Sec-Mon: Uma Arquitetura para Monitoração e Controle de Acordos de Níveis de Serviço Voltados à Segurança

Rafael da Rosa Righi[1,2], Diego Luis Kreutz[3], Carlos Becker Westphall[1]

[1]Programa de Pós-Graduação em Ciência da Computação (PPGCC)
Laboratório de Redes e Gerência (LRG) – Universidade Federal de Santa Catarina
Caixa Postal 476 – CEP 88.040-900 – Florianópolis, SC, Brasil

[2]Faculdade de Tecnologia SENAI Florianópolis
Serviço Nacional de Aprendizagem Industrial – SENAI-SC
Rodovia SC 401, n° 3730 – 88.032-005 – Florianópolis – SC – Brasil

[3]Universidade Luterana do Brasil (ULBRA), Campus de Santa Maria
Caixa Postal 21834 – 97.020-001 – RS – Brasil

righi@ctai.senai.br, kreutz@inf.ufsm.br, westphal@lrg.ufsc.br

Abstract. *The security of computers and systems is essential for organizations and universities. The outsourcing of security services and the construction of a specialized team in the protection of digital assets are the most important measures adopted to guarantee the security. In this scenario, the utilization of Security Service Level Agreements (Sec-SLA) is increasing between the involved parts, which defines metric and its quality of service. This article defines an architecture to monitor and control security service level agreements (Sec-Mon), where users and information technology staff can fiscalize each other in security aspects. We intent to contribute for the expansion and application of Sec-SLAs.*

Resumo. *A segurança de computadores e sistemas é vital para organizações e instituições de ensino. A terceirização dos serviços de segurança e a construção de uma equipe especializada na proteção de ativos digitais estão entre as principais medidas adotadas para garantir a segurança. Nesse cenário, é cada vez maior a utilização de acordos de níveis de serviço voltados à segurança (Sec-SLA) entre as entidades envolvidas, os quais definem métricas e suas qualidade de serviço. Este artigo define uma arquitetura para monitoração e controle de acordos de níveis de serviço voltados à segurança (Sec-Mon), onde as partes que firmam o contrato Sec-SLA podem fiscalizar uma a outra no cumprimento dos deveres de segurança. Busca-se, também, contribuir para a expansão e aplicação dos Sec-SLAs.*

1. Introdução

As redes de computadores e a internet são recursos cada vez mais utilizados por empresas e instituições de ensino. Elas usam esses recursos para dar suporte aos seus negócios e comunicações. Muitas vezes, para que as organizações continuem provendo com eficiência seus serviços, é necessária a terceirização de funções que não fazem

parte de suas especialidades. Nesse cenário encontram-se os acordos de níveis de serviço ou SLAs. Um SLA é um acordo formal negociado entre duas partes, um provedor de serviço e um cliente. Este acordo designa um entendimento comum sobre a qualidade, prioridades e responsabilidades a respeito do serviço [SLA Management Team, 2001; Buco et al., 2004]. Entretanto, uma companhia não deve apenas preocupar-se com o desempenho e a estabilidade de sua rede. Outro aspecto muito importante que também deve ser gerenciado é a segurança computacional. Segundo [Menegazzo, 2000], o gerenciamento da segurança compreende o estabelecimento e a monitoração de atividades que garantam a existência de sistemas e redes com algum nível de proteção.

A proteção de uma rede de computadores pode ser visualizada como um serviço oferecido por uma equipe ou empresa terceirizada. Sendo assim, a segurança pode ser mensurada (medida) e níveis de segurança podem ser estabelecidos. Percebe-se, portanto, uma relação entre os níveis de segurança e o SLA. Um Sec-SLA é um acordo de nível de serviço associado à área de segurança computacional [Righi et al., 2004].

O trabalho de [Righi et al., 2004] preocupou-se com a descrição de um Sec-SLA e com a especificação e validação de métricas para serem usadas nesses contratos. Contudo, não é suficiente definir as métricas e seus níveis aceitáveis. Para que um Sec-SLA tenha efeito dentro uma organização faz-se necessário um mecanismo de monitoração que verifique se as partes (tanto provedores como os clientes) têm cumprido com o acordado. Tendo em vista a preocupação crescente das empresas com a segurança da informação, a integração do Sec-SLA com um mecanismo de monitoração é uma evolução natural na contratação e terceirização de serviços de telecomunicações.

Este artigo apresenta uma arquitetura para monitoração e controle de um Sec-SLA chamada Sec-Mon. Suas justificativas principais são a necessidade de um ambiente que possibilite verificar o cumprimento do contrato Sec-SLA e a dificuldade de medir métricas de segurança, já que o uso de protocolos padrão para a gerência de redes como o SNMP [Case et al., 1999] nem sempre se aplica nesse contexto. A arquitetura Sec-Mon é inicialmente desenvolvida para atender o conjunto de métricas definidas por [Righi et al., 2004]. Ela é adaptada para monitorar acordos Sec-SLA *intracompany*. Nesses contratos os provedores de serviço são os administradores da rede (1ª parte) e os clientes são os usuários da organização (2ª parte). Pretende-se também contribuir para a expansão do conceito de Sec-SLA e para a popularização desse gênero de contratos.

Este documento está organizado em 5 seções. A seção 2 é responsável por exibir alguns aspectos teóricos associados ao Sec-SLA e os principais trabalhos relacionados com o tema tratado nesse artigo. A seção 3 descreve a arquitetura Sec-Mon, suas peculiaridades e contribuições. A seção 4 discute a implantação do ambiente de monitoração em um sistema real. O artigo encerra na seção 5, a qual reúne as principais idéias e resultados da pesquisa, além de citar os possíveis complementos sobre ela, a cargo de trabalhos futuros.

2. Contextualização do Sec-SLA e Trabalhos Relacionados

Os principais temas envolvidos nesse artigo são os acordos de níveis de serviço voltados à segurança (Sec-SLA), a terceirização de serviços e a gerência e monitoração de redes de computadores. Os acordos de níveis de serviço tornaram-se populares devido principalmente à terceirização da infra-estrutura de comunicação pelas organizações.

Esses acordos especificam os níveis de qualidade de serviço (QoS – *Quality of Service* [Dutta-Roy, 2000; Krief, 2004; Habib et al., 2005]) que o fornecedor se compromete em disponibilizar, além de cláusulas legais, como as conseqüências para cada parte se houver descumprimento de deveres. O contrato deverá selecionar um nível de serviço que contemple os anseios do cliente e as possibilidades do fornecedor.

Grande parte dos contratos de níveis de serviços é efetivada entre companhias diferentes, onde uma delas presta serviço à outra [Walt, 2003]. Um exemplo desta situação são duas filiais de uma mesma organização que se interligam através da utilização de serviços de uma segunda organização. Embora este esquema seja o mais encontrado, contratos de SLA implementados dentro de uma mesma organização também possuem significado e relevância [Muller, 1999], principalmente no âmbito desse artigo.

Nos SLAs tradicionais os principais aspectos são a disponibilidade do canal de comunicação, a vazão média que será entregue, a taxa de erros máxima e a identificação de possíveis picos de congestionamento [Left e Rayfield, 2003] . O acordo é chamado de Sec-SLA quando as métricas levadas em consideração no contrato são relacionadas com as propriedades de segurança. O Sec-SLA exibe os cuidados ou deveres relacionados à segurança que o fornecedor e o cliente do serviço devem tomar. A diferença de um SLA de telecomunicações para o Sec-SLA é percebida nos enfoques; o Sec-SLA preocupa-se com métricas relacionadas à criptografia ou não do canal de comunicação, integridade da informação enviada, números de vírus que chegam até os usuários finais, entre outras.

O presente artigo objetiva monitorar os acordos do tipo Sec-SLA e prover meios para que ambas as partes verifiquem se o acordado está sendo cumprido. O estudo de [Henning, 2000] apresenta os primeiros conceitos de Sec-SLA e as perspectivas de avanço na área. O trabalho realizado por [Righi et al., 2004] expandiu as definições de Sec-SLA existentes até então e especificou métricas e parâmetros para serem usados nesses contratos. A monitoração de acordos Sec-SLA é citada como imprescindível pelos dois estudos anteriores. Nesse sentido, essa pesquisa parte dos trabalhos já consolidados e busca complementa-los através do desenvolvimento do Sec-Mon.

O desenvolvimento de uma arquitetura para monitorar e controlar acordos do tipo Sec-SLA aproxima duas grandes áreas da computação: a segurança e a gerência de redes. Está situação não é exclusividade desse artigo. Outro estudo que une essas áreas é o realizado por [Gaspary e Fagundes, 2003]. Ele apresenta técnicas de como utilizar o protocolo SNMP para observar os objetos das MIB II e RMON e, baseado em seus valores, detectar diversos tipos de ataque (ex: varredura de portas e negação de serviço). A arquitetura Sec-Mon utiliza o protocolo SNMP em algumas circunstâncias. No entanto, a monitoração de métricas de segurança utilizando esse protocolo muitas vezes é difícil ou impraticável. Para verificar o cumprimento de métricas como a Gerência de Senhas (estipula a freqüência da troca de senhas) o Sec-Mon utiliza outros componentes ao invés do SNMP, descritos na seção 3.

A monitoração de um Sec-SLA também é diferente da monitoração de segurança realizada pelos sistemas de detecção de intrusão - IDS [Brandão et al., 2005]. Monitorar o Sec-SLA implica verificar o seu estado e se as partes estão realizando suas obrigações. Os sistemas de detecção de intrusão, nesse contexto, são componentes que prestam

serviço à arquitetura Sec-Mon definida, ou seja, seus registros (*logs*) auxiliam na tarefa de verificar se as métricas e os níveis de serviço estão sendo alcançados.

A terceirização de serviços de segurança é outro assunto relacionado ao Sec-Mon, pois esse tema geralmente está associado aos SLAs. Segundo [Mckenna, 2002], a terceirização dos serviços de segurança é algo iminente e, portanto, a gerência desses serviços deve ser profundamente estudada. Já [Navarro, 2001], afirma que a terceirização de serviços de segurança deve ser feita sempre que a segurança não faça parte dos ramos de atividade de uma empresa.

3. Arquitetura de Monitoração e Controle Sec-Mon

A arquitetura Sec-Mon define uma forma de monitorar contratos Sec-SLA realizados dentro de uma mesma companhia. Seu objetivo principal é permitir que os usuários saibam se os administradores da rede estão cumprindo com as suas responsabilidades de segurança. Da mesma forma, os administradores podem verificar quais usuários da rede estão de acordo com as métricas acertadas.

A Figura 1 apresenta a visão geral da arquitetura Sec-Mon. A arquitetura está dividida em quatro componentes: entidades, interface, ações ou processos e armazenamento de informações. A seção 3.1 descreve estes elementos, suas interações e como eles colaboram para alcançar o objetivo principal do Sec-Mon.

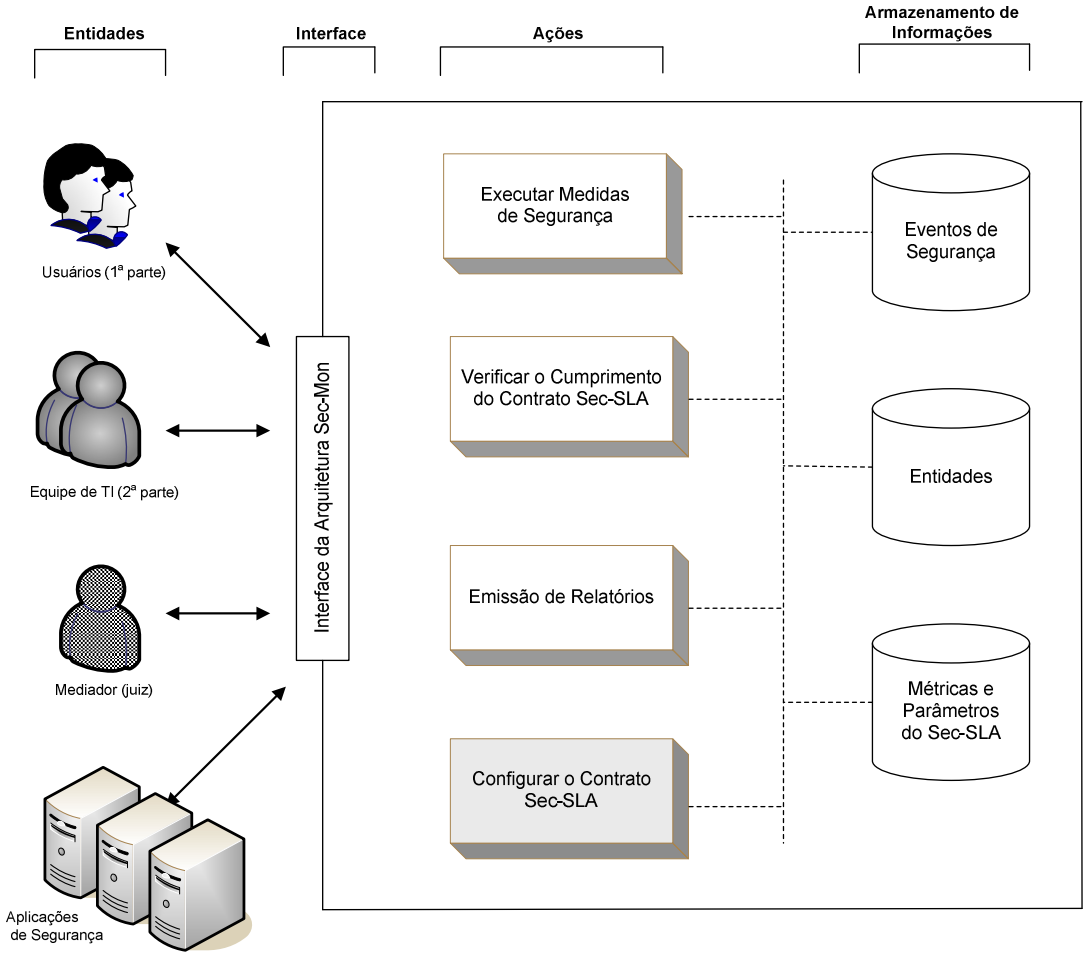

Figura 1: Visão Geral da Arquitetura de Monitoração e Controle Sec-Mon

3.1 Descrição dos Componentes do Sec-Mon

Esta seção relaciona os elementos da arquitetura projetada. A arquitetura que será explanada a seguir é eminentemente conceitual, ou seja, ela não está "presa" a tecnologias e implementações específicas. Desta forma, o Sec-Mon torna-se flexível, sendo possível sua implantação em cenários e organizações que se adaptam ao modelo de SLA *intracompany* [Muller, 1999].

3.1.1 Entidades do Sec-Mon

As principais entidades desta arquitetura são aquelas que firmam o contrato de segurança; neste caso, os usuários da rede interna e a equipe de TI da organização. Como mencionado anteriormente, as duas partes possuem direitos e deveres a cumprir e o Sec-Mon - neste contexto - será o responsável por centralizar as informações relativas ao acordo Sec-SLA e verificar a situação de cada contratante.

Os usuários da rede (1ª parte) estarão cadastrados na base de informações e, através de um nome de usuário senha, poderão executar diversas medidas relacionadas com a segurança e proteção da rede em que estão envolvidos. A 2ª parte do acordo, identificada pela equipe de TI, também usufrui do Sec-Mon para efetuar tarefas de segurança e monitorar os deveres da outra parte do contrato.

O mediador, também chamado de gerente ou juiz do sistema, é quem configura o Sec-Mon. Ele representa uma entidade neutra na arquitetura (Figura 2). Ele identifica quais métricas de segurança são utilizadas no contrato, seus parâmetros (níveis de serviço) e preenche esses valores na base de informações de métricas. O cadastro de usuários e da equipe de TI na base de dados e a configuração correta dos *scripts* e programas que dão suporte ao Sec-Mon também estão sob seus cuidados. Lembre-se que a arquitetura Sec-Mon parte do pressuposto que já existe, ou está em andamento, um acordo de segurança do tipo Sec-SLA.

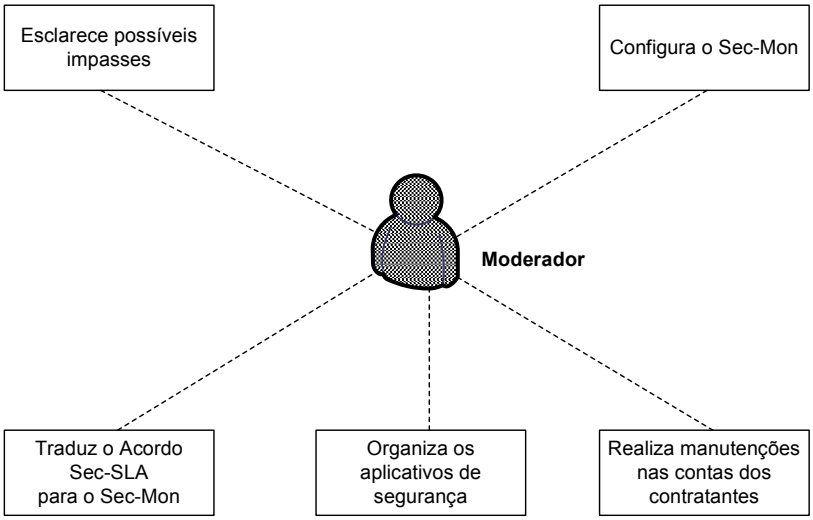

Figura 2: Relação de Funções da Entidade Moderador

Várias aplicações de segurança podem comunicar-se com o Sec-Mon, a fim de munir a arquitetura com informações de segurança e auxiliá-la na monitoração do

acordo Sec-SLA definido na organização. Exemplos de aplicações de segurança que podem ser configuradas para colaborar com o Sec-Mon são os sistemas IPS e IDS (mecanismos que atuam de forma pró-ativa e reativa – depende do contexto – no combate à incidentes de segurança), os antivírus e programas de verificação de integridade em sistemas de arquivos.

3.1.2 Interface do Sec-Mon

As entidades interagem com o Sec-Mon através de uma interface. Os usuários da rede, por exemplo, podem utilizar a interface para executar ações relacionadas com as métricas do Sec-SLA e/ou para observar relatórios sobre a situação do cumprimento do contrato estabelecido. Para as duas partes que firmam o Sec-SLA, esta interface pode se constituir de uma página Web, com processo de autenticação devidamente configurado.

A comunicação das aplicações de segurança com o Sec-Mon acontece através de outros artifícios. Eles são: *(i)* o Sec-Mon vasculha os registros (*logs*) gerados pelas aplicações e colhe os dados que lhe são pertinentes; *(ii)* as aplicações de segurança são programadas para inserirem dados nas bases de informações de segurança do Sec-Mon; *(iii)* transmissão no modelo *Web Services* (aplicação para aplicação), onde são designados através de padronizações XML os serviços e a estruturação da comunicação entre os envolvidos. A Seção 3.2 apresenta no exemplo de funcionamento do Sec-Mon estas técnicas.

3.1.3 Processos e Ações do Sec-Mon

O Sec-Mon possibilita que as duas partes envolvidas o contrato de segurança e o mediador (juiz) executem ações ou procedimentos na arquitetura. Estas ações são executadas a partir da interface descrita na seção 3.1.2 ou através da execução de aplicativos de segurança.

As ações que podem ser realizadas pelos administradores e usuários da rede estão associadas às métricas existentes no acordo Sec-SLA. Por exemplo, em um contrato Sec-SLA que exige que os usuários troquem suas senhas semanalmente, pode haver na arquitetura Sec-Mon um procedimento que possibilite os usuários definirem esta tarefa. Da mesma forma, se no contrato firmado conta que a equipe de TI deve realizar o backup diário das caixas de correio eletrônico dos usuários, pode haver um procedimento na arquitetura que auxilie nesta operação.

O Sec-Mon define também outra forma da arquitetura perceber as ações realizadas pelas partes envolvidas no contrato. Nesse esquema alternativo são configurados *scripts* que executam as funções relacionadas com as métricas do Sec-SLA e que informam à base de eventos do Sec-Mon as ações realizadas. Por exemplo, seria escrito um *script* chamado "troca_senha" que chama a aplicação tradicional para a troca de senhas do sistema operacional e depois comunica à arquitetura Sec-Mon o usuário que executou tal ação e as características do evento, como a data e a hora de lançamento.

3.1.4 Base de Informações do Sec-Mon

Os registros de todas as ações executadas no Sec-Mon pelos envolvidos são armazenados na base de informações – também chamada de base de eventos. Conforme

ilustrado na Figura 1, a base de informações chamada "Entidade" contém dados sobre as partes que firmaram o contrato e sobre o moderador especificado. A descrição do Sec-Mon é conceitual; portanto não fixa o tipo de banco de dados e os campos que devem ser instalados. Cada organização deve vislumbrar a sua realidade e transportá-la para as bases de dados. Exemplos de campos que podem existir neste base de informação são: nome completo, nome de *login*, endereço, laboratório ou sala, email, telefone para contato e senha e método de autenticação.

A base de informação chamada "Métricas e Parâmetros do Sec-SLA" contém todas as métricas fixadas no acordo e suas peculiaridades. Devem estar presentes nesta base de dados informações o seguinte: nome da métrica de segurança, por quem ela é cumprida (1ª ou 2ª parte), seus parâmetros (QoS), o parâmetro atual em execução, penalidades (no caso de descumprimento), data que entrou em vigor e alguma outra observação pertinente. A Tabela 1 apresenta um exemplo de registro desta base de informação.

Tabela 1: Exemplo de Registro na Base de Métricas do Sec-SLA

Id	Métrica Segurança	Data	Destino	P.1	P.2	P.3	P.4	Param. Atual	Penalidades	Obs
1	Troca de senhas	10/12/ 2005	Usuários	7d	21 d	30 d	45 d	P.1	advertência escrita	__

A terceira base de informação do Sec-Mon chama-se "Eventos de Segurança". Ela é a mais importante, pois é vital para a verificação do cumprimento (ou não) do acordo pelas partes que assinam o Sec-SLA. Todos os eventos relacionados com as métricas de segurança devem ser registrados. Eles formam a sustentação da arquitetura definida. Quanto maior a quantidade e a qualidade dos registros de segurança, maiores subsídios são fornecidos ao Sec-Mon para executar a sua monitoração e, conseqüentemente, mais apurados são os seus resultados.

Como mencionado, cada ação executada através da interface do Sec-Mon gera um registro nesta base de informação. As aplicações de segurança também podem comunicar o Sec-mon eventos de segurança, os quais também são armazenados em "Eventos de Segurança". Os itens que formam um registro são (pode haver outros): identificador do registro, data e hora de geração, métrica de segurança relacionada, entidade emissora, avaliação do moderador (quando for necessário), descrição textual do registro e um campo para guardar informações não textuais relacionadas com o evento, como figuras ou arquivos executáveis.

3.2 Exemplo de Funcionamento da Arquitetura Sec-Mon

Neste cenário de uso, supõe-se que o contrato de segurança estabelecido possui duas métricas de segurança. A Tabela 2 apresenta o conteúdo da base de informação "Métrica e Parâmetros do Sec-SLA" para este exemplo. Os usuários da rede devem trocar suas senhas mensalmente (no mínimo 10 dígitos), enquanto que a equipe de TI se compromete no seguinte: não deve entrar na rede da organização mais que 2 vírus (ou códigos maliciosos) no prazo de 1 ano a partir da data em que o Sec-SLA entrou em

vigor (01/03/2006). A equipe de TI executa um antivírus em todas as mensagens de e-mail, sendo seu dever evitar este tipo de transtorno.

Tabela 2: Contrato Sec-SLA para o Cenário-Exemplo

Id	Métrica Segurança	Data	Destino	P.1	P.2	P.3	P.4	P. Atual	Penalidade
1	Troca de senhas	01/03/ 2006	Usuários	7d	21d	30d	45d	P.3	suspensão da conta
2	Número de Vírus	01/03/ 2006	Equipe de TI	2/ ano	4/ ano	6/ ano	8/ ano	P.1	demissão do chefe de TI

A interface do Sec-Mon foi definida segundo o Web. Nela as entidades se autenticam e podem executar ações no sistema. Os usuários podem executar quatro ações, que são trocar a senha, verificar o cumprimento do contrato, verificar sua situação pessoal e comunicar a descoberta de um vírus em seu computador pessoal. Como se pode ver, o usuário pode avisar o sistema que foi infectado por um vírus. Neste caso, ele deve passar algumas características do problema e esperar uma avaliação do Moderador. Este irá verificar se é procedente a reivindicação do usuário e, caso seja, este fato contará negativamente para a equipe de TI.

A equipe de TI, por sua vez, pode executar os seguintes procedimentos através do Sec-Mon: parar/ativar remotamente o sistema Antivírus (por exemplo, o *AVG Server Free* 7.1), verificar o cumprimento do contrato Sec-SLA e verificar a situação da equipe. Neste exemplo, vê-se que o serviço de antivírus localiza-se em um servidor diferente daquele que hospeda a arquitetura Sec-Mon. No caso do Moderador, ele usará o Sec-Mon para averiguar se o contrato Sec-SLA está sendo obedecido pelas duas partes, verificar se existe alguma situação onde precisará agir como mediador (por exemplo, usuário comunica que foi infectado e o juiz precisa confirmar) e para produzir relatórios de penalizações. A Figura 3 mostra as ações para este cenário específico.

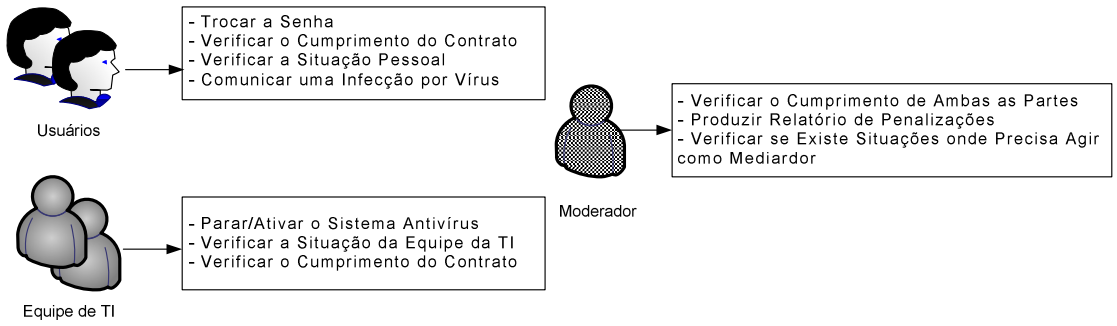

Figura 3: Relação de Ações e Procedimentos para o Cenário-Exemplo

Neste exemplo de utilização do Sec-Mon foram elaborados dois *script shell*. O primeiro possibilita os usuários a trocarem suas senhas e, através de conexão com o

banco de dados do Sec-Mon, adiciona na base "Eventos de Segurança" um registro relacionado à tarefa executada. O segundo foi implantado no servidor de arquivos da organização, onde ficam os dados pessoais dos usuários e reside o sistema antivírus. Ele varre os registros (*log*) do antivírus (AVG) e passa dados de infecção para a o Sec-Mon. Estes dois *scripts* são vitais dentro do contexto de monitoração e controle do Sec-Mon. Assim, tem-se a união entre a arquitetura Sec-Mon e as aplicações tradicionais para a proteção de rede de computadores A Figura 4 expõe a comunicação dos *scripts* com a arquitetura.

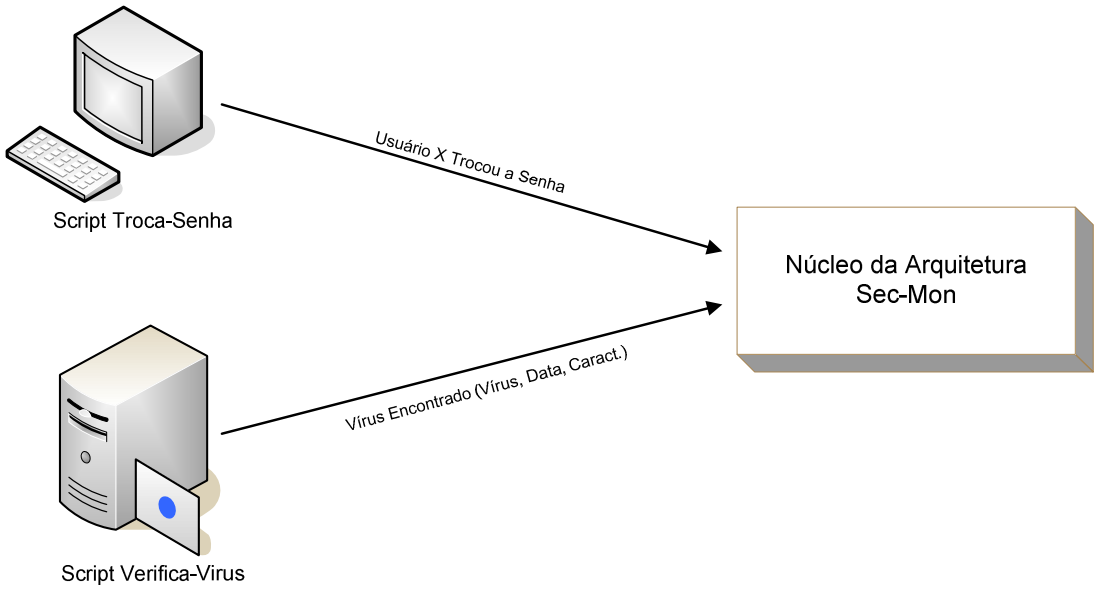

Figura 4: Comunicação entre os scripts e o Núcleo do Sec-Mon

A inteligência do Sec-Mon esta concentrada na ação **Verificar o Cumprimento do Contrato** e na base de informações **Eventos de Segurança**. A proteção desta base de dados e o desenvolvimento do processo que verifica o estado do Sec-SLA são muito importantes para a qualidade da monitoração e controle executados.

4. Implantação da Arquitetura Sec-Mon em um Ambiente Real

A construção do ambiente de monitoração Sec-Mon exige que o acordo Sec-SLA esteja estabelecido ou em fase final de preparação. Esta seção apresenta algumas decisões de projeto que estão sendo tomadas a fim de implantar a arquitetura Sec-Mon no Laboratório de Redes e Gerência (LRG-UFSC), o qual possui cerca de 30 usuários ativos. No ambiente escolhido as partes envolvidas no Sec-SLA são os administradores e usuários da rede de computadores do laboratório. A função do mediador (gerente do Sec-Mon) será realizada pelos professores responsáveis pelo LRG.

Um dos fatores essenciais para o sucesso de um Sec-Mon é relacionar com clareza as métricas que serão monitoradas. Nesse caso específico são utilizadas as métricas de segurança especificadas e validadas por [Righi et al., 2004] (observe a Tabela 2). No processo de escolha das métricas também foram levados em consideração os requisitos de segurança para redes de computadores classificados em [ISO 17799, 2005].

Tabela 3: Métricas utilizadas no Sec-SLA [Righi et al., 2004]

No	Métrica	Descrição
1	Número de vírus não detectados	Identifica o número de programas maliciosos que o usuário pode receber em determinado período.
2	Número de mensagens indesejadas recebidas	Define quantas mensagens indesejadas (SPAM) o usuário pode receber em seu correio eletrônico.
3	Treinamento de usuários	Informa a periodicidade com que os usuários participarão de treinamentos e palestras.
4	Controle Físico	Técnica utilizada para garantir a integridade física dos equipamentos e ativos digitais.
5	Política de backup	Mostra a freqüência dos backups, o meio de armazenamento e o tempo que eles são guardados.
6	Registro de eventos	Define qual a política adotada para arquivar os logs gerados pelos sistemas da organização.
7	Número de invasões	Calcula o número de invasões ao sistema vindas de dentro ou de fora da organização.
8	Gerência de senha	Apresenta a freqüência com que os usuários devem modificar sua senha e qual o seu formato (letras+ n^o).
9	Tempo de reparo	Informa o tempo que o departamento de TI leva para deixar o sistema operacional em caso de pane.
10	Plano de contingência	Exibe o plano que será executado em caso de uma atividade anormal ou inesperada acontecer na rede.

A implementação do Sec-Mon deve ser gradual. A interface de comunicação com o Sec-Mon será o navegador Web. A comunicação de aplicações externas que executam na rede de computadores com o Sec-Mon acontece através de scripts que lêem seus registros ou através de alterações nas próprias aplicações, como mostra o modelo conceitual. As bases de dados tornam-se tabelas armazenadas em um banco de dados, no caso o Mysql versão 4.0.2. O servidor de páginas Web e o banco de dados localizam-se no mesmo servidor. Este centralizará a maioria das funções do Sec-Mon.

Priorizou-se primeiramente a implementação das métricas "gerência de senhas" (métrica número 8) e "número de mensagens indesejadas recebidas" (métrica número 2). No caso da métrica 2 foi estipulado na interface uma forma dos usuários reportarem o recebimento desse tipo de mensagens. Essas informações são armazenadas na tabela de eventos e posteriormente avaliadas pelo mediador do Sec-Mon. Se elas forem consideradas válidas, serão contabilizadas no processo que verifica o cumprimento do Sec-SLA.

Outro aspecto relevante no processo de implementação do Sec-Mon é a montagem do diagrama de entidade-relacionamento (DER) do sistema. No caso do Sec-Mon que está sendo estabelecido, optou-se pelo DER exibido na Figura 5. Nessa figura observa-se que uma pessoa pode gerar um ou mais eventos. Cada evento está relacionado com uma métrica. A base de informação do modelo Sec-Mon conceitual "Métricas e Parâmetros do Sec-SLA" foi segmentada em três: métricas, penalizações e parâmetros. As métricas podem possuir um ou mais parâmetros (níveis de serviço), porém apenas um deles estará ativo por vez. A tabela de penalizações possui as atitudes

que são tomadas caso os níveis acordados no Sec-SLA não sejam alcançados. Uma pessoa pode sofrer várias penalizações e um tipo de penalização pode ocorrer (afetar) para várias pessoas. Por fim, toda penalização está associada a uma ou mais métricas.

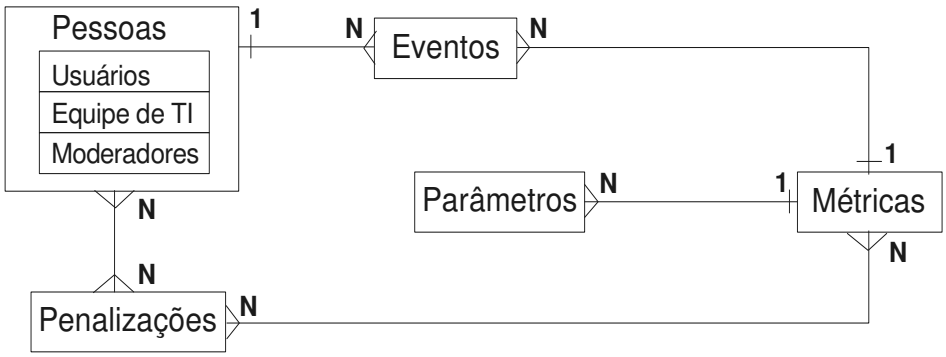

Figura 5: Diagrama Entidade-Relacionamento utilizado no protótipo Sec-Mon

5. Conclusão

A expansão dos acordos de níveis de serviço voltados à segurança (Sec-SLA) requer a existência de meios para monitorar e controlar esse tipo de contrato. A arquitetura Sec-Mon é um avanço na viabilização da adoção de Sec-SLAs, pois constitui um meio eficiente de averiguar ambas as partes do contrato, fazendo com que os administradores e usuários sejam capazes de fiscalizar um ao outro no cumprimento dos deveres de segurança.

O desenvolvimento do Sec-Mon aproxima a gerência e a segurança de redes de computadores. A arquitetura descrita nesse artigo preocupou-se em integrar as aplicações de segurança como *firewalls*, sistemas detectores de intrusão e programas antivírus com o ambiente de monitoração de acordos Sec-SLA. Seus componentes podem ser expandidos ou modificados, o que possibilita a implantação do Sec-Mon em diversos cenários de rede.

O protótipo da arquitetura Sec-Mon está em fase de desenvolvimento. A etapa que compreende a sua descrição e especificação foi vencida. A implementação dos componentes do Sec-Mon e a sua implantação em ambientes de produção são os atuais focos da pesquisa. Em trabalhos futuros, pretende-se exibir mais detalhes da implementação da arquitetura, assim como avaliações de sua utilização no Laboratório de Redes e Gerência (LRG-UFSC).

Referências

Brandão, José Eduardo M. S.; Fraga, Joni da Silva e Mafra, Paulo Manuel (2005). Composição de IDSs Usando Web Services. *In: V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG 2005)*. Florianópolis, SC, Brasil, pp. 339-342.

Buco, Melissa J.; Chang, Rong N.; Luan, Laura Z. e Ward, Christopher (2004). Utility Computing SLA Management based upon Business Objectives. *IBM Systems Journal*. IBM Corporation, ISSN: 0018-8670, 43(1): 159-178.

Case J.; Mundy, R.; Partain, D. e Stewart, B. (1999). Introduction to Version 3 of the Internet-standard Network Management Framework. *IETF Internet RFC 2570*, 23p. Available at: http:/www.ietf.org/rfc/rfc2570.txt.

Dutta-Roy, A (2000). The cost of quality in Internet-style network. *IEEE Spectrum*, 37(9):57-81.

Gaspary, Luciano P. e Fagundes, Leonardo L. (2003). Avanços Rumo à Integração de Tecnologias de Gerenciamento de Redes e Segurança. *Minicurso da Escola Regional de Redes de Computadores – ERRC*. PUCRS, Porto Alegre, Brasil.

Habib, Ahsan; Fahmy, Sonia e Bhargava, Bharat (2005). Monitoring and Controlling QoS Network Domains. *International Journal of Network Management*, 15(1), 11-29.

Henning, Ronda R. (2000). Security Service Level Agreements: Quantifiable Security for the Enterprise?. *In: Proceedings of the workshop on New Security Paradigms*, pages 54–60. ISBN:1-58113-149-6.

ISO 17799 (2005). Padrão Internacional ISO/EIC 17799: Tecnologia da Informação – Código de Prática para Gestão da Segurança de Informações, 81p.

Krief, Francine (2004). Self-aware management of IP networks with QoS guarantees. *International Journal of Network Management (IJNM)*, 14(5), 351-364.

Left, Avrahan e Rayfield, James (2003). Service Level Agreements and Commercial Grids. *IEEE Internet Computing*, 7(4):44–50.

Mckenna, Brian (2002). Managed Security Services— new economy relic or wave of the future? *Computers & Security*, 21(7):613–616.

Menegazzo, Cinara T. (2000). Raciocínio Baseado em Casos Aplicado a Diversos Domínios de Problema.. *Dissertação de Mestrado em Ciência da Computação da Universidade Federal do Rio Grande do Sul* – PPGCC-UFRGS, 171p.

Muller, Nathan J. (1999). Management of Service Level Agreements. *International Journal of Network Management*, 9(3):155–166.

Navarro, Luis (2001). Information Security Risks and Managed Security Service. *Information Security Technical Report,* 6(3):28–36.

Righi, Rafael da R., Pellissari, Felipe R. e Westphall, Carlos B. (2004). Sec-SLA: especificação e validação de métricas para acordos de níveis de serviço orientados à segurança. *In: IV Workshop de Segurança de Sistemas Computacionais (Wseg/ SBRC)*, pages 199–210. Gramado, RS. ISBN: 85-88442-84-1.

SLA Management Team. (2001). SLA Management Handbook. *Tele Management Forum*. Public Evaluation, Version 1.5 GB 917.

Walt, Andre V. D. (2003). Managed Security Services – who needs it? *Computer Fraud and Security,* 2003(8):15–17.