília, DF

bia.marilia@gmail.com, {gondim,rjacobi,carlacastanho}@cic.unb.br

1 Introdução

Ambientes ubíquos, ou *smartspaces*, caracterizam-se pela pulverização de dispositivos computacionais heterogêneos que colaboram para prover serviços de forma transparente ao usuário. Dispositivos móveis integram-se dinamicamente ao ambiente, provendo e demandando novos serviços e recursos. A gerência de um *smartspace* é, usualmente, realizada por um *middleware*, cujas responsabilidades incluem, além da gestão dos recursos computacionais do ambiente, prover mecanismos de segurança. Os dispositivos que integram *smartspaces* frequentemente apresentam restrições em termos de recursos computacionais. Desse modo, a implementação de mecanismos de autenticação e comunicação, e dos processos de administração do *middleware* não deve ser muito onerosa. Uma possível solução seria a adoção de protocolos de autenticação leves como os utilizados em *smartcards* PLAID(2009). Neste trabalho é proposto um protocolo ainda mais leve, porém seguro, de autenticação mútua entre dispositivos gerenciados pelo *middleware uOS* Buzeto(2009). O protocolo oferece os serviços de autenticação mútua e estabelecimento de chave com elevado nível de segurança, sendo ainda adequado às restrições impostas pela aplicação. *Smartspaces* como Gaia Roman(2002) adotam Cerberos para sua segurança. O *uOS* difere na abordagem por se restringir à autenticação mútua entre dispositivo e middleware.

2 Protocolo de Autenticação para o *Middleware uOS*

Assume-se que, no ambiente ubíquo, há uma solução de segurança de chaves similar a descrita em Bryant(1988), durante a qual armazena-se informações acerca das características do dispositivo e é gerada uma chave secreta compartilhada pelo dispositivo e *middleware*. A Figura 1 ilustra o protocolo. Seja *A* um dispositivo que se deseja autenticar e *B* o *middleware*. Ambos compartilham uma chave secreta *K*.

1. *A* envia um *hash* de seu identificador (*H(Ia)*), a cifragem de *Ia*, *Ra* e *Ra'* (aleatórios) e o HMAC associado a eles (*m1*).
2. *B* obtém a chave compartilhada com *A* e verifica a integridade da mensagem. Estando correta, *B* gera *m2* contendo *Rb* e *Rb'* (aleatórios), *Ia* e *Ra+1* e *Ra'+1*. É enviado junto com a mensagem seu HMAC, que utiliza como chave *Rb'*.
3. *A* decifra *m1* e autentica *B*. *A* gera *m3*, cujo conteúdo é o número *Rb* somado a 1, cifrada utilizando *Rb* como chave, junto ao HMAC de *m3*.
4. *B* recebe *m3* e autentica A. A partir de então o valor *Rb*+1 passa a ser utilizado como chave de sessão na comunicação entre *A* e *B*.

A utilização de código de autenticação de mensagens (HMAC) em todas as mensagens do protocolo eleva consideravelmente seu nível de segurança Bellare(2000). O protocolo resiste a ataques de *replay*, espelhamento e *man-in-the-middle*, além de

possibilitar a verificação da integridade das mensagens. Note que cada lado cifra e autentica não só os dados que envia mas também aqueles recebidos na mensagem anterior. O protocolo proposto foi implementado e integrado ao *middleware uOS*. Utilizou-se a plataforma de desenvolvimento Java na sua implementação. Nas cifração e decifração de mensagens foi utilizado o algoritmo AES, Daemen(2001) com chaves de 128 *bits* e, para a geração de *hash,* foi utilizado o algoritmo SHA1 NIST(1995) por ser leve e apresentar baixo nível de colisões.

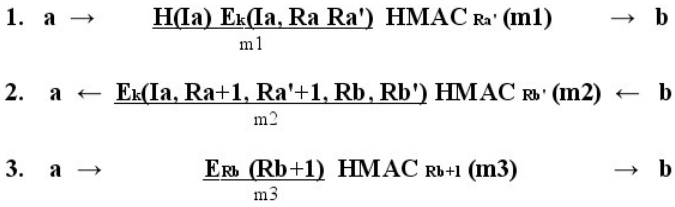

Figura 1. Protocolo de autenticação para o *middleware uOS*

3 Considerações Finais

Foi proposto e implementado um protocolo de autenticação mútua entre dispositivos, compatível com as exigências de um *smartspace*. Nos testes, realizados com um *laptop* como provedor e um celular Nokia N95 como cliente, a autenticação foi concluída em um tempo médio de 3,05 segundos. Os tempos necessários para a transmissão de mensagens criptografadas (com a chave de sessão criada durante a autenticação) foram 10% maiores que o necessário para a troca de mensagens em aberto. O resultado foi considerado satisfatório, pois o acréscimo de tempo com a cifragem das mensagens foi relativamente pequeno, comparado aos benefícios da comunicação segura.

Referências

Bryant, W., “Designing an Authentication System: A Dialogue in Four Scenes”. Project Athena Document, February 1988.

Buzeto, F. "DSOA: uma Arquitetura Orientada a Serviços para o Contexto de Computação Ubíqua". Qualificação de mestrado, PGInf, UnB. 2009.

NIST: National Institute of Standards and Technology. Secure Hash Algorithm authentication code (SHA). FIPS PUB 180-1, April 1995.

NIST: National Institute of Standards and Technology. “The keyed-hash message authentication code (HMAC)”. FIPS PUB 198, March 2002.

Bellare, M., Namprempre, C. “Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm”. LNCS Vol. 1976, Springer-Verlag, 2000.

Daemen, J., Rijmen, V., The Design of Rijndael: “The Wide Trail Strategy Explained”. New York, Springer-Verlag, 2000.

PLAID: "Protocol for Lightweight Authentication of Identity", https://www.govdex.gov.au/confluence/display/PLAID/Home, acessado em Julho 2009.

Román, M., Hess et all. "Gaia: A Middleware Infrastructure to Enable Active Spaces," *IEEE Pervasive Computing (accepted)*, 2002.