Sistema de Registro de Estações da UFRGS

**Caciano Machado, Daniel Soares, Leandro Rey, Luís Ziulkoski,
Rafael Tonin, Clarissa Marchezan, Eduardo Postal, Eduardo Horowitz**

[1]Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS

{caciano,daniel,leandro,luis,rtonin}@cpd.ufrgs.br

{clarissa,ecpostal,eduardoh}@inf.ufrgs.br

Resumo. *Atualmente, o processo de registro de IPs da UFRGS é realizado pelos administradores das subredes de cada unidade. Problemas como trocas indevidas de IP, roubos de IP, crescente utilização das redes sem fio e falta de administradores de rede em algumas unidades acabam dificultando o registro adequado das estações. Visando a facilitar o trabalho de gerenciamento foi projetado um novo Sistema de Registro de Estações inspirado em sistemas de NAC e em outros sistemas de registro. O sistema proposto se baseia na delegação do processo de registro para os próprios usuários e no uso de DHCP para a configuração das estações. Cada máquina que ingressa na rede é obrigada a realizar autenticação do usuário que se torna responsável pela máquina. O sistema é baseado em ferramentas de código aberto, prevê uma interface WEB para gerenciamento e suporte à rede sem fio.*

1. Introdução

O Sistema de Registro de Estações projetado auxilia os administradores delegando a tarefa de registro de estações para os usuários. No processo de registro são solicitadas as credenciais do cartão do usuário. Também são previstas uma interface WEB para gerenciamento dos registros de estações, uma rede sem fio isolada da rede corporativa da UFRGS para visitantes e usuários registrados, e uma rede cabeada também isolada da rede corporativa para as residências estudantis.

Foram herdadas algumas características encontradas em sistemas conhecidos como NAC. Os sistemas de NAC têm como foco permitir o ingresso apenas de máquinas que estejam em conformidade com especificações mínimas de configuração e segurança estabelecidas pela organização. O sistema proposto é bastante similar ao NetReg, desenvolvido pela Universidade de Carnegie Mellon, onde o foco é o gerenciamento das estações.

Serão apresentadas adiante a motivação para o desenvolvimento do novo sistema, e as soluções comerciais e de código aberto nas quais o sistema foi inspirado. Em seguida serão detalhados os principais elementos do sistema e um exemplo de funcionamento do registro de estação. Para finalizar apresentaremos as conclusões e considerações finais.

2. Motivação

Atualmente, a UFRGS utiliza um sistema de controle de IPs que permite o registro das estações, seus respectivos serviços e pessoas responsáveis. Entretanto, alguns problemas

tais como a falta de gerentes de rede em algumas unidades, expansão das redes sem fio e trocas/conflitos/roubos de IP indevidos (gerados por *Rogue Users* ou *Malware*) impedem que o sistema seja eficaz no controle das estações.

Os problemas listados, entre outros, implicam em uma quantidade de atribuições de endereços para as estações que os administradores não conseguem acompanhar sem comprometer suas demais atividades. Configurar as estações em um ambiente como o da UFRGS é uma tarefa onerosa e de difícil manutenção. Uma solução para isso é passar o trabalho do registro das estações para o próprio usuário. Nessa abordagem, cada máquina nova que ingressar na rede corporativa (cabeada ou sem fio) deve passar por um processo de registro baseado na identidade do usuário que associa a estação com um integrante da Universidade.

A solução proposta possibilita a realização de testes de vulnerabilidades e configuração das estações durante o processo de registro. Essa etapa do registro é característica de sistemas de NAC e ainda não foi implementada no sistema da UFRGS.

3. Soluções Existentes

O Sistema de Registro de Estações herdou algumas características de soluções comerciais abertas. Os sistemas de NAC (*Network Access/Admission Control* ou *Network Node Validation*) [Conover 2006] comerciais mais conhecidos e alguns sistemas de registro de estação abertos serão apresentados a seguir.

3.1. NAC

Uma das alternativas para os problemas de rede da UFRGS seria a utilização de sistemas de NAC. Os sistemas de NAC visam a controlar o acesso de dispositivos em uma rede protegida. Esse tipo de sistema assegura que apenas máquinas que estejam em conformidade com determinadas políticas de segurança consigam ingressar na rede. Essa medida minimiza incidentes de segurança e restringe o acesso à rede somente para computadores confiáveis. Cada vez que um dispositivo novo ingressa na rede ele será submetido a autenticação do usuário da rede, e a algum mecanismo de verificação de contaminação e vulnerabilidades.

Um sistema de NAC define uma ou mais das seguintes funcionalidades: avaliação de vulnerabilidades e configuração da estação antes da admissão; quarentena e remediação de estações comprometidas; controle de acesso à rede baseado na identidade do usuário; controle de recursos baseado na identidade do usuário e políticas; análise contínua de ameaças.

Entre os sistemas mais conhecidos e utilizados estão o Cisco NAC, Microsoft NAP e o TNC. Apesar de oferecerem soluções bastante completas, os sistemas de NAC comerciais foram descartados para implantação na UFRGS por apresentarem um custo muito elevado para o grande número de estações da Universidade (aproximadamente 10000). Além disso, a necessidade maior da UFRGS é de um sistema que facilite a gerência das estações e esse não é o foco dos sistemas de NAC.

3.2. NetReg

A solução na qual o sistema da UFRGS foi inspirado é o CMU NetReg [CMU NetReg]. O NetReg se baseia no registro de estações através da autenticação dos usuários. Atual-

mente, esse sistema é utilizado por várias outras instituições além da Universidade Carnegie Mellon.

O princípio de funcionamento do sistema é a utilização de um servidor de DHCP que distribui IPs temporários para máquinas ainda não registradas. Com esses IPs temporários os usuários das máquinas ingressam em uma rede isolada onde são submetidos a autenticação e podem registrar as estações via interface WEB. Após realizar o registro a máquina obtém acesso pleno à rede definitiva.

O sistema possui uma interface WEB que permite o gerenciamento das subredes, estações registradas, opções de DHCP, opções de DNS e a geração de relatórios de utilização dos recursos de rede. O sistema permite o bloqueio das máquinas diretamente nas portas dos *switches* que possuam tecnologia 802.1x [Congdon et al. 2003]. Apesar de oferecer uma solução bastante completa e eficiente o CMU NetReg não se adequou às necessidades da UFRGS pois o modelo do banco de dados do NetReg torna difícil a integração com as aplicações da Universidade. Por causa das dificuldades em encontrar um sistema que se adequasse à realidade da UFRGS decidiu-se projetar um novo modelo de banco de dados onde as necessidades de integração com as aplicações existentes são levadas em consideração.

4. Sistema de Registro de Estações

A seguir serão apresentados as principais características do cenário proposto para o Sistema de Registro de Estações da UFRGS e uma ilustração de um registro de estação. Também será feita uma breve descrição das redes sem fio e outras redes cabeadas associadas ao sistema.

4.1. Topologia da Rede

A rede da UFRGS é dividida em subredes com máscara de 24 bits. Cada uma dessas subredes é subdividida em blocos administrativos cuja responsabilidade é delegada para uma ou mais pessoas. Esses blocos são formados por conjuntos contíguos de IPs, ou seja, não podem haver conjuntos com números de IPs esparsos.

Para cada subrede válida cria-se uma outra subrede chamada de Rede Bogus que é utilizada pelo usuário durante o processo de registro. Por exemplo, a subrede 143.54.34.0/24 possui uma rede 10.54.34.0/24. Essas subredes compartilham o mesmo nível de enlace mas somente os IPs da Rede Real tem o tráfego liberado para a Internet.

4.2. DHCP e DNS

O sistema da UFRGS utiliza um servidor DHCP (ISC DHCPv3) [DHCP] centralizado para onde são encaminhadas as solicitações de DHCP das subredes. Esse servidor distribui IPs tanto para as máquinas que ainda não foram registradas (IP da Rede Bogus) quanto para as máquinas que já foram registradas (IP da Rede Real).

As configurações do servidor são definidas pelas informações de subrede, blocos, IPs e respectivas opções de DHCP contidas no banco de dados do sistema. Essas informações são passadas para o servidor de duas maneiras diferentes: criando novamente o arquivo de configurações do DHCP ou via interface OMAPI (Object Management API) [DHCP]. As operações via OMAPI permitem atualizar remotamente configurações

específicas do DHCP sem a necessidade de reinicializar o servidor contribuindo para a disponibilidade do serviço.

As operações possíveis de serem realizadas via OMAPI incluem a manipulação de objetos *host* e *group* que permitem, respectivamente, a criação e remoção de estações e a manipulação de blocos. O OMAPI não define objetos de subredes, logo é necessário criar novamente o arquivo de configuração do DHCP e reiniciar o servidor para operações com subredes.

As subredes, blocos e IPs podem ter configurações DHCP diferentes. Em caso de configurações conflitantes a prioridade das configurações segue a seguinte ordem, da mais prioritária para a menos prioritária: IP, bloco e subrede.

4.3. Perfis de usuário

O modelo do sistema prevê perfis de usuário que são atribuídos aos registros. Podem ser criados perfis para alunos, professores, funcionários ou qualquer outra classe de usuário que se deseje. Cada perfil define opções de DHCP que determinarão como a máquina do usuário será configurada. Entre as opções possíveis estão o tempo de duração do registro (*lease time*), servidores de DNS e Proxy HTTP.

4.4. Interface WEB do Sistema de Registro

A utilização da interface WEB é destinada aos responsáveis pelos blocos de subrede e administradores do sistema de registro. A interface prevê as seguintes funcionalidades: gerenciamento das subredes, blocos e IPs; bloqueios de IPs; pré-registro de estações; definição de permissões dos responsáveis pelos blocos; definição de opções DHCP.

O pré-registro permite que os responsáveis pelas subredes registrem estações sem a necessidade de utilizar a Rede Bogus. Essa funcionalidade é útil para registrar estações que não possuem navegador WEB ou mesmo para agilizar o processo de registro. Por exemplo: servidores, roteadores, estações de laboratórios de graduação, estações de salas de aula e telefones IP.

4.5. Redes sem fio corporativa, de Visitantes e Casas do Estudante

As redes sem fio também estão previstas no sistema. Para isso foi definido um mecanismo de autenticação dos usuários da UFRGS via Radius. O processo de autenticação de usuários da rede sem fio permite que seja obtido acesso à camada de enlace da subrede associado ao SSID selecionado. Após a autenticação na rede sem fio corporativa o usuário deve realizar o processo de registro da estação da mesma maneira que uma estação da rede cabeada.

A Rede de Visitantes é uma rede sem fio que permite o acesso de usuários através do número do cartão da UFRGS ou de *tickets* criados previamente. Para implantação da rede foi adotado o sistema de controle de acesso CoovaChilli [CoovaChilli], que opera como *gateway* de subrede. Foi implementado também um esquema de bloqueio de estações baseado na associação usuário-MAC que é feita pelo CoovaChilli.

Devido ao número elevado de incidentes de segurança, tentativas compartilhamento ilegal de arquivos e roubos de IP que ocorrem nas residências estudantis da UFRGS decidiu-se utilizar o CoovaChilli também nessas unidades. O esquema de bloqueio de

estações baseados em usuário e MAC é mais eficiente nesse ambiente onde as trocas de IP indevidas são freqüentes.

4.6. Processo de registro de estação

O procedimento de registro de estação típico segue basicamente os seguintes passos ilustrados nas Figuras 1, 2 e 3. O registro de estações foi validado na rede do CPD da UFRGS.

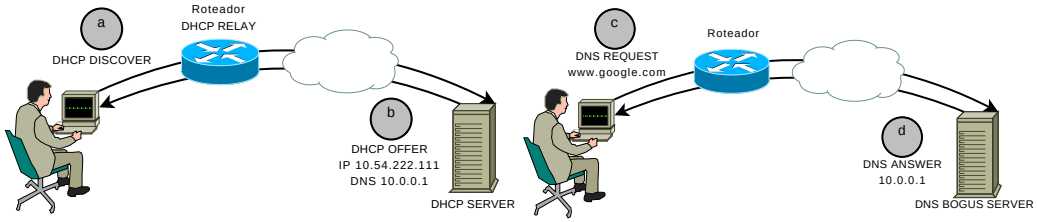

Figura 1. DHCP e DNS para Rede Bogus

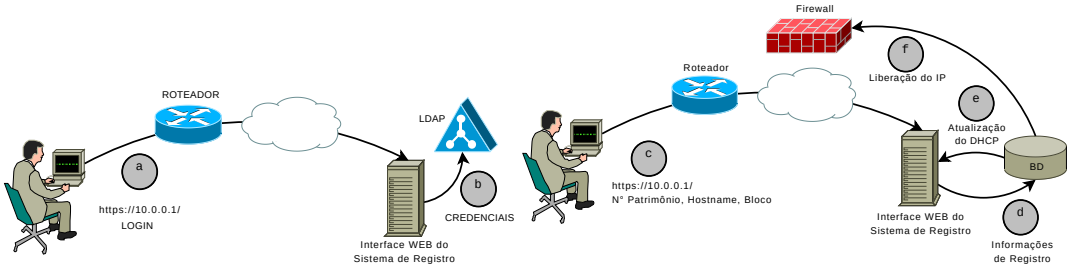

Figura 2. Registro de Estação

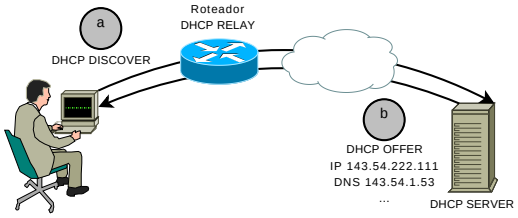

Figura 3. DHCP para Rede Real

1. Roteador da subrede repassa a requisição DHCP da máquina não registrada (1.a) para o servidor que por sua vez fornece um IP da Rede Bogus juntamente com um DNS Bogus (1.b).
2. Usuário requisita uma página WEB qualquer (1.c) e o servidor DNS Bogus informa o endereço da página de registro (1.d) ao invés do endereço da página solicitada.
3. Usuário acessa a página de registro e informa suas credenciais da UFRGS (número do cartão e senha) (2.a) para autenticação no LDAP institucional (2.b).
4. Usuário informa o número de patrimônio da estação, nome da estação e o bloco da subrede que deseja ingressar (2.c) [1]

[1]Os blocos das subredes compartilham o nível de enlace, logo não é possível atribuir automaticamente um bloco para a estação

5. Os dados do registro são armazenados no banco de dados (2.d), e o servidor DHCP (2.e) e o *firewall* (2.f) são atualizados.
6. Usuário reinicia sua interface de rede, faz uma requisição DHCP (3.a) e recebe um IP válido (3.b).

O exemplo apresentado é o caso mais típico de operação de registro. Existem vários outros casos previstos no modelo e foram omitidos alguns detalhes nessa simplificação.

5. Conclusão e Considerações Finais

O sistema de registro de IPs atual não atende às necessidades da Universidade. O novo Sistema de Registro de Estações foi projetado com os problemas apresentados em mente e visa a atenuá-los de diversas formas. A necessidade de autenticação do usuário para registro da estação é a peça chave do sistema pois livra o administrador da subrede dessa tarefa.

Como primeiro passo para a implantação do sistema de registro pretende-se implantar o CoovaChilli em uma das Casas do Estudante. Assim será possível testá-lo em ambiente de produção. Após sua validação, a rede sem fio de visitantes será colocada em operação. Em seguida será implantada a rede sem fio corporativa. Quanto à rede cabeada corporativa, serão selecionadas algumas unidades piloto da Universidade para adotar do novo sistema antes que ele seja definitivamente implantado.

Depois da implantação do sistema em todas as unidades será dada ênfase nos procedimentos de verificação de vulnerabilidades das estações. Para isso deverão ser definidas políticas de segurança adequadas ao ambiente da Universidade.

O uso do sistema integrado ao serviço de DHCP facilita o gerenciamento das estações da UFRGS e mantém atualizadas suas informações. Além disso, a operação de registro não é uma tarefa complicada e não necessita de treinamento dos usuários para sua realização. Após os testes que já foram realizados, tanto na rede corporativa quanto na rede de visitantes, acredita-se que o sistema trará um grande benefício para a gerência de rede e segurança dos usuários.

Referências

CMU NetReg. Carnegie mellon university network registration system. Disponível em: http://www.net.cmu.edu/netreg/. Acesso em: março de 2008.

Congdon, P., Aboba, B., Smith, A., Zorn, G., and Roese, J. (2003). Ieee 802.1x remote authentication dial in user service (radius) usage guidelines.

Conover, J. (2006). Nac vendors square off. In *Network Computing*, pages 55–64.

CoovaChilli. Coovachilli. Disponível em: http://coova.org/wiki/index.php/CoovaChilli. Acesso em: março de 2008.

DHCP. Dynamic configuration host protocol. Disponível em: http://www.isc.org/sw/dhcp/. Acesso em: março de 2008.