TEIAS DE CONFIANÇA

1. Introdução

Nos dias atuais, a informática está presente em todos os segmentos da sociedade, seja em nossas casas, em escolas, na indústria ou no comércio em geral. Esta presença significativa, associada ao extensivo uso das redes de computadores, tem tornado a informática elo vital das comunicações e mais recentemente do comércio eletrônico.

Neste contexto, não só nosso dinheiro mas também nossas informações pessoais, e porque não dizer nossas vidas, estão dependentes de todo este aparato tecnológico. Sendo assim, é cada vez mais crítico garantir requisitos mínimos de segurança, seja esta associada à integridade dos dados, aos direitos de acesso ou mesmo à verdadeira identidade dos componentes do sistema (usuários, computadores, processos e outros).

A segurança de tais sistemas computacionais está fortemente dependente da segurança inerente a cada um de seus componentes e das relações entre eles, as quais envolvem troca de dados e/ou procedimentos. Estas relações normalmente envolvem preceitos de confiança, ou seja, para que aconteça o intercâmbio de informações entre as componentes do sistema, necessariamente em algum nível do relacionamento uma entidade deve "confiar" na outra, seja na veracidade, autenticidade ou corretude de suas informações.

O paradigma de confiança tanto pode estar presente no nível de hardware, quando por exemplo a CPU solicita um operação de leitura do disco e "confia" ou não que os dados que recebeu da controladora são realmente os que estão gravados no disco; no nível de software, quando por exemplo um cliente tenta resolver um nome junto a um servidor DNS e obtém um endereço IP no qual ele irá ou não "confiar"; ou mesmo no nível do próprio usuário que pode ou não "confiar" na veracidade das informações que o sistema a ele apresenta. Estes diversos exemplos mostram o conceito de confiança presente em diferentes situações nas quais estão em jogo não só a segurança lógica (security) de um sistema como também a segurança física (safety) do mesmo.

Na comunidade de segurança, até hoje, o conceito de confiança tem sido até certo ponto tratado de forma superficial ou mesmo negligenciado. Normalmente associou-se a idéia de que relações de confiança, entre os componentes de um sistema, são ponto-a-ponto e binárias, onde ou tem-se total confiança ou nenhuma confiança. A confiança total tipicamente está presente entre componentes membros de um mesmo grupo de sistema, fortemente acoplados a este, onde existe ou total ou quase total conhecimento de seus procedimentos internos e segurança (tanto lógica quanto física). Nos demais casos tradicionalmente atribui-se um nível de "não confiança" ou "confiança mínima".

Em muitos casos, diante da veemente necessidade de se "confiar em alguém", foram definidas "entidades confiáveis", como é o caso das entidades certificadoras oficiais, e mecanismos de software foram implementados para assegurar a autenticidade e corretude das informações providas por tais entidades. Pode-se claramente ver um exemplo disto no atual modelo de comércio eletrônico através da Internet.

A observação de que em diferentes contextos o uso de relações de "confiança" torna-se cada vez mais necessário, é a motivação para o desenvolvimento deste trabalho, onde pretendemos propor uma abordagem para o conceito de "confiança" que se adeqüe à concepção atual e que seja extensível o suficiente para satisfazer as necessidades advindas das novas, e cada vez mais complexas, tecnologias.

Neste trabalho apresentamos, para discussão e avaliação, os preceitos básicos do modelo que denominamos de Teias de Confiança (WebS of Trust - WeST), que devem ser vistos não como as respostas para todas as perguntas, ao invés, são o início da discussão de uma área ainda obscura dentro da comunidade de segurança.

Nas seções que se seguem apresentamos o estado da arte em que se encontra o tema deste trabalho, discutimos sistemas correlacionados, apresentamos os objetivos deste trabalho, apresentamos nosso paradigma de confiança, as Teias de Confiança, para em seguida mostrar uma aplicação exemplo e analisar os questionamentos dela advindos. Por fim são tecidas as conclusões pertinentes ao trabalho que aqui é proposto.

1.1 Estado da Arte

Em toda a bibliografia pesquisada pudemos observar que os trabalhos na área de segurança ou não abordam o conceito de confiança, ou o fazem de forma tradicional, binária e ponto-a-ponto. A proposição de uma nova abordagem para confiança, como pretende-se neste trabalho, implica em inúmeras conseqüências passíveis de controvérsia e que portanto representam um sério entrave ao seu desenvolvimento.

Normalmente tem-se a imagem de que "confiamos em quem conhecemos", e esta visão está presente em todos os trabalhos relacionados ao assunto e que podem ser vistos na Seção 1.2. Nestes, a ênfase recai sobre os aspectos criptográficos envolvidos (chaves, autenticidade, certificação, etc.) de modo que tais aspectos validem ou não as relações de confiança entre duas entidades.

No nosso entendimento, a "confiança" a ser estabelecida entre as entidades de um sistema transcende aos mecanismos utilizados para ratificar a

identidade dos participantes, onde podemos dizer que "antes mesmo de saber se estamos falando com quem imaginamos, temos de saber se podemos e o que podemos conversar com o outro, e também se podemos acreditar em suas respostas". Este conhecimento é íntimo à entidade e apenas ela pode responder por ele.

Grandes esforços, feitos por grandes corporações, foram observados no sentido de desenvolver um modelo de confiança que possa ser largamente utilizado na Internet, uma vez que há uma demanda por isto. Porém tais esforços pecam ao normalmente basear seu modelo numa arquitetura hierárquica centralizada, a qual nem sempre é bem recebida por parte dos usuários.

Acreditamos que existe uma demanda por um conceito mais amplo de "confiança", a qual justifica o desenvolvimento deste trabalho.

1.2 Trabalhos Correlatos

Como dito, não existe especificamente nenhum trabalho que aborde confiança pelo mesmo ângulo que vemos; sendo assim, apresentamos algumas das diferentes abordagens que contribuem para nosso questionamento.

PGP

O sistema PGP [1] foi originalmente concebido para permitir a troca segura de mensagens entre usuários através da criação e validação das credenciais destes. No PGP, cada usuário é responsável pela geração e gerência de suas chaves públicas e privadas, as quais estão associadas a um identificador do usuário (tipicamente formado pelo e-mail do mesmo). Para que um usuário A conheça/confie em B, ele previamente deve ter de alguma forma (segura ou não) obtido e introduzido no sistema a chave pública de B. Da mesma forma, A pode pegar a chave pública de B, assiná-la (com sua chave secreta) e manda-la para C (que previamente conhecia A); desta forma A está "apresentando" B a C. Cada usuário deve informar ao PGP em quais usuários ele confia como "apresentadores" de novos usuários.

O sucesso do PGP vem do fato deste permitir que relações de confiança entre uma entidade e outra possam ser estendidas aos demais componentes do sistema, isto desde que haja relações de "apresentação" entre eles, tornando o sistema apropriado para o uso em redes largamente extensas e caóticas, como é o caso da Internet. Pelo mesmo motivo que o PGP é elogiado, ele também é criticado. O fato de uma entidade "confiar" em outra torna esta vulnerável a falsas informações advindas da outra entidade.

No nosso entender, à medida que se estabelece uma relação de confiança de uma entidade para com a outra, inerentemente herda-se a fragilidade que o PGP apresenta e não há forma absolutamente segura de contornar tal dificuldade.

A relevância do PGP para este trabalho está no fato de que ele foi um dos primeiros a apresentar um modelo que usa a confiança, ponto-a-ponto e binária, mas que não é hierárquico.

PolicyMaker

Blaze e outros [2] apresentaram um modelo, que denominaram de Gerência de Confiança (Trust Management), que trata da gerência das relações de confiança entre os componentes de um sistema. A abordagem do modelo está centrada no uso de técnicas criptográficas para certificar a autenticidade de uma entidade para em seguida, baseando-se em políticas definidas pelo usuário, "confiar" ou não a execução de certos serviços. Este modelo deu origem à uma ferramenta intitulada PolicyMaker [3].

O mérito do PolicyMaker está no fato de que ele permite à entidade localmente manter as informações (chaves, políticas, etc.) pertinentes às demais entidades com quem se relaciona, de forma completamente autônoma. Blaze, em outros trabalhos [4], discute a descentralização do mecanismo de Gerência de Confiança adotado pelo PolicyMaker.

O modelo de Gerência de Confiança apresentado no PolicyMaker tem seu foco na autenticidade das entidades participantes e o modelo de confiança continua a ser binário.

KeyNote

Como extensão ao PolicyMaker, Blaze e outros [5] propuseram um sistema mais complexo de Gerência de Confiança, que acrescenta uma linguagem para a definição de credenciais, "políticas" e "ações" a serem adotadas pelo sistema.

O KeyNote não introduziu significativas modificações ao modelo de confiança anteriormente proposto pelo PolicyMaker, estando seu mérito nas novas facilidades de utilização e na RFC a que deu origem.

1.3 Objetivos do Trabalho

Diante das motivações apresentadas anteriormente traçamos os objetivos deste trabalho, que são:

- definição de um conceito de confiança que seja poderoso o suficiente para atender as atuais necessidades do contexto de segurança, e flexível o suficiente para poder ser adaptado às contingências que ainda estão por vir;
- com base no conceito de confiança proposto, formular as relações de confiança entre as entidades de um sistema e as demais entidades;
- proposição de uma arquitetura de confiança que implemente o modelo proposto;

- proposição e implementação de um framework para o desenvolvimento de aplicações que possam fazer uso da arquitetura desenvolvida.
- avaliação dos resultados obtidos, comparando-os com os dos modelos existentes.

Todos estes objetivos são por demais complexos e serão tratados ao longo de um extenso projeto de pesquisa em desenvolvimento no Laboratório de Administração e Segurança de Sistemas (LAS) do Instituto de Computação da Unicamp. Neste artigo são apresentados os conceitos básicos que conduzirão esta empreitada.

2. Confiança

A imagem do conceito de confiança, que mais nos parece familiar, nos leva à idéia de associar confiança à segurança, ou seja, vendo os dois conceitos relacionados entre si, onde o quanto confiamos em uma entidade depende do quanto esta é segura. Esta visão, apesar de coerente e legítima, não é a que melhor pode expressar confiança entre entidades que são independentes entre si e que não necessariamente são plenamente visíveis, tendo seus detalhes internos revelados, aos olhos de terceiros. Este modelo de independência é o notoriamente visto em toda a Internet, ou mesmo em redes onde os clientes estão distribuídos ou fora do total controle da administração da rede. Sendo assim, é nosso objetivo propor uma definição para o conceito de confiança que transcenda à imagem popular, sendo flexível o bastante para ser aplicada às grandes redes hoje existentes, que não necessariamente são hierárquicas ou de total conhecimento de seus participantes, como é o caso da própria Internet.

2.1 Definição de Confiança

Na busca de uma definição adequada para confiança no escopo de segurança, vamos confrontar diversas definições e destas estabeleceremos a mais pertinente ao contexto.

Segundo o Dicionário Aurélio da Língua Portuguesa, tem-se:

- "**Confiança**: (S.) 1. Segurança íntima de procedimento 2. Crédito, fé 3. Boa fama 4. Segurança e bom conceito que inspiram as pessoas de probidade, talento, discrição, etc. 5. Esperança firme 6. Familiaridade 7.(Pop) Atrevimento, petulância 8.(Bras) Atos libidinosos; licença 9.(Bras/RS) Empregado (ou outra pessoa) de confiança."

Esta definição claramente associa confiança à segurança, boa fé, que tem-se de um procedimento, de forma pessoal. Apesar de tal definição trazer à luz o aspecto segurança, a mesma ainda não é suficiente para o propósito deste trabalho, uma vez que este conceito ainda pode ser mais estendido.

No Dicionário Collins da Língua Inglesa, tem-se a seguinte definição:

- "**Trust**: n. confidence in the truth, reliability, etc. of a person or thing; obligation arising from responsibility; charge or care; arrangement in which one person administers property, money, etc. on another's behalf; property held for another; group of companies joined to control a market. - v. believe in and rely on; expect or hope; consign to someone's care."

Nesta definição fica mais clara a relação entre confiança e credibilidade, veracidade que uma pessoa, ou coisa, possui, inclusive apontando a responsabilidade advinda de tal confiança.

A partir destas definições, neste trabalho, define-se confiança no contexto de segurança como sendo:

- **Confiança**: (S.) Veracidade, autenticidade, credibilidade de informações ou procedimentos advindos de outra entidade.

Nesta definição pretende-se deixar claro que a confiança que uma entidade tem em outra representa o quanto ela "acredita", "tem fé" nas informações e/ou procedimentos que a outra entidade lhe manda. Desta forma, confiar está intimamente ligado a acreditar.

2.2 Relações de Confiança

A definição de confiança nos permite estabelecer as relações de confiança, onde pretende-se expressar confiança que uma entidade tem em outra.

Tipicamente o que vemos está apresentado na Figura 1, onde temos duas entidades (A e B) e as relações de confiança entre elas são dadas pelas respostas às perguntas: "A confia em B?" e "B confia em A?". Este tipo de relação é o mais comum onde temos a confiança expressa como sendo um valor binário (sim ou não).

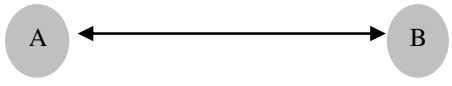

Figura 1 - Relações de Confiança entre A e B

Uma das propostas básicas deste projeto está em ampliar este tipo de relação de forma a permitir que relações de confiança possam assumir qualquer

domínio de valores, que não apenas os binários, desta feita temos relações como mostradas na Figura 2.

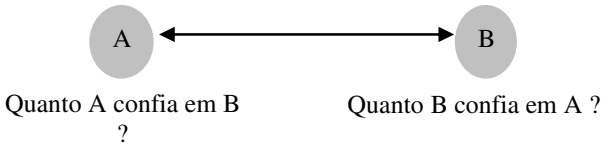

Figura 2 - Novas Relações de Confiança entre A e B

O objetivo em introduzir tal modificação está em permitir, ao nosso modelo de confiança, tanto satisfazer os paradigmas atuais quanto ser aplicável ao modelo de Teias de Confiança que apresentamos no Capítulo 3.

É relevante salientar que as entidades são vistas como sendo autônomas e que suas relações de confiança são de sua inteira responsabilidade.

2.3 Aplicações

Relações de confiança estão comumente presentes em diversos contextos computacionais, como por exemplo:

Relações Cliente/Servidor:
- Cliente fazendo consulta a servidor DNS
- Host (cliente) autenticando usuário (em servidor) NIS
- Cliente "montando" filesystem em servidor NFS
- Browser (cliente) abrindo página (de servidor) web

Relações Planares:
- Troca de chaves públicas entre hosts/usuários
- Mecanismos de autenticação de pacotes, etc.

Em todos estes exemplos existem relações em que necessariamente componentes do sistema (não necessariamente todao) necessitam confiar em outras.

3. Teias de Confiança

Partindo da definição de confiança e das relações que definimos na Seção 2, neste pretendemos contextualizar estas definições dentro de um paradigma maior de confiança, onde as relações não só estão presentes aos pares (ponto-a-ponto) como também podem ser vistas como parte de um grafo que contém todas as componentes do sistema.

3.1 Modelo Ponto-a-Ponto

A visão mais convencional de confiança leva justamente a um modelo ponto-a-ponto, onde estabelece-se uma relação de confiança entre duas entidades independentes. No contexto deste trabalho, esta relação tem um peso associado, que pode simbolicamente representar "o quanto" uma entidade "confia" na outra (Figura 3).

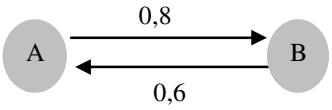

Figura 3 - Modelo de Confiança Ponto-a-Ponto

Tem-se a seguinte notação:

T_{AB} = "o quanto **A** confia em **B**" = 0,8
T_{BA} = "o quanto **B** confia em **A**" = 0,6

É pertinente enfatizar que se pode adotar qualquer representação para os diferentes valores de confiança, e que neste exemplo, $T \in \mathbb{R}$ entre 0 e 1. Tal abordagem poderia representar os valores percentuais de quanto uma entidade confia na outra.

Uma maior discussão sobre qual a representação ideal a ser adotada e os parâmetros para sua definição serão foco de subsequentes estudos ao longo do desenvolvimento deste trabalho. Neste ponto, nosso objetivo é lançar os fundamentos que guiarão tal empreitada.

3.2 Grafo de Confiança

Tendo como base o modelo ponto-a-ponto, surge a extensão natural onde tem-se um grafo orientado G=(V,E) que representa as diversas relações de confiança entre os diversos elementos do grafo (Figura 4).

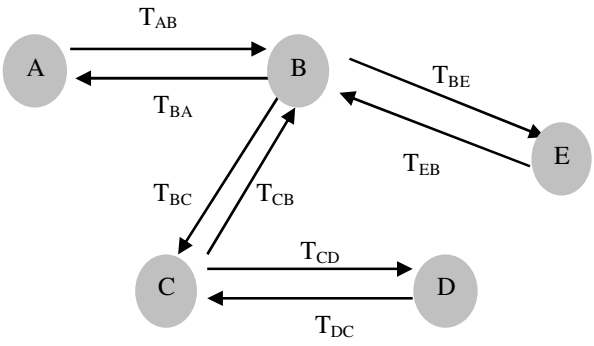

Figura 4 - Grafo de Confiança

Neste modelo os vértices representam as diversas entidades e as arestas expressam as relações de confiança, sendo seus pesos os níveis de confiança associados.

É natural observar que neste grafo são possíveis laços ou mesmo sub-grafos desconexos, uma vez que as relações de confiança entre as entidades tanto podem induzir relações circulares (A confia em B, que confia em C, que confia em A), quanto pode haver o caso onde não existe nenhuma relação de confiança entre subconjuntos de vértices do grafo.

Neste grafo, em relação a um dado vértice, definimos duas regiões de vizinhança:

- near WeST: que representa os vértices diretamente ligados, ou seja, com os quais existem arestas ligando;
- far WeST: que representa os vértices alcançáveis através de um caminho qualquer.

Como exemplo, se tomarmos como referencial o vértice B, seu near WeST é o conjunto de vértices {A,C,E} e seu far WeST é conjunto unitário {D}.

3.3 Caminhos de Confiança

Quando nos referimos a um vértice V qualquer, para cada vértice U de seu near WeST, por definição, existe um único caminho dado pela aresta que liga V a U. Porém para o caso de um vértice X pertencente ao conjunto far WeST podem existir diversos caminhos que liguem V a X. Estes caminhos denominamos de caminhos de confiança.

Ao nos utilizarmos do conceito de caminhos de confiança podemos inferir relações de confiança entre duas entidades que não estejam diretamente relacionadas. Isto pode vir a ser algo necessário quando estamos lidando com sistemas contendo um grande número de componentes, como é o caso da Internet.

Ao falarmos de caminhos de confiança num grafo de confiança dois questionamentos surgem:

- Dentre os diversos caminhos que ligam um vértice V a outro vértice U, pertencente ao far WeST de V, qual escolher e porque ?
- Uma vez que estamos inferindo a confiança entre um vértice V e um outro vértice U pertencente ao seu far WeST, tendo escolhido o caminho que os liga, qual o valor resultante da confiança entre os dois ?

Neste ponto do desenvolvimento deste trabalho ainda não temos as respostas para tais perguntas mas vemos duas frentes de estudo desta direção: os algoritmos para escolha de caminhos de confiança e o algoritmo para cálculo da confiança resultante ao longo de um caminho.

3.4 Teias de Confiança

Uma vez que cada vértice do grafo, ou seja, cada entidade do sistema, tem autonomia suficiente para responder por seus relacionamentos de confiança e escolher dentre os diversos possíveis caminhos de confiança qual aquele que mais lhe convém, a partir de um mesmo grafo contendo todos os componentes do sistema temos inúmeras visões diferentes, que correspondem à visão que cada componente tem do mesmo grafo. O conjunto de todas estas visões denominamos de Teias de Confiança (WeST).

4. Arquitetura WeST

A partir da teoria desenvolvida para o modelo de Teias de Confiança é nosso objetivo o desenvolvimento de uma arquitetura que dê suporte ao desenvolvimento e utilização de aplicações que façam uso deste paradigma. Esta arquitetura é apresentada nesta seção.

4.1 Modelo em Camadas

As aplicações que em alguma instância fazem uso de conceitos de confiança (PGP, PolicyMaker, KeyNotes e outros) trazem dentro de si (do espaço da aplicação) a infra-estrutura necessária ao desempenho de suas funções. O que vemos é uma arquitetura onde tem-se presente a aplicação e o sistema sobre o qual ela roda (Figura 5).

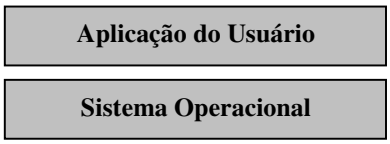

Figura 5 - Arquitetura Convencional

Nossa proposta está em desenvolver um arquitetura disposta em camadas que se interponha entre a aplicação do usuário e o sistema operacional, provendo de forma transparente à aplicação as facilidades de confiança de que ela necessite (Figura 6).

Figura 6 - Arquitetura WeST

Camada do Framework

Esta camada tem por função prover um framework que forneça as primitivas básicas para o desenvolvimento de aplicações que façam uso do paradigma de confiança WeST. Para facilitar o desenvolvimento de tais aplicações, a princípio, pretendemos disponibilizar primitivas similares às hoje existentes e que apenas acrescentam como parâmetro o nível de confiança desejado.
Exemplo: w_connect (sockfd, servaddr, servaddrlen, trustlevel)

Camada de Confiança

Camada que responde pela gerência das informações pertinentes à entidade (suas relações de confiança, parâmetros de configuração, etc.), implementa os algoritmos para determinação de caminhos de confiança e seus respectivos pesos, e assegura e provê os requisitos de confiança especificados pela aplicação.

Camada de Comunicação Segura

Enquanto que nos trabalhos relacionados ao assunto os aspectos criptográficos estão em primeiro plano, para nós eles fazem parte da camada de comunicação segura e basicamente compõem os mecanismos necessários para assegurar e prover a comunicação entre duas entidades da teia, atendendo os requisitos de confiança especificados pela camada de confiança.

5. Aplicação

A título de aplicação do modelo, aqui apresentamos (Figura 7) um exemplo que servirá de subsídio para considerações. Este exemplo basicamente é parte da rede interna do LAS.

Neste grafo os vértices {P,S,Q,V,O} representam hosts do domínio LAS (representado pelo vértice LAS) e os vértices {F,M,R} representam hosts do subdomínio GIP (vértice GIP). Os pesos nas arestas representam os níveis de confiança (percentuais) que cada vértice tem no outro.

Apenas como exemplo de aplicação do modelo, os serviços que um host confia a outro (cliente ou servidor) foram definidos com base nos pesos das arestas, ou seja, com base nas relações de confiança (Tabela 1).

T	Serviço
0	nenhum
> 0	ssh
0,1	cliente DNS, cliente proxy http
0,2	servidor NFS read-only
0,3	servidor NFS read-write (com auth)
0,4	yppasswd
0,6	relay SMTP
0,7	DNS stub
0,9	servidor NFS suid
1,0	confiança total

Tabela 1 - Associação entre Níveis de Confiança e Serviços

Se a escolha do caminho de confiança basear-se no caminho de maior peso resultante, e se adotarmos que o algoritmo para determinação do peso resultante de um caminho estipula ser valor como sendo o produtório dos pesos ao longo do caminho, temos a seguinte matriz de adjacência:

	P	Q,LAS	S	V	O	M,GIP	F	R
P	1,0	0,6	0,18	0,24	0,18	0,42	0,12	0,38
Q,LAS	0,1	1,0	0,3	0,4	0,3	0,7	0,21	0,63
S	0,1	1,0	1,0	0,4	0,3	0,7	0,21	0,63
V	0,1	1,0	0,3	1,0	0,3	0,7	0,21	0,63
O	0,1	1,0	0,3	0,4	1,0	0,7	0,21	0,63
M,GIP	0,1	1,0	0,3	0,4	0,3	1,0	0,3	0,9
F	0,1	1,0	0,3	0,4	0,3	1,0	1,0	0,9
R	0,1	1,0	0,3	0,4	0,3	1,0	0,3	1,0

Tabela 2 - Matriz de Adjacência WeST para a Rede LAS

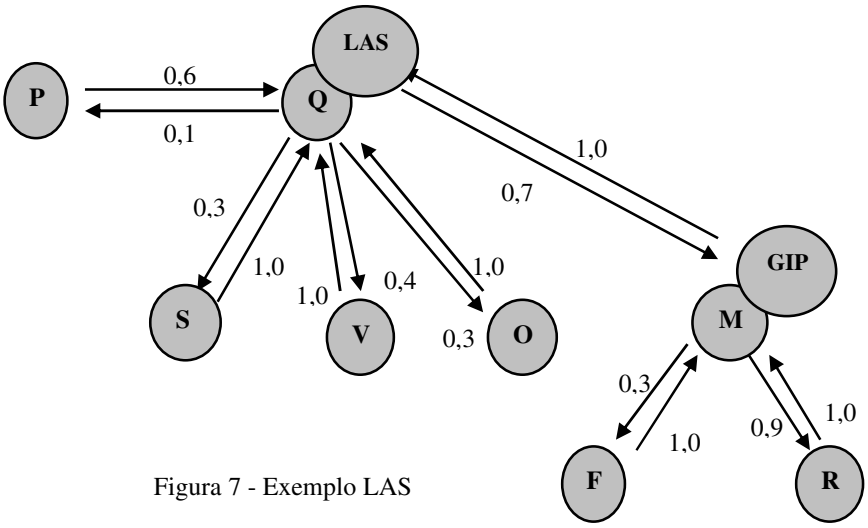

Figura 7 - Exemplo LAS

Por esta matriz podemos fazer algumas observações:

- todas as maquinas da rede LAS e GIP podem fazer uso do serviço de proxy oferecido pelo host P;
- apenas os hosts {S,V,O,M,R} podem acessar em modo read-write, mediante autenticação, o serviço de NFS do host Q;
- o host P pode ser relay de SMTP apenas para o host Q, e este pode ser relay apenas para o host M;
- fica clara a existência de uma relação hierárquica entre os hosts {S,V,O,M} e o host {Q}.

Escolhemos este exemplo para ilustrar que as relações de confiança podem ser utilizadas em associação com os serviços oferecidos entre as componentes do sistema, porém tal exemplo sucinta os seguintes questionamentos:

- Como determinar os pesos de cada aresta, ou seja, quais parâmetros devem ser levados em consideração para a escolha da relação de confiança presente entre as entidade do grafo ?
- Como relacionar os serviços e os níveis de confiança necessários para o desempenho destes serviços ?
- Uma vez que este grafo pode ser por demais extenso, como que uma entidade autônoma pode por si mesma determinar a relação de confiança que tem com outra de seu conjunto far WeST, sem para tanto deter o conhecimento de todo o grafo ?

Mais uma vez lembramos que nesta fase do trabalho estes e outros inúmeros questionamentos perfazem os subsídios para o desenvolvimento de toda a pesquisa.

6. Conclusão

Uma vez que o modelo WeST representa um novo paradigma para o conceito de confiança dentro do espectro de segurança, tanto encontramos vantagens no mesmo como desvantagens, a saber:

Vantagens

- O conceito mais amplo de confiança permite englobar a atual definição e estendê-la de forma a inferir relações de confiança entre entidades não diretamente relacionadas.
- Através deste modelo pode ser possível formalizar e determinar os requisitos de confiança necessários às diversas aplicações e serviços.
- Toda a complexidade de implementação do conceito fica completamente transparente à aplicação do usuário, sendo de responsabilidade do middleware WeST.
- A elaboração de um Framework contendo primitivas de comunicação similares às existentes facilita o porte e desenvolvimento de aplicações.
- O modelo tanto pode se comportar de forma hierárquica quanto planar.
- Os pesos das arestas, ou seja, as relações de confiança, podem ser dinâmicas, mudando de acordo com a contingência.
- O modelo é flexível, permitindo novas definições de pesos e requisitos.
- O modelo é extensível, permitindo que diferentes algoritmos para determinação de caminhos sejam usados (peso mínimo, comprimento mínimo, “custo” mínimo, etc.)

Desvantagens

- "Confiança” é um conceito normalmente binário e/ou subjetivo, o que em muito dificulta a sua formalização como um conceito de valores contínuos.
- A quase inexistência de modelos similares torna por demais extenso este trabalho.
- A complexidade do modelo implica numa maior dificuldade de implementação.

Não pretendemos propor um modelo de confiança, onde a mesma possa ser assegurada e garantida automaticamente e independentemente de qualquer intervenção humana. É nosso pensamento que, numa primeira instância, as entidades que participam do sistema sejam autônomas e que exista "alguém" que responda (se responsabilize) pelos relações de confiança pertinentes à entidade. Neste sentido, é possível que existam falhas de segurança na entidade e que estas se propaguem por outras entidades da rede. Porém, como todos sabemos o mesmo problema é hoje visto em todos os sistemas computacionais que de alguma forma dependam uns dos outros, e não sabemos até que ponto existe solução para este impasse.

É claro para nós que uma vez que os sistemas computacionais continuamente tornam-se mais complexos, com inúmeros componentes inter-relacionados e interdependentes, a busca pela segurança total onde todos os membros do sistema tenham confiança máxima entre si, até certo ponto, é como a busca pela "pedra filosofal", um árduo caminho que ninguém pode afirmar que terá um resultado final satisfatório e que portanto não será trilhado por este trabalho.

7. Referências Bibliográficas

[1] P. Zimmermann, *PGP User's Guide*, MIT Press, Cambridge, 1994.

[2] M. Blaze, J. Feigenbaum, J. Lacy. *Compliance Checking in the PolicyMaker Trust Management System*. Proceedings of 2nd Financial Crypto Conference. Anguilla 1998. LNCS #1465, pp 251-265, Springer-Verlag, 1998.

[3] M. Blaze, J. Feigenbaum, J. Lacy. *Decentralized Trust Management*. Proceedings of the 17th IEEE Symposium on Security and Privacy. pp 164-173. IEEE Computer Society, 1996.

[4] M. Blaze, J. Feigenbaum, J. Lacy. *The Role of Trust Management in Distributed Systems Security*. Chapter in Secure Internet Programming: Security Issues for Mobile and Distributed Objects (Vitek and Jensen, eds.). Springer-Verlag, 1999.

[5] M. Blaze, J. Feigenbaum, J. Lacy. *The KeyNote Trust-Management System Version 2*. IETF Network Working Group, RFC 2704, September 1999.