Sistema de Registro de Estações da UFRGS como Ferramenta de Segurança

João Ceron, Leandro Rey, Arthur Boos Jr, Caciano Machado, Fernando Macedo, Fábio Bringhenti, Marcio Pohlmann

[1] TRI - Time de Resposta a Incidentes de Segurança da
Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS

{ceron,leandro,boos,caciano,fmacedo,fbringhenti,marcio}@cpd.ufrgs.br

Resumo. *O Sistema de Registro de Estações da UFRGS foi desenvolvido para facilitar a gerência dos dispositivos com acesso à rede na universidade. No entanto, para o seu correto funcionamento é necessário monitorar e identificar possíveis exceções no sistema. Problemas de configuração de dispositivos e usuários mal intencionados devem ser rapidamente identificados pelo sistema. Este documento descreve as técnicas incorporadas ao sistema da UFRGS para auxiliar na administração de tais exceções.*

Introdução

A identificação dos usuários que acessam uma rede é um processo fundamental para garantir a política de segurança de uma instituição. Porém, identificar o usuário responsável por um determinado endereço passa por várias etapas como autenticação, autorização e contabilidade [Vollbrecht et al. 2000]. O controle da alocação de endereços IPs aos dispositivos é fundamental neste processo, auxiliando na organização e segmentação das redes de cada unidade da universidade.

Tarefas relacionadas com a alocação de IPs são complexas, sobretudo em ambientes heterogêneos como nas universidades públicas. Problemas como falta de gerentes de rede em algumas unidades acadêmicas, expansão de redes sem fio e a manutenção do endereçamento - trocas e conflitos de IPs - são muito onerosas para os administradores de rede. A complexidade da gerência deste processo bem como os problemas listados acima, motivou o desenvolvimento de uma solução automatizada. A Universidade Federal do Rio Grande do Sul desenvolveu o *Sistema de Registro de Estações da UFRGS*, denominado simplesmente SRE. O SRE foi concebido para controlar e identificar dispositivos conectados na rede, adaptando-se a necessidades particulares da própria universidade. Na solução desenvolvida é possível associar a cada dispositivo um responsável e um endereço IP, tudo sem a mediação de um gerente de rede. Isso é feito delegando a tarefa de registro de estações para os próprios usuários, que com o com o auxílio de uma base de dados central podem se identificar na rede.

Entretanto, alguns procedimentos devem ser seguidos pelos usuários e administradores de rede para assegurar o correto funcionamento do sistema, evitando, por exemplo, a ocorrência de endereços IPs duplicados e violações da política de segurança da

instituição. Para isso, tornou-se necessário desenvolver um conjunto de ferramentas e mecanismos que facilitem o gerenciamento do sistema de registro. Este trabalho, portanto, tem por objetivo descrever o conjunto de mecanismos desenvolvidos no *Sistema de Registro de Estações da UFRGS* que visam garantir as conformidades da política de acesso e segurança da instituição.

Este documento está organizado da seguinte forma: na seção são apresentadas características que devem ser observadas para a operação do sistema; na seção são discutidos os mecanismos implementados para a identificação e mitigação de anomalias; na seção os resultados são apresentados; por fim, as conclusões e considerações finais são descritos na seção .

Requisitos Funcionais

O *Sistema de Registro de Estações da UFRGS* caracteriza-se por realizar uma série de tarefas, como por exemplo, alocação dinâmica de endereços, gerenciamento de blocos de rede, funcionalidades dos dispositivos, histórico de utilização, entre outros serviços.

Algumas características da implementação foram inspiradas em sistemas já estabelecidos como o NAC (*Network Access Control*) [Conover 2006] da Cisco e o NetReg [CMU NetReg]. Os detalhes técnicos da implementação do SRE bem como suas funcionalidades fogem do escopo deste trabalho, afinal os mesmos já foram apresentados em outras edições do *workshop* [Tonin et al. 2008] e [Machado et al. 2009]. De uma forma geral, a implementação do SRE buscou observar as particularidades da própria universidade, um cenário bastante heterogêneo quanto aos dispositivos de rede. A infraestrutura de rede, como *backbone*, distribuição e acesso, apresentam uma gama de equipamentos que em sua maioria não suportam protocolos que facilitariam o controle de acesso, como por exemplo o protocolo 802.1x [Congdon et al. 2003]. Este cenário híbrido e pré-802.1x serviu como base para a definição dos vetores funcionais da solução de gerenciamento da UFRGS, o *Sistema de Registro de Estações*.

O princípio básico de funcionamento do SRE consiste no registro de novas estações, que é realizado pelo próprio usuário via interface Web. Este processo coleta informações do responsável pela máquina e também dados sobre o próprio dispositivo solicitante. Uma das principais atribuições do processo de registro é atrelar um endereço fixo IP a um dispositivo. Desta forma, nos próximos acessos o dispositivo registrado recebe o seu endereçamento automaticamente, sem intervenção de terceiros. O SRE, por sua vez, mantém na sua base de dados o responsável pelo endereço atribuído possibilitando uma fácil identificação do usuário.

O funcionamento apropriado do sistema depende da configuração das máquinas dos usuários e do seu registro na base de dados do SRE. O sistema deve assegurar que os dispositivos utilizem a configuração automática de endereçamento de rede e passem pelo processo de registro de estações. Tais premissas visam garantir para cada dispositivo uma relação única entre endereço de rede e endereço físico (IP,MAC). A duplicação de endereçamento físico (MAC) ou de rede (IP) causa diversos transtornos para os administradores de rede, como por exemplo:

a) inconsistência na base de dados - as informações vigentes na rede não refletem o estado da base de dados, ou seja, o IP registrado para um dispositivo está sendo utilizado por outro de forma irregular.

b) problemas de acessos - a duplicação de IPs na rede gera exceções em equipamentos influenciando na operação do dispositivo. Como resultado, as máquinas com o mesmo endereçamento de rede sofrem problemas de acesso.

c) bloqueios indevidos - naturalmente a filtragem de um endereço IP duplicado irá bloquear todos os dispositivos utilizando o mesmo endereço, inclusive o usuário que está utilizando de forma legítima.

Para que as exceções acima pudessem ser manejadas um conjunto de mecanismos foi desenvolvido e incorporado ao sistema SRE. Na sequência, serão discutidos métodos para a identificação de tais problemas e, posteriormente, formas para a mitigação dos mesmos.

Mecanismos de Gerenciamento de Segurança

A utilização dos recursos da rede deve ser constantemente verificada para satisfazer a política de acesso da instituição. O processo de verificação de exceções consiste em duas fases: identificação e mitigação de não conformidades do sistema. Na sequência, as fases são abordadas com maior nível de detalhamento.

Identificação

Na fase de identificação de exceções são apresentados aos gerentes dispositivos que não estão seguindo a política de acesso da instituição, como por exemplo, máquinas que não estão corretamente configuradas. Os dispositivos que estão utilizando um endereçamento IP indevido - não atribuído ao mesmo - são classificados como *rogue users*. A rápida identificação destes usuários impede que conflitos sejam gerados na rede e também no sistema de registro. Atualmente, a identificação de usuários *rogue* é implementada em duas etapas:

Coleta - esta etapa consiste em criar uma base de dados com todos os endereços MAC utilizados na rede da universidade. Os dados são computados a partir das tabelas ARP dos roteadores do *backbone*. Processo esse que é realizado periodicamente via requisições SNMP [Case et al. 1990].

Processamento - os MACs coletados na etapa anterior são comparados com os registrados no sistema de registro. Em caso de incongruências, alertas são gerados informando ao administrador da rede qual dispositivo está utilizando o endereçamento indevido.

Todo os dispositivos identificados como *rogue* são armazenados na base de dados do sistema e apresentados por uma interface Web (figura 3) ao gerente. Além de listar os dispositivos, a interface possibilita consultar os registros de *rogue* numa janela específica de tempo, definida pelos calendários na parte superior. A parte inferior da referida figura é responsável por exibir os registros classificados com *rogue* respectivamente: endereço de rede, endereço físico, data da última observação, e se o mesmo consta bloqueado no sistema.

O processo de identificação de usuários em estado *rogue* é relativamente simples, conforme descrito acima. No entanto, a localização física dos dispositivos de forma a desabilitá-los é uma tarefa complexa. Para isto foi desenvolvido uma ferramenta que faz uma varredura em todos os dispositivos da rede (*switches*) localizando de forma hierárquica o equipamento e porta na qual o respectivo MAC está presente. A interface desta ferramenta é apresentada na figura 2.

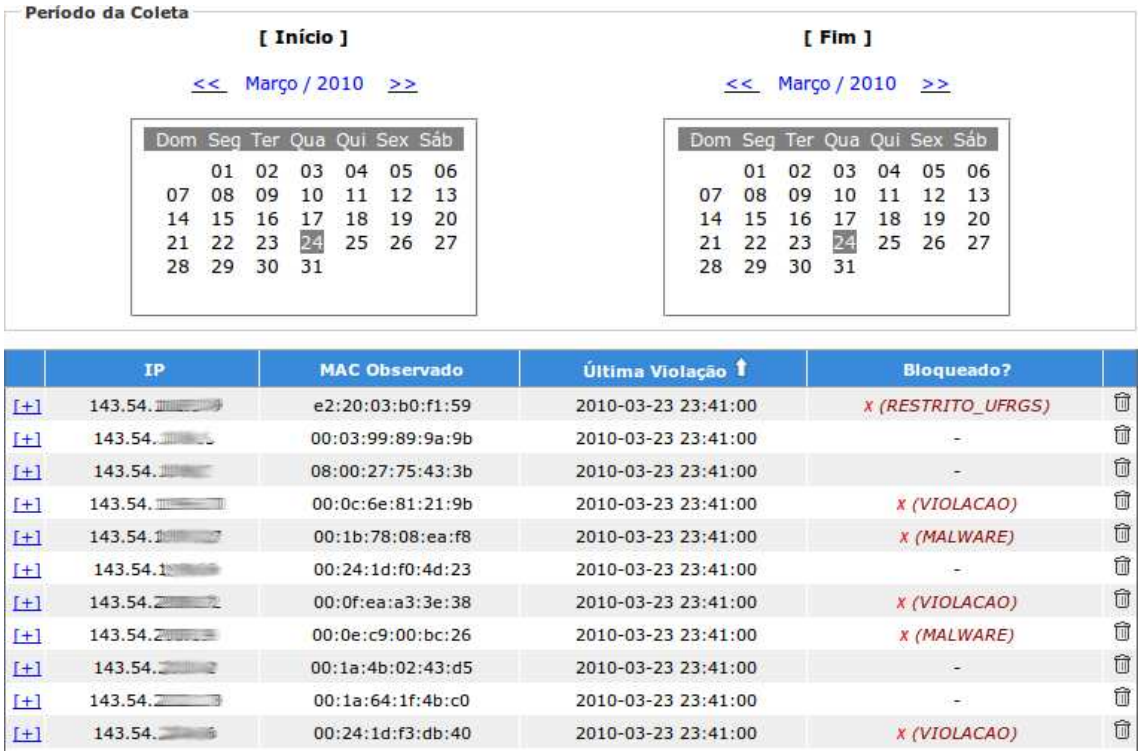


Figura 1. Interface para o gerenciamento de usuários em estado *rogue*.

Da mesma forma que a anterior, a interface dessa ferramenta permite definir um intervalo de tempo para a consulta de um endereço físico. Como resultado é apresentada uma lista de dispositivos nos quais o MAC consultado foi observado. Essas informações auxiliam o gerente da rede a identificar fisicamente uma máquina na sua unidade e, se for o caso, a corrigir a configuração do dispositivo.

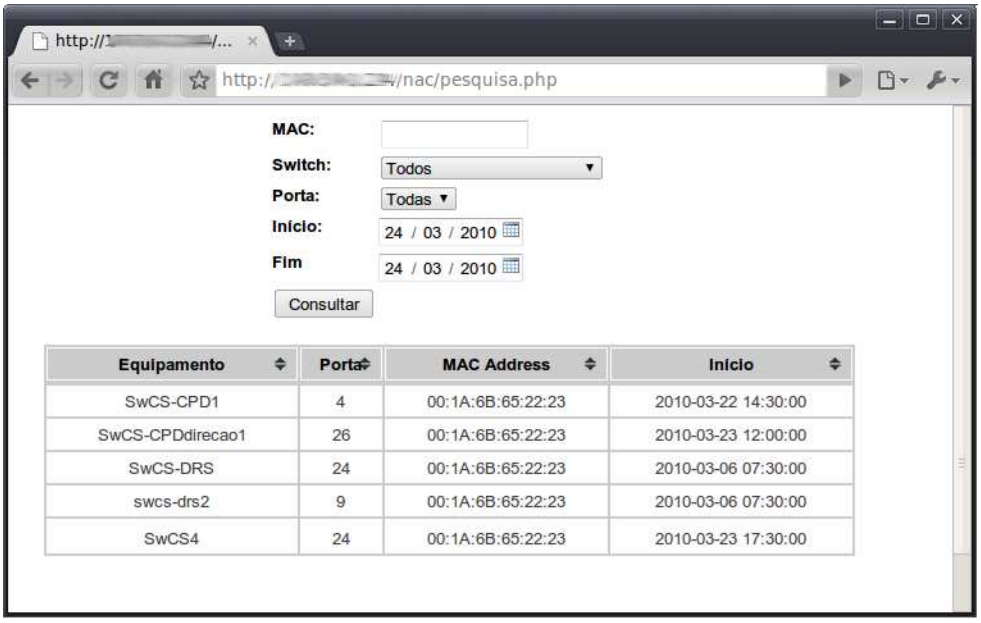


Figura 2. Localização de endereços físicos na rede.

Mitigação

Os dispositivos em desconformidade com a política de uso do sistema de registro devem ser moderados antes que prejudiquem o sistema como um todo. Para isso, o sistema implementa técnicas de mitigação que consistem basicamente na restrição de acesso. Essa restrição é feita através de uma filtragem do endereçamento de rede na *firewall* de borda da instituição. A figura 3 representa uma visão do processo de bloqueio de uma estação no sistema.

O bloqueio de um dispositivo pode ocorrer por três motivos que violam a política de acesso da instituição: máquinas que estão utilizando um IP indevido (*rogue*); estações que estão infectadas por algum tipo de *malware* ou sofreram algum incidente de segurança; e ainda, máquinas que foram bloqueadas por questões administrativas. Os bloqueios relacionados a incidentes de segurança ou administrativos não foram abordados por este trabalho, no entanto, mais informações sobre as técnicas implementadas podem ser obtidas em [Ceron et al. 2009].

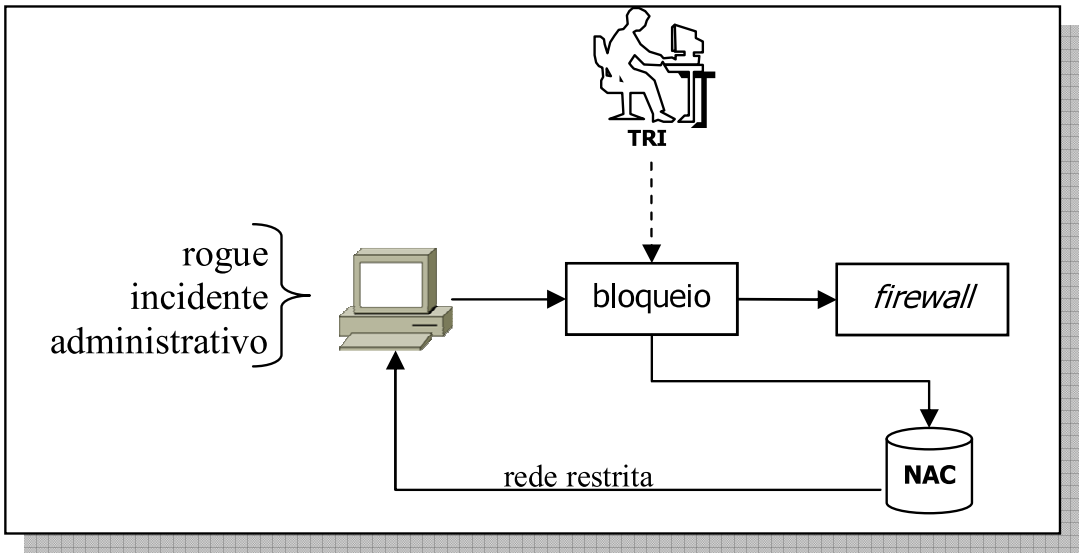


Figura 3. Bloqueio de usuários em não conformidade com a política de acesso da instituição.

Uma vez que um dispositivo de rede tenha sido classificado em uma destas categorias uma exceção é gerada para o analista de segurança, no caso, para o time de resposta a incidentes de segurança da UFRGS - TRI. O analista de segurança examina o alerta e, se necessário, faz o bloqueio manual do dispositivo irregular.

O processo de bloqueio dispara automaticamente uma série de ações automatizadas, entre elas a filtragem do dispositivo no *firewall* e alterações na base de dados do SRE. A filtragem impede que o dispositivo seja utilizado na rede de forma irregular, informando ao usuário através de um redirecionamento de conexões Web como o mesmo deve proceder para normalizar a sua situação. Para complementar o bloqueio, são inseridas informações referentes ao bloqueio na base de dados do SRE, como por exemplo, o horário e motivo do bloqueio. Adicionalmente, o SRE faz uma revogação temporária do endereço IP atribuído ao dispositivo. Tal revogação impede que o dispositivo utilize a

rede da unidade, ou seja, que receba o endereçamento previamente atribuído. Os dispositivos bloqueados, por outro lado, recebem um endereço de uma rede restrita, denominada rede *bogus*.

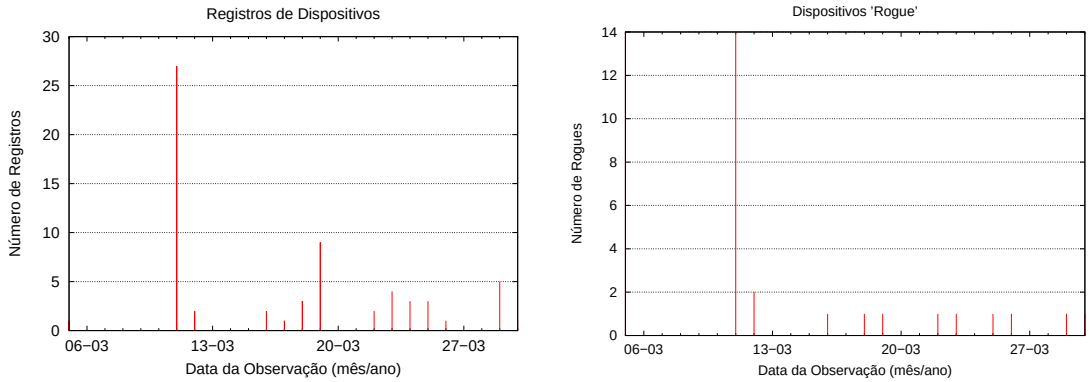
A rede *bogus* permite navegação externa apenas por meio de *proxy*, permitindo acesso a *sites* específicos, como por exemplo, *sites* de ferramentas de varredura *on-line* e atualização do sistema. O objetivo desta rede é abrigar todas as máquinas bloqueadas por incidentes de segurança ou incorretamente configuradas, impedindo que as mesmas acessem a rede de produção. Este cenário é mantido até que o dispositivo regularize a sua situação frente ao sistema SRE.

As medidas descritas acima visam alertar os usuários de problemas em seus dispositivos registrados no SRE. Da mesma forma, permitem que os problemas identificados sejam mitigados sem que haja comprometimento do sistema, gerando transtornos para os usuários e administradores.

Resultados

Os procedimentos descritos anteriormente foram incorporados *Sistema de Registro de Estações da UFRGS* e já vem auxiliando no gerenciamento de forma satisfatória. A identificação de inconformidades e a rápida mitigação das mesmas auxiliam na operação e também aumenta a confiabilidade no sistema, o que é muito importante no período inicial de implantação.

De forma pragmática, foi possível identificar um grande número de exceções de funcionamento no sistema em produção. Boa parte destes incidentes correspondem a máquinas que não estão corretamente configuradas, ou seja, estão utilizando um endereço de rede indevido. A fim de exemplificar o funcionamento de tais mecanismos a figura 4 apresenta informações do processo de migração de uma unidade de ensino ao SRE.



(a) Distribuição de registros.

(b) Distribuição de *rogues*.

Figura 4. Processo de migração de uma unidade de ensino.

A figura 4(a) apresenta informações sobre a alocação - processo de registro - de IP no respectivo bloco da unidade. Oficialmente a migração da unidade iniciou no dia 11/03, onde é possível notar no gráfico um grande número de novos registros. No decorrer do tempo, nota-se a diminuição de registros, até a completa migração dos dispostivos.

A figura 4(b), por outro lado, exibe informações de usuários *rogue* identificados durante o processo de migração. Como esperado, um número maior de usuários *rogue* são identificados na fase inicial da migração. O início da transição envolve certa adaptação dos usuários que necessitam reconfigurar os dispositivos, o que pode levar algum tempo. Logo após a fase inicial, o número de exceções cai drasticamente. No entanto, ainda é possível identificar alguns casos pontuais. Esses casos caracterizam usuários mal intencionados que tentam forçar um novo endereçamento sem efetuar o registro no sistema, uma vez que o seu IP legítimo tenha sido bloqueado.

Conclusão e Considerações Finais

Esse trabalho discute procedimentos de segurança que foram implementados no *Sistema de Registro de Estações da UFRGS* para identificar exceções de funcionamento e garantir a operação do mesmo. Foram apresentados alguns requisitos funcionais e também os mecanismos implementados para a mitigação dos problemas.

Uma avaliação prática pôde determinar que as técnicas implementadas foram úteis no gerenciamento do sistema, auxiliando na administração de conflitos de endereçamento. Pretende-se dar continuidade nesse processo, automatizando algumas tarefas que hoje necessitam da intervenção do gerente, como por exemplo, o bloqueio automático de máquinas irregulares. Por fim, a gerência integrada tende a aprimorar o sistema e facilitar as tarefas de identificação e registro de dispositivos na rede da universidade.

Referências

Case, J. D., Fedor, M., Schoffstall, M. L., e Davin, J. (1990). Simple network management protocol (snmp).

Ceron, J., Junior, A., Machado, C., Rey, L., e Martins, F. (2009). O processo de tratamento de incidentes de segurança. In *III Workshop de Tecnologia da Informação das IFES*, Belém, PA, Brasil.

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., e 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.

Machado, C., Soares, D., Rey, L., Ceron, J., e Junior, A. (2009). Implantação do Sistema de Gerenciamento de Redes Wireless da UFRGS. In *III Workshop de Tecnologia da Informação das IFES*, Belém, PA, Brasil.

Tonin, R., Machado, C., Postal, E., Rey, L., e Ziulkoski, L. (2008). Sistema de Gerenciamento de Redes Wireless da UFRGS. In *II Workshop de Tecnologia da Informação das IFES*, Gramado, RS, Brasil.

Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., e Spence, D. (2000). AAA Authorization Framework.