Informações sobre os certificados digitais

Introdução

Grids computacionais consistem de recursos de processamento e de armazenamento distribuídos e interconectados, e visam atender a grupos de usuários geograficamente dispersos. De forma geral, tanto usuários quanto recursos pertencem a domínios administrativos distintos que interagem entre si de forma cooperativa. O gerenciamento desse ambiente cooperativo certamente envolve questões de segurança, requerendo mecanismos que permitam autenticar usuários e recursos e estabelecer níveis e prioridades de acesso.

Os Grids utilizam mecanismos baseados em criptografia de chave pública ou assimétrica, que viabilizam a efetivação de propriedades importantes relativas à proteção da informação, como sigilo, integridade, autenticidade e irretratabilidade (ou não repúdio). Tanto recursos físicos quanto usuários recebem um par de chaves distintas, uma de uso estritamente privado e outra tornada pública. Após a geração do par de chaves, a chave pública correspondente precisa ser assinada digitalmente por uma entidade certificadora confiável - e, idealmente, reconhecida internacionalmente - para confirmar a identidade do usuário ou do recurso computacional. Essa entidade é conhecida como autoridade de certificação ou CA (Certification Authority), e o procedimento de assinatura é chamado de emissão de um certificado digital. Os certificados digitais são um dos elementos fundamentais da infraestrutura de segurança em ambientes distribuídos e cooperativos, pois facilitam a autenticação de usuários e recursos de organizações diferentes de modo seguro [1][2].

No ambiente de Grid, o arquivo de chave privada (userkey.pem) e o arquivo de certificado (usercert.pem) correspondem ao par de chaves da criptografia de chave pública. O arquivo userkey.pem (ou resourcekey.pem no caso de um recurso) contém a chave privada criptografada, que só pode ser decriptografada mediante o fornecimento de uma senha. O arquivo usercert.pem contém a chave pública e outras informações importantes, como o nome do titular do certificado e a organização à qual pertence, a identificação da CA que assinou o certificado e a assinatura digital da CA. O papel da autoridade certificadora é fundamental, pois ela estabelece uma conexão confiável entre a identidade do usuário e a sua chave pública. A assinatura digital da CA no arquivo do certificado do usuário declara oficialmente que a chave pública presente no arquivo pertence àquele usuário. Os arquivos de certificado são codificados no formato X.509 [3].

ANSP Grid CA

Os certificados digitais dos usuários e recursos do GridUnesp foram assinados pela ANSP Grid CA, a autoridade certificadora raiz da rede acadêmica paulista, gerida pela rede ANSP. A ANSP Grid CA é uma entidade reconhecida internacionalmente, sendo membro oficial do TAGPMA (The Americas Grid Policy Management Authority), o qual por sua vez pertence à federação IGTF (International Grid Trust Federation) [4]. A ANSP Grid CA, a primeira autoridade da cadeia de certificação, tem a função de criar, manter e controlar todos os certificados por ela emitidos, incluindo a revogação de certificados comprometidos ou com prazo de validade expirada.

Os certificados digitais foram criados no NCC, que é uma autoridade de registro ou RA (Registration Authority) reconhecida e autorizada pela ANSP Grid CA. A autoridade de registro atua como intermediário entre a autoridade de certificação e os usuários dos recursos computacionais sob sua responsabilidade, reconhecendo e validando a autenticidade de cada usuário e de cada recurso perante a autoridade de certificação, visando o cumprimento adequado das normas de segurança relativas à emissão e gerenciamento dos certificados digitais. O NCC, por sua vez, confia nos pesquisadores responsáveis pelos projetos submetidos ao GridUnesp, os quais conhecem pessoalmente os seus usuários e confiam neles. Essa cadeia hierárquica de confiaça é fundamental, pois viabiliza a emissão de certificados digitais para todos os usuários do GridUnesp e permite manter a integridade do sistema. Vale lembrar que o GridUnesp mantém estreita parceria com a comunidade internacional; de posse de certificados digitais reconhecidos internacionalmente, os usuários poderão ter acesso a recursos externos.

Pelas razões expostas, lembramos aos usuários que qualquer indício de comprometimento da segurança do certificado (suspeita de violação da chave privada) deve ser imediatamente informado à equipe de suporte técnico do GridUnesp, através do email < support@grid.unesp.br>, para que o certificado seja revogado e um novo seja emitido. O procedimento é simples e deve ser disparado sempre que o usuário suspeitar da integridade de seu certificado. A violação do certificado digital, que é de uso pessoal e intransferível, compromete a segurança dos sistemas computacionais não apenas do GridUnesp mas também de sistemas pertencentes a domínios administrativos externos à Unesp. Esse procedimento é essencial para garantir a segurança de toda a infraestrutura. Os pesquisadores responsáveis por projetos devem zelar pela integridade da infraestrutura de segurança reforçando aos membros de seu grupo a guarda e uso adequados dos certificados.

Recomendamos também aos usuários a instalação do certificado raiz da ANSP Grid CA em seus navegadores web, disponível em: http://gridca.ansp.br/en/carootcert

O certificado raiz da ANSP Grid CA também está disponível no repositório internacional de autoridades certificadoras acadêmicas mantido pela TERENA (Trans-European Research and Education Networking Association): https://www.tacar.org/cert/list

Referências

[1] RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1. Disponível em http://www.rsasecurity.com/rsalabs/faq/files/rsalabs_faq41.pdf

[2] Overview of the Grid Security Infrastructure. Disponível em http://www.globus.org/security/overview.html

[3] A. Arsenault, S. Turner, PKIK Working Group. Internet Draft. Internet X.509 Public Key Infrastructure - PKIK Roadmap. October 22, 1999.

[4] D. Simmel, S. Rea, A. Stolk, "An Introduction to The Americas Grid Policy Management Authority (TAGPMA) and the International Grid Trust Federation (IGTF)", CLCAR´12 (Conferencia Latinoamericanda de Computación de Alto Rendimiento), Ciudad de Panamá, Agosto de 2012. Disponível em http://www.tagpma.org/files/CLCAR-Paper15-Simmel-Rae-Stolk.pdf

R. L. Iope (01-03-2013)