Privacidade e Segurança da Informação em Dispositivos Móveis

Cleber Okida

Instituto de Matemática e Estatística - Universidade de São Paulo
Mestrado em Ciência da Computação

16 de Outubro de 2009

Introdução

Criptografia sem certificado

Introduzido por Al-Riyami e Paterson [1] é uma variante da criptografia baseada em identidade, que limita a capacidade de custótia de chaves do centro de geração de chaves (KGC), e não possui um custo tão caro de gerenciamento como em certificação digital.

Esquemas de acordo de chaves

fornece um meio seguro e eficiente para duas partes se comunicar em um canal contraditório, controlado por um adversário.

Objetivos

PKC + IBE $\neq$ CL

A combinação natural de um protocolo de acordo de chaves baseado em identidade com um protocolo acordo de chaves baseado em chave pública não pode oferecer maior segurança.

Projeto Borboleta

Aplicação na segurança de prontuários médicos.

Sumário

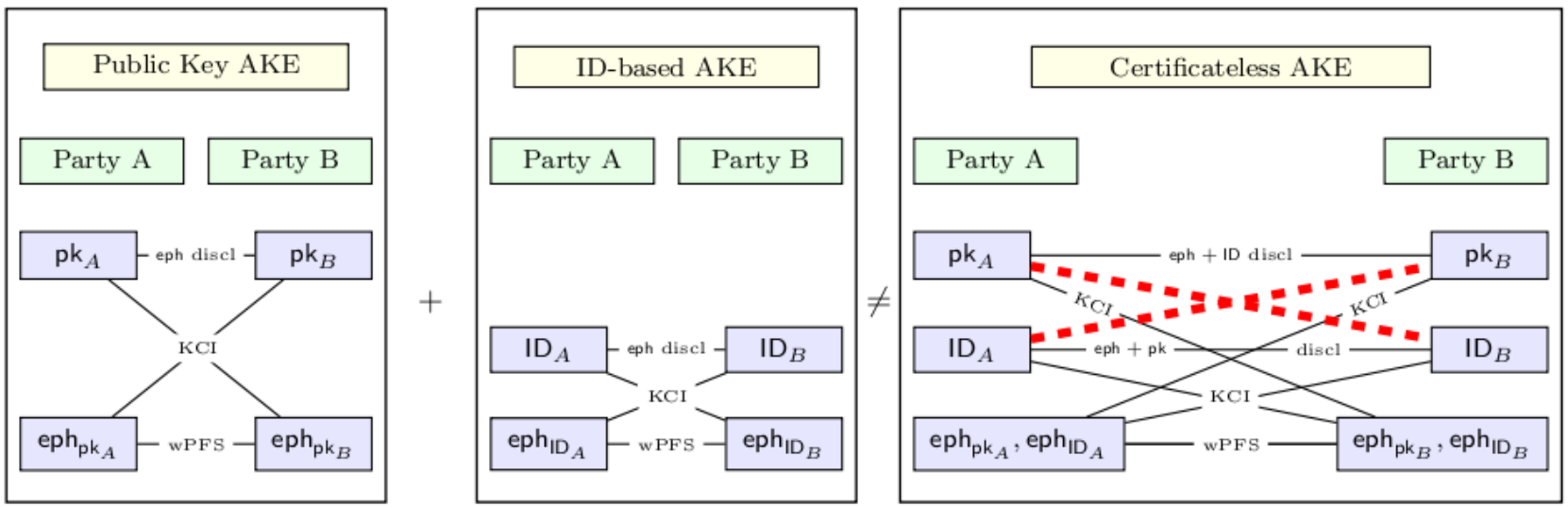
Segurança exigida a protocolos de acordo de chaves

- Resistência a ataques de personificação básica
- Resistência a ataques de chaves compartilhadas desconhecidas (UKS)
- Segurança da chave conhecida
- *"Perfect Forward Secrecy"* fraco (wPFS)
- Resistência a ataques de personificação chaves comprometidas
- Resistência a divulgação de segredos efêmeros
- Resistência ao vazamento de segredos efêmero do KGC

Porque PK-AKE + ID-AKE $\neq$ CL-AKE em nosso modelo ?

Uma sessão só é considerada "recente", desde que cada entidade ainda tenha pelo menos um segredo não comprometido.

Porque PK-AKE + ID-AKE ≠ CL-AKE em nosso modelo ?



Porque PK-AKE + ID-AKE $\neq$ CL-AKE em nosso modelo ?

Esta composição não pode oferecer o nível desejado de segurança, porque não existem garantias de segurança, se entidade A ainda tem uma chave descomprometida no PK-AKE e B ainda tem uma chave descomprometida no ID-AKE (ambos equemas AKE estão quebrados, neste momento).

Notações utilizadas

q	um valor primo grande;
$\mathbb{G}_1$	grupo aditivo cíclico de ordem prima q;
$\mathbb{G}_2$	grupo multiplicativo cíclico de ordem prima q;
$\mathbb{G} = \langle g \rangle$	g é um gerador do grupo G;
$\mathbb{Z}_q$	conjunto dos números inteiros mod q;
a, b, c, x, y	valores inteiros mod q;
$Q, R \in \mathbb{G}_1$	pontos da curva elíptica em $\mathbb{G}_1$;
A, B	usuários do sistema criptográfico (entidades);
ID_A	Identificação da entidade A;
$n \in \mathbb{N}$	um valor natural;
$H(\cdot) \rightarrow 0, 1^n$	Funções hash que retorna um valor de n bits;

Emparelhamentos

$e{:}\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ é um "Emparelhamento Bilinear":

Bilinear:	Para quaisquer $P, Q, R \in \mathbb{G}_1$, temos: $e(P+Q, R) = e(P, R) \cdot e(Q, R)$ e $e(P, Q+R) = e(P, Q) \cdot e(P, R)$. caso particular $a, b \in \mathbb{Z}_q$: $e(aQ, bQ) = e(Q, Q)^{ab}$ $= e(abQ, Q) = e(Q, abQ)$
Não degenerativo:	$\forall \langle Q, R \rangle, e(Q, R) \neq$ identidade $\mathbb{G}_2$;
Eficiente:	$\forall \langle Q, R \rangle, \exists A \rightarrow A \equiv e(Q, R)$

Problemas de interesse

"Problema do Logaritmo Discreto" (DLP):

Dado $b \in \mathbb{G}$ e g um gerador de $\mathbb{G}$ Encontrar um valor $a \in \mathbb{Z}_q$, tal que $b = g^a$.

Problemas de interesse

"Problema de Diffie-Hellman Bilinear" (BDH):

Dados $Q, aQ, bQ, cQ \in \mathbb{G}_1$, onde $a, b, c \in \mathbb{Z}_q^*$ e Q um gerador do grupo $\mathbb{G}_1$: encontrar o valor $e(Q, Q)^{abc} \in \mathbb{G}_2$.

Problemas de interesse

"Problema de Decisão de Diffie-Hellman Bilinear" (DBDH):

Dados $Q, aQ, bQ, cQ \in \mathbb{G}_1$ e $z \in \mathbb{G}_2$, onde $a, b, c \in \mathbb{Z}_q^*$ e Q um gerador do grupo $\mathbb{G}_1$: decidir se $z = e(Q, Q)^{abc}$.

Problemas de interesse

"Problema Gap de Diffie-Hellman Bilinear" (Gap-BDH):

Dados $Q, aQ, bQ, cQ \in \mathbb{G}_1$ e $z \in \mathbb{G}_2$, onde $a, b, c \in \mathbb{Z}_q^*$ e Q um gerador do grupo $\mathbb{G}_1$,
como o oráculo que resolve o problema de decisão em $\mathbb{G}$, podemos encontrar o valor $e(Q, Q)^{abc} \in \mathbb{G}_2$.

Inicialização - KGC

KGC sorteia um $s \in \mathbb{Z}_p$(chave mestra)
calcula chave pública sP
seleciona as 3 funções Hash

$H_1 : \{0,1\}^* \rightarrow \mathbb{G}$
$H_2 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}^8 \times \mathbb{G}_T^6 \rightarrow \{0,1\}^n, n \in Z \text{ e } n > 0$
$H_3 : \mathbb{G} \rightarrow \mathbb{G}$

Inicialização - Usuário

Participante U	sorteia um valor secreto $x_u \in \mathbb{Z}_p$
	calcula chave pública $x_u P \in \mathbb{G}$
	gera chave secreta parcial
	$\{sH_1(ID_U), sH_3(H_1(ID_U))\} \in \mathbb{G}^2$ para o KGC

Troca de Mensagens

Usuário A sorteia um valor secreto $r_A \in \mathbb{Z}_p$

Usuário B sorteia um valor secreto $r_B \in \mathbb{Z}_p$

Ambos trocam suas mensagens $A \rightarrow B : E_A = (r_A P, x_A P)$

$B \rightarrow A : E_B = (r_B P, x_B P)$

Cálculo de K_A e $K_{'A}$

$$
\begin{aligned}
K_A &= e(H_1(ID_B), sP)^{r_A} e(sH_1(ID_A), r_B P) \\
&= e(H_1(ID_B), P)^{r_A s} e(H_1(ID_A), P)^{r_B s} = K_B = K
\end{aligned}
$$

$$
\begin{aligned}
K'_A &= e(H_3(H_1(ID_B)), sP)^{r_A} e(sH_3(H_1(ID_A)), r_B P) \\
&= e(H_3(H_1(ID_B)), P)^{r_A s} e(H_3(H_1(ID_A)), P)^{r_B s} = K'_B = K'
\end{aligned}
$$

Cálculo de L_A e L'_A

$$
\begin{aligned}
L_A &= e(H_1(ID_B), sP)^{x_A} e(sH_1(ID_A), x_B P) \\
&= e(H_1(ID_B), P)^{x_A s} e(H_1(ID_A), P)^{x_B s} = L_B = L
\end{aligned}
$$

$$
\begin{aligned}
L'_A &= e(H_3(H_1(ID_B)), sP)^{x_A} e(sH_3(H_1(ID_A)), x_B P) \\
&= e(H_3(H_1(ID_B)), P)^{x_A s} e(H_3(H_1(ID_A)), P)^{x_B s} = L'_B = L'
\end{aligned}
$$

Cálculo de N_A e $N_{'A}$

$$\begin{aligned} N_A &= e(H_1(ID_B), sH_1(ID_A)) \\ &= e(H_1(ID_B), H_1(ID_A))^s = N_B = N \end{aligned}$$

$$\begin{aligned} N'_A &= e(H_3(H_1(ID_B)), sH_3(H_1(ID_A))) \\ &= e(H_3(H_1(ID_B)), H_3(H_1(ID_A)))^s = N'_B = N' \end{aligned}$$

Cálculo da chave de sessão

$$SK = H_2(A, B, E_A, E_B, r_a r_B P, x_a x_B P, r_a x_B P, x_a r_B P, K, K', L, L', N, N')$$

Problemas de desempenho e armazenamento

Criptossistemas baseados em curvas elípticas utilizam tabelas grandes para armazenar resultados de operações "geradoras" de chaves.
A limitação de processamento do PDA inviabiliza a geração de chaves públicas e secretas dentro do mesmo.
Sabendo que a geração de chaves será feita apenas durante o cadastro do profissional da saúde, e se houver uma chave revogada, então podemos utilizar de um computador auxiliar para realizar essas operações.

Considerações de eficiência

- Cada participante deve calcular 5 exponenciações em $\mathbb{G}$ e 10 emparelhamentos.
  1. Se utilizarmos o Gap-BDH então poderemos omitir H_3 poupando 2 consultas hash e reduz a complexidade do protocolo a 3 exponenciações em $\mathbb{G}$ e 5 emparelhamentos.
  2. Se o protocolo for utilizado para os mesmos usuários (i.e. VPNs) podemos reduzir para 4 exponenciações em $\mathbb{G}$ e 4 emparelhamentos.
     - Ainda se utilizarmos o Gap-BDH, reduzimos ainda mais as consultas resultando em 2 exponenciações em $\mathbb{G}$ e 2 emparelhamentos.

Será utilizado o algoritmo AES de 128 bits, por isso o hash deverá ser de no mínimo 256 bits.

Possíveis estratégias para adversário

1. O adversário não deve obter o valor secreto x_I de ID_I nem x_J de ID_J.
2. O adversário não deve obter a chave secreta do efêmero r_I de ID_I nem r_J de ID_J.
3. O adversário não deve obter o valor secreto x_J de ID_J e nem substituir a chave pública E_J de ID_J e não deve também obter a identificação baseada em chave secreta (chave parcial) de ID_I.
4. O adversário não deve obter a chave secreta do efêmero ID_J nem o valor secreto de ID_I
5. O adversário não deve obter a chave secreta do efêmero ID_I nem o valor secreto de ID_J

Possíveis estratégias para adversário - Continuação

6. O adversário não deve obter o valor secreto x_I de ID_I nem substituir o valor secreto de ID_I e não deve também obter a identificação baseada em chave secreta de ID_J (chave parcial)
7. O adversário não deve obter a chave secreta do efêmero r_J de ID_J nem a identificação baseada em chave secreta x_I de ID_I
8. O adversário não deve obter a chave secreta do efêmero r_I de ID_I nem a identificação baseada em chave secreta x_J de ID_J
9. O adversário não deve obter a identificação baseada em chave secreta de ID_I nem de ID_J

Demonstração

Estratégia 1

A probabilidade de que B é capaz de encontrar uma solução para o desafio CDH é:

$$Adv^{B}(k)[CDH] \geq \frac{Adv^{M}(k)[\prod]}{9q_0q_1^2}$$

Dúvidas

http://lsd.ime.usp.br
cleberok@ime.usp.br


Lippold, G and Boyd, C and Nieto, J.G.,*Strongly Secure Certificateless Key Agreement*, Pairing 2009, Springer, 2009, `http://eprint.iacr.org/`.


Swanson, C. M., *Security in Key Agreement: Two-Party Certificateless Schemes*, University of Waterloo - Canadá, 2008, `http://hdl.handle.net/10012/4156`


Silverman, J., *Arithmetic of elliptics curves*, Springer, 2009


Washington, L., *Elliptic curves: number theory*, CRC Press, 2008


Sattam S. Al-Riyami and Kenneth G. Paterson, *Certificateless Public Key Cryptography*, ASIACRYPT 2003


R. Sakai and K. Ohgishi and M. Kasahara, *Cryptosystems based on pairing*, 2000