SecFuNet – Security for Future Networks

Djamel F. H. Sadok

Centro de Informática - Universidade Federal de Pernambuco (UFPE)
Caixa Postal 7851 - CEP 50732-970 – Recife – PE – Brasil

jamel@di.ufpe.br

Resumo. *A Internet do futuro será baseada principalmente na virtualização de redes e na computação em nuvens. Sendo assim, um dos maiores desafios para sua implementação será prover a esta arquitetura de redes virtualizadas e acesso as nuvens um alto grau de segurança. O projeto SecFuNet propõe o desenvolvimento de um arcabouço capaz de prover autenticação segura, identificação segura e transferência segura de dados, bem como uma infraestrutura segura de redes virtualizadas e a privacidade em redes virtuais e nuvens. Este desenvolvimento explorará técnicas baseadas em micro controladores, gerência de recursos, algoritmos tolerantes a intrusão e protocolos de criptografia. Este arcabouço será obtido através da elaboração e desenvolvimento de uma arquitetura coerente para redes virtuais e acesso as nuvens. A arquitetura proposta fornecerá soluções que permitam o gerenciamento da segurança das comunicações entre todas as máquinas conectadas a nuvens públicas, através das redes virtuais. Assim, se torna necessário a existência de um esquema coerente e robusto de identificação e um sistema robusto de autenticação. Os algoritmos robustos a intrusões são necessários para criar um ambiente seguro. A arquitetura proposta também precisa garantir a segurança na infraestrutura virtual através do isolamento destas redes e do controle de acesso para usuários e gerentes de rede. A identificação dos usuários autorizados não pode, no entanto, comprometer a privacidade dos dados. Além disso, é necessário desenvolver um esquema ergonômico de segurança que seja funcional para todos os usuários, mesmo aqueles que não possuem conhecimentos na área de computação. Finalmente, o esquema proposto deve levar em conta a heterogeneidade dos equipamentos (com ou sem fio), para preservar a interoperabilidade.*

A arquitetura proposta vai resolver cada um destes desafios através do uso de ilhas seguras de computação (micro controladores seguros como os utilizados em smart cards e em módulos confiáveis - Trusted Platform Module, TPM) que atuarão na identificação, autenticação e privacidade. A virtualização é outra ferramenta que será utilizada para resolver os desafios propostos. A infraestrutura virtualizada segura e os algoritmos robustos a intrusões vão garantir a estrutura necessária para se criar um ambiente seguro. Um ambiente seguro e um controle de acesso robusto se tornam, portanto, pilares essenciais para a construção da arquitetura segura proposta. Esta arquitetura pode ser dividida em diversas redes virtuais: a Internet legada que é utilizada atualmente, a nova Internet baseada na identificação robusta e na garantia da privacidade dos clientes, novas redes pós-IP, dentre outras. A arquitetura

proposta permitirá que estas redes virtuais compartilhem o mesmo substrato físico através da virtualização. A arquitetura garantirá o isolamento entre estas redes. Além disso, a utilização de micro controladores seguros permitirá o desenvolvimento de novos esquemas de segurança compatíveis com a Internet legado, que evitará a execução de alguns tipos de ataque existentes.

Os desafios resolvidos pelo projeto podem ser organizados nos seguintes work packages (WPs):

- *WP1: Nova arquitetura segura baseada em micro controladores seguros. O desenvolvimento de diferentes esquemas de segurança, como o EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) pode se beneficiar das ilhas seguras e coexistir com esquemas legados como o EAP-SIM (Extensible Authentication Protocol-Subscriber Identity Module). O aumento na segurança é derivado da execução de algoritmos criptográficos dentro das fronteiras seguras dos micro controladores ao invés da execução em computadores desprotegidos. Os micro controladores podem ser utilizados para acessar cada uma das redes virtuais, auxiliando a criptografia e outros algoritmos, além do que é proposto pelas TPMs.*

- *WP2: Servidor de autenticação com alta segurança com conjunto de micro controladores seguros, permitindo a privacidade dos usuários nas redes.*

- *WP3: Esquema de identificação segura baseada no uso de micro controladores seguros e infraestruturas de autenticação e autoração (IAAs) como o OpenID, Higgins e Shibboleth, que permitam o desenvolvimento de sistemas de gerência para esquemas de identidade federados.*

- *WP4: Esquema seguro para garantir o isolamento entre redes virtuais de forma que uma rede não consiga reduzir o desempenho de outras redes através de ataques. Além disso, prover um gerenciamento e controle seguro de recursos virtualizados através do esquema de identificação proposto, garantindo isolamento e privacidade nos recursos alocados para as redes virtuais.*

- *WP5: Resiliência contra ataques e falhas na infraestrutura.*

- *WP6: Esquemas criptográficos para a Internet legado e para a nova Internet.*

- *WP7: Ambiente de testes para a avaliação dos esquemas propostos assim como para a publicação em sítios web, documentos e artigos científicos.*