Representando opiniões em cadeias de confiança SPKI/SDSI

José de R. B. Pinheiro Júnior, Vladimir Moreira Rocha , Fabio Kon

[1]Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo

{jrbraga,vmoreira,kon}@ime.usp.br

Resumo. *O SPKI/SDSI é um modelo de segurança flexível e extensível que permite autenticação, confidencialidade e controle de acesso de forma igualitária e descentralizada. No entanto, este modelo não é apropriado para ambientes dinâmicos de grande escala como grades computacionais, cujos recursos e sujeitos envolvidos podem variar largamente ao longo do tempo. Neste trabalho, estende-se o modelo SPKI/SDSI para incluir um modelo de opinião baseado em lógica subjetiva. A eficácia da proposta é avaliada através de simulações.*

Abstract. *SPKI/SDSI is a flexible and extensible decentralized security model that provides authentication, confidentiality, and access control. However, SPKI/SDSI certification chains are not suitable for large scale, highly dynamic enviroments such as computational grids. This work extends the SPKI/SDSI model by including an opinion model based on subjective logic. A simulation is performed to evaluate the effectiveness of the proposal.*

1. Introdução

Prover segurança no acesso às informações é uma tarefa árdua e envolve questões que podem ou não ser técnicas. Se por um lado as tecnologias de segurança surgiram para dificultar a tentativa de acesso não autorizado a informações, por outro, pessoas ou agentes de um sistema computacional dotados de privilégios podem acabar utilizando suas prerrogativas para executar ações indevidas. Considere, por exemplo, um sistema dito seguro que proteja informações privilegiadas de uma empresa. Neste caso, basta apenas que um funcionário, possivelmente novo na empresa, para o qual foi delegado o direito de acessar um software corporativo, utilize este sistema de forma indevida para que as informações estejam comprometidas. Acontece que o referido usuário poderia necessitar destes direitos concedidos para executar suas funções dentro da corporação, de outra forma seu trabalho estaria prejudicado.

A questão por trás dos fatos discorridos anteriormente é que uma parte dos sistemas de segurança não estão preparados para considerar os históricos de relacionamentos entre os sujeitos participantes. Nestes casos, um sujeito recebe direitos de uso de recursos de uma forma binária e sobre ele não é tomado qualquer valor que considere o fato dele não possuir um histórico que permita estabelecer seu grau de confiança . É importante ressaltar que um usuário, mesmo legítimo, pode, em determinado momento, executar ações indevidas e então passar a ser não confiável. No mundo real é bastante comum afirmações do tipo: “depois que eu emprestei dinheiro para fulano, ele não me parece o mesmo”, o que indica que as opiniões podem mudar com o tempo.

Em ambientes de rede centralizados, este problema é resolvido pelos administradores. Cabe a eles, os administradores, e não aos verdadeiros donos do recurso decidir sobre quem é ou não confiável. Em geral, nestes casos, existe uma ou mais base de dados que é responsável pela identificação e controle de acesso aos recursos. Cabe ao dono de um recurso confiar totalmente nestes administradores e assim delegar a eles o direito de uso. O administrador teria que "conhecer" todos os sujeitos (ou grupos deles) e decidir por eles se alguém é confiável ou não.

Em ambientes mais particulares, como o de grades computacionais [5, 3], estas tarefas se fazem mais difíceis de tratar. Nestes casos é comum, e bem provável, que as grades sejam formadas por domínios administrativos diferentes. Dessa forma, usando a mesma solução anterior, caberia aos administradores decidir sobre o uso dos recursos da grade. Esta estratégia facilita a administração, porém dificulta o uso em ambientes de maior escala em que milhares de recursos podem ser adicionados ou retirados com facilidade todos os dias. O verdadeiro dono do recurso não poderia intervir sobre o uso de seus recursos devendo submeter-se às políticas de segurança definidas pelo administrador do domínio ao qual pertence, com mais, ou menos, direitos cedidos do que desejado.

As grades oportunistas são um caso particular de grades computacionais [15]. Nestas grades, usuários cedem seus recursos ociosos à grade e estes podem ser utilizados por aplicações da grade de acordo com sua disponibilidade. Sistemas como estes devem ser bastantes escaláveis e necessitam de um cuidado maior quanto à segurança, pois o custo administrativo de incluir ou retirar centenas de recursos sob demanda seria muito alto.

Uma solução a ser considerada quanto ao controle de acesso aos recursos de forma descentralizada são as cadeias de confiança (*Trust Chains*) [12]. As cadeias de confiança são baseadas nas relações de confiança mútua entre sujeitos. Através destas relações, os sujeitos podem transmitir o direito de acesso aos seus recursos de forma direta ou indireta. No primeiro caso, o dono do recurso cede o recurso a um terceiro em que confia. Eventualmente, este mesmo sujeito pode redelegar os recursos que lhes foram delegados, o que pode acontecer subseqüentemente formando uma cadeia de confiança.

O SPKI/SDSI [4] é uma opção de implementação dos conceitos de redes de confiança. No SPKI/SDSI, cada sujeito gerencia seu próprio espaço de nomes localmente. O sujeito, representado por sua chave pública, decide sobre o uso de seus recursos de acordo com políticas sobre as quais tem total controle. O SPKI/SDSI no entanto, reflete a confiança entre sujeitos de uma forma binária; assim, quando decide se um usuário é confiável, parte do princípio que possui total certeza dessa afirmação. O que nos faz retornar à questão colocada anteriormente, de que não se considera as interações entre os sujeitos para se tomar decisões relativas à segurança dos recursos. Este trabalho apresenta uma extensão ao modelo do SPKI/SDSI prevendo a utilização dos conceitos de lógica subjetiva para representar as relações de confiança entre sujeitos.

Este artigo está organizado da seguinte forma. Primeiramente, na Seção 2 descreve-se o modelo de redes de confiança do SPKI/SDSI e seus conceitos básicos. A seguir, apresenta-se os trabalhos relacionados na área. Na seção seguinte discute-se o modelo definido por Jøsang como uma forma de exprimir opiniões para representar, através do uso de lógica subjetiva, a opinião de um sujeito sobre suas relações de confiança. Este modelo será usado para estender o SPKI/SDSI. Na Seção 5 apresenta-se

uma simulação em um ambiente que representa uma grade computacional oportunista. Finalmente, discorre-se sobre as conclusões acerca do trabalho, suas implicações e caminhos futuros a serem seguidos.

2. Modelo de cadeias de confiança SPKI/SDSI

O SDSI [17] foi projetado no MIT por Ronald Rivest e Butler Lampson. Seu desenvolvimento foi motivado pela complexidade das infra-estruturas de chave públicas, em especial sua dependência em espaços de nomes globais. O SDSI é uma infra-estrutura de chaves públicas com espaço de nomes locais, o que concede a ele características de descentralização. O SPKI (Simple Public Key) foi desenvolvido por Carl Ellison e outros [4] e é um sistema simples e flexível de autorização. A união dos dois projetos constituiu o SPKI/SDSI um sistema de autenticação e autorização que combina os espaços de nomes locais do SDSI com o sistema de autorização do SPKI.

No SPKI/SDSI, a identificação é feita através de chaves públicas e não por um nome. O SPKI/SDSI relaciona uma chave pública a um nome no espaço de nomes local do usuário. Esta relação é conhecida somente localmente, ou seja, o nome associado não necessita ser globalmente único. O SPKI/SDSI permite a definição de grupos, onde cada grupo possui um nome e um conjunto de membros, podendo referenciar também outros grupos.

Como uma solução totalmente distribuída, o SPKI/SDSI permite flexibilidade nas definições de certificados. Cada usuário é responsável por gerenciar seus próprios certificados, ou seja, é uma autoridade certificadora. Existem dois tipos de certificados no SPKI/SDSI: o Certificado de Nome (*Name Certs*) e o Certificado de Autorização (*Auth Certs*). O Certificado de Nome providencia autenticidade de um nome local, ou seja, ele certifica que o nome criado dentro do espaço de nomes do emissor é válido. O Certificado de Autorização concede uma autorização de acesso a um recurso ao sujeito do certificado.

Um Certificado de Nome é composto por quatro campos: *issuer*, *identifier*, *subject* e *validity specification* [2]. O *issuer* é a chave pública que assina o certificado. O *identifier* identifica o nome local que se está definindo. O *subject* é representado por uma chave pública ou por um nome. Caso o *subject* não seja iniciado por uma chave pública, considera-se que o nome pode ser encontrado dentro do espaço de nomes local. O *validity specification* descreve as condições de validade do certificado, podendo indicar um intervalo de tempo ou até mesmo uma lista de revogação.

Um Certificado de Autorização consiste de cinco campos: *issuer*, *subject*, *delegation* , *tag* e *validity specification*. Os dois primeiros têm função análoga ao Certificado de Nome explanado anteriormente, sendo que o *subject* pode também indicar um grupo. O campo *delegation* indica se o certificado pode ser delegado ou não. O *tag* especifica que tipo de autorização (ou autorizações) o sujeito do certificado receberá. O *validity specification* tem função análoga ao Certificado de Nome.

Através da indicação do campo *delegation*, um Certificado de Autorização pode permitir que o sujeito do certificado delegue seus direitos a outros sujeitos. A Figura 1 mostra um exemplo típico de delegação que poderia ocorrer no SPKI/SDSI. O detentor do recurso sistema de arquivos (ou um sistema de gerenciamento que o represente) emite um certificado com delegação para D_1 permitindo o direito de escrever ou ler (RW), negando porém a possibilidade que este direito possa ser redelegado (ND). Para o delegado D_2,

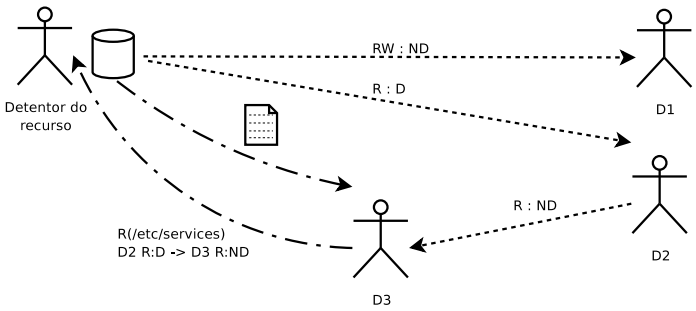


Figura 1. Delegação de um Certificado

no entanto, é permitido somente a leitura (R), sendo que este direito pode ser repassado a terceiros (D). Na mesma Figura, o delegado D_2 repassa o direito de leitura para o D_3 indicando que este não pode ser redelegado. Ao acessar um determinado arquivo, D_3 prova que tem este direito apresentando toda a cadeia de delegação ($D_2\ R : D \longrightarrow D_3\ R : ND$). Uma cadeia de autorização pode ser reduzida para uma delegação entre o dono do recurso e aquele que o recebeu [9].

3. Trabalhos relacionados

O modelo provido pelo SPKI/SDSI possui uma vantagem crucial para ambientes distribuídos: não possuir um ponto único de falha. No entanto, a dificuldade de gerenciar uma base totalmente distribuída apresenta alguns problemas. Em primeiro lugar, o modelo exige que para cada acesso a um recurso exista uma cadeia de autorização a ser validada. Em seguida, o modelo não define um repositório de certificados, distribuído ou não. Estes dois pontos resultam na proibição do acesso ao recurso desejado caso uma cadeia não seja resolvida. Santin *et al* [18] propõe uma extensão ao modelo SPKI/SDSI para a construção de novas cadeias de autorização baseado no conceito de federações. No modelo proposto, as federações permitem que seus membros compartilhem certificados de nomes e de autorização.

O tamanho da cadeia também pode ser um problema em sistemas de segurança que se baseiam no SPKI/SDSI. A questão aqui não se refere somente ao problema de busca dessa cadeia, mas pela impossibilidade do delegador limitar o seu tamanho. Suponha que um sujeito (Beto) delega, através de um certificado apropriado, um recurso para outro sujeito (Márcia). Beto não tem como controlar para quantos outros sujeitos Márcia irá redelegar o certificado inicial, ou o que seria pior, quantas vezes sucessivamente o certificado seria redelegado. Vários trabalhos tratam de questões relativas ao formalismo dos espaços de nomes, resolução de cadeias e redução de tuplas para o SPKI/SDSI [1, 9, 10, 14, 2].

Mesmo que não houvesse o problema de resolução de cadeias em um sistema baseado no SPKI/SDSI, as relações de confiança providas por esse modelo são baseadas na assinatura em cadeia de certificados. A medida de relação de confiança entre os participantes desta cadeia é binária, ou seja, uma cadeia é considerada completamente válida ou inválida. Em nenhum momento é levado em conta que os sujeitos podem possuir níveis de confiança diferentes entre eles, assim como acontece nas relações humanas. Da mesma maneira, a redução de cadeias esconde o caminho pelo qual o certificado se originou e também o nível de confiança que os sujeitos que fazem parte dele possuem entre si. Na

próxima seção, apresentar-se-á uma forma de exprimir opiniões entre sujeitos em uma cadeia de confiança com o objetivo de minimizar os problemas aqui relatados.

4. Exprimindo opiniões em uma rede SPKI/SDSI

Em alguns ambientes específicos, como os de grades computacionais, podem haver relacionamentos de confiança entre sujeitos de uma forma bem dinâmica. O modelo de cadeias de confiança implementado pelo SPKI/SDSI, por outro lado, não valoriza este tipo de interação. Para exemplificar, considere a cadeia de confiança na Figura 2; ela representa a relação de confiança entre os sujeitos de A até D. Caso C não seja muito confiável, porque age de forma indevida ou até mesmo por ser novo na grade, toda a cadeia poderia estar comprometida.

Figura 2. Cadeia de certificação com o nó C não muito confiável

Neste trabalho é proposta a utilização do conceito de lógica subjetiva na relação de confiança entre os usuários. A lógica subjetiva é definida como uma lógica que opera em nossas crenças subjetivas a respeito do mundo [11]. Assim, a confiança em um sujeito, ou em uma chave criptográfica que o representa, poderia ser medida através de opiniões geradas por outros sujeitos. Esta quantificação poderia ser utilizada pelo provedor do recurso para decidir, utilizando suas políticas de segurança, sobre o uso de seus recursos.

4.1. Modelo de Jøsang

Para representar a opinião, utilizou-se o modelo definido por Audun Jøsang [11, 12]. A opinião é definida como a crença de um determinado sujeito tem sobre uma sentença que pode ser verdadeira ou falsa. Assim, por exemplo, pode-se utilizar este modelo para representar a seguinte opinião: "a chave de um determinado sujeito é autêntica". A opinião ω é expressa matematicamente como:

$$\omega = \{b, d, u\} \quad \text{tal que} \quad b + d + u = 1, \quad \{b, d, u\} \in [0, 1]^3 \tag{1}$$

onde b, d e u são números reais que representam, respectivamente, crença, descrença e incerteza. A opinião é representada através da letra ω e de letras sobresescritas e subscritas de tal forma que

$$\omega_p^A = \{b_p^A, d_p^A, u_p^A\} \tag{2}$$

representa a opinião que um sujeito A possui sobre uma sentença p, com a crença, a descrença e a incerteza definida por b_p^A, d_p^A, u_p^A, respectivamente.

Jøsang descreve vários operadores lógicos para combinar opiniões [12]. Os operadores definidos podem ser equivalentes aos tradicionais como *OR*, *AND*, *NOT* ou não tradicionais como CONJUNÇÃO, RECOMENDAÇÃO e CONSENSO. A CONJUNÇÃO é usada quando um sujeito necessita juntar opiniões a respeito de duas sentenças independentes. A RECOMENDAÇÃO acontece quando um sujeito B recomenda ao sujeito A a sua opinião sobre uma sentença p. A opinião resultante pode ser interpretada como a opinião A a partir da opinião que B possui. O CONSENSO é relativo à opinião formada sobre uma sentença a partir de duas outras opiniões. A seguir a definição mais formal de cada um destes operadores.

Definição 1: **CONJUNÇÃO**

Seja $\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ e $\omega_q^A = \{b_q^A, d_q^A, u_q^A\}$, opiniões sobre as sentenças p e q, respectivamente. A conjunção de ω_p^A e ω_q^A sobre as sentenças binárias p e q é definida por

$$\omega_{p\Lambda q}^A = \omega_p^A \Lambda \omega_q^A = \{b_{p\Lambda q}^A, d_{p\Lambda q}^A, u_{p\Lambda q}^A\} \qquad \text{onde} \qquad \begin{cases} b_{p\Lambda q}^A = b_p^A b_q^A \\ d_{p\Lambda q}^A = d_p^A + d_q^A - d_p^A d_q^A \\ u_{p\Lambda q}^A = b_p^A u_q^A + u_p^A b_q^A + u_p^A u_q^A \end{cases}$$

Definição 2: **RECOMENDAÇÃO**

Sejam A e B dois sujeitos onde $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$ é a opinião de A sobre a recomendação de B e seja p uma sentença binária onde $\omega_p^B = \{b_p^B, d_p^B, u_p^B\}$ é a opinião de B sobre p em recomendação a A. Então a opinião de A sobre p como resultado da recomendação de B é definida por

$$\omega_p^{AB} = \omega_B^A \otimes \omega_p^B = \{b_p^{AB}, d_p^{AB}, u_p^{AB}\} \qquad \text{onde} \qquad \begin{cases} b_p^{AB} = b_B^A b_p^B \\ d_p^{AB} = b_B^A d_p^B \\ u_p^{AB} = d_B^A + u_B^A + b_B^A u_p^B \end{cases}$$

Definição 3: **CONSENSO**

Sejam $\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ e $\omega_p^B = \{b_p^B, d_p^B, u_p^B\}$, respectivamente as opiniões tomadas pelos sujeitos A e B sobre uma afirmação. A opinião do CONSENSO tomada por um sujeito imaginário [A,B] representando A e B é definida por

$$\omega_p^{A,B} = \omega_p^A \oplus \omega_p^B = \{b_p^{A,B}, d_p^{A,B}, u_p^{A,B}\} \qquad \text{onde} \qquad \begin{cases} b_p^{A,B} = b_B^A b_p^B \\ d_p^{A,B} = b_B^A d_p^B \\ u_p^{A,B} = d_B^A + u_B^A + b_B^A u_p^B \end{cases}$$

4.2. Aplicando o modelo de Jøsang no SPKI/SDSI

Nesta subseção apresenta-se a aplicação do modelo de Jøsang no SPKI/SDSI. Estende-se os conceitos de opinião para representar a confiança entre sujeitos de uma cadeia SPKI/SDSI, destacando-se quais operações que poderiam ser usadas para compor uma opinião sobre esta cadeia. Ademais, define-se um gerador de opiniões que trata eventos de segurança para gerar opiniões sobre sujeitos através da um sistema de créditos.

Os conceitos de lógica subjetiva associados ao modelo de Jøsang podem ser tomados para tentar minimizar o problema apresentado na Figura 2. Opiniões sobre os componentes de uma determinada cadeia de confiança poderiam nortear as decisões sobre o uso de recursos. As operações definidas por Jøsang, apresentadas anteriormente, podem ser aplicadas sobre a cadeia para compor uma opinião.

Definição 4: **Opinião entre sujeitos**

Seja A um sujeito e b a sentença que afirma “O sujeito B é confiável”, então

$$\omega_b^A = \{b_b^A, d_b^A, u_b^A\}$$

é a opinião de A sobre B ser confiável ou não.

A Figura 3 apresenta uma cadeia de confiança utilizando os conceitos de opinião aqui apresentados. Neste exemplo o sujeito A deseja verificar uma cadeia de confiança através de delegações feitas a partir dele até o sujeito final D. Ele possui opiniões bem formadas sobre a credibilidade de cada um dos participantes da cadeia, com exceção do sujeito C. Na falta dessa informação, ele usa a sua opinião sobre a recomendação dada por E para compor a opinião sobre C. A opinião final sobre a cadeia é conseguida através do consenso de todas as opiniões tomadas pelo provedor do recurso A sobre cada um dos sujeitos, incluindo a recomendação dada por E sobre C.

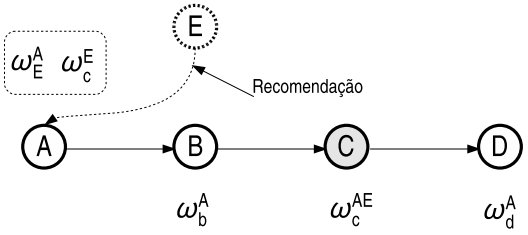


Figura 3. Cadeia de certificação com o nó C não muito confiável

A Figura 4 mostra duas situações que representam a mudança de opinião de um sujeito a partir de seu comportamento. Inicialmente elas partem de uma opinião ω_0, totalmente imprecisa, que é representada no modelo como a tupla $\{0, 0, 1\}$. Na primeira situação, o sujeito possui um comportamento hostil e sua opinião mudaria ao longo do tempo com uma tendência crescente da descrença. No caso extremo, a opinião poderia alcançar a situação de total descrença no ponto $\omega_I = \{0, 1, 0\}$. Na outra situação, um comportamento amistoso faria a opinião mudar até um ponto que indicaria uma crença maior. Note na figura apresentada, que uma vez que a opinião poderia representar se um determinado usuário é confiável ou não, as áreas hachureadas simbolizariam regiões onde se classificariam os amigos, inimigos ou desconhecidos, sendo eles muito confiáveis, pouco confiáveis ou sem muita certeza disso, respectivamente.

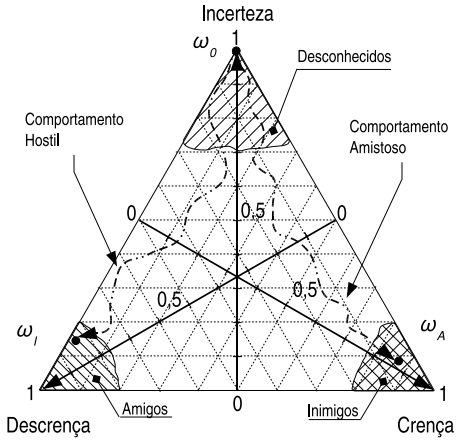


Figura 4. Mudança de opinião

Para gerar uma opinião é necessário ter mecanismos que obtenham informações que sejam usadas para decidir se um sujeito é confiável ou não. A Figura 5 mostra os tipos de dados de entrada que poderiam ser usados para compor um julgamento. O histórico de relacionamentos entre pares, indicando uso correto de recursos cedidos, poderia influ-

enciar positivamente a crença em um sujeito. Os registros (*logs*) de eventos de segurança relevantes, por outro lado, poderia ser usado para aumentar a descrença em um sujeito. Um usuário poderia intervir manualmente sobre a apreciação da credibilidade de um sujeito de acordo com suas próprias convicções. O padrão de uso de um usuário, por sua vez, poderia ser usado para apontar ações indevidas que fogem daquilo que é esperado para um determinado sujeito. Finalmente, outras informações poderiam ser utilizadas da mesma maneira a contribuir na definição de um ponto que represente a opinião sobre um sujeito.

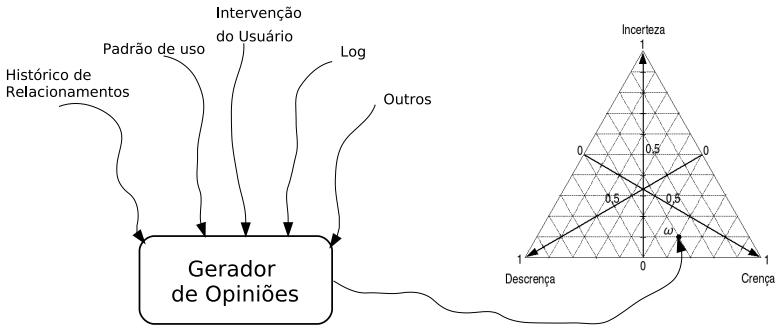


Figura 5. Gerador de opiniões

A Tabela 1 mostra uma possível maneira de incrementar a opinião através de um sistema de crédito. Neste sistema, as operações de crédito de crença e descrença ocorreriam de acordo com pesos w definidos para cada operação. Estes pesos poderiam ser associados a valores ponderados de acordo com valores padrão ou definidos através de intervenção do usuário. Assim, de acordo com a mesma tabela, uma operação de crédito de crença corresponderia a um débito do mesmo valor de descrença para manter a relação definida em (1). Um aumento da incerteza, por sua vez, corresponderia uma diminuição de crédito na crença e descrença. Dessa maneira, a opinião poderia mudar de acordo as várias interações entre sujeitos.

Tabela 1. Sistemas de créditos para o modelo de opinião.

Operação de credito	b	u	i
Crença	+w	-w	0
Descrença	-w	+w	0
Incerteza	$-\frac{w}{2}$	$-\frac{w}{2}$	+w

4.3. Extensão do Modelo SPKI/SDSI

Para estender o SPKI/SDSI propõe-se a criação de um Certificado de Opinião. Um Certificado de Opinião contém quatro campos: *issuer*, *subject*, *opinion* e *validity specification*. O *issuer* é o dono da opinião, o sujeito que dará seu juízo sobre um outro. O *subject* é o sujeito a ser julgado, aquele sobre o qual foi formada uma opinião. O campo *opinion* é a opinião propriamente dita; ela é composta de três subcampos: crença, descrença e incerteza, de acordo com o definido por (1) e (2). Esta opinião é construída sobre a seguinte sentença "*issuer* confia no *subject*". Finalmente, *validity specification*, representa o contexto no qual esta opinião foi gerada.

A extensão proposta agrega ao modelo SPKI/SDSI a possibilidade de pares de sujeitos ajuizarem opiniões entre si, o que traz vantagens claras. A composição de opiniões resulta numa verificação de cadeia que considera as opiniões não binárias tomadas para todos os sujeitos envolvidos. Através desta extensão, é possível provar matematicamente que uma cadeia longa resulta numa opinião composta (conjunção) que tende a aumentar a incerteza. Caso haja o conceito de federação, uma confiança maior entre os membros, reforçará as relações entre eles permitindo que o uso de seus recursos possam ser priorizados. Finalmente, o teor não binário para a confiança entre sujeitos permite que o acesso aos recursos possa ser efetuado com restrições (menos disco do que o desejado, por exemplo), de acordo com políticas de segurança apropriadas. Por exemplo, um sujeito cuja a opinião tende a ser confiável poderia obter o acesso a leitura e escrita em um sistema de arquivos; um outro sujeito, não confiável, teria o acesso ao recurso negado. No mesmo exemplo, um sujeito medianamente confiável poderia obter o acesso ao sistema de arquivos somente para leitura. A seguir apresentar-se-á um ambiente de simulação usado para validar as extensões do modelo SPKI/SDSI propostas aqui.

5. Simulações e resultados obtidos

Esta seção apresenta a implementação de uma simulação de um ambiente de grade na qual se aplicou a extensão do modelo SPKI/SDSI proposta neste trabalho. A grade utilizada foi definida de acordo com a arquitetura do InteGrade[1] [13, 6, 7]. Uma grade InteGrade é constituída, conceitualmente, de aglomerados (*clusters*) de computadores organizados de forma hierárquica. No InteGrade, dois módulos cooperam no gerenciamento dos recursos de um aglomerado: o LRM (*Local Resource Manager*) e o GRM (*Global Resource Manager*). O primeiro é responsável pela coleta de informações e pelo controle de uso dos recursos locais em um determinado nó, enquanto o seguinte é responsável por escalonar processos e pela comunicação com gerenciadores de outros aglomerados. O módulo LUPA (*Local Usage Pattern Analyzer*) compila um conjunto de informações que representam, com certo grau de confiança, o padrão de uso de um determinado usuário. Além destes anteriormente citados, existem outros módulos cujas funções são de armazenamento de aplicações, controle de submissão e controle de condições de compartilhamento.

Para realizar os experimentos, utilizou-se Java e o simulador do projeto Bamboo [2] que permite comunicação usando mensagens assíncronas. O ambiente de grade simulado foi composto por 100 sujeitos que representam os gerenciadores LRM. Por questão de simplificação, considerou-se que cada sujeito controla apenas um recurso que pode ser acessado com ou sem restrições. O GRM[3], por sua vez, provê o serviço usado para resolver as cadeias de delegação, ou seja, como buscar opiniões relativas aos sujeitos desconhecidos pertencentes a uma determinada cadeia. Finalmente, o módulo LUPA disponibiliza informações sobre os perfis de uso dos sujeitos na grade.

A inicialização do ambiente ocorre da seguinte forma. Inicialmente as opiniões entre os sujeitos da grade é incerta ($\omega = \{0, 0, 1\}$, para o modelo de opinião usado). Em seguida, os sujeitos delegam seus recursos para outros sujeitos da grade de forma aleatória. Os sujeitos tentam acessar os recursos e, de acordo com as ações tomadas[4],

[1] `http://www.integrade.org.br`
[2] `http://www.bamboo-dht.org`
[3] O GRM já possui um serviço de busca na sua implementação original. Este serviço foi representado na simulação.
[4] Estas ações são executadas considerando que alguns sujeitos presentes na grade podem ter atitudes hostis.

as opiniões entre os pares de sujeitos são geradas. As opiniões foram atualizadas utilizando as operações de crédito mostradas na Tabela 2, com o peso w fixado em 0.1. Finalmente, as cadeias de confiança foram criadas através da redelegação dos recursos de forma aleatória, porém, em eventos independentes dos anteriores. No ambiente simulado,

Tabela 2. Sistemas de créditos para o modelo de opinião.

Ações executadas	**Operação de crédito**	**w**
Acesso legítimo ao recurso	Crença	0.1
Acesso legítimo ao recurso, porém fora do padrão de uso	Descrença	0.1
Acesso ilegítimo ao recurso	Descrença	0.1

cada sujeito da grade apresenta uma cadeia de confiança sempre que necessita acessar um recurso. Três níveis de opinião foram definidos para permitir o controle de acesso aos recursos. Os recursos podem ser acessados sem nenhuma restrição, se o resultado da **conjunção** entre as opiniões sobre cada elemento da cadeia atingir um nível de confiança considerado aceitável ($W_r(b, d, i)$ onde $b \geq 0.6, d \leq 0.2, i \leq 0.2$). Caso a opinião sobre a cadeia esteja entre os valores $W_b(b, d, i)$ onde $0.2 < b < 0.6, d \leq 0.2, 0.2 < i < 0.7$), uma restrição é feita no acesso ao recurso. Em ambos os casos anteriores, se o dono do recurso não possuir opinião sobre um outro sujeito que pertence à cadeia apresentada a ele, este poderá fazer uma busca na rede e compor uma **recomendação**. Finalmente, se a opinião tomada para a cadeia estiver em níveis altos de desconfiança ($d > 0.2$), o acesso ao recurso é negado, apesar da cadeia ser considerada válida.

O experimento foi dividido em duas partes. Na primeira considerou-se individualmente um determinado sujeito cujo comportamento foi variando de amistoso a hostil[5]. As cadeias de delegação deste sujeito foram classificadas entre aceitas, aceitas com restrição ou negadas. Na última parte do experimento, analisou-se a classificação de todas cadeias da grade quando as atitudes dos sujeitos tendiam a ser hostis. O objetivo destes experimentos foi verificar de que forma o comportamento de um sujeito na grade, e conseqüentemente as opiniões sobre ele, afetam positiva ou negativamente a classificação das cadeias.

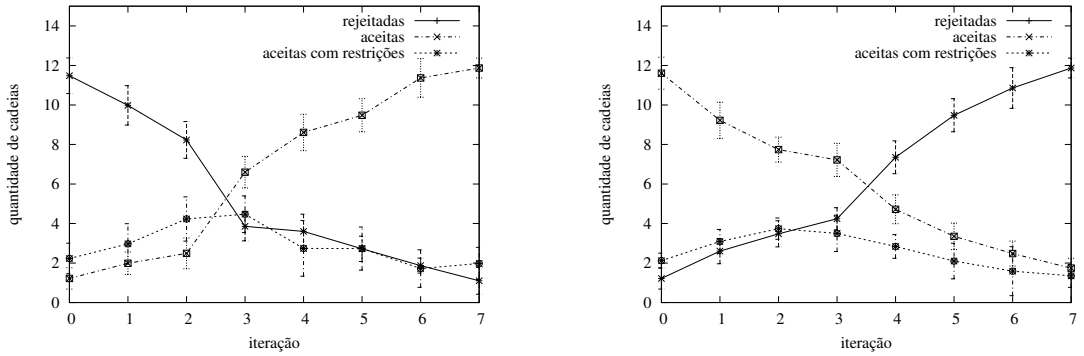
5.1. Ambiente de simulação

A simulação foi executada em um PC de 2.4 GHz, 1 GByte de memória RAM e sistema operacional GNU/Linux. Para a comunicação entre os nós do simulador, utilizou-se a topologia de rede baseada no *King* [8]. Esta topologia, muito utilizada em simulações de redes de grande área, representa uma situação realista de uma grande variedade de nós da Internet, com suas restrições de largura de banda e latência. No caso do Bamboo, para os parâmetros como o tempo de atualização das estruturas internas, mensagens *keep-alive*, entre outros, utilizou-se os valores pré-definidos pelo simulador ([16]).

[5]Dentro da simulação um comportamento amistoso foi representado como o acesso a recursos sobre os quais os sujeitos tem direito. O caso contrário foi associado a comportamento hostil.

5.2. Comportamento individual

No primeiro experimento mediu-se como a mudança de comportamento de um sujeito influenciou a classificação das suas cadeias. Por exemplo, inicialmente um sujeito toma atitudes que geram opiniões favoráveis a ele na grade, em seguida ele muda de comportamento e procede com tendência[6] agressiva. As opiniões tomadas sobre as atitudes dos sujeitos seguiram o modelo de gerador de opiniões definido na Figura 5, considerando o padrão de uso dos usuários e registros de eventos de segurança de acordo com as operações de crédito da Tabela 2. As variações dos comportamentos analisados foram: (i) pouco confiável a muito confiável; (ii) muito confiável a pouco confiável; (iii) permanecendo como muito confiável e (iv) permanecendo como pouco confiável.



(a) pouco confiável a muito confiável

(b) muito confiável a pouco confiável

Figura 6. Classificação de cadeias sem mudança de comportamento

Para o comportamento (i), o sujeito faz acessos que permitem aumentar seu nível de confiança. Na Figura 6(a), pode-se observar que inicialmente a maioria das cadeias são rejeitadas com baixa incidência de cadeias aceitas com ou sem restrições. Ao longo do tempo, em cada iteração, as cadeias rejeitadas diminuem e, conseqüentemente, as cadeias aceitas aumentam. É interessante notar que na curva que representa as cadeias aceitas com restrição obtém-se uma elevação transitória; neste intervalo o sujeito poderia ser considerado medianamente confiável e usaria os recursos de forma limitada.

Para o comportamento (ii), o sujeito faz acessos que permitem aumentar seu nível de confiança. Na Figura 6(b), podemos observar que o comportamento das curvas é o inverso ao experimento anterior, ou seja, inicialmente a maioria das cadeias são aceitas e a cada passo da simulação elas vão diminuindo. Assim como no experimento anterior, um aumento transitório também ocorre nas cadeias aceitas com restrições.

Na Figura 7 mostra-se os dois últimos comportamentos: (iii) e (iv). No caso do sujeito muito confiável, o experimento mostra que a quantidade de cadeias aceitas se mantém, com pequenas variações, ao longo do tempo. Quando um sujeito é pouco confiável, e mantém essa atitude ao longo do experimento, a totalidade de cadeias aceita é nula. O resultados obtidos nestas duas situações indicam que há estabilidade na aceitação das cadeias quando o comportamento é mantido.

[6]Como, em nossa simulação, os eventos são gerados de forma aleatória, o termo tendência significa que há uma probabilidade maior de um sujeito efetuar ações indevidas.

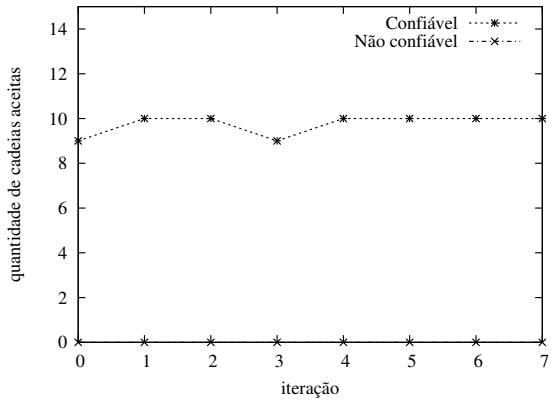


Figura 7. Cadeias aceitas sem mudança de comportamento

5.3. Comportamento coletivo

No segundo experimento analisou-se a classificação das cadeias em relação à quantidade de sujeitos não confiáveis que a grade possui. A Figura 8 mostra a relação entre o percentual de cadeias aceitas/rejeitadas e o percentual de sujeitos não confiáveis presentes na grade. Um usuário não confiável invalida a cadeia toda, por isto o gráfico mostra somente as curvas das cadeias rejeitadas e aceitas. As duas curvas, que são complementares, mostram que o aumento da quantidade de GRMs não confiáveis na grade aumenta o número de cadeias rejeitadas.

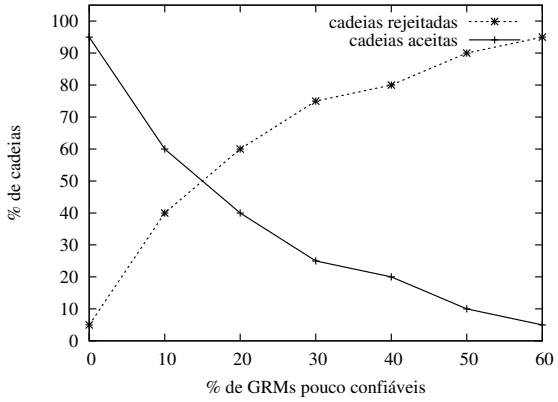


Figura 8. Cadeias aceitas com sujeitos não confiáveis

De acordo com os resultados obtidos durante a simulação, pôde-se notar que a classificação das cadeias de forma a permitir, negar ou retringir os acesso aos recursos possui uma relação direta com as atitudes tomadas pelos sujeitos. Ademais, sujeitos que acessaram somente recursos sobre os quais possuem total direito de acesso, de acordo com o perfil esperado, tem uma opinião tendendo para uma credibilidade total. Por outro lado, o oposto ocorre com sujeitos totalmente mal intencionados. A possibilidade de limitar o acesso aos recursos de acordo com opiniões intermediárias (entre fortemente confiável e fracamente confiável) permite que sejam definidas políticas de segurança mais flexíveis. Finalmente, conclui-se, através dos resultados obtidos, que a extensão ao modelo do SPKI/SDSI contemplando conceitos de lógica subjetiva para prover opiniões entre sujeitos pode ser uma boa opção para uma implementação real.

6. Conclusões e Trabalhos Futuros

A extensão aqui proposta para o SPKI/SDSI introduz um conceito novo ao modelo inicial: a subjetividade. Com este conceito é possível atribuir valores contínuos (não binários) para representar a confiança que sujeitos podem ter sobre outros. A partir dessa característica é possível representar mais adequadamente a forma com que humanos se relacionam, valorando suas relações de confiança de acordo com informações históricas.

O modelo baseado em lógica subjetiva proposto por Jøsang é considerado adequado para a representação de opiniões. O formalismo usado nas suas definições, foi um dos pilares sobre os quais foi baseado a proposição inicial deste trabalho. Deve-se, no entanto, verificar se as operações matemáticas definidas são suficientes ou se existe a necessidade de acrescentar outras que representem necessidades específicas. Experimentos em ambientes reais poderão indicar possíveis extensões no modelo de Jøsang.

As simulações corroboraram as idéias inicialmente traçadas. De acordo com os resultados, a extensão do modelo SPKI/SDSI se faz adequada ao comportamento de um ambiente dinâmico como o de grades computacionais. Assim como esperado, houve uma categorização de sujeitos de acordo com suas ações, dando a eles opiniões que refletiram suas atitudes. Futuramente, realizar-se-á implementações que, executadas em ambiente de grande escala, confrontarão os resultados obtidos na simulação com aqueles executados em um ambiente real e verdadeiramente hostil.

Uma arquitetura de segurança para grades computacionais que utilizem da extensão do SPKI/SDSI aqui apresentada é o próximo passo a ser seguido. A flexibilidade e a descentralização providas pelo SPKI/SDSI são características que permitirão que esta arquitetura seja usada em ambientes heterogêneos e dispersos sobre uma rede de grande abrangência. A utilização das cadeias de confiança, sobretudo com a proposta de extensão ao modelo SPKI/SDSI, permitirá uma granularidade menor na definição de políticas de segurança em ambientes de grades computacionais, em geral, e oportunistas em particular.

Referências

[1] Martín Abadi. On SDSI's linked local name spaces. *Journal of Computer Security*, 6(1-2):3–21, 1998.

[2] Dwaine Clarke, Jean-Emile Elien, Carl Ellison, Matt Fredette, Alexander Morcos, and Ronald L. Rivest. Certificate chain discovery in spki/sdsi. *J. Comput. Secur.*, 9(4):285–322, 2001.

[3] Raphael Y. de Camargo, Andrei Goldchleger, Marcio Carneiro, and Fabio Kon. Grid: An Architectural Pattern. In *The 11th Conference on Pattern Languages of Programs (PLoP'2004)*, pages 337–356, Monticello, Illinois, USA, September 2004.

[4] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, Southwestern Bell, and T. Ylonen. SPKI Certificate Theory. Internet RFC #2693, 1999.

[5] Ian Foster and Carl Kesselman. *The Grid 2: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann Publishers Inc., 2003.

[6] Andrei Goldchleger. Integrade: Um sistema de middleware para computação em grade oportunista. Dissertação de mestrado, IME/USP, December 2004.

[7] Andrei Goldchleger, Fabio Kon, Alfredo Goldman vel Lejbman, and Marcelo Finger. InteGrade: Object-Oriented Grid Middleware Leveraging Idle Computing Power of Desktop Machines. In *Proceedings of the ACM/IFIP/USENIX Middleware'2003 1st International Workshop on Middleware for Grid Computing*, pages 232–234, Rio de Janeiro, Brazil, June 2003.

[8] Krishna P. Gummadi, Stefan Saroiu, and Steven D. Gribble. King: Estimating Latency Between Arbitrary Internet End Hosts. In *Proc. of the Second ACM SIGCOMM Workshop on Internet measurment*, pages 5–18, New York, NY, USA, 2002.

[9] Joseph Y. Halpern and Ron Van der Meyden. A logical reconstruction of spki. In *CSFW '01: Proceedings of the 14th IEEE Workshop on Computer Security Foundations*, pages 59–70, Washington, DC, USA, 2001. IEEE Computer Society.

[10] Jon Howell and David Kotz. A formal semantics for spki. In *ESORICS '00: Proceedings of the 6th European Symposium on Research in Computer Security*, pages 140–158, London, UK, 2000. Springer-Verlag.

[11] Audun Jøsang. Artificial reasoning with subjective logic. In *Second Australian Workshop on Commonsense Reasoning*, Perth, Australia, 1997.

[12] Audun Jøsang. An algebra for assessing trust in certification chains. In *Network and Distributed Systems Security Symposium (NDSS 99)*, San Diego, USA, 1999. The Internet Society.

[13] José De Ribamar Braga Pinheiro Júnior and Fabio Kon. *Minicurso de Segurança em Grades Computacionais*, chapter 2, pages 66–111. Simpósio Brasileiro de Segurança de Informação e de Sistemas Computacionais - (SBSEG), September 2005.

[14] Ninghui Li. Local names in SPKI/SDSI. In *CSFW '00: Proceedings of the 13th IEEE Computer Security Foundations Workshop (CSFW'00)*, pages 2–15, Washington, DC, USA, 2000. IEEE Computer Society.

[15] Michael Litzkow, Miron Livny, and Matt Mutka. Condor - A Hunter of Idle Workstations. In *Proceedings of the 8th International Conference of Distributed Computing Systems*, pages 104–111, Palo Alto, CA, June 1988.

[16] Sean Rhea, Dennis Geels, Timothy Roscoe, and John Kubiatowicz. Handling Churn in a DHT. In *Proc. of the 2004 USENIX Annual Technical Conference*, pages 127–140, Boston, Massachusetts, June 2004.

[17] Ronald L. Rivest and Butler Lampson. SDSI – A simple distributed security infrastructure. Presented at CRYPTO'96 Rumpsession, 1996.

[18] Altair Santin, Joni da Silva Fraga, Emerson Ribeiro de Mello, and Frank Siqueira. Extending the SDSI / SPKI Model through Federation Webs. In *Communications and Multimedia Security (CMS2003)*, pages 132–145, Turim, Italy, January 2003.