Proposta de Plano de Estudos

Modelos de Segurança em Assinatura sem Certificado

MAC5801 - Tópicos Especiais em Ciência da Computação

aluna: Denise Hideko Goya

orientador: Routo Terada

Instituição:

Departamento de Ciência da Computação

Instituto de Matemática e Estatística

Universidade de São Paulo

São Paulo, setembro de 2008

1 Resumo

O modelo de criptografia de chave pública sem certificado é uma alternativa ao modelo convencional que requer a manutenção de uma infra-estrutura de chaves públicas. Também é uma opção para a eliminação da custódia de chaves do modelo de criptografia assimétrica baseada em identidades.

Propomos neste documento, um plano de estudos de modelos de segurança para protocolos de assinatura sob o modelo sem certificado.

2 Introdução

O modelo convencional de criptografia de chave pública requer uma infra-estrutura de chaves públicas (ICP), para certificar a legitimidade dessas chaves. A manutenção de uma ICP, entretanto, implica custos e confere maior complexidade aos sistemas. O modelo de criptografia de chave pública baseada em identidade, proposto em [Shamir 1984], dispensa a necessidade da ICP, uma vez que a chave pública de um usuário é sua própria identificação (ou seja, dados pessoais, como nome, número do CPF ou telefone celular, etc). Em [Boneh, Franklin 2001] foi apresentado o primeiro esquema eficiente de cifragem baseado em identidade, que foi demonstrado seguro no modelo de oráculos aleatórios.

Uma característica inerente ao modelo de criptografia de chave pública baseada em identidade é a de custódia de chaves, em que uma entidade conhece as chaves secretas de todos seus usuários. A custódia de chaves é indesejável em vários tipos de aplicações; em particular, impossibilita a garantia de irretratabilidade.

Em [Al-Riyami, Paterson 2003], foi introduzido o paradigma de criptografia de chave pública sem certificado, que une propriedades do modelo convencional com o baseado em identidade. Nesse

paradigma, ICP e certificados digitais se fazem desnecessários, pois a identidade de um usuário fica parcialmente relacionada com a chave secreta. E não há custódia de chaves, pois o usuário é o único conhecedor de sua chave criptográfica secreta. Ademais, para uso interno a uma dada instituição (por exemplo, uma empresa ou órgão do governo) este paradigma é apropriado, uma vez que a entidade geradora das chaves (chamada *Key Generating Centre*, KGC) pode ser um membro idôneo desta instituição.

A similaridade entre os protocolos de [Al-Riyami, Paterson 2003] e [Boneh, Franklin 2001] indica que aplicações desenvolvidas sobre identidades podem ser convertidas para o modelo sem certificado, ao custo da necessidade de divulgação das chaves públicas (ou da manutenção de um diretório de chaves). O modelo sem certificado poderia ser uma ponte entre sistemas baseados em identidade com os que requerem ICP, em particular, a ICP-Brasil.

3 Tópicos em Desenvolvimento

A proposta de [Al-Riyami, Paterson 2003] tem sido amplamente estudada e estendida nos últimos anos, na busca de melhores resultados nos quesitos segurança, eficiência computacional e derivação de protocolos.

Estudos em criptanálise revelaram vários tipos de ataque sobre o modelo. O ataque de substituição de chave pública talvez seja o que compromete maior número de protocolos já propostos. Como exemplo, citamos [Terada, Goya 2007], cujo esquema foi estudado em [Castro, Dahab 2007b]. Em muitos casos, protocolos sujeitos a esse ataque foram inicialmente demonstrados seguros usando determinadas hipóteses (que foram posteriormente exploradas culminando em quebra).

Esse tipo de ataque está intimamente relacionado com o aspecto análise formal de segurança, que é o alvo principal deste plano de estudos.

Em análise formal de segurança, há várias questões a serem consideradas durante o projeto

de protocolos e algoritmos, como modelo de segurança para esquemas sem certificado, modelo de demonstração (padrão ou por oráculos aleatórios) e problemas envolvidos nas reduções.

Especialmente dentre os protocolos com maior eficiência computacional, é comum encontrarmos demonstrações sustentadas em hipóteses bastante fortes (talvez questionáveis), como a dificuldade de problemas matemáticos pouco conhecidos (por exemplo, p-*BDHI* em [Libert, Quisquater 2006] ou q-*BSDH* em [Zhang, Wang 2008]). Reduções polinomiais pouco eficientes, com folgas relativamente grandes (como em [Barbosa, Farshim 2008]) devem ser evitadas.

O controverso modelo de oráculos aleatórios para segurança demonstrável tem sido dominante entre as propostas de esquemas sem certificados, sob a justificativa de que os protocolos são mais viáveis para implementações práticas. Mas há estudos como o de [Dent et al. 2008] que usam o modelo padrão e forte modelo de adversários, ao custo de menor desempenho computacional.

Em [Dent 2006], há um levantamento dos modelos de segurança dos esquemas de cifragem desenvolvidos até então. Desconhecemos trabalho equivalente para esquemas de assinatura e seria importante uma discussão detalhada em torno do assunto, para que possamos melhor avaliar cada protocolo.

4 Plano de Estudos

Nosso plano de estudos envolve a investigação dos modelos de segurança descritos nos vários esquemas de assinatura já propostos. Serão estudados prioritariamente os seguintes trabalhos:

- Certificateless signature: a new security model and an improved generic construction [Hu et al. 2007];
- A certificateless signature and group signature schemes against malicious PKG [Zhang, Wang 2008];

- Certificateless public key signature: security model and efficient construction [Zhang et al. 2006];

Os seguintes trabalhos também serão analisados, pois podem acrescentar algum conhecimento importante:

- Security analysis of two signature schemes and their improved schemes [Zhang, Mao 2007];
- Two notes on the security os certificateless signatures [Castro, Dahab 2007b];
- Generic transformation from weakly to strongly unforgeable signatures [Huang et al. 2008];

Adicionalmente, pretendemos olhar os modelos de segurança nas seguintes variantes sobre assinaturas:

- Security mediated certificateless signatures [Yap et al. 2007];
- Simulatability and security of certificateless threshold signatures [Wang et al. 2007];
- Efficient certificateless signatures suitable for aggregation [Castro, Dahab 2007a];
- A provably secure ring signature scheme in certificateless cryptography [Zhang et al. 2007];
- Certificateless universal designated verifier signature schemes [Ming et al. 2007];

O objetivo principal é a compilação dos modelos de segurança existentes para assinatura sem certificado. Eventualmente podemos alcançar:

- Melhoria em demonstrações de segurança de protocolos existentes (reduções mais eficientes ou para problemas melhor estudados);

- Descoberta de falhas em demonstrações de segurança sobre protocolos existentes;
- Quebra de protocolos existentes;
- Modelos de segurança alternativos;
- Nova forma de ataque ao modelo sem certificado;

Referências

[Al-Riyami, Paterson 2003] Al-Riyami, S. S., Paterson, K. G. (2003). Certificateless public key cryptography. In *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security*, volume 2894 of *Lecture Notes in Computer Science*, Taipei, Taiwan. Springer.

[Barbosa, Farshim 2008] Barbosa, M., Farshim, P. (2008). Certificateless signcryption. In *ASIACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pages 369–372, New York, NY, USA. ACM.

[Boneh, Franklin 2001] Boneh, D., Franklin, M. K. (2001). Identity-based encryption from the weil pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229, London, UK. Springer-Verlag.

[Castro, Dahab 2007a] Castro, R., Dahab, R. (2007a). Efficient certificateless signatures suitable for aggregation. Cryptology ePrint Archive, Report 2007/454. http://eprint.iacr.org/.

[Castro, Dahab 2007b] Castro, R., Dahab, R. (2007b). Two notes on the security of certificateless signatures. In *Provable Security*, volume 4784 of *Lecture Notes in Computer Science*, pages 85–102, Berlin/Heidelberg. Springer.

[Dent 2006] Dent, A. W. (2006). A survey of certificateless encryption schemes and security models. Cryptology ePrint Archive, Report 2006/211. http://eprint.iacr.org/.

[Dent et al. 2008] Dent, A. W., Libert, B.,, Paterson, K. G. (2008). Certificateless encryption schemes strongly secure in the standard model. In *Public Key Cryptography - PKC 2008*, volume 4939 of *Lecture Notes in Computer Science*, pages 344–359, Berlin/Heidelberg. Springer.

[Hu et al. 2007] Hu, B., Wong, D., Zhang, Z.,, Deng, X. (2007). Certificateless signature: a new security model and an improved generic construction. *Designs, Codes and Cryptography*, 42(2):109–126.

[Huang et al. 2008] Huang, Q., Wong, D., Li, J.,, Zhao, Y.-M. (2008). Generic transformation from weakly to strongly unforgeable signatures. *Journal of Computer Science and Technology*, 23(2):240–252.

[Libert, Quisquater 2006] Libert, B., Quisquater, J.-J. (2006). On constructing certificateless cryptosystems from identity based encryption. In *Public Key Cryptography 2006 (PKC'06)*, volume 3958 of *Lecture Notes in Computer Science*, pages 474–490, New York, NY, USA. Springer-Verlag.

[Ming et al. 2007] Ming, Y., qin Shen, X.,, Wang, Y.-M. (2007). Certificateless universal designated verifier signature schemes. *The Journal of China Universities of Posts and Telecommunications*, 14(3):85–94.

[Shamir 1984] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, volume 196/1985 of *Lecture Notes in Computer Science*, pages 47–53, New York, NY, USA. Springer-Verlag New York, Inc.

[Terada, Goya 2007] Terada, R., Goya, D. H. (2007). A certificateless signature scheme based on bilinear pairing functions. In *Symposium on Computer and Information Security 2007*, volume 2C4-5 of *Information, and Communication Engineers*, pages 1–7, Tokyo, Japão. IEICE Institute of Electronics.

[Wang et al. 2007] Wang, L., Cao, Z., Li, X.,, Qian, H. (2007). Simulatability and security of certificateless threshold signatures. *Information Sciences*, 177(6):1382–1394.

[Yap et al. 2007] Yap, W.-S., Chow, S., Heng, S.-H.,, Goi, B.-M. (2007). Security mediated certificateless signatures. In *Applied Cryptography and Network Security - ACNS 2007*, volume 4521 of *Lecture Notes in Computer Science*, pages 459–477. Springer.

[Zhang, Wang 2008] Zhang, G., Wang, S. (2008). A certificateless signature and group signature schemes against malicious pkg. In *22nd International Conference on Advanced Information Networking and Applications, AINA 2008*, pages 334–341. IEEE Computer Society.

[Zhang, Mao 2007] Zhang, J., Mao, J. (2007). Security analysis of two signature schemes and their improved schemes. In *Computational Science and Its Applications ICCSA 2007*, volume 4705 of *Lecture Notes in Computer Science*, pages 589–602. Springer Berlin.

[Zhang et al. 2007] Zhang, L., Zhang, F.,, Wu, W. (2007). A provably secure ring signature scheme in certificateless cryptography. In *Provable Security*, volume 4784 of *Lecture Notes in Computer Science*, pages 103–121. Springer.

[Zhang et al. 2006] Zhang, Z., Wong, D. S., XU, J.,, FENG, D. (2006). Certificateless public key signature: Security model and efficient construction. In *4th. International Conference on Applied Cryptography and Network Security, ACNS'06*, volume 3989 of *Lecture Notes in Computer Science*, Singapore. Springer.