Acordo de Chave sem Certificados sob Emissão de Múltiplas Chaves Públicas*

Denise Goya[1], **Vilc Rufino**[1,2], **Routo Terada**[1]

[1]Instituto de Matemática e Estatística – Universidade de São Paulo (USP)

[2]Centro de Estudos da Marinha em São Paulo – Marinha do Brasil

{dhgoya,vilc,rt}@ime.usp.br

1. Introdução

O modelo de criptografia de chave pública sem certificados definido por [Al-Riyami e Paterson 2003] dispensa certificados digitais e permite que o usuário possua múltiplas chaves públicas.

Propomos aplicar essa multiplicidade a protocolos de acordo de chaves, com o objetivo de reduzir as consequências do comprometimento de uma chave secreta única. Essa abordagem nos conduz a duas possibilidades: (1) protocolos não interativos com autenticação mútua, sem certificados, que geram chaves diferentes a cada execução e (2) protocolos interativos com maior incerteza sobre a chave resultante. Ambas possibilidades são avaliadas sob o caso em que as chaves são independentes entre si. Na alternativa (1), adicionalmente é avaliado o caso das chaves serem deterministicamente relacionadas com uma principal.

O ponto de partida de nossas investigações é o protocolo interativo de acordo de chaves sem certificados de [Lippold et al. 2009], por ser o único até o momento que atende o modelo de segurança de [Swanson 2008], que é o mais completo por ora. Adicionamos, portanto, o uso de múltiplas chaves públicas ao protocolo mais seguro disponível.

O impacto dessa abordagem é a produção de novos protocolos, aplicáveis em diferentes contextos. A alternativa (1) é útil em ambientes com comunicação restritiva, tal como em aplicações militares ou comunicações via satélite ou submarina. A variante com chaves deterministicamente relacionadas tem uso potencial em redes de sensores. O caminho (2) deve tornar o protocolo original mais robusto e é merecedor de investigação.

2. Negociação Não Interativa de Chaves de Sessão com Autenticação

Em um cenário em que a comunicação é restrita, ocorre por canal unidirecional ou *off-line*, sem interatividade e com necessidade de sigilo, as soluções mais comuns envolvem: (1°) pré-distribuição de chaves secretas e (2°) protocolo de acordo de chaves em que a chave negociada deterministicamente é usada como semente para gerar uma chave de sessão. Nossas propostas diferem dessas soluções e são esboçadas a seguir.

2.1. Com Pré-distribuição de Chaves Públicas

São realizadas pequenas modificações no protocolo de [Lippold et al. 2009]: primeiramente, cada usuário A gera seus múltiplos pares de chaves dados por $\langle r_{A_i}, r_{A_i}P\rangle$, onde

*Projeto Fapesp n° 2008/06189-0

i é um índice e cada r_{A_i} é aleatório independentemente selecionado por A. O que chamamos par de chaves principal de A é definido igualmente ao protocolo original, em que a chave secreta é dada por $\langle x_A, sH_1(ID_A), sH_3(ID_A)\rangle$ e a pública, por $\langle x_A P, ID_A\rangle$. O valor x_A é o aleatório escolhido pelo usuário; os demais componentes da chave secreta são os segredos parciais emitidos pela autoridade de confiança. É necessária uma pré-distribuição de chaves públicas – e não de secretas, como no (1°) método convencional. As chaves secretas são armazenadas por A de forma segura. Elimina-se a fase de troca de mensagens. No novo cálculo de K_A, K'_A e SK, troca-se r_A por r_{A_i} e r_B por r_{B_j}.

Dependendo de como for realizado o gerenciamento das chaves secretas no lado de cada usuário, o risco de comprometimento de um único r_{A_i} é menor do que o risco de comprometimento da chave secreta única do (2°) caso, o que revelaria todas as chaves de sessão. E a descoberta de uma só chave de sessão SK não compromete as demais, pois os r_{A_i} são independentes. A demonstração de segurança deve se basear num subconjunto do modelo de [Swanson 2008], dada a não interatividade, acrescida de análises sobre o gerenciamento dos múltiplos pares de chaves.

2.2. Sem Pré-distribuição de Chaves

O objetivo de se estudar esse caso particular é avaliar a viabilidade de aplicação em ambientes altamente restritivos, como redes de sensores. Os múltiplos pares de chaves são dados por funções determinísticas aplicadas sobre um par principal. O ganho almejado desta abordagem é que a descoberta de uma só chave de sessão não revele as outras. A escolha dessas funções determinísticas deve ser tal que o conjunto das chaves públicas não forneça indícios da secreta principal e nem comprometa a segurança do protocolo.

Algumas condições iniciais do protocolo de [Lippold et al. 2009] podem ser relaxadas, com a finalidade de obtermos maior eficiência computacional. Ao trocarmos a hipótese de dificuldade do problema computacional Diffie-Hellman bilinear por uma mais forte – Diffie-Hellman bilinear lacunar – a quantidade de cálculos cai para praticamente a metade; e a relação determinística das chaves induz a uma variante que requer o cálculo de três emparelhamentos finais. Resta avaliar se todas essas modificações juntas não impedem que a correta redução na demonstração de segurança. Alternativamente, outro protocolo de acordo de chaves sem certificado pode ser alvo de estudo da multiplicidade de chaves deterministicamente relacionadas.

Referências

Al-Riyami, S. S. e Paterson, K. G. (2003). Certificateless public key cryptography. In *ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*. Springer. Cryptology ePrint Archive, Report 2003/126, `http://eprint.iacr.org/`.

Lippold, G., Boyd, C., e Nieto, J. (2009). Strongly secure certificateless key agreement. In *Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*. Springer. Cryptology ePrint Archive, Report 2009/219, `http://eprint.iacr.org/`.

Swanson, C. M. (2008). Security in key agreement: Two-party certificateless schemes. Master's thesis, University of Waterloo - Canadá. `http://hdl.handle.net/10012/4156`.