

Resumo

As comunicações através da *Internet* são por natureza inseguras. Há uma crescente necessidade de comunicações seguras, para as quais é necessária a autenticação das entidades, e confidencialidade e integridade dos dados. Muitas das soluções existentes, de entre as quais o SSL/TLS, dependem do PKIX, o qual recorre a certificados X.509 emitidos, tipicamente, por Autoridades de Certificação comerciais. A emissão dos certificados tem custos económicos e administrativos. Devido aos custos, alguns servidores *Web* usam certificados *self-signed*, os quais não permitem uma autenticação transparente. As CA comerciais não têm autoridade sobre as entidades que certificam, desempenham o papel de notário e definem as próprias políticas dos serviços que fornecem muitas vezes limitando as suas responsabilidades.

O DNSSec permite garantir a autenticidade e integridade dos registos DNS. Apesar de oferecer protecção contra muitas ameaças, até à data, isoladamente, não tem justificado o investimento e sua manutenção, o que tem impedido a sua implementação em larga escala. Esta tese apresenta uma solução com base num novo modelo de certificação, o ScalSec, que é baseada no DNSSec. É definido um novo registo para o DNSSec que permite adicionar um resumo de chave por nó. Cada nó assume-se como CA local e emite certificados para cada serviço. Ao DNSSec é adicionado apenas o resumo que representa o nó. O cliente recorre aos certificados X.509 adaptados e ao DNSSec, juntamente com os novos registos por nó, para autenticar o servidor. Suporta-se sinónimos DNS de forma transparente, sem modificações nos certificados.

Foi melhorado um cliente TLS, o do projecto *Mozilla*, comum ao *Firefox* e ao *Thunderbird*, clientes *Web* e de email, respectivamente. Foram também criados scripts que permitem a gestão automática dos certificados num nó, bem como a actualização dos respectivos registos no DNS.

Abstract

The communications over the Internet are by nature insecure. There is a growing need for secure communications, for which it is necessary to authenticate the entities, and confidentiality and integrity of data. Many of the existing solutions, including the SSL/TLS, depend on PKIX, which uses X.509 certificates issued, typically, by commercial Certification Authorities. The issuance of certificates has economic and administrative costs. Due to cost reasons, some Web servers use self-signed certificates, which do not allow a transparent authentication. The commercial CAs do not have authority over the certified entities, playing the role of notary and define their own policies for services they provide often limiting their responsibilities.

The DNSSec ensures the authenticity and integrity of DNS records. Despite it offers protection against many threats, so far, alone, has not justified the investment and maintenance, which has prevented its implementation on a large scale. This thesis presents a solution based on a new model of certification, the ScalSec, which is based on DNSSec. A new resource record for the DNSSec is defined which allows a hash of a key per node to be added. Each node takes itself as local CA and issues certificates for each service. In DNS-Sec is added only the hash that represents the node. The client uses the X.509 adapted certificates and the DNSSec, together with new resource records per node, to authenticate the server. It supports DNS CNAME resource records in a transparent manner, without modifications to the certificates.

A TLS client was improved, from the Mozilla project, common to Firefox and Thunderbird, Web and e-mail clients, respectively. We have also created scripts that allow the automatic management of the certificates in a node and the update of the relevant records in DNS.