

Resumo

O Sistema de Arquivo e Acesso Intranet (SAA), desenvolvido e utilizado na PT Comunicações, tem como objectivo complementar o sistema RETA (Recolha e Tratamento de Alarmes) e está inserido na arquitectura de gestão de alarmes. Este sistema, tal como todos do género, necessita de melhorias contínuas, sendo certo que a perfeição nunca será atingida. Mesmo assim, a vontade de melhorar foi determinante para avançar com este projecto ambicioso, que teve como objectivos a *Implementação de um Módulo de Autenticação e de Gestão de Perfis de Utilizador*.

Apesar de os objectivos serem claros, o meio para os atingir era à partida desconhecido, já que não estávamos familiarizados com este sistema. Assim, iniciámos um estudo pormenorizado do Sistema de Arquivo e Acesso Intranet, bem como de vários métodos de Autenticação Automática (do inglês *Single Sign On*).

Foi configurado e implementado um módulo de Autenticação Automática baseado em *Kerberos*, que permite aos utilizadores serem autenticados de uma maneira totalmente transparente e com maior segurança. Esta autenticação, que tira proveito da obrigatoriedade do utilizador ter de introduzir as suas credenciais de cada vez que faz o *login* na sua estação de trabalho, consiste numa troca de *tickets* entre a estação de trabalho do utilizador e um servidor *Kerberos* funcionando como *Key Distribution Center* (KDC). A primeira vantagem inerente a este método de autenticação é a diminuição do número de credenciais diferentes que cada utilizador tem de memorizar, visto que com este método o utilizador apenas tem de introduzir as suas credenciais uma única vez (quando faz *login* na sua estação de trabalho). Em segundo lugar, o aumento da segurança na autenticação, visto que nenhuma *password* é enviada para o servidor Web (em substituição é enviado um *ticket*).

Na continuidade do módulo de Autenticação Automática implementado, foi desenvolvido um método semi-automático de registo, onde praticamente todas as informações necessárias ao registo são obtidas através do servidor LDAP da PT Comunicações e automaticamente preenchidas no formulário de registo. O utilizador apenas tem de seleccionar o Domínio de Gestão onde deseja ser inserido e uma *password* de reserva, apenas utilizada caso o servidor *Kerberos* sofra alguma anomalia.

Um outro resultado obtido com este projecto foi o desenvolvimento e implementação de um módulo de Gestão de Perfis de Utilizador. Com este novo método de gestão, o perfil de cada utilizador é influenciado não só pelo seu perfil individual, mas também pelo perfil do Grupo de Gestão onde está inserido. Assim, a tarefa do Administrador é facilitada, visto que esta nova organização permite definir pormenorizadamente as funcionalidades a que cada colaborador tem acesso, bem como a camada da rede que terá de gerir.

Referimos ainda o facto que todas as funcionalidades mencionadas nesta dissertação passaram a fase de testes, e inclusive, encontram-se todas em ambiente de produção.

Abstract

The Archives and Intranet Access System (AAS) (from the Portuguese *Sistema de Arquivo e Acesso Intranet*) was created by and is used in PT Comunicações and aims at being a complement to the CAA system (Collection and Analysis of Alarms) (from the Portuguese *Recolha e Tratamento de Alarmes*) and is part of the architecture of the alarms management. Although perfection will never be obtained, this system, like all of the kind, needs continuous improvements. Therefore, the will to improve was fundamental to develop this ambitious project with the goal *Implementation of a Single Sign on and Users' Profiles Management Module*.

Although the aims were clear, the means to achieve them were unknown, given that there was no familiarity with this system. Consequently, a thorough study was conducted about the Archives and Intranet Access System, as well as about the several existing methods of Single Sign On.

A module of Single Sign On based on Kerberos was configured and implemented, allowing users to be signed on in a transparent and safe way. This authentication, which takes advantage of the fact that the user must insert their credentials each time they logon to their workstation, consists of an exchange of tickets between the user's workstation and a Kerberos server acting as a Key Distribution Center (KDC). The first advantage of this signing on method is the smaller number of different credentials that

each user must memorize, given that with this method the user must insert their credentials only once (when they logon to their workstation). Secondly, the signing on is safer, given that no password is sent to the Web server (instead of it a ticket is sent).

Within the context of the implemented Single Sign On module, it was created a semiautomatic register method, where almost all the information needed to the register is obtained through the LDAP server of PT Comunicações and it is automatically filled in in the register form. The user must only select the Management Domain in which they want to join and a backup password, only to be used if the Kerberos server suffers any anomaly.

Another result obtained with this project was the development and implementation of a Users' Profile Management module. With this new management method, the profile of each user is influenced not only by their own individual profile, but also by the profile of Management Group to which they belong. Therefore, the administrator's task is made easier given that this new organization allows a detailed definition of the functions to which each user may have access, as well as the network layer that they will have to manage.

Let us still add that all the functionalities mentioned in this report passed all the tests and are currently in a production environment.