4º SBRC
RECIFE - 24 A 26 DE MARÇO 86

Fracionamento-disseminação : uma técnica para a segurança de dados em sistemas distribuídos

J.Fraga

Universidade Federal de Santa Catarina
DEEL - CTC - caixa postal 476,
Florianopolis, SC.

Resumo

A isolação física entre os componentes do sistema distribuído e a redundância de recursos são usadas em um sistema distribuido no sentido de tolerar um certo número de intrusões, sem violações da segurança de dados ("data security"). Com este objetivo, uma técnica de armazenamento de arquivos é introduzida : "fracionamento-disseminação".

1. Introdução

Os mecanismos e princípios usados para manter a segurança das informações em um sistema distribuído são normalmente baseados sobre a noção de "evitar intrusões". Estes mecanismos são concebidos para prevenir violações de segurança tais como a negação de serviço (a não disponibilidade dos dados), a revelação maliciosa ou acidental de dados sensíveis e suas modificações não autorizadas. Contudo a complexidade e as características de sistemas distribuídos tornam difícil o "evitar intrusos".

Os mecanismos de controle de acesso e os serviços de autentificação concebidos nestas bases, são usados em sistemas distribuídos onde os recursos são acessíveis por meio do subsistema de comunicação. O acesso pode ser obtido ou por meio da apresentação do identificador único do recurso solicitado ou por aquele do cliente. O grau de segurança destes recursos é probabilista. Isto depende da dificuldade de adivinhar estes identificadores.

Muitas vezes, a proteção física dos diferentes elementos de um sistema distribuido é bastante dificultada. Em muitos casos, a criptografia é usada em adicao aos mecanismos citados acima. Contudo, o aspecto "confidencialidade", fornecido pela criptografia não é suficiente para excluir todas às possíveis violações de segurança resultante de uma intrusão. Esta confidencialidade, também não é absoluta; ela depende de fatores como da relação entre a capacidade de processamento do intruso e a potência do algoritmo de cifragem/decifragem e da integridade das entidades de gestão de chaves criptograficas.

Nos sistemas distribuídos existem, de uma maneira geral, uma oposição entre as técnicas utilizadas para a seguranca de dados e as técnicas de disponibilidade/confiabilidade. Este conflito é originado do fato que a diminuição dos pontos de acesso aos objetos protegidos, a fim de restringir as possilidades de intrusões, conduz a uma diminuição da redundância dos objetos, e por consequência de suas disponibilidades.

Diante destes fatos, nos introduzimos a noção de "tolerancia as intrusões" /Fraga85a/, /Fraga85b/. Um sistema tolerante a intrusões deve :

- Suportar um certo número de intrusões, procurando minimizar o impacto das mesmas sobre a segurança dos dados.
- Diminuir a criticidade que representa os mecanismos e informações de acesso com respeito a disponibilidade no sistema.

Duas estratégias foram consideradas para atingir estes objetivos. A primeira diz respeito ao armazenamento de arquivos no sistema. Um arquivo é armazenado usando uma técnica que chamamos "fracionamento-disseminação":

- o fracionamento consiste em decompor o arquivo em partes elementares e reproduzir estas partes em vários exemplares. O resultado destas operações é o que chamamos frações.
- disseminacao indica a operação pela qual estas frações são ditriduidas aleatóriamente entre um conjunto de sítios de arquivamento do sistema.

O fracionamento-disseminação de um arquivo é realizado de tal maneira que, um certo número de intrusões nos sítios de armazenamento não coloca em perigo a segurança dos dados no sistema..

A segunda estratégia está ligada a redução da dependência da segurança do sistema em relação as informações de acesso (nomes e chaves). O uso de técnicas de voto e de esquemas de limiar ("threshold schemes" /Shamir79/) deve permitir um aumento na disponibilidade destes objetos e por consequência uma diminuição do risco de violação do sistema.

2. Descrição geral do sistema

A aplicação das estratégias citadas acima esta sendo considerada para um sistema distribuido, compreendendo uma rede local de estações de trabalho (sítios de usuário) que correspodem ao "dominio físico" de seus utilizadores e de computadores especializados (sítios de serviço).

Os executivos locais destas máquinas são incluídos em um sistema operacional de rede (NOS) /Fletcher80/ que utiliza :

- uma camada "suporte de serviço", responsável pela implantação do modelo servidor/cliente.
- Uma camada "kernel de sistema distribuido" (ou camada de comunicação inter-processos) que compreende o servico de IPC inter-máquina e uma base para a construção dos mecanismos de confidencialidade e de segurança do sistema. Esta base é constituída de facilidades criptograficas e de um serviço de "portos".

O serviço de transporte é do tipo datagrama. As mensagens são cifradas com redundâncias de modo a assegurar a integridade e a autenticidade dos dados transferidos no suporte de comunicação. Os mecanismos de detecção e de recobrimento de erros provenientes de falhas e intrusões ativas sobre o suporte de comunicação são incluidos na camada suporte de serviço.

2.1 Serviços de base (sistema de arquivos)

O sistema contém dois tipos de computadores especializados : os A sítios de arquivamento (com dispositivos de memória de massa) e os S sítios de segurança (figura 1). A partir destes sítios é formado um sistema de arquivos confidencial e seguro, construido sobre quatro serviços de base : serviço de gestão de arquivos, o serviço de fracões, o serviço de diretórios e o serviço de autentificação. Esta decomposição funcional é semelhante àquelas propostas em /Birrel80/ e /Tanenbaum83/.

Serviço de gestão de arquivos

O serviço de gestão de arquivos está localizado no sítio de usuário. Este serviço oferece uma interface bem definida de serviço de arquivos que permite o armazenamento e a recuperação de arquivos a partir dos serviços de frações (sítios de arquivamento). As operações de arquivo são : "criar arquivo", "abrir arquivo", "fechar arquivo", "apagar arquivo", "ler arquivo", "escrever arquivo". Acessos mais elementares sobre um arquivo, disponíveis a um utilizador, são executados nos sítios de usuário.

Serviço de gestão de frações

O serviço de gestão de frações é fornecido pelos "servidores de arquivamento" (sitios de arquivamento"). As operações destes servidores constituem em simples alocação de espaço sobre a memória física e em transferências de dados (as frações) entre esta memória e o suporte de comunicação.

Serviço de diretórios

Os sitios de segurança fornessem o suporte para os serviços de diretórios e para o controle de concorrência e de acesso aos arquivos. Estes sítios formam uma estrutura de diretórios redundantes. Cada arquivo e designado no sistema distribuido por um identificador único de arquivo "IUF". Estes identificadores são gerados nos sítios de usuário e correspondem a números inteiros cuja unicidade é garantida pelos campos "número de sitio" e "data" que indicam rspectivamente, o sítio e a data da criação do arquivo.

A principal operação do serviço de diretórios consiste na transformação de nomes simbólicos em IUF. Esta operação precede uma "abertura de arquivo" e é acompanhada pela verificação de uma lista de controle de acesso, associada ao arquivo. Esta lista é gerada quando da criação do arquivo.

Serviço de autentificação

Os sítios de segurança executam também as funções de um serviço de autentificação distribuido. Este seviço consiste em assegurar "associações confidenciais" cliente/servidor e a autentificação dos utilizadores do sistema. Este serviço é descrito em parágrafos posteriores.

2.2 Sítios de segurança : falhas e intrusões

Cada sitio de seguranca interage com os processos-utilisadores e os servidores de arquivamento de maneira completamente independente dos demais sítios de segurança do sistema. Os resultados destas interações são submetidos a um voto majoritário nos sítios de usuário e nos de arquivamento. Nestas condicões, um certo número de sítios corrompidos ou falhos não pode comprometer nem a continuidade nem a segurança dos serviços de repertório e de autentificação. Para simplificar a notação, nos chamaremos servidores de seguranca as entidades executoras destes dois serviços baseados nos sítios de segurança.

2.3 Coerência das múltiplas copias

A coerência dos objetos neste sistema distribuido é mantida a partir das operações de arquivo que são construidas sobre um mecanismo de controle de

concorrência e uma técnica de "versoes imutáveis" /Tripathi83/.

O mecanismo de controle de concorrência é feito a partir dos sítios de segurança, utilisando a técnica de "locks" a duas fases /Keller81/. A granularidade do "lock" é o arquivo, sendo exclusivo para o modo "ler/escrever" e compartilhado para o modo "ler". O acesso é conseguido a partir da obtenção da maioria dos "locks" enviados pelos servidores de segurança no pedido de abertura de arquivo. Se o número de "locks" é insuficiente, estes devem ser abandonados. Os "locks" são mantidos durante uma "sessão" para a operacoes sobre o arquivo. Uma sessão é a conexão do serviço de gestão de arquivos aos servidores de arquivamento, estabelecida durante o período de abertura de arquivo.

O mecanismo de versões múltiplas é implantado a partir dos sítios de arquivamento. Uma operação de escritura de fração (modo ler/escrever arquivo) cria frações para a nova versão do arquivo. Esta versão é designada versão corrente quando da operação fechar arquivo. Os servidores de segurança são os coordenadores destas designações /Fraga85b/.

3 Fracionamento-disseminação

Nós propomos um serviço de arquivo que deve suportar o objeto-arquivo como uma sequência linear de bytes sem estrutura nenhuma interna, conhecida pelo serviço de gestão de arquivos. Esta sequência linear de bytes só deve existir nos sítios de usuário.

No procedimento de armazenamento, o arquivo é decomposto em $\underline{N}$ frações. Cada fração é então reproduzida em $\underline{R}$ copias o que conduz a $\underline{M}$ ($=\underline{N}.\underline{R}$) exemplares de frações de um arquivo. As frações e suas copias são disseminadas a partir do sítio de usuário, em direção dos sítios de arquivamento.

3.1 Condições necessárias para o fracionamento-disseminação

Para que o fracionamento-disseminação atenda a sua finalidade de tolerância aos intrusos, são duas as condições necessárias :

(a) As $\underline{R}$ copias de uma mesma fração são armazenadas sobre $\underline{R}$ sítios de arquivamento diferentes. Em caso contrario, a disponibilidade do arquivo seria não ótimo (condição de disponibilidade).

(b) A proporção de um arquivo em um sítio de arquivamento é dado pela relação Tk/N onde Tk é o número de frações do arquivo no sítio. O conteúdo da proporção Tk/N não deve permitir a recuperação de informações significativas do arquivo fracionado (condição de confidencialidade).

O número N e o algorítmo utilisado no fracionamento do arquivo são fatores determinantes para que a proporção Tk/N não revele informações contidas no arquivo. O algorítmo de fracionamento deve percorrer o texto do arquivo e distribuir sequencialmente as unidades elementares de acesso (bytes ou menos) entre as $\underline{N}$ frações. Esta composição das frações pode ser executada de diversas maneiras. A figura 2 mostra um exemplo possível de composições das frações.

Para T = max Tk (k=1,2,...,A) e as condições citadas acima nós obtemos :

$$A * T \quad N * R \qquad (T/N \quad R/A) \quad (1),$$

onde A.T é a capacidade disponível de arquivamento para frações de um

onde A.T é a capacidade disponível de arquivamento para frações de um arquivo e N.R é o número total de exemplares de frações de um arquivo.

3.2 Matriz de arquivamento

Os armazenamentos e as recuperações dos arquivos são realizadas utilizando uma matriz de arquivamento que é constituída de palavras de um código "m-out-of-n". Os valores do peso (m) e do comprimento (n) do código são respectivamente R e A. A matriz de arquivamento é então constituída de N linhas e A colunas (figura 3).

Cada fração do objeto é associada, de maneira aleatória, a uma palavra de código da matriz. Os bits a "1" de uma palavra de código associada a uma fração Fi (i=1..N) representam suas R copias. Os servidores de arquivamento alocados para estas R copias são determinados a partir dos números das colunas (1..A) onde estão colocados os bits a "1" da palavra de código.

3.4 Considerações sobre o fracionamento-disseminação

A implementação da técnica do fracionamento-disseminação deve considerar dois aspectos importantes para a confidencialidade de um arquivo :

(a) O fracionamento de um arquivo deve ser realizado de modo a tornar o mais complexo possível o estabelecimento de ligações entre as diferentes partes do arquivo fracionado. O valor de N é uma medida desta complexidade.
(b) As informações de um arquivo são disseminados o mais possível entre os sítios de arquivamento.

Nos introduzimos duas grandezas que permitem medir a disseminação de um arquivo no sistema:

- A dispersao D de um arquivo corresponde ao número mínimo de sítios de arquivamento, necessários para que alguém possa se habilitar ao acesso de uma copia do arquivo.
- A dissimulacao C representa o número mínimo de sítios de arquivamento aos quais é necessário acessar para que se tenha a certeza da obtenção de uma copia do arquivo. Representa também, o número de sítios de arquivamento necessários para se acessar a todos os arquivos.

A figura 4 ilustra a distinção entre estas duas variáveis. No exemplo da figura 4.a, a dissimulação (C) do objeto e de tres sítios de arquivamento, isto porque, para se estar seguro da obtenção de uma copia do objeto com acessos quaisquer (sem escolha de sítio), é necessário tres sítios. A dispersão D neste caso, corresponde a dois sítios porque em alguns casos pode se ter uma copia do objeto com dois sítios (sitios 1 e 3 ou 2 e 4 na figura 4.a).

A figura 4.b apresenta um exemplo da disseminação na qual a dissimulação C e a dispersão D de um objeto coincidem (3 sitios).

Estes exemplos ilustram duas propriedades da disseminação :

(a) A dissimulação C de um objeto para A e R fixos é uma invariante (independe de N). Isto pode ser facilmente verificado se consideramos as R copias de cada fração sobre sítios distintos. Neste caso, os sítios de arquivamento podem ser divididos em dois subconjuntos disjuntos de (R-1) e (A-(R-1)) elementos. O subconjunto de (A-(R-1)) elementos deve conter no menos uma copia de cada fração (condição a da

seção 3.1), por consequência :

$$C = A - R + 1$$

(b) A dispersão D de um objeto, ao contrário, depende do fracionamento. A dissimulação de um objeto corresponde a dispersão máxima que se pode obter para este objeto ($D \leq C$).

3.5 Tipos de fracionamentos propostos

Duas possibilidades para o particionamento de um arquivo foram consideradas. A primeira corresponde ao que chamamos fracionamento saturado onde a matriz de arquivamento é composta pelo código "R-out-of-A" completo. Isto representa uma partição do arquivo com o número máximo de frações ($N = \binom{A}{R}$). Neste caso, o número de frações de um arquivo em um sítio é máximo (Tk é constante e dado por $T = \binom{A-1}{R-1}$) e as frações são menores.

A utilisação do código "R-out-of-A" completo permite a dispersão máxima de um objeto (D C). O exemplo da figura 4.b corresponde a um fracionamento saturado com a matriz formada pelo código "2-out-of-4" completo.

A segunda e o fracionamento não saturado onde a matriz é composta de palavras escolhidas do codigo "R-out-of-A" ($N < \binom{A}{R}$). A matriz de arquivamento derivada de algumas palavras do código "R-out-of-A" determina uma dispersão não máxima do arquivo ($D < C$) :

$$A - (R-1) > D \geq N/T$$

Isto implica a que se pode acessar a uma copia com um número de sítios de arquivamento inferior a 'A - (R-1)' (ver figura 4.a onde o fracionamento é não saturado, com a matriz de arquivamento formada por quatro das seis palavras do codigo "2-out-of-4").

O fracionamento saturado apresenta uma complexidade exponencial de processamento em função de A e o fracionamento não saturado representa uma alternativa nos casos onde o número de sítios de arquivamento é grande.

4. Controles criptográficos

A criptografia é usada neste sistema em vários níveis deste sistema. As operações criptográficas estão disponíveis a partir do kernel de cada sítio. Esta facilidade foi concebida para um algorítmo convencional (DES) e apresenta um gerador de chave em cada sitio.

4.1 Chave associada ao arquivo

Na criação de um arquivo, é gerada localmente, no sítio de usuário, um número aleatório: a "chave associada ao arquivo" KF. Este número é importante para o cálculo da matriz de arquivamento do arquivo (é a partir deste valor que se associa cada fração do arquivo a uma palavra da matriz de arquivamento) e também para o cálculo dos nomes das frações que servem como direitos para o acesso as frações que estao dispersas no sistema.

As chaves KF são objetos sensíveis o que significa que o sistema deve fornecer um meio de evitar a liberação de uma chave como consequência de

uma intrusão. Contudo, o sistema tem também de fornecer um meio de fazer estes objetos disponíveis em presença de falhas parciais do sistema. Os esquemas de limiar ("threshold schemes" /Shamir79/) resolvem os conflitos entre a confidencialidade e a disponibilidade de objetos. Nestes esquemas, uma chave KF é associada a um número n de "valores imagens" de KF: Kj (j=1..n) e o conhecimento de :
- um número de imagens Kj maior ou igual ao limite t (t < n) permite o cálculo da chave KF,
- um número de imagens Kj inferior a t e insuficiente para a restauração da chave.

O esquema de limiar usado em nosso sistema tem n = S (S e o número de sítios de segurança) e t = S/2 + 1. A imagem Kj é armazenada no sítio de segurança Sj (j=1..S) e copias desta imagem são liberadas em cada pedido de "abertura" para o correspondente arquivo. Isto implica a que :
(a) se um intruso obtém S/2-1 imagens Kj, o segredo da chave KF não é comprometido,
(b) a restituição de KF é garantida mesmo no caso da destruição de S/2-1 imagens de KF (por sabotagens ou falhas nos sítios de segurança).

4.2 Chaves e nomes para o serviço de comunicações

O kernel do sistema distribuído assegura serviços que são decisívos para a segurança do sistema: o serviço de "portos" e o serviço de gestão de chaves para a comunicação. O serviço de IPC inter-máquina usa a noção de "porto". Portos são objetos protegidos pelo kernel, noqual mensagens são colocadas e removidas. Dois direitos são associados a cada porto: o direito de recepção e o direito de emissão.

Uma chave criptografica KC é associada com cada porto. Esta chave é usada para a cifragem de mensagens enviadas ao porto e para a decifragem das mensagens recebidas no porto. O kernel de cada sitio gestiona e protege para o processo local uma tabela de portos de recepção (direitos de recepção) e uma de portos de emissão (direitos de emissão). Estas tabelas são constituídas de "representações globais" dos portos (identificadores globais) e das chaves associadas a estes portos.

A segurança das transferências sobre o suporte de comunicação depende do estabelecimento do que é chamado associação confidencial. Uma associação confidencial é um par de portos que permite a dois processos se comunicarem. Para estabelecer uma associação confidencial, um proceso-utilisador deve alocar um porto e enviar este porto (o direito de emissão) ao processo de destinação. Isto consiste no envio de mensagens "pedido de associação" ao processo desejado para a comunicação, usando os sítios de segurança do sistema (serviço de autentificação) como intermediários. Nestas transferências são usadas as associações confidenciais entre um processo (processo-utilizador ou servidor) e os servidores de segurança (estas associações são descritas no parágrafo 4.3).

Nestas transferências dos "pedidos de associação", o kernel do sítio local usa o esquema de limiar para o cálculo de imagens KCj da chave KC associada ao porto. Os pedidos de associação são compostos da representação global do porto e de uma das imagens KCj. As mensagens são roteadas diferentemente, em direção ao sítio do processo de destinação, usando os diferentes servidores de segurança do sistema. Tal procedimento permite a reconstituição do direito de emissão (reconstituição de KC) no sítio de

destinação em presença de S/2-1 sítios de segurança corrompidos ou falhos.

4.3 Conexão dos utilisadores

Um usuário do sistema deve possuir um conjunto de "chaves privadas" ¢(KB1,KB2,...,KBs). Cada uma destas chaves é usada para a autentificação do utilizador com um dos servidores de segurança do sistema. Estas autentificações correspondem ao estabelecimento de associações confidenciais com os servidores de segurança do sistema.

Cada KBj é usada para cifrar o identificador do utilizador e o direito de emissão (representação global e chave associada) de um porto alocado no sítio de usuário, para o correspondente servidor Sj. Estes objetos cifrados são enviados a um porto público do servidor Sj. O usuário é considerado conectado ao sistema quando o número de associações confidenciais com os servidores de segurança é igual ou maior que o número de servidores necessários (S/2+1) para assegurar o correto funcionamento do sistema.

5. Procedimentos de armazenamento e de recuperação de arquivos

O armazenamento e a recuperação de um arquivo dependem essencialmente da determinação dos locais de armazenamento e dos nomes das frações do arquivo. Isto é efetuado no sítio de usuário, a partir de parâmetros liberados dos sítios de segurança. Sem estes parâmetros a repredução das condições de acesso às frações de um arquivo é muito improvável.

5.1 Armazenamento do arquivo

(1) O sítio de usuario deve receber dos servidores de segurança o IUF arquivo e as imagens da chave KF quando do pedido de abertura do arquivo. Estes objetos são enviados após a verificação dos direitos de acesso do usuário pelos servidores de segurança. As imagens permitem a reconstituição de KF.

(2) Composição das frações, e associação de um número de ordem a cada fração Fi (i=1..N).

(3) Um valor aleatorio VAi é calculado para cada fração. Este valor é o resultado da aplicação de uma "função a sentido único" (e.g., a função H(I,M) proposta por Davies /Davies81/) sobre uma composição g de IUF e do número de ordem i da fração, tendo KF como vetor de inicialisação (I) : VAi = H(KF,$\overline{g}$(IUF,i)).

(4) A matriz de arquivamento do arquivo é calculada associando as frações Fi em ordem crescente de seus valores VAi às palavras do codigo "R-out-of-A".

(5) Valores de deslocamento dij (j=1..R) correspondentes a Fi são determinados na matriz de arquivamento a partir dos números das colunas que possuem os bits "1" da palavra de código associada à fração Fi.

(6) um nome Nomij para cada copia de fração Fi é calculado pela concatenação do IUF com VAi e os respectivos valores de dij. Estes identificadores de frações sao utilisados nas interações com os sitios de arquivamento.

(7) As frações e seus respectivos nomes são enviados aos sítios de arquivamento, realizando o que denominamos a "disseminação". A figura 5 apresenta uma esquematização destas etapas.

5.2 Recuperação de um arquivo

O procedimento de reconstituição do arquivo deve repetir as etapas de (1) a (6) do parágrafo anterior, na determinação da localização e dos nomes NOMij das frações. Para a reconstituição do arquivo devemos utilizar redundâncias concatenadas às proprias frações e que permitam a detecção de erros. Nós utilizamos um "checkword" criptográfico, calculado a partir da aplicação da função H de Davies em cada fração, (o vetor de inicialização e a chave KF). Neste caso o valor de cada função é aquele da primeira copia obtida e certificada como correta. Isto nos permite tolerar (R-1) sítios de arquivamento corrompidos ou falhos no sistema.

6. Conclusões

Neste trabalho introduzimos a noção de tolerância a intrusões. A fim de minimizar o efeito de uma intrusão, estratégias são usadas para reduzir as informações acessíveis a partir de uma intrusão. O "fracionamento-disseminação" é uma destas técnicas. O armazenamento de arquivos através do fracionamento-disseminação contribui para a confidencialidade das informações e possibilita o recobrimento de erros acidentais ou intencionais (negação de serviço e modificação não autorizada).

A fragmentação-disseminação de um arquivo é realizada de tal maneira que o estabelecimento de uma correlação entre frações de um mesmo arquivo, presentes em um sítio é muito difícil. A complexidade dos algorítmos utilizados para o fracionamento-disseminação (descritos em 5.1 e 5.2) é uma função linear do tamanho dos arquivos. Os acessos são sómente possíveis com o uso de parâmetros associados com o objeto disseminado (KF e IUF). Estes parâmetros são armazenados nos sítios de segurança usando técnicas de voto e esquemas de limiar o que permite um aumento de suas disponibilidades e um decréscimo do risco de violação do sistema na presença de sítios de segurança corrompidos ou falhos.

O estudo apresentado neste artigo foi realizado no quadro do projeto SATURNO /Deswarte85a/, /Deswarte85b/. Este sistema tolerante á falhas e a intrusoes está em desenvolvimento no Laboratoire d'Automatique et d'Analyses de Systemes (LAAS) na França.

7. Referencias

/Birrell80/ A.D.Birrell, R.M.Needham : "A universal file server" IEEE Transactions on Software Engineering, Vol SE-6, No 5, september 1980.

/Davies81/ D.W.Davies : "Protection", 'in Distributed Systems. Architecture and Implementation', Lecture Notes in Computer Science 105, Springer-Verlag, 1981.

/Deswarte85a/ Y. Deswarte, J.C. Fabre, J. Fraga, D. Powell and J.C. Laprie: "A Fault and intrusion tolerance distributed systems", LAAS research report No. 85054, 1985.

/Deswarte85b/ Y. Deswarte, J.C. Fabre, J. Fraga, D. Powell and J.C. Laprie: "A Fault and intrusion tolerance distributed systems", IEEE Newsletter Junho 1985.

/Fletcher80/ J.G.Fletcher and R.W.Watson: "Service support in a network operating system" COMPCON`80 Spring, San Francisco, USA, fev. 1980.

/Fraga85a/ J. Fraga and D. Powell: "A fault and intrusion tolerant file system", 3th International Conference on Computer Security, IFIP/SEC`85, Dublin, Irlanda, agosto 1985.

/Fraga85b/ J.Fraga : "La securite des donnees par la tolerance aux intrusions", These de doctorat, LAAS/INPT, No 11, 1985.

/Shamir79/ A. Shamir: " How to share a secret", Communication of the ACM, vol. 22, No. 11, Nov. 1979.

/Tanenbaum83/ A.S.Tanenbaum and S.J.Mullender: "On distributed file servers", Journees Europeenes d'Etude sur les Systemes Informatiques Distribues, INRIA, Le Mont Saint Michel, France, septembre 1983.

/Tripathi83/ A.R. Tripathi and P.S.Wang: "An object-oriented design model for reliable distributed systems", 3th Symposium on Reliability in Distributed Software and Database Systems, Clearwater Beach, Floride, october 1983.

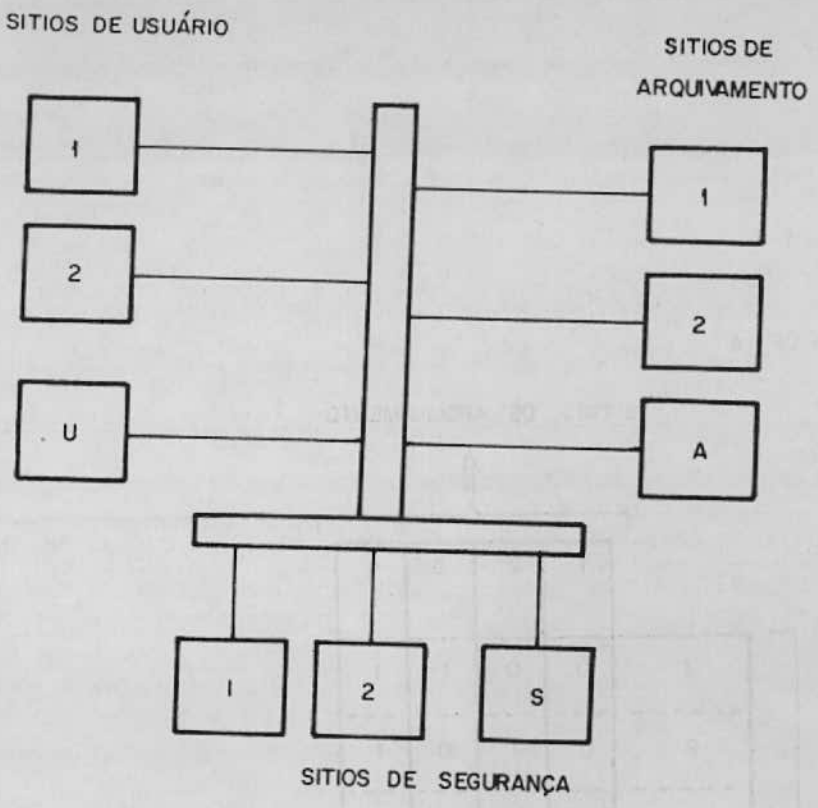

figura 1: Vista geral do sistema

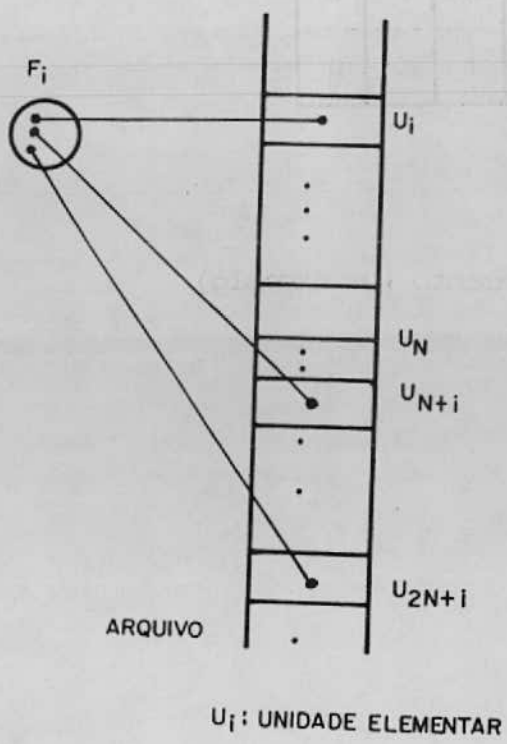

figura 2: Composição das frações

CÓDIGO R-OUT-OF-A
(R=2 et A=4)

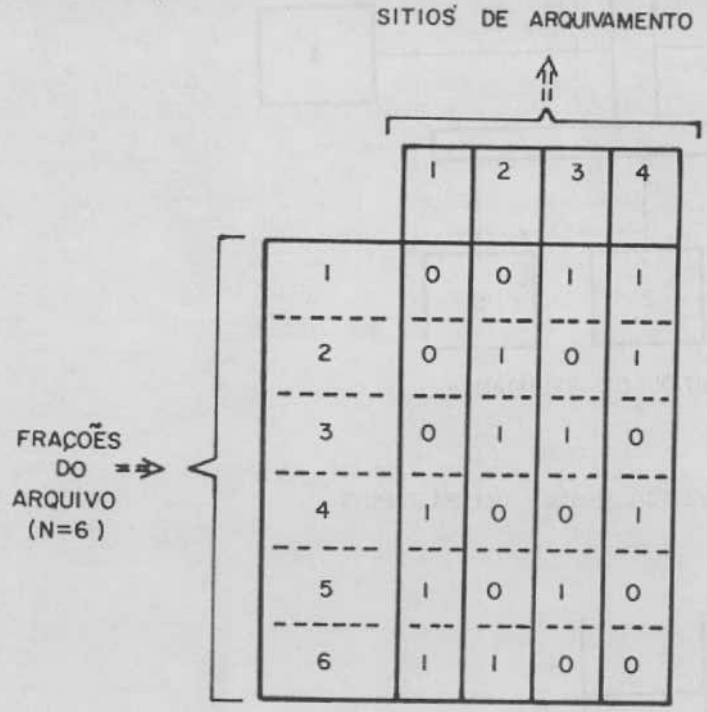

figura 3 : Matriz de arquivamento (um exemplo)

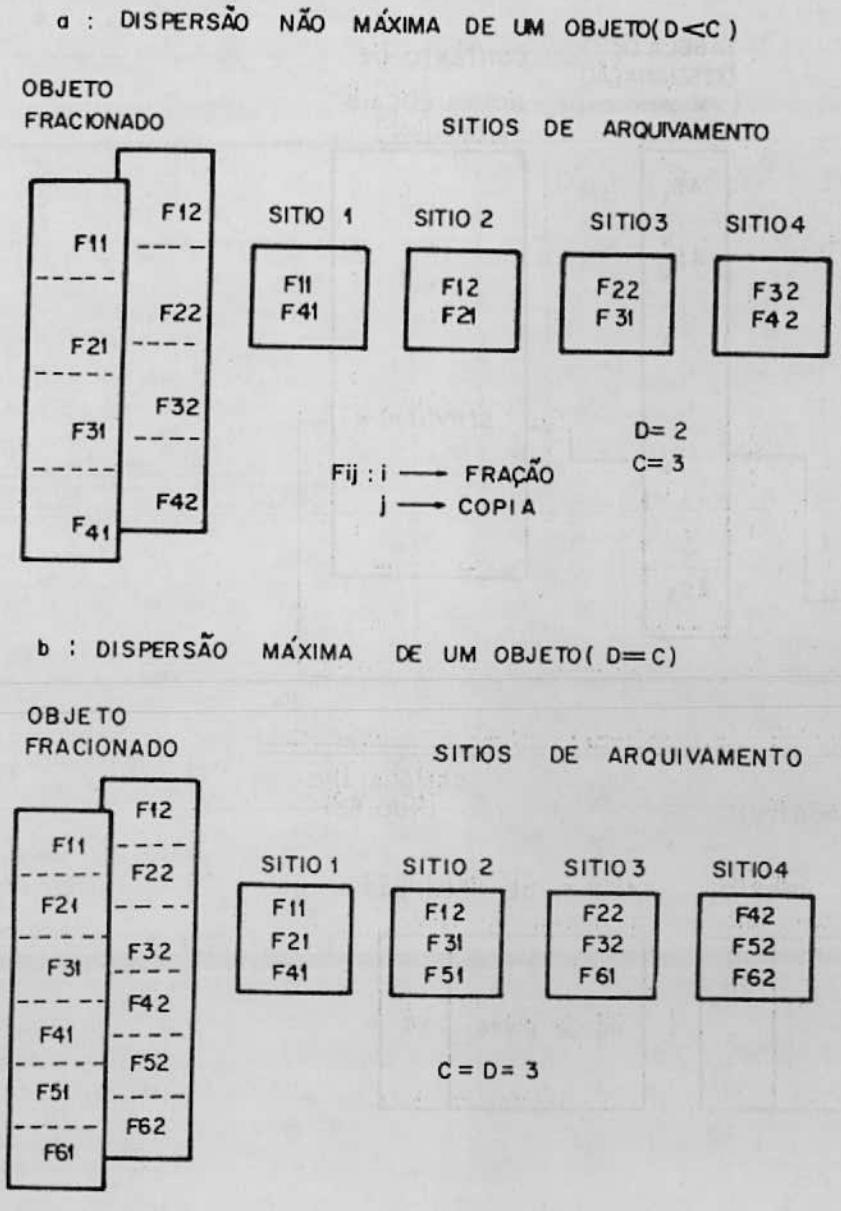

figura 4: Fracionamento-disseminação de um arquivo

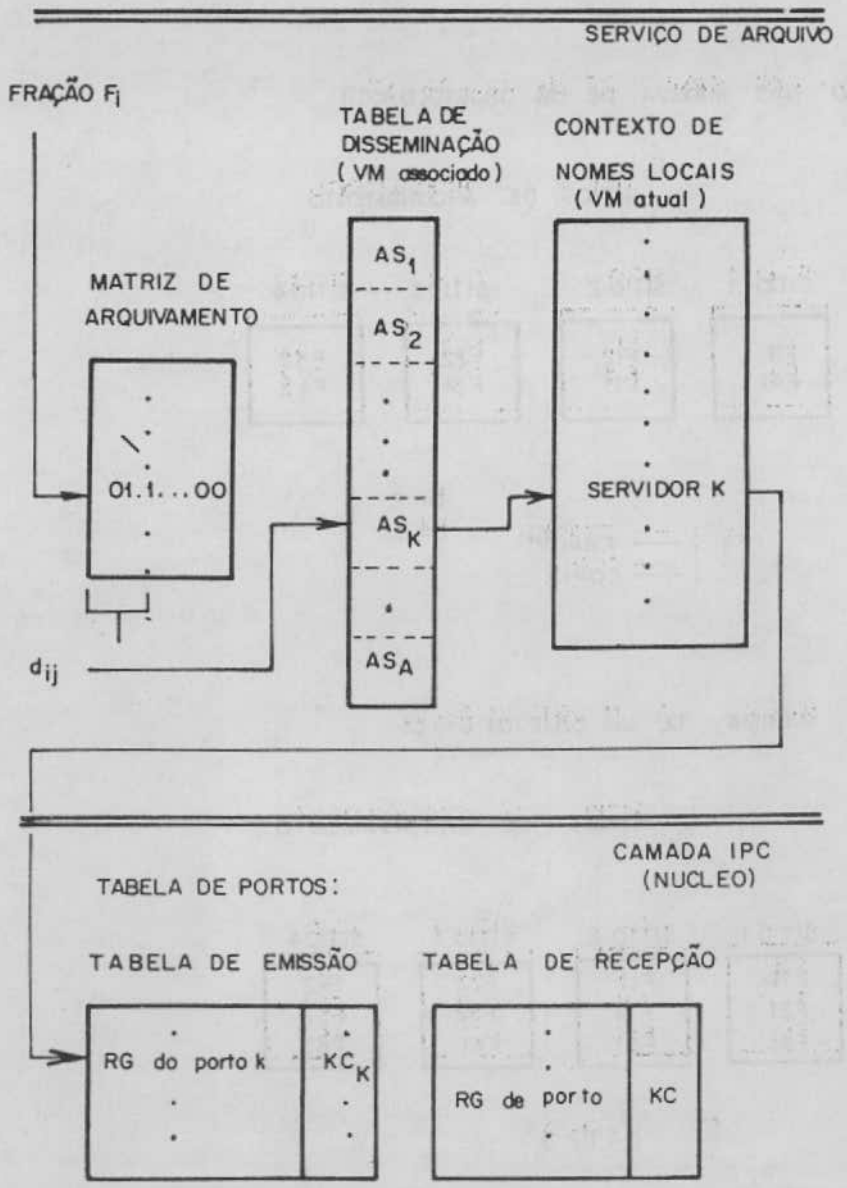

figura 5: Etapas do fracionamento-disseminação