CONTROLE DE ACESSO ÀS REDES VIRTUAIS EMULADAS

Helio Corrêa Filho
helio@lrg.ufsc.br
Fesurv – Fundação do Ensino Superior de Rio Verde
Departamento de Ciência da Computação
Setor Universitário - Cx. Postal 104 - CEP 75901-970
Rio Verde - Goiás

Augusto Venâncio Neto
augusto@fesurv.br
Fesurv – Fundação do Ensino Superior de Rio Verde
Departamento de Ciência da Computação
Setor Universitário - Cx. Postal 104 - CEP 75901-970
Rio Verde - Goiás

Solange Teresinha Sari
solange@npd.ufsc.br
Rede Metropolitana de Alta Velocidade de Florianópolis – RMAV-FLN
Laboratório de Redes e Gerência - LRG
Universidade Federal de Santa Catarina – UFSC
Florianópolis – SC

Carlos Becker Westphall
westphal@lrg.ufsc.br
Laboratório de Redes e Gerência – LRG
Universidade Federal de Santa Catarina – UFSC
Florianópolis – SC

Resumo

Este trabalho tem como objetivo analisar as ameaças à segurança do serviço de redes virtuais emuladas e testar as políticas e parâmetros de segurança a fim de criar procedimentos de controle de acesso, através de procedimentos de gerência. Por isso, um ambiente de teste foi implementado especialmente para a execução de experimentos que permitiram otimizar os atributos de segurança e estabelecer ações preventivas e reativas aos possíveis ataques.

Palavras Chaves: ATM, Redes Emuladas, Gerência de Redes, Políticas de Segurança.

1 Introdução

O uso de redes virtuais emuladas permite manter a compatibilidade com os protocolos das redes comuns às redes locais já existentes de forma transparente, bem como utilizar novas aplicações desenvolvidas para o ATM (*Assynchronous Transfer Mode*), como se estivesse executando em redes locais tradicionais (*Ethernet* ou *Token-Ring*), [LANE21/95] e [ALLES/95]. Antes de qualquer transmissão de dados, através da rede ATM, os clientes LANE – LECs, devem conectar-se sucessivamente aos servidores LANE (LAN *Emulation*): LECS (LAN *Emulation Configurator Server*), LES (LAN *Emulation Server*) e BUS (*Broadcast and Unknown Server*), para obter sucesso na conexão de uma ELAN (*Emulated Local Area Network*).

De acordo com Laurent [LAUREN/96], as especificações do serviço LANE possuem poucas características de segurança para conexões ELANs. A autora descreve três categorias clássicas de ameaças à segurança das ELANs: (*i*) **Confidencialidade**: Desvio antes e após o estabelecimento da conexão, Conexão Espiã, e Conexão Imprópria; (*ii*) **Integridade**: Mascaramento durante e depois do estabelecimento da conexão, e Injeção de Dados (*iii*) **Disponibilidade**: Obstrução de comutadores ATM, roteadores ou repetidores. O ATM

implementa os mecanismos de autenticação, confidencialidade, integridade de dados, e controle de acesso para o plano de usuário, bem como, os mecanismos para autenticação e integridade para o plano de controle sinalização UNI (*User Netework Interface*) e NNI (*Network Network Interface*), especificado pela af.sec.100 [SEC100/99]. No entanto, esses mecanismos não são estendidos aos serviços de redes virtuais. O gerenciamento do serviço LANE apresentado em três módulos: ELAN.MIB, LES.MIB e BUS.MIB, e especificado pela af.lane.0057 [LANE57/96], não contempla mecanismos de segurança.

O objetivo deste trabalho é utilizar as políticas de segurança definidas administrativamente no módulo ELAN.MIB, bem como os parâmetros de segurança dos próprios equipamentos, para criar procedimentos de controle de acesso às redes virtuais emuladas, através ações preventivas e reativas de gerenciamento.

2 Controle de Acesso

2.1 Infra-estrutura do Ambiente

A estrutura principal do ambiente de teste utilizou equipamentos ATM que conectam as redes: POP-SC (Ponto de Presença da Rede Nacional de Pesquisa em Santa Catarina - RNP), POP-UFSC (Ponto de Presença da Rede Catarinense na UFSC), redeUFSC e Cluster da UFSC e da RMAV-FLN (Rede Metropolitana de Alta Velocidade de Florianópolis). As conexões são de interfaces IISP (*Interim Interswitch Signaling Protocol*) com 155 Mbps.

Para a realização dos experimentos de segurança foi adicionado um roteador (IBM 8210) e duas estações (NT e AIX) com as mesmas características dos demais, conforme mostra a topologia física da Figura 2-1.

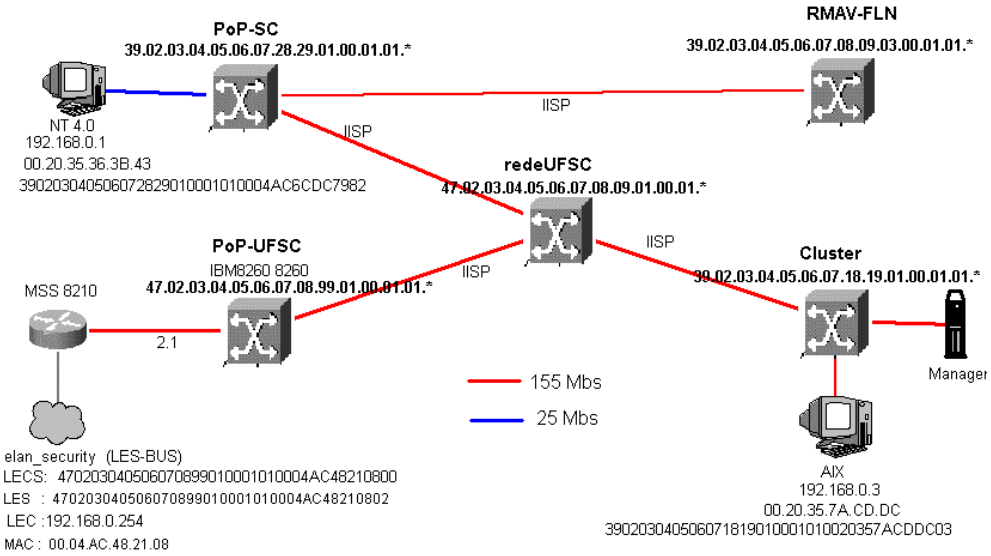

Figura 2-1 - Topologia física do ambiente de estudos.

Nesta configuração, os servidores LANE são implementados no roteador, onde é configurada uma rede virtual, denominada elan_*security*, para avaliar as políticas de segurança. Utilizamos três tipos de LECs (LAN *Emulation Clients*), estação NT, estação UNIX e o próprio roteador.

2.2 Experimentos

O objetivo geral dos experimentos é observar o comportamento dos servidores LANE, através do registro de eventos, durante a configuração dos LECs alternando as políticas de segurança: Endereço ATM, Endereço MAC (*Medium Access Control*), Tipo da ELAN, Tamanho Máximo de *Frame* e Nome da ELAN. Não será testada a política *byRteDesc* – Descritor de Rota, porque no ambiente de teste não são utilizados estações *proxy*. Inicialmente são analisadas as políticas de forma individual e depois a combinação delas. A cada experimento são utilizados os três tipos de LECs quando possível.

- **Nome da ELAN** - Configurando a política *byElanNm* no LECS com prioridade 10, e especificando a *elan_security*, observamos que o LEC se registra com sucesso quando este é configurado com o nome da ELAN especificado no LECS. Caso o nome seja diferente ou até mesmo com sintaxe diferente, o LEC não é registrado. Esta política oferece maior flexibilidade permitindo que o LEC também se registre usando um *alias* para o nome da ELAN.

- **Tipo da ELAN** – Configurou-se a política *byLanType* no LECS com prioridade 10, especificando o tipo da rede como *Ethernet*, e a *elan_security* estando configurada como *Ethernet*. Para cada tipo de LECs são utilizados os valores possíveis para o tipo da ELAN: *Ethernet*, *Token-Ring* ou *Unspecified*. Verificou-se que utilizando o tipo da ELAN diferente daquele configurado no LECS, o LEC não se registra. Consideramos que esta política é muito fácil de ser deduzida, tendo em vista que há somente três tipos de ELANs a serem testadas.

- **Endereço MAC** – Configurou-se a política *byMACAddress* no LECS com prioridade 10, especificando o endereço MAC do LEC da estação AIX. Com esta configuração tentamos registrar a estação AIX e o roteador. A estação AIX se registrou com sucesso, mas considerando que poderia assumir outros endereços MAC o registro não é garantido para todos os LEC, nesta estação. Já o roteador foi rejeitado sendo o mesmo equipamento dos servidores LANE. De modo geral, os resultados mostraram a vulnerabilidade desta política devido à facilidade com que o atacante pode alterar o endereço MAC.

- **Endereço ATM** – Configurou-se a política *byAtmAddr* no LECS com prioridade 10 e especificando o prefixo de rede da RCT (Rede Catarinense de Ciência e Tecnologia) e *Cluster*. Os LECs com endereço ATM de mesmo prefixo de rede, especificado, foram registrados com sucesso, ao contrário dos LECs pertencentes às redes RMAV e POP-SC. A utilização do prefixo de rede ATM apresenta maior segurança, pois seu tamanho e flexibilidade dificultam a dedução, conseqüentemente, restringe o acesso a ELAN, todavia, permite o acesso apenas aos LECs que estiverem seus prefixos incluídos na política.

- **Tamanho Máximo de *Frame*** – Configurou-se a política *byPktSize* no LECS com prioridade 10, especificando o tamanho do *frame* igual 1516, o mesmo definido na configuração da ELAN. Configuramos a estação NT com tamanho de *frame* diferente do especificado no LECS e o seu registro foi negado. Esta política é útil na criação de uma ELAN *default* designando LECs para tal função, baseado no tamanho de *frame*.

Após a realização dos experimentos mencionados e outros experimentos testando a combinação de políticas de segurança, concluímos que para obter maior confiabilidade é necessário utilizar três políticas: endereço ATM (*byAtmAddr*), nome da ELAN (*byElanNm*) e

tipo da ELAN (*byLanType*), estabelecidas com valores de prioridades diferentes. Sendo que o menor valor de política deve ser do *byAtmAddr*, por ser a política mais segura devido ao seu tamanho e flexibilidade que dificultam a dedução do prefixo de rede ATM; a segunda política utilizada deve ser o byElanNm, considerando que suas características oferecem restrições ao acesso na configuração de um LEC, e também por permitir a utilização de um *alias*, personalizando, assim, cada ELAN; e, por último, deve-se utilizar a política *byLanType*, que define qual o tipo da ELAN que será aplicada na configuração do LEC, restringindo a três tipos de ELAN - *Ethernet*, *Token-Ring* ou *Unspecified*.

Dessa forma para que um LEC consiga se registrar ele terá de atender os requisitos especificados nas três políticas, lembrando que a menor prioridade será verificada primeiro, resultando em maior segurança no controle de acesso nas ELANs.

2.3 Procedimentos de Controle

Para inibir as ameaças ao serviço LANE foram definidos procedimentos de controle (que a seguir foi ordenado) utilizando as políticas de segurança, bem como os recursos de segurança adicionais oferecidos pelo ambiente de estudo. Em cada ameaça foram analisadas as possibilidades de ocorrência e as possíveis ações preventivas e reativas, sempre procurando inibir ou restringir o acesso de clientes não-autorizados. O controle de acesso de usuários e o sigilo de senhas são considerados como regras importantes de segurança. Como procedimento de controle básico considera-se o uso das políticas nome da ELAN, tipo da ELAN e prefixo ATM, e correlaciona os objetos das MIBs (*Management Information Bases*). Outro controle necessário é a verificação da tabela de registros de erros para cada servidor LANE.

[1] Verificar o número de acessos negados no LES e LECS, bem como o número de requisições inválidas, e depois comunicar ao operador;

[2] Analisar a tabela de registro de erros dos servidores LECS, LES e BUS (*lecsErrLogTable*, *lesErrLogTable* e *busErrLogTable*, respectivamente);

[3] Conferir o endereço MAC do LEC recém conectado e fazer a autenticação na porta do comutador;

[4] Criar procedimentos de controle para a camada de rede;

[5] Identificar os LECs conectados por VPCs (*Virtual Path Connection*) nos comutadores e verificar as políticas de segurança;

[6] Detectar apropriações indevidas de conexões usando *Sniffer*;

[7] Se a modificação na tabela *lesLeArpMacTable* for feita pelo gerente deve ser feita uma verificação se este LEC não é um espião;

[8] Verificar o tráfego no BUS por LEC;

[9] Verificar o incremento de requisições de resolução de endereços no LES.

2.4 Gerência de Segurança

O sistema de registro de erros implementado no equipamento que fornece o serviço LANE possui uma interface pouco amigável. Os erros são registrados seqüencialmente, mostrando o subsistema, a descrição do erro e a causa provável. Embora, o sistema seja flexível na apresentação dos eventos, o mesmo não permite a inferência de informações. Analisando dois ou mais subsistemas, em uma rede com muitos LECs, os eventos são registrados tão rapidamente que fica impraticável a visualização dos dados. Os eventos podem ser armazenados em um arquivo de uma máquina remota que possua o sistema de registro (*syslogd*), no entanto a forma de apresentação e análise continua a mesma. A alternativa é enviar os eventos (*traps*) para uma máquina de gerência que pode analisar os dados e fazer inferências tomando ações quando necessário.

A ferramenta de gerenciamento *Tivoli NetView* 5.12 para AIX foi utilizada para monitoramento dos objetos gerenciáveis, bem como para a correlação de variáveis através de regras. Lembrando que os objetos gerenciáveis estão definidos na especificação [LANE57/96]. Na console da ferramenta é apresentada à topologia da rede baseada no endereçamento IP, assim como uma área de controle de eventos (*workspace)*. A área de trabalho denominada '*Events'* apresenta todos os eventos associados aos diversos nodos das diferentes redes.

Para fazer a correlação, selecionamos variáveis para serem coletadas periodicamente e em seguida definimos eventos de notificação. Por exemplo, o evento denominado RMAVFLN_SEC_LECS que registra os ataques ao LECS com severidade crítica:
1501: Valor diferente de zero para as variáveis: `lesStatAccDenied, lecsStatAccDenied, lecsStatInvaldReq, lecsStatInvaldDest, lecsStatInvaldAddr, lecsStatNoConf e lecsStatConfError da tabela lecsStatTable.`

Configuramos diferentes eventos, e em seguida descrevemos as regras de correlação baseadas nos procedimentos de controle:

- **Estatística dos Servidores LANE** - Regra sec_LANEserver para tratamento dos eventos 1501 e 1503 relacionados aos ataques efetuados nos servidores LECS e LES;

- **Registro de Eventos do Equipamento** - Regra sec_8210ELS para tratamento dos eventos da classe IBM_8210 relacionados aos eventos emitidos pelo sistema de registro de eventos do equipamento;

- **Registro do LEC nos LES** - Regra sec_LESLEC para tratamento do evento 1505 relacionado aos possíveis ataques dos LECs ao LES;

- **Requisições do LEC ao BUS** - Regra sec_BUSLEC para tratamento do evento 1511 relacionado aos possíveis ataques dos LECs ao BUS;

- **Requisições do LEC ao LES (BUS)** - Regra sec_BUSLESLEC para tratamento dos eventos 1511 e 1513 relacionados aos possíveis ataques dos LECs ao BUS e ao LES.

A Figura 2-2, apresenta a regra sec_BUSLEC: se num período de 15 minutos 3 eventos (1511) acontecerem, então uma ação será tomada e o evento será repassado para a área de controle de eventos. O evento 1511 (*rising*=130000 e *falling*=100000: `busLecRecvs`) especifica os limiares para o número de requisições *broadcast*, *multicast* e desconhecidas recebidas pelo BUS de um determinado LEC.

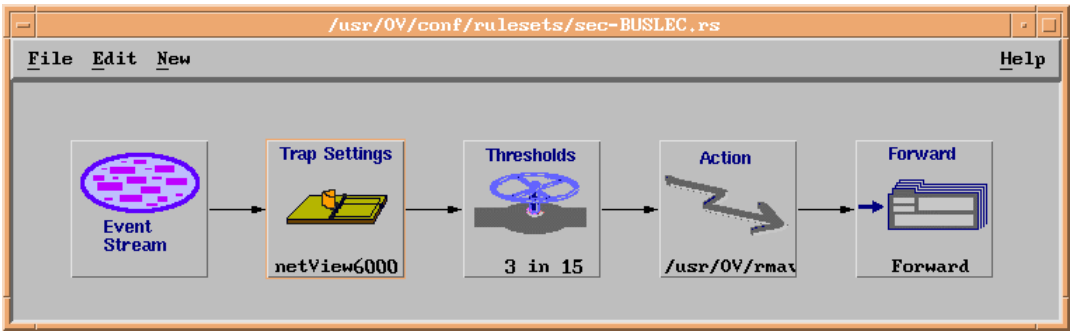

Figura 2-2 - Regra sec_BUSLEC

O Quadro I, define a ação a ser tomada na regra sec_8210ELS, isto é comunica o operador o evento recebido do equipamento. Considerando que o evento recebido possui formato diferente dos eventos configurados pela ferramenta de gerência, faz-se necessário um *parse* para selecionar a informação de interesse.

```
#!/bin/sh
# hr:min:sec
# subsys_name.event_num:
# message_text
#
TMP=/tmp/.sec8210els.tmp
LOGPATH=/usr/OV/rmav/log
LOGFILE=sec8210els.log
SUBJECT="LOGFILE: sec8210els"
cat > $TMP << __EOF__
Registro de Evento do IBM8210 MSS
---------------------------------
 Time Stamp : $1
 ATM addr   : ${17}
__EOF__
case $2 in
 "LES.382:")
  cat $TMP | mail -s "$SUBJECT" operator@rmav-fln.ufsc.br
  ;;
  *)
   cat $TMP >> $LOGPATH/$LOGFILE
  ;;
esac
rm -rf $TMP > /dev/null 2>&1
```

Quadro I - Script que define a ação tomada na regra sec_8210ELS.

3 Considerações Finais

Com a análise das ameaças ao serviço LANE foi possível estabelecer alguns procedimentos de controle às diversas camadas da rede ATM. A implementação desses procedimentos ficou restrita às ações preventivas e reativas configuráveis no sistema de gerência local ou remoto.

Na gerência local foram configuradas as políticas de segurança para o LECS e para cada instância LES/BUS, isto é, só será permitido acesso aos LECs que possuírem o mesmo prefixo de rede (política *byATMaddress*), o mesmo nome da ELAN (política *byElanName*) e também com o mesmo tipo de ELAN (política *byElanType*), proporcionando assim, maior segurança aos recursos gerenciados.

No sistema de registro de eventos, foram analisados os eventos associados à quebra de segurança nos subsistemas dos servidores LANE, e posteriormente, configurados para enviar mensagens de alerta para o gerente remoto.

À gerência remota ficou incumbida de coletar e analisar as variáveis estatísticas que representam erros e falhas nos servidores LANE. A ferramenta de gerência (*NetView*) permitiu fazer inferências sobre os eventos recebidos, bem como tomar ações corretivas e preventivas dos possíveis ataques analisados.

Ao término deste trabalho (dissertação de mestrado) ficam em abertos os seguintes segmentos para ampliar a pesquisa:

- Propor uma MIB que forneça dados relativos à segurança;
- Realizar um estudo de desempenho em uma ELAN que utiliza políticas de segurança e comparar o seu desempenho com uma ELAN que não faça uso das políticas de segurança.

Referências Bibliográficas

[ALLES/95] ALLES, Antony. ATM Internetworking. In: Engineering InterOp. Las Vegas: Cisco Systems, Inc. May, 1995.

[LANE21/95] ALTMAN, Asher, BULLARD, Carter, FINKELSTEIN, Louis et al. *The* ATM *Forum Technical Committee*: LAN *Emulation Over* ATM, *Version 1.0*, af-LANE-0021.000, Jan., 1995.

[LANE57/96] ALTMAN, Asher, BULLARD, Carter, FINKELSTEIN, Louis et al. The ATM *Forum Technical Committee*: LAN *Emulation Servers Management Specification 1.0*, af-LANE-0057.000 – Mar., 1996.

[LAUREN/96] LAURENT, Maryline. *Security Flows Analysis of the* ATM *Emulated* LAN *Architecture*. IFIP, *Conference on Communications and Multimedia Security*. Essen, Germany, Set.,1996.

[SEC100/99] ALTMAN, Asher, BULLARD, Carter, FINKELSTEIN, Louis et al. The ATM *Forum Technical Committee*: ATM *Security Specification Version* 1.0 AF-SEC-0100.000. Feb., 1999.