Resumo

Actualmente, muitas empresas estão a adoptar arquitecturas SOA (*Service Oriented Architecture*) para exporem/consumirem serviços, implementados na forma de WS (*Web Services*). Um dos objectivos do uso das arquitecturas SOA é permitir a integração de aplicações implementadas em ambientes heterogéneos e distribuídos que, muitas vezes, estão localizados para lá das fronteiras da própria organização.
Com a introdução deste novo estilo de arquitectura, surgiram também novas preocupações de segurança a ter em conta na implementação dos sistemas envolvidos. Como SOA permite a partilha de informação e processos entre organizações, foram introduzidas novas formas de interacção entre os componentes da arquitectura, surgindo também novos tipos de ataques aos sistemas. Estes ataques não são detectados/prevenidos pelas tecnologias de segurança tradicionais. Por consequência, uma empresa que necessite de implementar uma arquitectura SOA com exposição dos seus WS para o exterior, deverá também implementar as medidas de segurança mais adequadas para não colocar em perigo a restante infra-estrutura interna.
Este trabalho tem como objectivos a identificação dos novos riscos de segurança aos quais as arquitecturas SOA ficam expostas, identificação dos requisitos de segurança deste tipo de arquitecturas e das tecnologias já disponíveis para implementar algumas medidas de segurança específicas das arquitecturas SOA. No final deste trabalho, são sugeridas algumas medidas de segurança a implementar num caso prático, na arquitectura SOA do Banco BPI. Como já existem equipamentos de infra-estrutura disponíveis para introduzir alguma segurança nas arquitecturas SOA, no caso prático apresentado, está também descrito o processo de avaliação das XML *Security Gateways* existentes actualmente no mercado.

Abstract

Nowadays, many enterprises are adopting SOA (Service Oriented Architecture) to expose/consume services, implemented using WS (Web Services). One of the main

goals when using SOA is to allow application integration through heterogeneous and distributed environments that, many times, are located beyond the companies' boundaries.

With the introduction of this new style of architecture, new security concerns emerged, that are to be considered during system's implementation. As SOA allows the share of information and processes through different organizations, new types of interaction among the architecture's components were introduced, thereby emerging new types of system's attacks. These attacks aren't detected/prevented by the traditional security technologies. Consequently, a company that needs to implement SOA with WS accessed from the outside will have to implement new security measures and expose its services without endangering the security of the internal infrastructure.

The main goal of this work is the identification of the new security risks at which SOA will be exposed, identification of this type of architecture's security requirements and the technologies available to implement some security measures specific to the SOA. At the end of this work, some security measures are suggested that can be applied in a real SOA environment, at Banco BPI. As there are many types of equipment available that we can introduce at the infrastructure to add some security to the architecture, for this real case, the XML Security Gateways' process of evaluation is described.