

“CPAut” – Uma Arquitetura de Controle de Acesso para o CRS/INPE-MCT

**Luciano G. Machado, Érico M. H. Amaral, Roben C. Lunardi, Cristiano A. Berni,
Koiti Ozaki, Raul Ceretta Nunes**

Laboratório de Tolerância a Falhas GMicro/CT – Universidade Federal de Santa Maria
Av. Roraima, S/N, Bairro Camobi, CEP 91.501-970, Santa Maria, RS, Brasil

{luciano12,koitiosaki@gmail.com}
{erico,roben,cberni,ceretta}@inf.ufsm.br

***Resumo.** Este artigo descreve a implementação de um Portal Cativo, utilizando tecnologias WEB, que tem por finalidade garantir a confidencialidade e integridade de imagens de satélites e documentos restritos, manipuladas pelo CRS/INPE-MCT. Este modelo integra um mecanismo de controle de acesso e um sistema de autenticação e autorização de conexões a um repositório de informações, definido por meio de níveis de acessos baseados em um esquema de perfis.*

1. Introdução

A necessidade de implementação de medidas de Segurança da Informação tem crescido de maneira expressiva nos últimos anos. O valor da informação se tornou mais expressivo para as organizações, que muitas vezes tem em seu negócio um diferencial competitivo baseado unicamente em informações [Barros 2005].

Se não bastasse o valor das informações para suas detentoras, há ainda uma preocupação crescente dos governos e órgãos reguladores quanto à vulnerabilidade de certas informações. Escândalos recentes provenientes de alterações de informações contábeis de empresas forçaram a criação de leis e normas que trazem às empresas motivações adicionais para o tratamento do problema de segurança dessas informações. Além disso, incidentes que levaram ao vazamento de informações pessoais de milhões de consumidores também trouxeram preocupações quanto à proteção deste tipo de informação [Sêmola 2005].

A prevenção contra as ameaças citadas pode ser obtida através da aplicação de métodos de controle de acesso. O controle de acesso é importante para manter o sigilo do conteúdo dos dados e objetiva limitar as ações realizadas por usuários maliciosos, evitando a quebra da privacidade devido a acessos desnecessários ou não autorizados [Braecklein, 2004].

Este trabalho propõe um serviço de autenticação/autorização capaz de gerenciar o acesso às imagens mantidas e utilizadas no Centro Regional Sul / Instituto Nacional de Pesquisas Espaciais – Ministério da Ciência e Tecnologia (CRS/INPE – MCT), aliado a um custo reduzido e de fácil implementação, o qual é denominado CPAut. O serviço atua tanto sobre rede cabeada, quanto sobre rede sem fio, disponibilizando aos administradores da rede uma ferramenta específica para a gerência de permissões e

acessos às imagens.

O artigo está assim organizado: na seção 2 é descrito detalhadamente o serviço CPAut; na seção 3 é apresentado o protocolo que deve ser utilizado para acesso às imagens; na seção 4 é apresentado as conclusões e na seção 5 alguns trabalhos futuros.

2. O CPAut

Esta seção apresenta as funções do CPAut (seção 2.1), sua arquitetura (seção 2.2), seu funcionamento (seção 2.3) e alguns detalhes de sua implementação (seção 2.4).

2.1. Funções do CPAut

O CPAut é um serviço de autenticação/autorização desenvolvido para controlar o acesso dos usuários ao repositório de imagens de satélites do CRS/INPE, o qual permite que usuários legítimos, visitantes e integrantes do centro, tenham possibilidade de acessar dados e imagens de satélites em um repositório compartilhado. Além disso, permite aplicar restrições diferenciadas aos usuários, ou seja, nem todos os usuários terão os mesmos níveis de acesso. A figura 1 mostra uma visão simplificada do uso do serviço.

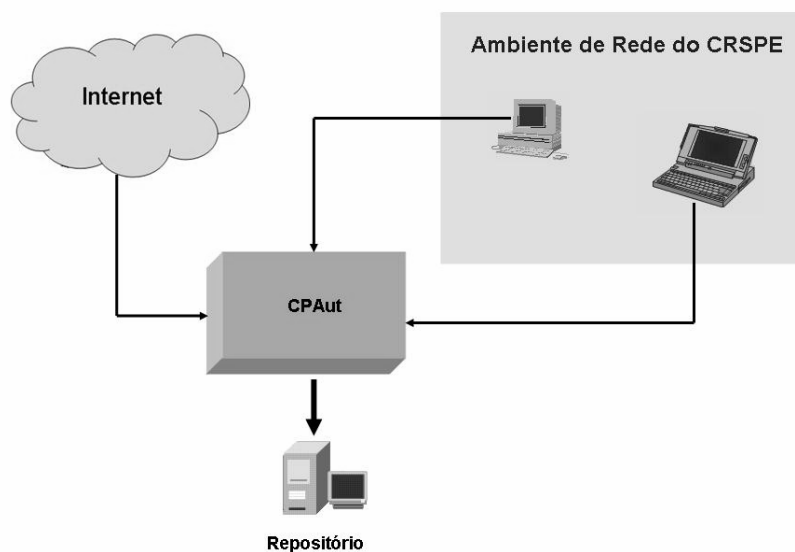


Figura 1 – Visão simplificada do serviço.

No CPAut, os usuários devem ser cadastrados em função de perfis pré-determinados pelos administradores da rede do CRS/INPE - MCT (Grupo de Suporte) ou através de uma página *web* disponibilizada pelo serviço.

A característica principal do serviço é definir um modelo de autenticação/autorização capaz de direcionar para uma página de *login* os usuários que desejem ter acesso ao repositório. Uma vez autenticados, os usuários terão o acesso ao repositório em função de seu perfil, ou seja, o controle de acesso é baseado em perfis [Ferraiolo et al. 2001].

A fim de agregar um nível de segurança adicional e obedecer as recomendações da política de segurança do CRS/INPE, o CPAut determina que usuários da rede sem fio do CRS devem autenticar-se no momento que se conectam à rede.

Observe que este serviço é uma aplicação baseada na idéia sugerida pelo uso de Captive Portals [Poger 1997], o qual estabelece que no momento em que um usuário desejar acessar o repositório de dados ele deve ser redirecionado a uma página de login, onde deverá fornecer informações necessárias a sua autenticação/autorização. Para garantir privacidade e confidencialidade, a conexão estabelecida entre o usuário e a página de login é criptografada (Protocolo SSL) entre as partes. No caso de sucesso (usuário e senha corretos), o usuário é considerado autenticado e terá acesso autorizado aos dados permitidos pelo seu perfil.

2.1. Arquitetura do CPAut

A arquitetura do CPAut é definida a partir de três componentes: Portal, NoCatAuth e Repositório de Imagens, conforme mostra a figura 2.

O Portal tem a função de cadastrar, autenticar e autorizar os usuários que desejam acessar o repositório de imagens e possui dois módulos: módulo Auth, cuja função é autenticar os usuários; e módulo Auto, responsável por determinar o nível de acesso do usuário.

O NoCatAuth é um componente opcional do CPAut, que nada mais é do que um Captive Portal responsável pela autenticação dos usuários da rede sem fio. Sua utilização fica limitada a instituições ou empresas que desejarem ter um grau de segurança maior para sua rede sem fio. Em locais onde não há conectividade sem fio sua aplicação não será necessária.

O Repositório de imagens é o componente responsável por disponibilizar os dados e imagens de satélites aos usuários. Ele organiza as informações em três diretórios: “publico”, “restrito” e “secreto”.

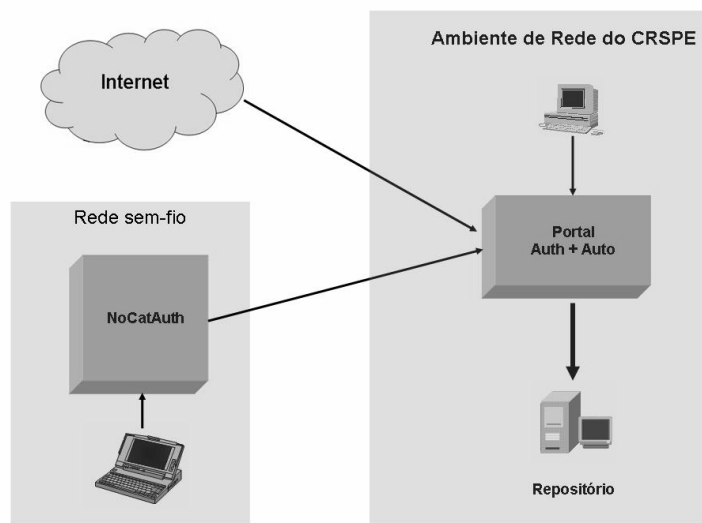


Figura 2 – Arquitetura do CPAut.

2.2. Funcionamento do CPAut

O funcionamento do CPAut é baseado em três atributos para autenticar/autorizar os usuários:

- modo de realização do cadastro;
- local de conexão da rede do usuário; e
- tipo de usuário.

Para o CPAut existem dois modos de realização do cadastro:

- via web; e
- via administrador de rede.

Os clientes que realizam cadastro via web são limitados a terem acesso apenas ao diretório “publico”, enquanto que para os usuários que realizarem cadastro via administrador de rede podem ter acesso a qualquer diretório.

Outra característica que influencia no perfil de acesso é o local em que o usuário está conectado a rede. Usuários conectados dentro da rede do CRS podem ter acesso a todos os diretórios, dependendo apenas do seu perfil (nível de acesso). Já os usuários conectados fora da rede do centro têm acesso limitado, podendo nesse caso acessar no máximo o diretório “restrito” (usuário nível 3 conectado fora do CRS) e nunca o “secreto”.

O CPAut também faz uma outra diferenciação entre usuários:

- móveis; e
- não-móveis.

Os usuários móveis são os que usufruem de dispositivos móveis para através de uma rede sem fio (*wireless*) terem acesso ao repositório dados e imagens de satélites. De acordo com a política de segurança o CPAut define um grau de segurança adicional a estes usuários. Como uma rede sem fio é sabida menos segura do que uma rede convencional, o CPAut força estes usuários a autenticarem-se para obterem acesso a rede do CRS. Desta forma, estes usuários passam por autenticação em duas fases: primeira, uma autenticação inicial para conectar-se a rede; e segunda, uma nova autenticação e conseqüente autorização necessária para poderem ter acesso ao repositório.

2.3. Implementação do CPAut

A implementação do CPAut foi dividida em três partes: instalação do NoCatAuth, implementação do módulo principal do CPAut, chamado Portal, e implementação do repositório de dados e imagens. A seguir é detalhada cada uma destas partes.

2.3.1. NoCatAuth

Módulo responsável pela autenticação dos usuários móveis. Para sua instalação foram necessárias duas máquinas: *Gateway* e Servidor de Autenticação. O *Gateway* possui duas interfaces de rede, uma responsável pela conexão à *Internet* e a outra responsável por distribuir endereços IP e redirecionar os usuários móveis a uma página de *login*. O Servidor de Autenticação contém a base de dados dos usuários.

Seguiu-se a recomendação do desenvolvedor do NoCatAuth de instalar o

Gateway e o Servidor de Autenticação em máquinas separadas para garantir um maior nível de segurança.

2.3.2. Portal

Módulo principal deste trabalho, o qual deve cadastrar e autenticar/autorizar usuários antes de dar acesso ao repositório de imagens de satélites. Sua implementação foi desenvolvida na linguagem PHP e o gerenciador de banco de dados utilizado foi o MySQL.

A comunicação entre CPAut e usuários é realizada através de um canal seguro (Protocolo SSL), onde todo o tráfego de informações é criptografado entre ambas as partes.

Para o cadastro o CPAut verifica se o endereço IP do usuário faz parte da rede do CRS. Esta verificação influi nos campos do cadastro que é retornado ao usuário. Para os usuários oriundos da rede interna do CRS, o cadastro requer que sejam preenchidas um número maior de informações. Já os usuários da *Internet* preenchem um cadastro básico em virtude de terem acesso apenas ao diretório “publico”.

O módulo Auth é responsável por receber as informações do usuário (*login* e senha), abrir uma sessão e verificar na base de dados de usuários se o mesmo é cadastrado e dessa forma autenticá-lo.

O módulo Auto vai analisar o cadastro do usuário através de seu *login*, consultar alguns campos e definir o nível de acesso do usuário. A consequência desta operação são os diretórios que são retornados para o usuário.

Para cada um dos diretórios é verificado se existe uma sessão registrada (sessão aberta na página de *login*), caso contrário, não é permitido o acesso ao diretório e o usuário é direcionado a página inicial do CPAut.

2.3.3. Repositório de Dados e Imagens

Módulo com a finalidade de disponibilizar aos usuários dados e imagens de satélites através de uma conexão segura (HTTPS). O repositório tem sua estrutura de dados organizada através de três diretórios: “publico”, “restrito” e “privado”.

Sua implementação foi sobre a plataforma Linux Fedora e o servidor Web utilizado foi o Apache.

3. Protocolo para Acesso às Imagens de Satélites

Os usuários que desejarem ter acesso as imagens devem seguir o protocolo abaixo:

1. O usuário ao tentar acessar a página do repositório de imagens é direcionado a uma página de *login*/cadastro;
2. Caso seja cadastrado, deverá entrar com suas informações de usuário e senha para que o CPAut possa autenticá-lo. Do contrário deverá preencher seu cadastro via *web* ou procurar o administrador de rede do CRSPE para cadastrá-lo;
3. Após sua autenticação, seu perfil é verificado pelo CPAut e os diretórios adequados são disponibilizados; e

4. O usuário pode visualizar as imagens permitidas e/ou fazer *download* para sua máquina.

Convém ressaltar que o protocolo anterior só pode ser seguido pelos usuários móveis após seu acesso a rede ser autenticado pelo NoCatAuth.

4. Conclusões

O advento e a conseqüente abrangência da *Internet* nos dias atuais, permitiram a facilidade ao acesso à informações e documentos por qualquer pessoa em qualquer parte do mundo. Num primeiro instante, pode-se avaliar essa situação como amplamente vantajosa, mas, num segundo instante, constata-se que existem determinadas informações que são de caráter confidencial ou sigilosas, e que são capazes de ameaçar, por exemplo, o direito de privacidade de uma pessoa ou de uma instituição. Motivado por esta nova demanda de segurança, este trabalho desenvolveu uma arquitetura capaz de controlar o acesso a determinado tipo de informação sem a necessidade de instalar programas clientes nos dispositivos dos usuários do sistema e sem custos adicionais para o CRS/INPE – MCT.

Ao término deste trabalho conclui-se que com uma arquitetura simples baseada em portal captivo pode-se atender a requisitos do cliente, no caso específico deste trabalho o CRS/INPE, pois atrela um nível de segurança maior para os dados e imagens de satélites armazenadas em repositórios compartilhados mas com dados que devem ser disponíveis em função do perfil do cliente.

Adicionalmente, o CPAut assume um caráter genérico, podendo ser adaptado, com pequenas alterações, a outros tipos de informações que se deseje disponibilizar.

5. Trabalhos Futuros

Como trabalhos futuros, prevê-se a substituição do módulo Auto do CPAut por um módulo de controle de acesso baseado em contextos. A utilização desse módulo possibilitará o uso mais eficiente ao modelo, ampliando o espectro de aplicações. Para tal é necessário agrupar informações na forma de Contextos e isolar a lógica que trata políticas de controle de acesso da lógica que trata da imposição da política (regras).

Também como trabalho futuro prevê-se migrar toda a implementação do CPAut da linguagem PHP para a linguagem Java e implementar a geração de arquivos de *log* dos usuários. Com isto acredita-se poder obter um melhor nível de segurança.

Agradecimentos

Este projeto é parte do convênio de cooperação INPE/UFSM, no qual trabalham a equipe de suporte do CRS/INPE e os pesquisadores do Laboratório de Tolerância a Falhas do GMicro/UFSM, apoiado por fundos de pesquisas de ambas instituições.

Referências

- Amaral, E. M. H. (2005), Segurança em Redes Wireless – Proposta de um Serviço de Autenticação Baseado em Agentes Proxy, Trabalho de Graduação, UFSM, 2005.
- Barros, A. Q. P. de, (2005), Tendências do Mercado de Serviços de Segurança da Informação.

- Booch, G.; Rumbaugh, J. & Jacobson, I., (1999), "The Unified Modelling Language User Guide", Addison Wesley Longman, Inc., 1999. 1, p.19-36, abr.
- Braecklein, M.; et all. (2004), "New System Cardiological Home Monitoring With Integrated Alarm Function." OpenECG Workshop, Berlin.
- Brinkley, D. L.; Schell, R. R. (1995) Concepts and Terminology for Computer Security. In: Abrhams, M. D.; Jajodia, S.; Podell, H. J. (Ed.). Information Security: an Integrated Collection of Essays. Los Alamitos, CA: IEEE Computer Society Press, jan. 1995. p.40-97.
- Chang, P., Ishii, H. (1999), Implementing Secure Services over a Wireless Network – A Captive Portal and Traffic Shaping Approach. Independent Study in Advanced Networks, San Francisco State University.
- Ferraiolo, D. F., Sandhu, R. S., Gavrila, S. I., Kuhn, D. R., and Chandramouli, R. (2001). Proposed NIST standard for role-based access control. Information and System Security, 4(3):224–274.
- Poger, E., Baker, M. G. (1997), Secure Public Internet Access Handler (SPINACH). Computer Science Department, Stanford University
<http://mosquitonet.stanford.edu/publications/spinach.html>
- Sêmola, M. (2003) Gestão da Segurança da Informação: Uma visão executiva. Editora Campus.