FACULDADE SENAC DE CIÊNCIAS EXATAS E TECNOLOGIA

André Sabino Petean Galvão

Análise dos aspectos de segurança dos protocolos de compartilhamento NFS e CIFS

São Paulo
2005

ANDRÉ SABINO PETEAN GALVÃO

Análise dos aspectos de segurança dos protocolos de compartilhamento NFS e CIFS

Trabalho de conclusão de curso apresentado à Faculdade Senac de Ciências Exatas e Tecnologia, como exigência parcial para obtenção do grau de Especialista em Segurança de Redes e Sistemas.

Orientador: Prof. Dr. Volnys Borges Bernal

São Paulo
2005

Galvão, André Sabino Petean

Análise dos aspectos de segurança dos protocolos de compartilhamento NFS e CIFS / André Sabino Petean Galvão. – São Paulo, 2005.
45 f.

Trabalho de Conclusão de Curso – Faculdade Senac de Ciências Exatas e Tecnologia.
Orientador: Prof. Dr. Volnys Borges Bernal.

1. Segurança da Informação 2. Protocolos NFS e CIFS I. Título

Aluno: André Sabino Petean Galvão
Título: Análise dos aspectos de segurança dos protocolos de compartilhamento NFS e CIFS

A banca examinadora dos Trabalhos de Conclusão em sessão pública realizada em 09/03/2005, considerou o(a) candidato(a):

(X) aprovado ( ) reprovado

1) Examinador(a) Prof. Msc. Luis Gustavo Gasparini Kiatake
2) Examinador(a) Prof. Murilo Rivau Fernandes
3) Presidente Prof. Dr. Adilson Eduardo Guelfi

Dedico este trabalho à minha mãe, cujo gosto pelo estudo me incentivou a seguir firme em busca de meu objetivo.

AGRADECIMENTO

À minha família, à minha namorada e aos meus amigos, a quem tive de dedicar menos tempo até concluir este trabalho.

Ao meu orientador Prof. Dr. Volnys Borges Bernal, cujos ensinamentos propiciaram a concretização deste trabalho.

Ao Programa de Incentivo à Pós-Graduação da Dataprev, do qual me beneficiei para custear minha especialização.

“Genialidade é 1% inspiração e 99% transpiração.”

(Thomas Alva Edison)

RESUMO

Os protocolos NFS e CIFS permitem o compartilhamento via rede de recursos entre sistemas com arquitetura cliente-servidor, quaisquer que sejam suas plataformas de hardware e software. A análise dos aspectos de segurança destes protocolos aponta em ambos vulnerabilidades do ponto de vista da segurança da informação, que implicam em diminuição dos níveis de eficiência dos serviços de segurança oferecidos por eles e independem das formas de implementação de ambos, pois decorrem da estrutura e do modo de funcionamento de seus mecanismos internos. Os serviços de segurança de confidencialidade, autenticação, integridade, disponibilidade, controle de acesso e auditoria foram considerados para análise, e o de irretratabilidade foi excluído porque não se aplica a um sistema de compartilhamento de arquivos. Constatou-se neste trabalho que o protocolo NFS não oferece os serviços de confidencialidade e auditoria, oferece níveis de segurança baixos para os serviços de autenticação (de parceiros e usuários), integridade (no acesso simultâneo e na transmissão de dados) e controle de acesso, e oferece nível de segurança médio para o serviço de disponibilidade. Já o protocolo CIFS também não oferece os serviços de confidencialidade e auditoria, oferece níveis de segurança baixos para os serviços de autenticação de parceiros, integridade na transmissão de dados e disponibilidade, e oferece níveis de segurança médios para os serviços de autenticação de usuários, integridade no acesso simultâneo e controle de acesso. Versões modificadas do NFS e do CIFS, como por exemplo o CNFS, podem implementar os serviços ausentes ou oferecidos com baixo nível de segurança pelas versões padrão.

Palavras-chave: Segurança da Informação, Protocolos NFS e CIFS, Compartilhamento de Rede.

ABSTRACT

The NFS and CIFS protocols permit the network sharing of resources among client-server systems, regardless of the type of hardware or software platforms). The analysis of these protocols' security aspects points out some vulnerabilities in both of them, in terms of information security, implying in the reduction of the efficiency level concerning the security services offered by these protocols, regardless of their implementation forms, as these vulnerabilities are originated by the structure and functioning forms of the protocols' internal mechanisms. The security services concerning confidentiality, authentication, integrity, availability, access control and auditing have been considered for analysis; irrevocability was excluded because it does not apply to a file sharing system. Our studies have indicated that the NFS protocol does not cover the confidentiality and auditing services, and it presents low security levels regarding partners and users' authentication services, as well as concerning integrity (in simultaneous access and data transmission) and access control services. The NFS protocol offers medium security level in terms of availability service. The CIFS protocol also does not offer the confidentiality and auditing services; and it presents low security levels regarding services such as partners' authentication, data transmission integrity and availability. CIFS presents medium security levels concerning services such as users' authentication, integrity in simultaneous access and access control. NFS and CIFS' modified versions, for example, the CNFS, can implement the missing services, as well as those that offer low security level in the standard versions.

Keywords: Information Security, NFS and CIFS protocols, Network Sharing.

SUMÁRIO

1 INTRODUÇÃO

Uma das maiores vantagens de se interligar computadores via rede é facilitar a troca de informações entre eles, permitindo o compartilhamento de recursos como sistemas de arquivos e diretórios, impressoras, etc. Para propiciar o compartilhamento de recursos entre computadores cujas plataformas de hardware e software são heterogêneas, foram desenvolvidos protocolos de compartilhamento padronizados e documentados de maneira a permitir sua implantação em redes com diversos tipos de equipamentos e sistemas operacionais.

Atualmente, devido ao uso majoritário da pilha de protocolos TCP/IP (*Transmission Control Protocol* / *Internet Protocol*) em redes de computadores do mundo inteiro, e também devido ao uso maciço dos sistemas operacionais Windows e Unix em servidores de rede, os protocolos mais populares para compartilhamento de recursos via rede são o NFS (*Network File System*), cuja versão mais difundida é a de número 3 (IETF, 1995), e o CIFS (*Common Internet File System*, anteriormente denominado SMB - *Server Message Block*), na versão 1.0 (SNIA, 2002). No entanto, existem protocolos para compartilhamento de recursos cujo uso é mais restrito, como por exemplo o *AppleTalk* e o AFP (*Apple File Protocol*), usados em sistemas operacionais Apple Macintosh, e o NFSP (*NetWare File Sharing Protocol*), usado em redes Novell NetWare.

Os protocolos NFS e CIFS diferem substancialmente em suas características estruturais e de funcionamento, inclusive no que se refere aos mecanismos responsáveis pela segurança dos recursos compartilhados por meio deles. E apesar destes dois protocolos serem implementáveis em diversos sistemas operacionais, no que se refere aos servidores usados para compartilhamento de arquivos, o primeiro

é majoritariamente implementado em sistemas operacionais da família Unix, e o segundo, em sistemas da família Windows. As origens distintas do NFS e do CIFS, detalhadas mais adiante, constituem uma razão plausível para tal segmentação.

O compartilhamento de recursos precisa ser feito de forma segura, para que as informações circulantes na rede sejam protegidas de adulterações e entidades não autorizadas não obtenham acesso a elas. No entanto, os protocolos NFS e CIFS foram projetados duas décadas atrás, quando não havia a mesma preocupação com a segurança da informação que há hoje em dia, e mesmo tendo passado por modificações importantes ao longo destes vinte anos, tanto o NFS quanto o CIFS possuem em suas versões mais recentes vulnerabilidades de segurança conhecidas.

O objetivo deste trabalho é analisar os aspectos de segurança dos protocolos NFS e CIFS, tomando por base suas particularidades de funcionamento e enfocando o compartilhamento de arquivos em rede para sistemas de arquitetura cliente-servidor. O levantamento das vulnerabilidades de segurança e a análise comparativa entre os dois protocolos foram elaborados de acordo com o estudo dos padrões normativos definidos e documentados pelas entidades internacionais competentes – pela RFC da IETF (*Internet Engineering Task Force*), no caso do NFS, e pela referência técnica da SNIA (*Storage Networking Industry Association*), no caso do CIFS – e de maneira que independam das formas de implementação de ambos os protocolos.

Segue a organização dos demais capítulos deste trabalho:

- Capítulo 2 - descreve as características gerais dos protocolos NFS e CIFS, enfocando o funcionamento dos mecanismos de compartilhamento de arquivos;

- Capítulo 3 – apresenta conceitualmente os serviços de segurança da informação, restringindo-se aos serviços de segurança relevantes para um sistema de compartilhamento de arquivos;
- Capítulo 4 – destaca as principais vulnerabilidades de segurança dos protocolos NFS e CIFS, constatadas por meio da análise dos seus mecanismos de funcionamento;
- Capítulo 5 – traz comparações entre aspectos de segurança dos protocolos NFS e CIFS, enumerando para cada serviço de segurança os aspectos em que os dois protocolos se equiparam, como também os aspectos nos quais um protocolo leva vantagem sobre o outro;
- Capítulo 6 – faz a conclusão deste trabalho, com as considerações finais e sugestões para trabalhos futuros.

2 CARACTERÍSTICAS GERAIS DOS PROTOCOLOS NFS E CIFS

2.1 Características gerais do protocolo NFS

Desenvolvido pela empresa fabricante de computadores Sun Microsystems, que em 1985 o distribuiu pela primeira vez, em conjunto com o sistema operacional SunOS 2, o protocolo NFS (IETF, 1995) provê acesso remoto transparente a arquivos compartilhados via rede, e foi desenvolvido para funcionar independentemente de equipamento, sistema operacional, arquitetura de rede e protocolo de transporte. Tal independência é obtida por meio do uso da RPC (*Remote Procedure Call* - chamada de procedimento remoto), cujos protocolos são descritos usando a XDR (*eXternal Data Representation* - representação externa de dados) (ALMEIDA, 1997).

A RPC é uma biblioteca de procedimentos por meio da qual um processo (processo cliente) pode fazer com que um outro processo (processo servidor) execute uma chamada a um procedimento como se o fizesse em seu próprio espaço de endereçamento. Desta maneira, o processo cliente e o processo servidor não precisam residir na mesma máquina.

A XDR especifica um padrão para formato de dados portável, e é utilizada pelas chamadas RPC para assegurar que os dados sejam representados da mesma maneira em computadores, sistemas operacionais e linguagens de programação distintos. Esta padronização também resolve o problema dos diversos alinhamentos

estruturais, ordenação de bytes, e representações de tipos de dados em máquinas diferentes que se comunicam.

2.1.1 Filosofia de funcionamento

Os clientes NFS são os responsáveis pelo trabalho relativo à conversão do acesso a arquivos genérico, provido pelos servidores, em um método de acesso a arquivos utilizável por aplicações e usuários. O protocolo NFS assume uma implementação *stateless* de servidor (STERN, 1992), pois o servidor não precisa manter informação sobre o estado de qualquer um dos seus clientes para funcionar corretamente. Em caso de pane isto é uma vantagem, pois um cliente precisa apenas de refazer a tentativa de requisição até que o servidor responda, sem tomar conhecimento da pane ocorrida com o servidor. Porém em muitos casos o servidor NFS mantém um *cache* de operações prévias, no intuito de melhorar seu desempenho.

Dois níveis de transparência são proporcionados pela montagem de um sistema de arquivos, utilizando NFS:

- para o cliente, o sistema de arquivos parece residir no disco ligado ao sistema local, e os arquivos e diretórios, sejam eles locais ou remotos, são vistos da mesma forma, pois o servidor esconde a localização do arquivo na rede;
- o servidor esconde a estrutura de seu sistema de arquivos, fazendo com que o sistema de arquivos remoto pareça ter a mesma estrutura que a do cliente.

O NFS realiza o primeiro nível de transparência definindo um conjunto genérico de operações de sistema de arquivos, executados como um sistema virtual (VFS –

Virtual File System), e o segundo nível surge na definição de nós virtuais (vnodes – *virtual nodes*) relacionados às estruturas inode do sistema de arquivos do Unix, mas que ocultam a real estrutura do sistema físico de arquivos.

Ações que operam em todo o sistema de arquivos, como verificar a quantidade de espaço restante no sistema de arquivos, são chamadas operações VFS. Chamadas que operam em arquivos ou diretórios são operações vnode. No lado do servidor, implementar um VFS envolve converter as operações genéricas de VFS e vnode em ações apropriadas para o sistema de arquivos real subjacente. Esta conversão ocorre de forma invisível ao processo do cliente, que faz uma chamada de sistema direta, transformada pelo cliente VFS em uma operação vnode, convertida pelo servidor em uma operação equivalente, porém adequada ao seu sistema de arquivos.

2.1.2 Autenticação de usuários e checagem de permissões

Cada chamada RPC possui um campo para parâmetros de autenticação, e o conteúdo deste campo é determinado pelo tipo de autenticação usado por servidores e clientes NFS (IETF, 1995). Um servidor pode suportar, ao mesmo tempo, várias modalidades de autenticação, identificadas pelos seguintes parâmetros:

- AUTH_NONE - autenticação nula, não há passagem de informação de autenticação;
- AUTH_UNIX - autenticação Unix, por meio dos IDs de usuário e de grupo fornecidos pelo cliente;

- AUTH_DES - autenticação por meio de um esquema de chaves públicas, com troca de chaves de sessão encriptadas com o algoritmo DES;
- AUTH_KERB - autenticação por meio do esquema Kerberos (chaves privadas), com troca de chaves de sessão encriptadas com o algoritmo DES.

O servidor NFS verifica permissões ao obter, em cada requisição remota, as credenciais contidas na informação de autenticação da chamada RPC, sendo que no modelo de autenticação Unix são usados os IDs de usuário e de grupo, o que implica no compartilhamento da lista de IDs por parte do cliente e do servidor, ou em um mapeamento local dos IDs de usuário e grupo, por parte do servidor. Na prática, tipicamente o servidor segue um esquema de mapeamento estático, ou um mapeamento estabelecido pelo usuário que faz uso do cliente NFS no momento da montagem.

2.1.3 Particularidades de funcionamento

O comportamento padrão da RPC, enquanto protocolo de ligação, é conectar cliente e servidor usando o número de versão NFS mais alto que ambos suportarem.

A implementação do NFS Version 3 (NFSv3) usualmente combina um projeto *stateless* com a escolha de um protocolo de transporte de rede não confiável – o UDP, normalmente usando a porta 2049 – e isto implica na possibilidade de retransmissão, inclusive com possíveis danos, de requisições não-idempotentes. Quando usado no contexto de um servidor de arquivos, o termo idempotente pode distinguir entre tipos de operações; uma requisição idempotente é uma requisição que o servidor pode executar mais de uma vez com resultados equivalentes –

algumas operações NFS são obviamente não-idempotentes, pois não podem ser reprocessadas sem atenção especial simplesmente porque podem falhar se for feita uma segunda tentativa (ex.: um arquivo só pode ser removido uma única vez).

Contudo, o protocolo NFS também pode ser implementado com o protocolo de transporte TCP, sendo que para o NFS Version 4 (NFSv4), mais recente e ainda pouco utilizado, a RFC recomenda o uso de protocolos de transporte com controle de congestionamento; incluem-se nesta condição os protocolos SCTP e TCP, sendo que este último permite maior interoperabilidade.

2.2 Características gerais do protocolo CIFS

O protocolo CIFS (SNIA, 2002) tem por objetivo prover um mecanismo aberto, e independente de plataforma, para sistemas clientes requisitarem serviços de arquivo de sistemas servidores da rede. O CIFS é baseado no padrão do protocolo SMB, originalmente desenvolvido pela Intel e pela Microsoft no início dos anos 80 para ser executado em redes locais do tipo PC-Network (substituídas posteriormente pelo padrão Ethernet), que faziam uso do protocolo NetBIOS (*Network Basic Input/Output System*). Inúmeros aplicativos foram escritos para uso com a interface de programação do NetBIOS, o que motivou vários fornecedores de software, mesmo após o surgimento de novos padrões para redes locais, a implementá-lo sobre outros protocolos de rede, dentre eles o TCP/IP.

A partir do lançamento do sistema operacional Windows 2000, passou a ser suportado o transporte de pacotes SMB sobre TCP/IP sem encapsulamento NetBIOS, porém para manter a compatibilidade com seus predecessores o Windows

2000 inclui suporte a este encapsulamento. Em 1996, por razões meramente mercadológicas, a Microsoft renomeou o protocolo SMB e deu a ele o nome de CIFS. Hoje em dia, esta nova designação é mais usada como referência ao conjunto de aplicativos que habilitam o compartilhamento de diretórios, arquivos, impressoras e outros dispositivos conectados em rede, enquanto que o termo SMB é usado tipicamente quando discutido o protocolo de compartilhamento de arquivos em si.

2.2.1 Filosofia de funcionamento

No sentido de realizar acesso a um arquivo em um servidor CIFS (SNIA, 2002), um cliente tem de:

- analisar e segmentar o nome completo deste arquivo para determinar o nome do servidor;
- determinar o nome relativo do arquivo dentro deste servidor;
- resolver o nome do servidor para um endereço da camada de transporte (obter o endereço IP, usando DNS – *Domain Name System* – ou NetBIOS);
- conectar-se ao servidor (se não houver alguma conexão estabelecida disponível) e então trocar mensagens CIFS com ele.

A primeira mensagem deve indicar os dialetos do protocolo CIFS suportados pelo cliente, os quais serão comparados com a lista de dialetos suportados pelo servidor, que por sua vez retornará uma mensagem respondendo qual dialeto escolheu.

Uma vez estabelecida a conexão, as regras para seu encerramento confiável são:

- se um servidor receber de um cliente - com o qual já está conversando - uma requisição para estabelecer uma conexão de transporte, ele deve encerrar todas as outras conexões de transporte com este cliente, no intuito de propiciar ao cliente recuperar-se de uma situação de reinicialização repentina, em que não foi possível terminar de forma limpa suas atividades de compartilhamento de recursos com o servidor;
- um servidor pode derrubar a conexão de transporte com um cliente a qualquer momento, se este cliente estiver gerando requisições ilógicas ou malformadas, contudo o servidor deve primeiro retornar ao cliente um código de erro que indique a causa do fechamento da conexão, sempre que possível;
- se um servidor obtiver um erro irrecuperável no transporte para um cliente (ex.: falha de envio) a conexão deve ser abortada;
- um servidor pode terminar a conexão de transporte quando um cliente não tiver recursos abertos nele, no entanto para auxiliar seu desempenho recomenda-se o término da conexão depois de decorrido algum tempo ou se os recursos do servidor estiverem escassos.

O protocolo CIFS inclui um mecanismo denominado *oplocks* (*opportunistic locks*, ou “travas oportunistas”), que permite ao cliente bloquear um arquivo de maneira revogável pelo servidor em determinadas condições, com o propósito de propiciar ao cliente fazer um *cache* seguro de dados de arquivo. Há três tipos de *oplocks*:

- exclusivo, capaz de garantir a um cliente que ele seja o único a abrir um determinado arquivo;

- *batch*, que permite a um cliente adiar o fechamento de um arquivo aberto e reaberto repetidamente por uma aplicação;
- nível II, que pode ser revogado pelo servidor sem que o mesmo espere por uma resposta do cliente, garantindo somente que esta revogação aconteça antes de um outro cliente escrever no arquivo com sucesso.

Dois outros mecanismos habilitam que um cliente controle como outros clientes acessam um arquivo, *byte range lock* e *sharing lock* (bloqueios de seqüência de bytes e de compartilhamento, respectivamente), que podem ser mantidos por quanto tempo o cliente desejar e ficam expostos à aplicação, a qual tem controle explícito sobre a obtenção e a liberação destes tipos de bloqueios.

2.2.2 Autenticação de usuários e checagem de permissões

O protocolo CIFS requer autenticação de usuários no servidor para permitir acesso aos arquivos, e cada servidor autentica seus próprios usuários. Um servidor requer do cliente o provimento de um nome de usuário e de alguma prova de identidade, na maioria das vezes uma derivação criptográfica de uma senha, para permitir o acesso aos seus recursos. A granularidade de autorização fica por conta do servidor, que pode usar, por exemplo, o nome da conta para conferir listas de controle de acesso individualmente nos arquivos, ou ter uma lista de controle de acesso que se aplique a todos os arquivos na árvore de diretório.

Quando um servidor valida o nome da conta e a senha apresentados pelo cliente, um identificador que representa esta instância autenticada do usuário é retornado para o cliente no campo UId da resposta SMB. Este UId deve ser incluído

em todas as requisições subseqüentes feitas em benefício do usuário daquele cliente. A autenticação de usuário permite ao servidor verificar se o cliente conhece a senha de um usuário, e a autenticação de mensagem permite ao servidor e ao cliente a verificação das mensagens de uma sessão. O servidor determina, por meio do campo *SecurityMode* da mensagem CIFS, o estilo de autenticação a ser usado por seus clientes nas requisições de arquivos compartilhados.

A autenticação de usuário é baseada no conhecimento compartilhado da sua senha, e o estilo desta autenticação pode envolver o envio pelo cliente de senhas em texto puro para o servidor (desencorajado porque expõe a senha do usuário, e desabilitado por padrão), ou ainda envolver um protocolo de desafio/resposta, pelo qual o servidor envia um “desafio” ao cliente e recebe dele uma resposta comprobatória de seu conhecimento da senha de usuário. Esta resposta é criada a partir do desafio pela encriptação do mesmo com uma chave de sessão de 168 bits, derivada da senha do usuário, e então retornada ao servidor para que este a valide por meio do mesmo cálculo computacional.

Mensagens entre servidor e cliente podem ser autenticadas ao se computar um código MAC (*Message Authentication Code*) anexo a cada mensagem, construído com uma chave MD5 de forma análoga a do protocolo IPSec, usando uma “chave MAC” computada da chave de sessão e usando também a resposta ao desafio do servidor. O código MAC se situa tanto sobre o texto da mensagem como sobre um número seqüencial implícito, para prevenir ataques de repetição.

2.2.3 Particularidades de funcionamento

Como mencionado anteriormente, a partir do lançamento do sistema operacional Windows 2000, a Microsoft introduziu o protocolo SMB executado diretamente sobre o protocolo TCP e sem necessidade de suporte NetBIOS, e o renomeou para CIFS (não há, até o momento presente, opção de uso do protocolo UDP). Não somente foi dispensado o NetBIOS, como todos os sistemas de apoio (como resolução de nomes, navegação e até autenticação) foram substituídos por serviços padronizados. A resolução WINS, por exemplo, foi substituída pelo DNS dinâmico, e agora o sistema Kerberos é usado para autenticação. No âmago destas alterações reside o serviço Active Directory do Windows 2000, baseado no padrão X.500.

3 SERVIÇOS DE SEGURANÇA RELEVANTES PARA UM SISTEMA DE COMPARTILHAMENTO DE ARQUIVOS

Conceitualmente, um serviço de segurança é uma funcionalidade relacionada à segurança que pode vir a ser oferecida por um componente de software (STALLINGS, 1998). O suporte do componente de software a este serviço de segurança depende dos seguintes fatores:

- da relevância do serviço de segurança em relação à finalidade do software;
- do nível de segurança almejado;
- do custo envolvido;
- da viabilidade tecnológica.

Desta forma, qualquer concepção de sistema de compartilhamento de arquivos – o qual não deixa de ser um componente de software - deve considerar tais fatores na definição de quais serviços de segurança este sistema irá implementar, e em que nível de segurança eles serão oferecidos.

Para simplificar a avaliação dos serviços de segurança oferecidos por um sistema de compartilhamento de arquivos, neste trabalho será atribuído um nível de segurança para cada um destes serviços – nível baixo, médio ou alto - como acontece no seguinte exemplo: na transferência de arquivos de um sistema servidor para um sistema cliente, o serviço de segurança de sigilo pode ser oferecido com o uso de criptografia simétrica, mas se o algoritmo usado for fraco e exigir pouco esforço computacional para ser decifrado, o nível de segurança deste serviço pode ser considerado baixo.

A seguir serão descritos os serviços de segurança sugeridos para implementação em um modelo conceitual de protocolo de compartilhamento de arquivos (exclui-se o serviço de irretratabilidade, não aplicável neste contexto).

3.1 Confidencialidade (sigilo)

Com referência a sistemas de compartilhamento de arquivos, o serviço de confidencialidade precisa abranger não somente arquivos e diretórios como também as informações de autenticação, como chaves de sessão e IDs de usuários. As entidades não autorizadas devem ser impedidas de tomar conhecimento do conteúdo dos arquivos armazenados no servidor, e das informações contidas nos dados que trafegam pelo canal de comunicação entre este servidor e seus clientes, sendo que para este fim considera-se como entidade um usuário, aplicativo, processo do sistema, equipamento ou computador.

Qualquer informação armazenada ou transmitida em texto puro está vulnerável do ponto de vista do sigilo, contudo se for implementado em ambas as situações um protocolo de criptografia de dados, dois problemas importantes apresentam-se:

- o desempenho do sistema de compartilhamento de arquivos fica prejudicado, de forma diretamente proporcional ao poder computacional exigido em cada operação de encriptação ou decriptação de dados, e à quantidade de repetições destas operações exigida pela leitura, escrita e execução dos arquivos;

- o sigilo das informações dependerá também da implementação de um mecanismo seguro de distribuição de chaves criptográficas entre clientes e servidores de arquivos.

3.2 Autenticação

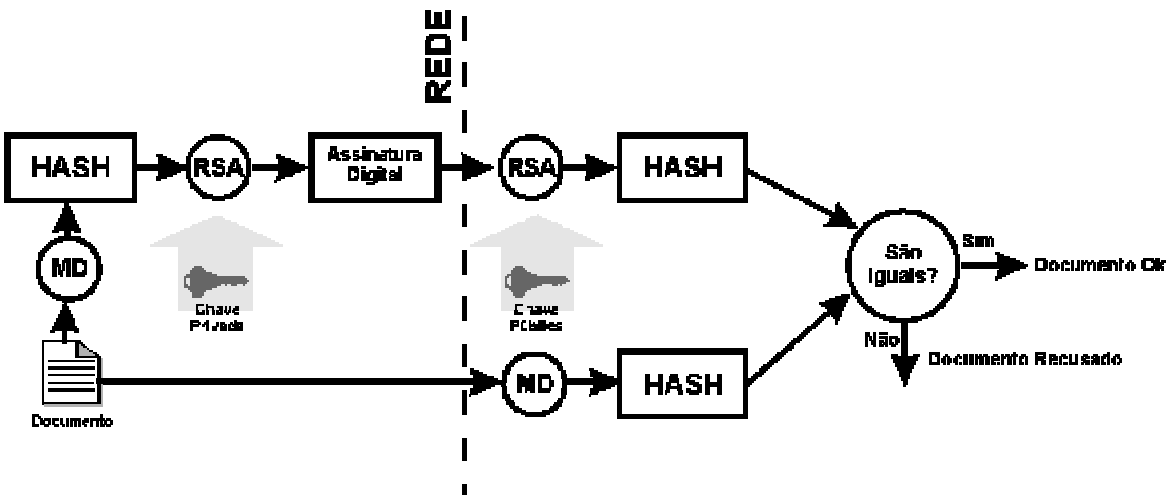
O serviço de autenticação subdivide-se em dois tipos, no que se refere aos protocolos de compartilhamento de arquivos:

- a autenticação do parceiro de comunicação nas interações entre entidades, comprobatória da identidade dos parceiros e certificadora de que nenhuma destas entidades é impostora;
- a autenticação de um usuário no sistema, a qual garante a autenticidade do usuário que requisita um recurso do servidor, verificando se este usuário não é um impostor.

Tradicionalmente, em uma rede que utilize a pilha de protocolos TCP/IP, o mecanismo de autenticação das entidades parceiras de comunicação é a verificação de endereço IP. O nível de segurança deste mecanismo de autenticação é muito baixo, pois um equipamento impostor pode facilmente se fazer passar por uma das entidades parceiras caso assumisse o endereço IP dela. Uma maneira recomendável de se autenticar os parceiros em uma conexão remota é usar criptografia assimétrica, estabelecendo uma conexão segura e autenticada entre as duas entidades, na medida em que somente com sua chave privada uma entidade pode decifrar uma mensagem enviada pela entidade parceira, já que a parceira usa a chave pública daquela entidade para criptografar a mensagem. Este mecanismo é

usado, por exemplo, pelos protocolos SSL (*Secure Socket Layer*) e SSH (*Secure Shell*), muito empregados atualmente para autenticação de parceiros de comunicação, respectivamente em servidores WWW (*World Wide Web*) e servidores de acesso remoto.

A título de exemplo, um mecanismo semelhante ao de assinatura digital seria uma alternativa para autenticar usuários com um bom nível de segurança, mesmo que para seu funcionamento seja necessário implementar um sistema centralizado de gerenciamento e distribuição de chaves criptográficas assimétricas via rede. O mecanismo sugerido funcionaria da seguinte maneira: a cada requisição do cliente, o servidor de arquivos receberia uma mensagem de autenticação de usuário, a qual teria anexo um *hash* de seu conteúdo, criptografado com a chave privada do usuário. O servidor, por sua vez, aplicaria na mensagem o mesmo algoritmo usado pelo cliente para gerar o *hash* e decifraria o conteúdo criptografado com a chave pública do usuário, comparando o *hash* decifrado com o *hash* que ele mesmo gerou. Caso os *hashes* sejam realmente idênticos, comprova-se a identidade do usuário responsável pela requisição remetida pelo cliente.



Fluxograma 1 – Assinatura Digital

Fonte: Trinta; Macedo, 1998

3.3 Integridade

Em um sistema de compartilhamento de arquivos, é imprescindível que o protocolo utilizado garanta um alto nível de segurança para o serviço de integridade, tanto no transporte quanto no armazenamento dos dados compartilhados entre clientes e servidores. Além de impedir que entidades não autorizadas modifiquem o conteúdo de quaisquer arquivos compartilhados na rede, o serviço de integridade do protocolo de compartilhamento precisa controlar também os acessos simultâneos a estes arquivos, no intuito de evitar a corrupção acidental do conteúdo dos mesmos.

Quanto à manutenção da integridade das informações trocadas entre clientes e servidores que compartilham arquivos, durante a transmissão das mesmas, faz-se necessária a prevenção contra ataques capazes de explorar vulnerabilidades do serviço de integridade existentes nesta transmissão. Um destes ataques é o *Man In The Middle*, por meio dos quais entidades não autorizadas obtêm acesso aos dados que trafegam via rede, ao se interporem no caminho entre os parceiros de uma comunicação em andamento, e podem alterar esses dados sem que nenhuma das entidades parceiras detecte suas intervenções. O emprego de criptografia (algoritmos de *hash* e verificadores criptográficos) na transmissão de informações pela rede é eficiente contra este tipo de ataque, porém o nível de segurança fica comprometido se clientes e servidores de arquivos trocarem chaves simétricas por meio da rede, pois elas podem ser capturadas por terceiros e usadas para violar a comunicação entre os parceiros.

Para evitar adulteração ou perda de informações, mesmo que acidentais, é necessário manter um nível satisfatório de segurança nas operações em que dois ou mais clientes requisitam acesso simultâneo a arquivos compartilhados por um servidor. Conforme foi descrito no Capítulo 2, as implementações atuais do protocolo CIFS já utilizam os mecanismos denominados *oplocks*, *byte range lock* e *sharing lock*, com a finalidade de gerenciar o compartilhamento simultâneo de arquivos, e tais mecanismos garantem um bom nível de segurança ao serviço de integridade.

3.4 Disponibilidade

Indubitavelmente, quando um recurso relacionado a um sistema de informação é implementado em uma corporação, instituição de ensino ou mesmo em um laboratório, espera-se que sua taxa de disponibilidade seja próxima de 100%, ou seja, o sistema deve estar pronto para atender a uma requisição de uso a qualquer momento. É com o objetivo de garantir que os dados compartilhados em uma rede estejam sempre disponíveis para os usuários autorizados, que se implementam nos servidores de arquivos mecanismos capazes de manter em níveis aceitáveis o serviço de segurança de disponibilidade. Entende-se por disponibilidade, neste caso, não somente o funcionamento ininterrupto do sistema de compartilhamento de arquivos, mas também um desempenho próximo do ideal, compatível com os recursos físicos e lógicos empregados nele.

Um bom modelo de protocolo de compartilhamento de arquivos aproveitaria as características dos protocolos NFS e CIFS que propiciam um bom nível de segurança para o serviço de disponibilidade, como a recuperação rápida em caso de pane (NFS) e o controle eficiente das conexões entre cliente e servidor (CIFS), e

eliminaria as vulnerabilidades relativas à disponibilidade, como a incapacidade de diferenciar um servidor lento de um servidor inoperante (NFS) e o funcionamento dependente de um serviço de resolução de nomes (CIFS) – as quais serão detalhadas mais adiante.

Há também soluções de compartilhamento de arquivos cujo armazenamento de dados não é feito por um servidor centralizado, o que permite redundância no fornecimento de acesso a arquivos e diretórios, e garante o serviço de disponibilidade em caso de falha de servidor. Um exemplo interessante deste tipo de solução é o GFS (*Global File System*) (SOLTIS; RUWART; O'KEEFE, 1996), sistema em que vários dispositivos de disco, distribuídos em nós independentes e interligados via rede, são logicamente agrupados em um espaço de armazenamento unificado denominado NSP (*Network Storage Pool*). O NSP faz com que o sistema de arquivos aparente ser local para cada nó, enquanto o GFS sincroniza o acesso a arquivos em todo o bloco de dispositivos. O GFS é totalmente simétrico (todos os nós de armazenamento são iguais e não há um servidor centralizado que poderia representar um gargalo ou ponto individual de falha), usa *cache* para leitura e gravação e mantém plenamente a semântica do sistema de arquivos Unix.

3.5 Controle de acesso

O nível de segurança do serviço de controle de acesso implementado por um protocolo de compartilhamento de arquivos está fortemente vinculado ao nível de segurança do serviço de autenticação, pois um servidor precisa identificar inequivocamente os usuários responsáveis pelas requisições de acesso recebidas por ele, para garantir que somente as entidades autorizadas consigam acesso aos

seus arquivos, como também que as autorizações de acesso sejam concedidas apenas pelos responsáveis e que não sejam alteradas indevidamente. Assim sendo, para implementar o serviço de controle de acesso com um bom nível de segurança, um servidor de compartilhamento de arquivos deve gerenciar de forma segura as permissões de acesso concedidas aos seus clientes em decorrência da autenticação dos mesmos.

O gerenciamento do serviço de controle de acesso pode ser feito pelo protocolo de compartilhamento de arquivos em conjunto com o sistema operacional, usando listas de controle de acesso (ACLs) e um sistema centralizado de gerenciamento de IDs de usuários, nos moldes do que atualmente se implementa com o protocolo CIFS em redes com o sistema operacional Windows 2000 instalado no controlador de domínio. Desta maneira alcança-se um bom nível de segurança.

3.6 Auditoria

Armazenar informações sobre as requisições recebidas de seus clientes seria a única maneira de um servidor de arquivos propiciar a auditoria da utilização dos arquivos compartilhados. Neste caso, o nível de segurança oferecido pelo serviço de auditoria é diretamente proporcional ao detalhamento das informações coletadas pelo servidor, e das informações constantes em cada pacote de dados gerado pelo cliente, conforme o padrão do protocolo de compartilhamento.

Contudo, deve-se evitar a coleta excessiva de informações sobre a utilização dos arquivos compartilhados, porque o armazenamento das mesmas no servidor e a sobrecarga nos pacotes que trafegam pela rede a cada requisição dos clientes podem ocasionar lentidão no funcionamento do sistema como um todo.

4 VULNERABILIDADES DE SEGURANÇA DOS PROTOCOLOS NFS E CIFS

As vulnerabilidades de segurança dos protocolos NFS (IETF, 1995) e CIFS (SNIA, 2002) descritas a seguir advêm das particularidades estruturais e de funcionamento destes protocolos, e independem das formas de implementação dos mesmos. Consideram-se nesta análise as vulnerabilidades referentes ao provimento dos serviços de segurança da informação descritos no Capítulo 3.

De início, ressalta-se que nenhum dos dois protocolos se propõe, em sua concepção, a prover o serviço de confidencialidade. Para garantir este serviço de segurança seria necessário aplicar métodos criptográficos no armazenamento de dados no servidor e no transporte de dados entre ele e seus clientes, mas tais métodos não são suportados pelo NFS e pelo CIFS em suas formas nativas, exigindo uso de aplicativos adicionais. Outrossim, não faz parte da proposta do NFS e do CIFS o serviço de auditoria, pois clientes e servidores de ambos os protocolos não guardam registros que propiciem a identificação inequívoca das entidades que realizaram operações de compartilhamento de arquivos, a cronologia destas operações e a quantificação das mesmas.

4.1 Vulnerabilidades de segurança do protocolo NFS

As chamadas RPC, usadas para a comunicação entre o cliente e o servidor NFS, incluem parâmetros de segurança usados especificamente para autenticar o sistema cliente junto ao servidor, pois a autenticação do usuário solicitante do acesso via NFS é feita apenas no momento em que este usuário realiza o *login* no sistema cliente. Adicionalmente, o servidor pode controlar o acesso ao serviço *portmapper* – serviço do Unix que administra o NFS - por meio da configuração de uma lista de sistemas clientes permitidos (identificados pelo endereço IP).

Dentre os tipos de autenticação usados pelo servidor NFS para autenticar as transmissões de dados compartilhados com seus clientes, dois não oferecem segurança alguma: o nulo, no qual nenhuma informação de autenticação é transferida; e o de credenciais de sistema, em que são informados os identificadores de usuário e grupo do Unix, os quais podem ser facilmente obtidos por quaisquer usuários do sistema operacional, permitindo a qualquer um se fazer passar pelo verdadeiro usuário. Outros dois tipos de autenticação oferecem alguma segurança com o uso de chaves de sessão cifradas, contudo isto é feito por meio de algoritmos fracos para os padrões atuais: um dos tipos com esquema de chaves públicas Diffie-Hellman e o outro com chaves privadas Kerberos versão 4 - ambos os tipos usando criptografia pelo algoritmo DES.

O servidor NFS (STERN, 1992) deixa transparente a localização dos arquivos na rede, fazendo com que, para seus clientes, o sistema de arquivos remoto pareça residir no disco ligado ao sistema local; tanto arquivos quanto diretórios são vistos da mesma forma, sejam eles locais ou remotos (embora a localização efetiva de arquivos ou diretórios possa ser facilmente verificada com o uso de comandos NFS). Esta transparência pode facilmente acarretar em alterações ou remoções acidentais

de arquivos e diretórios por parte do cliente, causando danos à integridade dos dados compartilhados pelo servidor NFS.

Não há mecanismo de recuperação para operações incompletas caso o servidor NFS eventualmente fique indisponível, as requisições RPC podem ser repetidas e os clientes NFS são notificados por meio de um *acknowledgement* (pacote que informa o reconhecimento dos dados) a cada requisição completada; cada pedido NFS contém informação suficiente para seu atendimento, sem qualquer referência de estado no cliente ou no servidor.

Desta forma, o tempo de recuperação necessário para que um servidor NFS volte a funcionar após uma parada é minimizado, porém os clientes NFS não conseguem diferenciar um servidor que parou de funcionar de um servidor muito lento, e após um tempo de espera (*timeout*) seguem retransmitindo pedidos até que os mesmos sejam completados, seja por meio de um *acknowledgement* do servidor ou devido a um erro de chamada RPC. Este comportamento gera sobrecarga desnecessária no tráfego de pacotes entre o servidor NFS e seus clientes, que pode acarretar em diminuição da disponibilidade dos recursos de rede para outros serviços oferecidos pelo servidor.

Uma rede de compartilhamento de arquivos pelo protocolo NFS pára de funcionar se o servidor for restaurado e os clientes não forem reinicializados, pois quando é feita a reconstrução dos sistemas de arquivo do servidor todos os números de *inode* (identificador do arquivo no disco para um sistema Unix) anteriormente gerados são reconfigurados, fazendo com que todos os *file handles* (manipuladores de arquivos) dos clientes tornem-se inválidos, em virtude do processo randômico de renumeração dos *inodes* que ocorre na restauração dos sistemas de arquivo do servidor.

A semântica do sistema de arquivos Unix não é totalmente atendida pelo serviço NFS. Neste sistema operacional é possível travar um arquivo aberto (*lock*), de forma que outros processos não obtenham acesso a ele, e quando este arquivo é fechado o *lock* é liberado; tal operação garante a integridade do arquivo que está sendo usado por algum processo do sistema local. Em um servidor *stateless* como o NFS, não se pode associar um *lock* a um arquivo aberto, porque o servidor não sabe quais arquivos estão abertos. No entanto, o cliente NFS pode emular o travamento de um arquivo, como é feito, por exemplo, quando uma operação de remoção é dirigida a um arquivo aberto: o cliente envia um pedido RPC NFS para renomear o arquivo, acrescentando ao seu nome os caracteres ".nfs" e um sufixo que torna este nome único para o sistema; quando eventualmente o arquivo é fechado, o cliente então efetua a operação de remoção do arquivo previamente desvinculado.

4.2 Vulnerabilidades de segurança do protocolo CIFS

Um cliente CIFS (SNIA, 2002) obrigatoriamente deve ter meios de resolver o nome de um servidor CIFS para um endereço de rede, seja por meio dos protocolos NetBIOS ou DNS, e este servidor também obrigatoriamente deve registrar seu nome em um serviço de resolução de nomes conhecido de seus clientes. Esta imposição implica em uma dependência do serviço CIFS em relação ao serviço de resolução de nomes disponível na rede local, a qual compromete a disponibilidade do servidor, pois no caso de indisponibilidade do mesmo o serviço CIFS não irá funcionar. De maneira análoga, pelo fato do protocolo CIFS ser dependente do DNS ou do NetBIOS (este último ainda implementado por razões de compatibilidade), caso seja

explorada uma vulnerabilidade de segurança de um destes dois protocolos e o serviço de resolução de nomes seja usado de forma maliciosa por uma entidade atacante, o servidor CIFS sofrerá indiretamente as conseqüências deste ataque.

Recomenda-se por padrão que não se habilite a autenticação dos usuários com envio de senhas em texto puro para um servidor CIFS, pois isto expõe a senha do usuário a qualquer aplicação que tenha acesso à rede. Esta vulnerabilidade é evitada se os sistemas clientes usarem o protocolo de desafio/resposta no envio das credenciais de autenticação do usuário (conforme descrito no Capítulo 2), as quais serão checadas no servidor perante o diretório de usuários local e as listas de controle de acesso (ACLs).

O servidor CIFS efetua a autenticação dos usuários de seus sistemas clientes usando os recursos do próprio sistema operacional, e os métodos de geração de credenciais de usuário atualmente encontrados nas diversas versões do Windows, como o LAN Manager, o NTLMv2 e o Kerberos, não oferecem muita segurança porque geram credenciais que não demandam grande esforço computacional para serem decifradas.

5 COMPARAÇÕES ENTRE ASPECTOS DE SEGURANÇA DOS PROTOCOLOS NFS E CIFS

Considerando-se as vulnerabilidades de segurança dos protocolos NFS e CIFS, podem ser feitas comparações entre eles, no intuito de verificar em quais aspectos os dois protocolos são equivalentes e em quais aspectos um protocolo é mais seguro que o outro. Tais comparações, da mesma forma que o levantamento de vulnerabilidades do capítulo anterior, são feitas considerando-se apenas as características estruturais e de funcionamento do NFS e do CIFS, e independem das formas de implementação dos mesmos.

As comparações entre aspectos de segurança dos protocolos NFS e CIFS que se seguem estão divididas por serviço de segurança.

5.1 Confidencialidade, irretratabilidade e auditoria

Os protocolos NFS e CIFS não oferecem o serviço de confidencialidade para os sistemas de compartilhamento de arquivos que os utilizam (nenhum deles oferece criptografia nativa). O emprego de qualquer um destes protocolos não impede que entidades não autorizadas obtenham acesso aos arquivos armazenados pelos servidores, na medida em que os dados permanecem disponíveis em sua forma pura. Também ficam vulneráveis ao acesso por parte de entidades não autorizadas as informações contidas nas requisições de clientes, pois elas trafegam de forma aberta pelos canais de comunicação entre clientes e servidores.

O serviço de irretratabilidade não se aplica a um sistema de compartilhamento de arquivos e desta forma não é oferecido pelo NFS e pelo CIFS, como também não é oferecido o serviço de auditoria, inviabilizado pela ausência de registros em *log* das operações efetuadas por clientes e servidores.

5.2 Autenticação

O mecanismo de autenticação de usuários do protocolo CIFS possui um nível de segurança consideravelmente superior ao do protocolo NFS. O servidor CIFS recebe do cliente uma prova da identidade do usuário (normalmente uma derivação criptográfica da senha) e a verifica, enquanto no caso do NFS o cliente é quem verifica os números de ID do usuário e do grupo do usuário no Unix, propiciando que uma entidade impostora possa facilmente se fazer passar pelo usuário autêntico apenas informando estes números de ID.

Os protocolos NFS e CIFS oferecem nível baixo de segurança para a autenticação de parceiros. Os servidores NFS usam uma lista de clientes, designados pelo endereço IP ou pelo nome no DNS, para identificar aqueles para os quais devem liberar o acesso aos arquivos compartilhados, enquanto os servidores CIFS somente identificam seus clientes por meio do serviço de resolução de nomes disponível na rede (NetBIOS ou DNS); ambos os mecanismos são muito vulneráveis a ataques de entidades impostoras.

5.3 Integridade

Os protocolos CIFS e NFS não garantem a integridade dos dados compartilhados entre clientes e servidores nos canais de comunicação, porque não possuem mecanismos de verificação de conteúdo de arquivos, capazes de garantir aos parceiros de comunicação que durante o tráfego das informações não houve dano ou adulteração do conteúdo dos arquivos por parte de entidades não autorizadas (como, por exemplo, em caso de ataques *Man In The Middle)*.

Os servidores NFS não mantêm controle de estado sobre as conexões com seus clientes, e isto faz com que seu mecanismo de gerenciamento de acessos simultâneos a arquivos compartilhados seja bem menos eficiente que o mecanismo empregado pelos servidores CIFS, que realizam este tipo de controle. O controle de estado, feito por meio de seqüências de mensagens trocadas entre clientes e servidores CIFS, permite que se estabeleçam conexões confiáveis e a implementação do mecanismo de *oplocks.* Tal mecanismo propicia ao cliente a realização de um *cache* seguro de dados, com bloqueio de arquivo passível de revogação pelo servidor, liberando acesso simultâneo para outro cliente sem comprometer a integridade do arquivo em questão.

5.4 Disponibilidade

O protocolo NFS oferece um nível de segurança maior do que o do protocolo CIFS para o serviço de disponibilidade. O NFS não recupera operações incompletas, minimizando o tempo de recuperação caso uma eventual falha torne inoperante o servidor. O CIFS, por sua vez, tem seu funcionamento dependente de um serviço de resolução de nomes disponível na rede (NetBIOS ou DNS), e este vínculo compromete sua própria disponibilidade.

Contudo, nenhum dos dois protocolos oferece redundância para os serviços de compartilhamento de arquivos oferecidos pelo servidor aos seus clientes.

5.5 Controle de acesso

A concessão de permissões de acesso a arquivos remotos oferece maior nível de segurança quando usado o protocolo CIFS, porque com o uso do protocolo NFS quem controla o acesso aos arquivos compartilhados pelo servidor é apenas o cliente, que após conceder a permissão de acesso ao usuário envia a sua requisição ao serviço NFS residente no servidor. O serviço NFS tem acesso irrestrito aos arquivos armazenados no servidor e atende prontamente as requisições de seus clientes, e como os clientes NFS usam os números de identificação de usuário e de grupo do Unix para controle de acesso, números idênticos podem se referir a usuários diferentes no servidor e no cliente, havendo a possibilidade de se permitir acesso equivocadamente a entidades não autorizadas.

O servidor CIFS realiza controle de acesso local para os arquivos compartilhados, inclusive com o auxílio de mecanismos do próprio sistema operacional Windows (de acordo com a versão instalada no servidor), como por exemplo as listas de controle de acesso (ACLs).

5.6 Tabela comparativa entre os protocolos NFS e CIFS

No intuito de consolidar os resultados deste trabalho, a seguir a Tabela 1 resume a análise comparativa entre os protocolos NFS e CIFS, no que se refere aos

serviços de segurança da informação (com a atribuição de níveis de segurança para os serviços oferecidos, como descrito no Capítulo 3):

Tabela 1 – Protocolos NFS e CIFS, comparados quanto aos serviços de segurança.

<table>
<tr><th colspan="2" rowspan="2">SERVIÇO</th><th colspan="2">PROTOCOLO</th></tr>
<tr><th>NFS</th><th>CIFS</th></tr>
<tr><td colspan="2">CONFIDENCIALIDADE</td><td colspan="2">Serviço não oferecido: as informações trafegam pelo canal de comunicação e são armazenadas no servidor em sua forma pura.</td></tr>
<tr><td rowspan="2">AUTENTICAÇÃO</td><td>DE PARCEIROS</td><td>Nível baixo: lista de clientes autorizados, identificados pelo endereço IP ou pelo nome no DNS.</td><td>Nível baixo: clientes se identificam pelo nome no DNS ou no NetBIOS.</td></tr>
<tr><td>DE USUÁRIOS</td><td>Nível baixo: usuários identificados no cliente, por meio dos IDs de usuário e de grupo do Unix.</td><td>Nível médio: usuários identificados no servidor, por meio de derivação criptográfica da senha.</td></tr>
<tr><td rowspan="2">INTEGRIDADE</td><td>NO ACESSO SIMULTÂNEO A ARQUIVOS</td><td>Nível baixo: servidor não controla o estado das conexões com seus clientes.</td><td>Nível médio: servidor controla o estado das conexões com seus clientes, propiciando o uso do mecanismo de oplocks.</td></tr>
<tr><td>NA TRANSMISSÃO DE DADOS ENTRE CLIENTE E SERVIDOR</td><td colspan="2">Nível baixo: não há checagem do conteúdo dos dados após sua transmissão do servidor para o cliente.</td></tr>
<tr><td colspan="2">DISPONIBILIDADE</td><td>Nível médio: servidor minimiza o tempo de restabelecimento de seus serviços após uma falha, não recuperando operações incompletas.</td><td>Nível baixo: funcionamento do servidor depende diretamente da disponibilidade de um serviço de resolução de nomes na rede (DNS ou NetBIOS).</td></tr>
</table>

Tabela 1 – (cont.).

SERVIÇO	PROTOCOLO	
	NFS	**CIFS**
CONTROLE DE ACESSO	Nível baixo: controle de acesso feito apenas no cliente, cuja requisição é atendida no servidor por um serviço cujo acesso a recursos é irrestrito.	Nível médio: controle de acesso feito no servidor, com auxílio de mecanismos do sistema operacional Windows.
AUDITORIA	Serviço não oferecido: servidor não registra informações sobre as requisições atendidas.	

6 CONCLUSÃO

Após a análise dos aspectos de segurança dos protocolos de compartilhamento NFS e CIFS, confirmou-se a premissa de que haveria em ambos vulnerabilidades significativas do ponto de vista da segurança da informação. É possível afirmar que tanto o NFS quanto o CIFS não permitem que clientes e servidores compartilhem arquivos com total segurança em um ambiente de rede, se levarmos em consideração que existem serviços de segurança não oferecidos por ambos os protocolos, e que a maioria dos serviços oferecidos apresenta níveis baixos de segurança.

Ressalta-se, no entanto, que os serviços de segurança oferecidos de forma ineficiente ou mesmo não oferecidos pelos protocolos NFS e CIFS podem ser implementados em versões modificadas dos mesmos, como por exemplo o CNFS (HARRINGTON; JENSEN, 2003), cujo protótipo habilita o controle de acesso criptográfico em um servidor de arquivos NFS. Desta maneira é possível aumentar o nível de segurança de um serviço de compartilhamento de arquivos, mantendo a compatibilidade entre os sistemas que fazem uso do mesmo protocolo.

REFERÊNCIAS

IETF - THE INTERNET ENGINEERING TASK FORCE. **RFC 1813: NFS Version 3 Protocol Specification**. Jun. 1995. Disponível em: <http://www.ietf.org/rfc/rfc1813.txt>. Acesso em: 10 jan. 2005.

SNIA – STORAGE NETWORKING INDUSTRY ASSOCIATION. **Common Internet File System (CIFS) Technical Reference:** SNIA Technical Proposal. Revisão 1.0, Mar. 2002. Disponível em: <http://www.snia.org/tech_activities/CIFS/CIFS-TR-p00_FINAL.pdf>. Acesso em: 10 jan. 2005.

ALMEIDA, Rubens Q. **Arquitetura TCP/IP.** Unicamp, 1997. Disponível em: <http://www.redes.unb.br/download/tcpip.pdf> Acesso em: 23 mar. 2005

STERN, Hal. **Managing NFS and NIS**. O'Reilly, 1992.

STALLINGS, William. **Network and Internetwork Security:** principles and practice. 2nd Edition, Prentice Hall, 1998.

TRINTA, Fernando A. M., MACÊDO, Rodrigo C. **Um estudo sobre criptografia e assinatura digital.** Universidade Federal de Pernambuco, 1998. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm> Acesso em: 20 jan. 2005.

SOLTIS, Steven R., RUWART, Thomas M., O'KEEFE, Matthew T. **The Global File System:** technical report. Laboratory for Computational Science and Engineering, University of Minnesota, 1996.

HARRINGTON, Anthony, JENSEN, Christian. Cryptographic access control in a distributed file system. **SACMAT '03: Proceedings of the eighth ACM symposium on Access control models and technologies**, Como, Italy, p. 158-165, ACM Press, 2003.

GLOSSÁRIO

Active Directory: componente do sistema operacional Windows 2000 que atua como autoridade central de segurança de rede.

Algoritmo: seqüência finita e não ambígua de instruções computáveis para solucionar um problema.

Arquitetura cliente-servidor: toda arquitetura de rede onde estações (microcomputadores) executam aplicações clientes que utilizam programas servidores para transferência de dados do próprio servidor ou para comunicação com outras estações e suas aplicações clientes.

Cache: local de armazenamento de dados que o computador precisará usar em curto tempo ou usa com mais freqüência.

Criptografia: conjunto de técnicas que permitem ocultar informações, tornando-as ininteligíveis para aqueles que não tem acesso às convenções combinadas.

DES (Data Encryption Standard): algoritmo de encriptação com tamanho de chaves de 56 bits, criado em 1977 nos Estados Unidos.

Diffie-Hellman: método de troca de chaves criptográficas que permite a definição de uma chave de sessão para a comunicação segura entre duas entidades, mesmo em um meio de comunicação inseguro.

DNS (Domain Name System): base de dados hierárquica e distribuída, usada para a resolução de nomes de domínios em endereços IP e vice-versa.

Ethernet: tecnologia de interconexão para redes locais, padronizada como IEEE 802.3, e que define cabeamento e sinais elétricos para a camada física e formato de pacotes e protocolos para a camada de controle de acesso ao meio (Media Access Control - MAC) do modelo OSI.

Granularidade: nível de detalhamento.

Hash: método que utiliza algoritmos para transformar dados de tal forma que o resultado seja exclusivo e não possa ser retornado ao formato original. A função do hash é verificar qualquer modificação em um dado.

Idempotentes: termos de resultados equivalentes.

Inode: identificador único que um arquivo recebe no sistema operacional Unix.

IPSec: sistema de padrões abertos que empregam criptografia para auxiliar na comunicação segura em redes IP.

Kerberos: protocolo de autenticação entre aplicações cliente-servidor, que usa criptografia de chave simétrica.

LAN Manager: protocolo de autenticação de rede nativo do sistema operacional Windows NT 4.0, que trabalha com senhas de no máximo 14 caracteres, convertidas para letras maiúsculas e divididas em dois blocos de sete letras.

MD5: algoritmo capaz de gerar um hash de 128 bits a partir de uma mensagem de um tamanho qualquer, usado como mecanismo de verificação de integridade.

NetBIOS (Network Basic Input/Output System): controlador de dispositivos de hardware do tipo PC-Network, cuja interface para programação de aplicação ainda é implementada em redes Ethernet com o protocolo TCP/IP.

NTLMv2: segunda versão do protocolo NTLM (originado pela evolução do protocolo LAN Manager), permite um espaço de chaves de 128 bits para as chaves derivadas de senhas e usa o algoritmo HMAC-MD5 para checagem de integridade de mensagens.

RFC (Request For Comments): documento técnico ou informativo cujo assunto varia desde especificações, padrões e normas técnicas até questões históricas acerca da Internet.

RPC (Remote Procedure Call): protocolo para execução remota de procedimentos em computadores ligados em rede, que pode ser implementado sobre diferentes protocolos de transporte.

SMB (Server Message Block): protocolo de compartilhamento originalmente desenvolvido para ser executado em redes locais do tipo PC-Network com a interface do NetBIOS, e que recebeu em 1996 o nome de CIFS, após o lançamento do sistema operacional Windows 2000, que por sua vez foi a primeira versão do Windows a suportar o transporte de pacotes SMB sobre TCP/IP sem encapsulamento NetBIOS.

SSH (Secure Shell): protocolo de conexão remota que usa criptografia assimétrica para autenticação de parceiros e sigilo da comunicação.

SSL (Secure Socket Layer): protocolo usado para transferência segura de informações pela Internet, é muito utilizado para autenticação de servidores Web (por meio de certificados digitais) e, opcionalmente, dos clientes também.

TCP/IP (Transmission Control Protocol / Internet Protocol): conjunto de protocolos de comunicação utilizado para troca de dados entre computadores em ambientes de redes locais ou remotas, como a Internet.

UDP (User Datagram Protocol): protocolo da camada de transporte do modelo OSI orientado a datagrama, realiza transmissão rápida e não confiável de informações, na medida em que não controla o fluxo das mesmas.

Unix: sistema operacional multiusuário e multitarefa, composto basicamente pelo sistema de arquivos, núcleo (kernel) e interpretador de comandos (shell). Possui várias versões (ou distribuições), de diferentes fabricantes.

Windows: denominação comum aos sistemas operacionais desenvolvidos pela Microsoft Corporation.

WINS (Windows Internet Name Services): serviço de resolução de nomes compatível com NetBIOS, oferecido por servidores com sistema operacional Windows.

WWW (World Wide Web): rede de documentos hipertexto veiculados na Internet.

X.500: protocolo que especifica um modelo para a conexão de serviços de diretórios locais, a fim de formar um diretório global distribuído.