Análise Comparativa entre Protocolos para Troca de Certificados Digitais

Ricardo C. Branco, Lucas V. Dias, Tiago A. Rizzetti

Universidade Federal de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores
Núcleo de Estudos em Redes, Segurança e Sistemas Computacionais

{*branco, lucas_dias*}*@redes.ufsm.br*, {*rizzetti*}*@ctism.ufsm.br*

19 de Setembro de 2019

Cronograma

- Alternativas à troca de certificados digitais de forma segura
- Autenticação mútua sem necessidade de uma terceira entidade
- Menor dependência em relação a Autoridade Certificadora (AC)
- Troca de certificados *online* de forma segura, sem necessidade de métodos *offline* para o mesmo

Public Key Infrastructure (1/2)

- Infraestrutura de chave pública (ICP)
- Alternativa consolidada para fornecer estabelecimento de relações de confiança entre entidades envolvidas em uma transação digital
- AC raiz delega permissões a ACs intermediárias
- Somente entidade raiz tem poder de revogação de certificados
- AC intermediária provê assinatura de certificados a clientes finais
- Para troca de mensagens utilizando certificados digitais como métodos de autenticação, cliente retira do certificado a chave pública da AC e realiza a validação do certificado

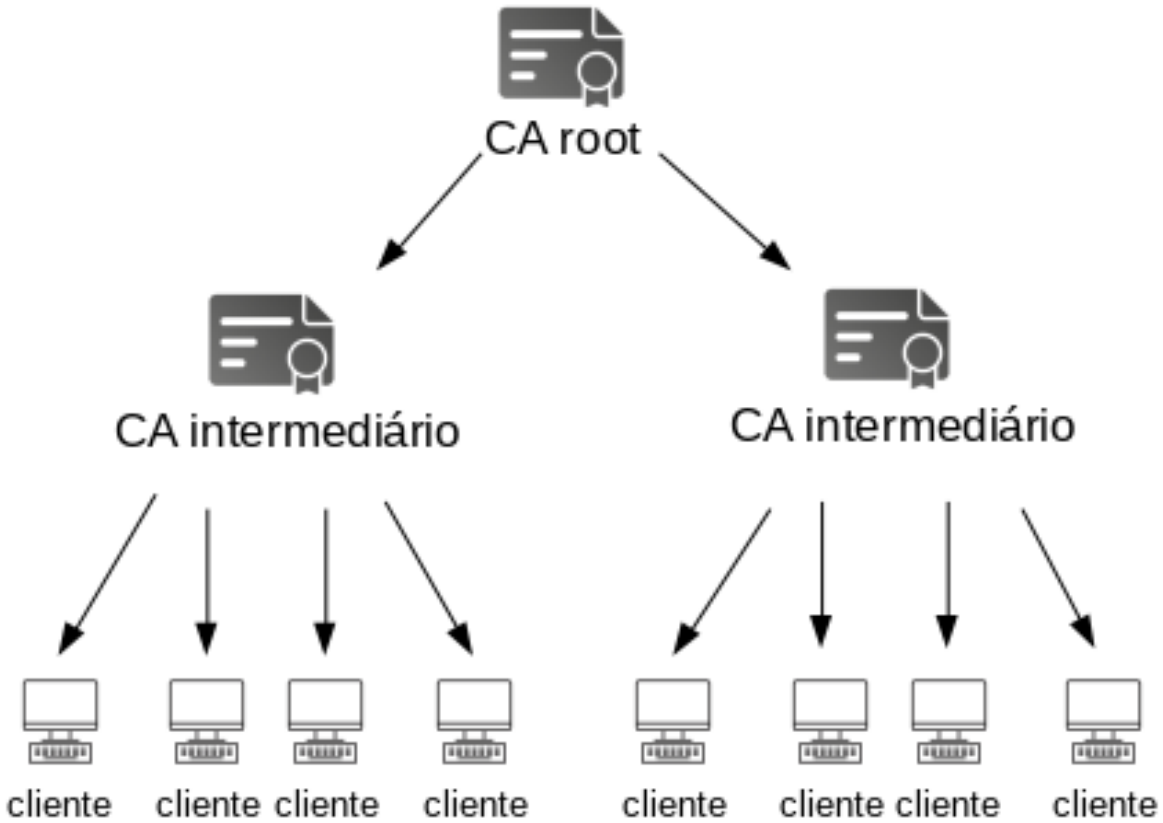


Figura: Estrutura básica de uma PKI

Internet Key Exchange (1/2)

- Projetado para troca de chaves e negociação de associações de segurança para comunicações seguras
- Fornece uma estrutura para estabelecer associações de segurança e chaves criptográficas, sem mecanismos específicos para autenticação
- Utilização do protocolo IPSec para prover segurança
- Dividido em duas fases:
  - *IKE_INIT*
    - define associação de segurança e parâmetros que serão utilizados para definição do algoritmo *Diffie-Hellman*
  - *IKE_AUTH*
    - cálculo do segredo *Diffie-Hellman* e do restante das chaves que serão utilizadas na comunicação e envio de informações para identificação

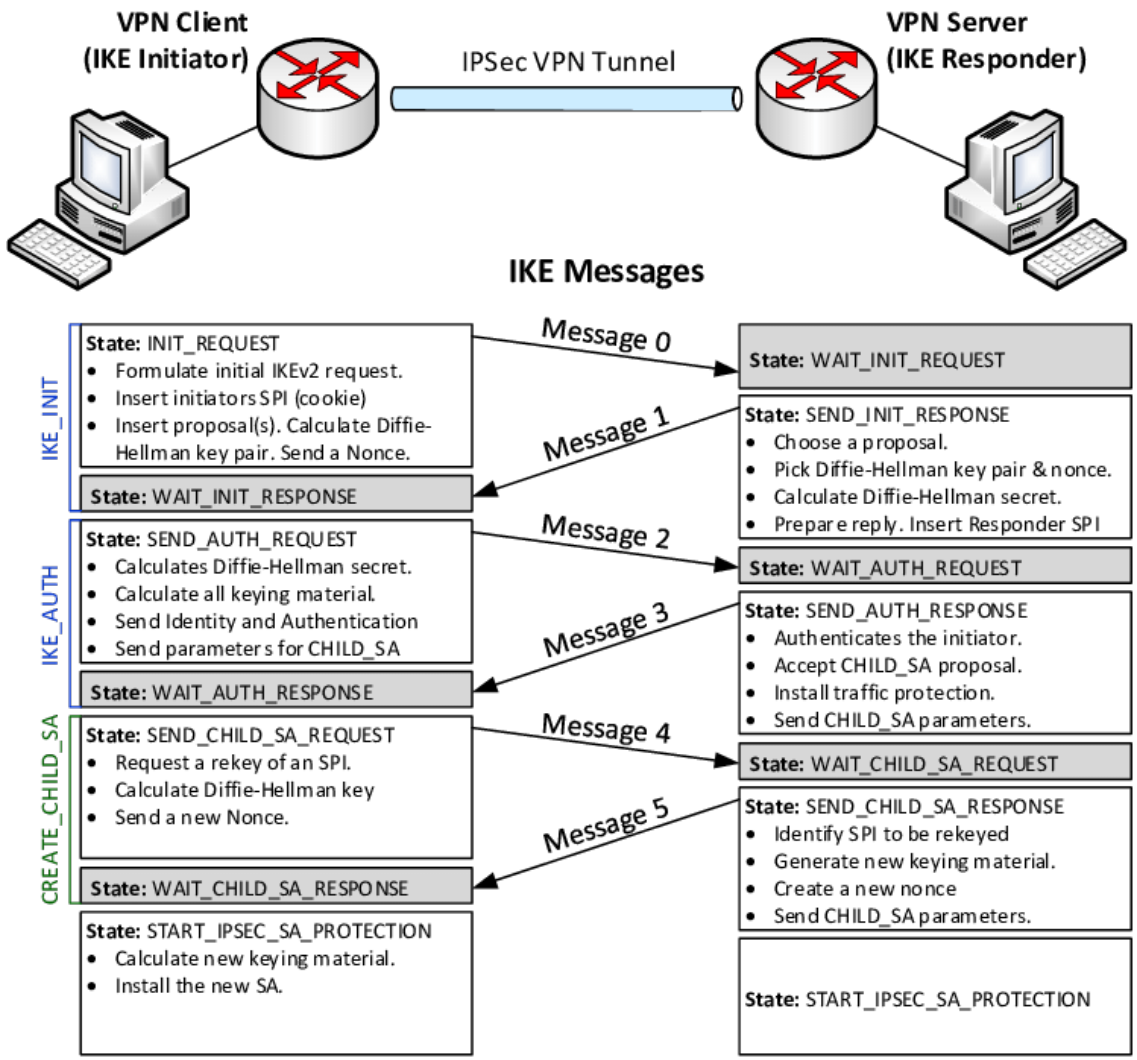


Figura: Troca de mensagens do protocolo IKEv2

Motivação para Desenvolvimento da Proposta

- Autenticação mútua, independente de uma terceira parte online
- Segurança provida através da assinatura, com a chave privada do remetente, do *hash* do certificado do remetente, juntamente com a *hash* da chave de sessão, escolhida através de um acordo de *Diffie-Hellman*
- Suporte a diferentes algoritmos de *hash* e criptografia assimétrica, conforme necessidade

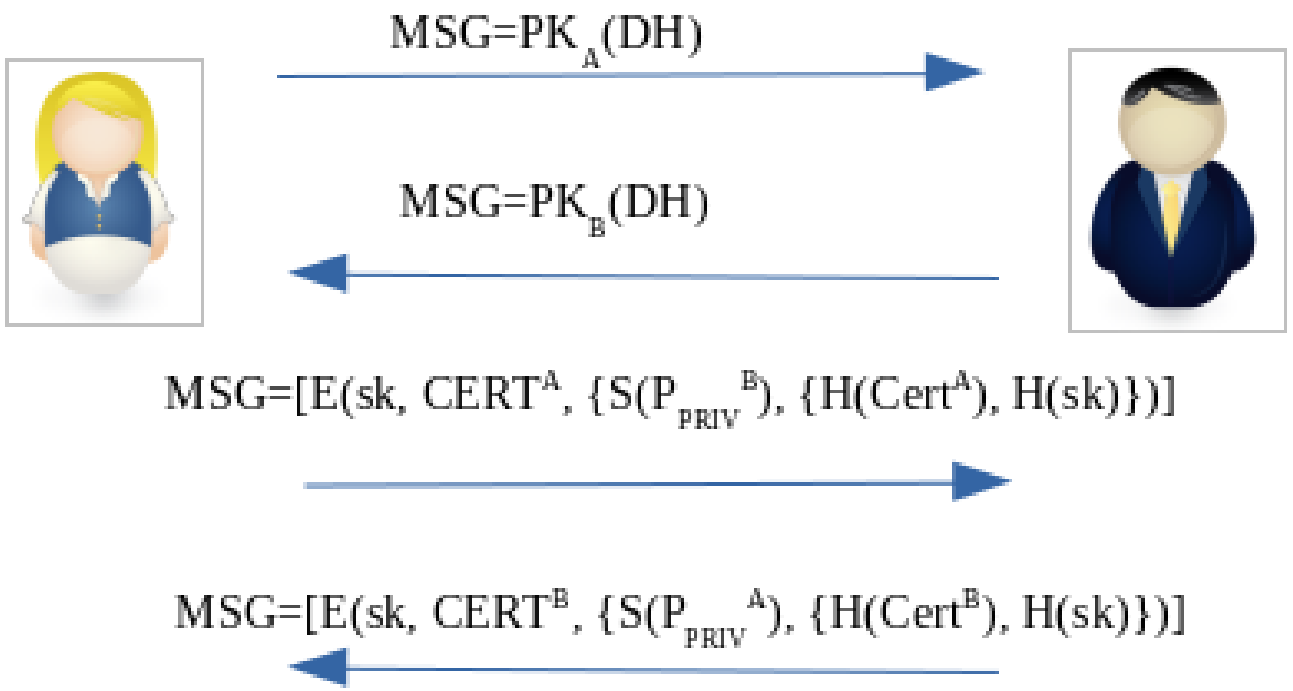
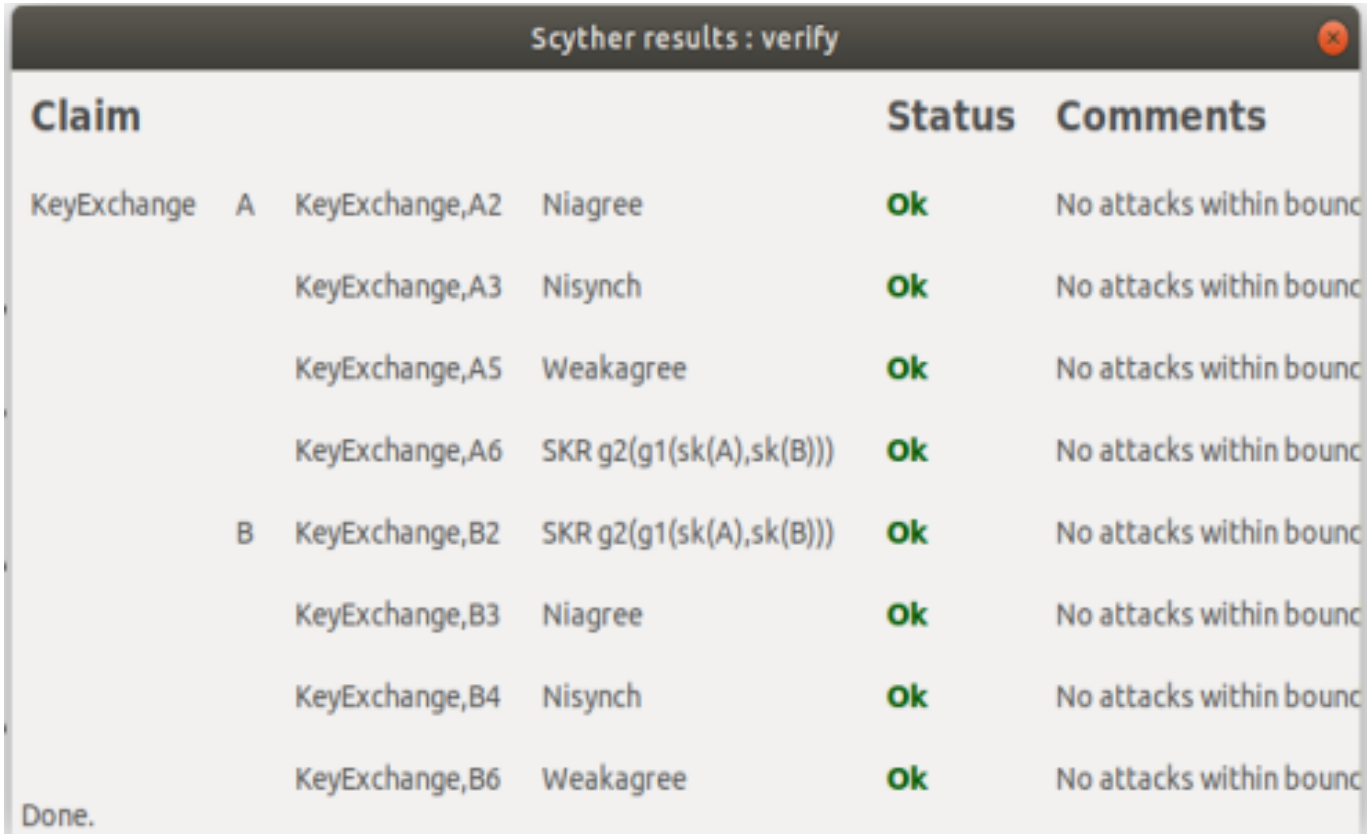


Figura: Estrutura do protocolo proposto

- Assinatura da mensagem garante autenticidade e integridade
- Cifração da mensagem com chave de sessão garante confidencialidade
- Assinatura da *hash* do certificado e chave de sessão garantem uma segurança em relação a ataques de replicação, reflexão e temporização
- Acordo *Diffie-Hellman* garante que a mensagem, ao ser interceptada, não poderá ser compreendida pelo atacante

- Utilização do *software Scyther* para validação da proposta
- Resultados promissores, *software* não encontrou vulnerabilidades durante execução de testes
- Trabalhos futuros contemplarão um *software* para testes de possíveis vulnerabilidades existentes
- Com um menor número de mensagens e a independência da disponibilidade de uma AC, garantimos uma comunicação segura



Scyther results : verify

Claim				Status	Comments
KeyExchange	A	KeyExchange,A2	Niagree	Ok	No attacks within bounc
		KeyExchange,A3	Nisynch	Ok	No attacks within bounc
		KeyExchange,A5	Weakagree	Ok	No attacks within bounc
		KeyExchange,A6	SKR g2(g1(sk(A),sk(B)))	Ok	No attacks within bounc
	B	KeyExchange,B2	SKR g2(g1(sk(A),sk(B)))	Ok	No attacks within bounc
		KeyExchange,B3	Niagree	Ok	No attacks within bounc
		KeyExchange,B4	Nisynch	Ok	No attacks within bounc
		KeyExchange,B6	Weakagree	Ok	No attacks within bounc

Done.

Figura: Troca de mensagens do protocolo proposto e possíveis ataques

Considerações Finais (1/2)

- Menor número de mensagens, menor vulnerabilidade a problemas na comunicação
- Independência da disponibilidade da AC
- Métodos isolados da autoridade certificadora para garantir a identidade dos nós e a autenticidade da comunicação
- Comunicação com a AC para que a mesma assine seu certificado digital
- *Uniform Resource Locator* para verificação da lista de revogações

- Liberdade de implementação de diversos tipos de algoritmos de *hash* e cifração
- Descentralização do processo de validação de certificados digitais
- Segurança baseia-se, em parte, nas propriedades matemáticas utilizadas pelo acordo *Diffie-Hellman* e algoritmos de *hash*, os quais já foram amplamente testados na literatura

- Abdel Hakeem, S., Arslan, S., and Kim, H. (2017). Ike hardware engine based on cam for concurrent processing of massive user sessions. pages 154–159.
- Casimiro, A., d Lemos, R., and Gacek, C. Operational semantics and verification of security protocols.
- Gutmann, P. (2002). Pki: it's not dead, just resting. Computer, 35(8):41–49.
- Moecke, C. T., Custódio, R. F., Kohler, J. G., and Carlos, M. C. (2010). Uma icp baseada em certificados digitais autoassinados. Simpósio Brasileiro em Segurança da Informaçao e de Sistemas Computacionais, pages 91–104.
- William Stallings, L. B. (2014). Segurança de Computadores: Princıpios e Práticas. Rio de Janeiro.
- Zhou, J. (2000). Further analysis of the internet key exchange protocol. Computer Communications, 23(17):1606–1612.

- Ricardo Branco - graduando em CST em Redes de Computadores
- Lucas Dias - graduando em CST em Redes de Computadores

NERSEC

Núcleo de Estudos em Redes, Segurança e Sistemas Computacionais