

Segurança Informática e nas Organizações

Exame Final
13 de Janeiro de 2016

João Alegria | 68661

Segurança Informática e nas Organizações

1º Semestre, 2015/16

Questões 1-20: Exame Final

Questões 11-20: 2º Teste Intermédio

13 de janeiro de 2016

- Todas as perguntas têm a mesma cotação.
- Todas as respostas devem ser justificadas.
- A duração total do exame é de 3h, a duração total do teste intermédio é de 1h 30m.

1. Ao aplicar uma cifra informática por blocos explique porque é necessário utilizar métodos diferenciados para os blocos intermédios e para o último bloco a ser cifrado ou decifrado.
2. Na definição das políticas de segurança, quais a dimensões que devem ser consideradas?
3. Em que consiste um *CVE* e como este pode ser utilizado para manter um sistema seguro?
 - a. Como pode um *CVE* facilitar a realização de ataques?
 - b. Que mecanismo reduz a sua utilização por atacantes?
4. Considerando o princípio de *Kerckhoff*.
 - a. Descreva o seu impacto para aplicações de código livre utilizando cifras públicas.
 - b. Descreva o seu impacto para aplicações sem código conhecido e/ou utilizando cifras secretas.
5. Descreva com detalhe como uma cifra pode ser utilizada para calcular um *Message Authentication Code*.
6. Considerando os modos de cifra CBC e CTR, qual o resultado após a decifra, se na transmissão se corromper 1 bit do criptograma ou do Vetor de Inicialização?
7. Descreva a razão pela qual o cartão de cidadão português contém 7 certificados de chave pública e qual a função de cada certificado presente?
8. Compare os requisitos de confinamento associados ao armazenamento de chaves simétricas e assimétricas e o impacto da descoberta de cada uma das chaves.
9. No âmbito de uma PKI, explique em que consiste e qual a utilidade de uma cadeia de certificação e como esta é utilizada para o acesso seguro a serviços na Internet.
10. Porquê uma entidade certificadora expõe informação semelhante via CRL, Delta-CRL e OCSP?
 - a. Refira o propósito de cada método, limitações e vantagens.

11. No contexto da tentativa de descoberta de uma chave WEP, descreva o processo de reinjeção de tramas e o que motiva este processo.
12. Considerando a autenticação direta com senha partilhada e a autenticação por desafio resposta, ambos com segredos escolhidos pelos utilizadores:
 - a. Descreva com detalhe e compare os métodos.
 - b. Como pode um atacante no canal de comunicação descobrir o segredo partilhado?
13. No contexto de chaves de utilização única:
 - a. Explique o conceito, as vantagens e as desvantagens.
 - b. Descreva a sua utilização com equipamentos SecurID.
14. Descreva o funcionamento do modo AES-CCMP e qual o seu propósito no contexto de redes de comunicação sem fios (IEEE 802.11i).
15. No contexto da associação a uma rede sem fios IEEE 802.11:
 - a. Quais as fases que compõem a norma IEEE 802.1x.
 - b. Qual o propósito de cada fase.
 - c. Quais os elementos participantes em cada fase e que informação lhes está associada.
16. Explique como funciona uma Firewall do tipo *Stateful Packet Filter*.
17. Distinga controlo de acesso mandatório (ou obrigatório) de controlo de acesso discricionário e forneça exemplos da existência de ambos os modelos no contexto de um sistema operativo.
18. Descreva o mecanismo de elevação de privilégios existente nos sistemas Linux e controlado através das permissões de um ficheiro.
 - a. Qual a utilidade deste mecanismo?
 - b. Quais os riscos deste mecanismo?
19. Descreva os tipos de cópias de ficheiros (*backups*) vulgarmente realizados e os métodos que permitem reduzir as necessidades de armazenamento das cópias efetuadas.
20. Considere que se pretende criar um sistema de armazenamento composto por 10 discos de 1TB cada, com a capacidade de suportar a falha um qualquer disco.
 - a. Descreva como se pode construir este sistema e quais as características operacionais final (desempenho, espaço disponível, falhas suportadas).
 - b. Como é possível suportar a falha simultânea de dois discos, ou mesmo de todos os discos, e que desvantagens têm de ser consideradas para cada um dos casos?

Segurança 2015/2016

2º teste + Exame Final - 13 janeiro 2016

1. Ao aplicar uma cifra informática por blocos explique porque é necessário utilizar métodos diferenciadores para os blocos intermédios e para o último bloco a ser cifrado ou decifrado.

As cifras por blocos, em alguns modos (ECB, CBC) têm de se aplicar o texto com dimensões múltipla do tamanho do bloco. Existem vários métodos para aumentar a dimensão do texto de forma previsível, tais como Cypher Text Stealing, PKCS#7 e PKCS#5. A este processo dá-se o nome de padding.

O Cyphertext Stealing é um método em que se roubam N bytes do final do penúltimo bloco, sendo que são adicionados estes bytes ao último bloco de texto de forma a tornar o texto múltiplo do tamanho do bloco.

O último bloco é depois cifrado e enviado como penúltimo bloco (troca-se a ordem entre último e penúltimo). O resultado é que a cifra ocorre normalmente mas o tamanho do criptograma não aumenta. No entanto, necessita que o texto ocupe um mínimo de 2 blocos.

No decifro, depois de se decifrar o penúltimo bloco do criptograma, roubam-se de volta os bytes suficientes para compor o último bloco. Este depois é descifrado e volta-se a trocar a sua ordem (último pelo penúltimo). De notar que os bytes "roubados" são sempre cifrados e decifrados duas vezes. No entanto, o número de blocos cifrados ou decifrados não se altera.

Este método é o mais complexo. Os outros métodos são mais simples mas têm o inconveniente de aumentar sempre o tamanho do criptograma.

O PKCS#7 funciona adicionando bytes com o valor dos bytes em falta. Ou seja, se o último bloco tiver 5 bytes em falta para ser múltiplo do tamanho do bloco, não adicionados 5 bytes com o valor 5.

O PKCS#5 é igual mas apenas foi definido para blocos de 8 bytes (DES).

2. Na definição das políticas de segurança, quais as dimensões a considerar?

Devem ser considerados:

• Princípio do privilégio mínimo - Este princípio afirma que os sujeitos devem usufruir, em cada instante, apenas dos direitos necessários e suficientes para a execução das tarefas que lhes estão atribuídas.

• Políticas em Sistemas Distribuídos - Definição de conjunto de máquinas e redes de domínio, definição do universo de utentes válidos, definição de atividades ilícitas.

3. Em que consiste um CVE e como pode ser utilizado para manter um sistema seguro?

- Como pode um CVE facilitar a realização de ataques?
- Que mecanismo reduz a sua utilização por atacantes?

Um CVE consiste num dicionário público de vulnerabilidades e exposições de segurança para gestão de vulnerabilidades e detecção de intrusões.

É um método que fornece uma linguagem comum para referir os problemas e facilita a partilha de dados entre investigadores e base de dados vulneráveis.

a. Uma vez que as vulnerabilidades se encontram acessíveis publicamente, um indivíduo é capaz de realizar um ataque a partir do estudo da vulnerabilidade. Uma vez que esta está sempre associada a um software ou a um sistema operativo, o atacante só precisa de um sistema "compatível" com as especificações declaradas no CVE.

b. Um mecanismo para a redução da utilização por atacantes é limitar o acesso a este tipo de dicionários, deixando apenas acesso a entidades competentes e validadas para tal.

4. Considerando o princípio de Kerckhoff:

- Descreva o seu impacto para aplicações de código livre utilizando cifras públicas.
- Descreva o seu impacto para aplicações com código conhecido e/ou utilizando cifras secretas.

5. Descreva com detalhe como uma cifra pode ser utilizada para calcular um Message Authentication Code.

Um MAC é um autenticador de mensagens onde é produzido um valor a partir da síntese de uma mensagem e de uma chave simétrica partilhada entre o emissor e pelo receptor da mesma.

O MAC só pode ser gerado e validado por estas duas entidades, o que não acontece nas assinaturas digitais, uma vez que, qualquer um que detenha a chave pública do par de chaves pode verificar a autenticidade da mensagem.

O MAC apenas garante que a mensagem é íntegra para os participantes envolvidos.

6. Considerando os modos de cifra CBC e CTR, qual o resultado após a decifra, se na transmissão se corromper 1 bit no criptograma ou do vetor de inicialização?

A propagação de erros no modo CBC ocorre quando um erro no criptograma afeta o bloco de texto liso correspondente e um bit no bloco seguinte. Erros de perda de bits são irreversíveis.

No modo CTR não há propagação de erros entre blocos, um erro afeta apenas um bloco de texto liso. Erros de perda de bits são irreversíveis.

7. Descreva a razão pela qual o cartão português contém 7 certificados de chave pública e qual a função de cada certificado presente?

7 certificados de chave pública

→ 2 relativos às chaves do próprio

→ 5 para indicar a cadeia de certificação

8. Compare os requisitos de confinamento associados ao armazenamento de chaves simétricas e assimétricas e o impacto da descoberta de cada uma das chaves.

As cifras simétricas são chaves partilhadas por dois ou mais interlocutores, onde é permitida a confidencialidade para todos os conhecedores da chave e autenticação de mensagens e onde os detentores da chave secreta podem decifrar a informação cifrada com a mesma. Porém, se a chave for partilhada em rede, não há como privar alguém de ler, escrever ou até mesmo passar-se pelo autor, o que não valida a autenticidade.

As cifras assimétricas usam um par de chaves distintas - uma pública para cifrar e uma privada (pessoal e imtransmissível) para decifrar. A componente privada só deve ser conhecida e usada pela entidade a que está associada; a componente pública pode e deve ser publicamente divulgada para ser usada por qualquer entidade.

O uso da chave privada do par de chaves permitirá simular o autor em causa.

Ambas as chaves (tanto as simétricas como a privada das assimétricas) devem ser guardadas num local de confinamento e não devem ser guardados em claro (devem ser cifrados).

Em relação ao impacto:

- **Cifras Simétricas** - se for descoberta uma chave para as comunicações desse tipo é fica comprometido (uma vez que a comunicação é feita 2x2). E, devido a isso, tem de se gerar um novo par e passar ao cliente em causa.

- **Cifras Assimétricas** - a pública não há problema algum porque o objetivo é mesmo ser partilhada. Mas se a privada for descoberta, a comunicação com todos os N interlocutores é comprometida (porque é de 1:N). Assim, tem de ser gerado um novo par de chaves, onde todos os clientes têm de ser avisados e todos os serviços têm de mudar a chave e a distribuição é complexa.

9. No âmbito de um PKI, explique em que consiste e qual a utilidade de uma cadeia de certificações e como esta é utilizada para o acesso seguro a serviços de internet.

A PKI é uma infraestrutura (hardware, software, pessoas, políticas) cujo objetivo é fazer um bom uso de chaves assimétricas e certificados de chave pública.

Para esse bom uso é necessário:

- Criação de um par de chaves assimétricas para cada entidade envolvida (definição de políticas de geração e troca de chave)
- Criação e distribuição de certificados de chave pública (definição dos atributos do certificado e políticas envolvidas)
- Definição e uso de cadeias de certificação (hierarquia de certificações, certificados de outros CAs)
- Atualizações, publicações e consulta de CRLs (políticas para anular certificados)
- Uso de estruturas de informação e protocolos que permitem a cooperação entre componentes, serviços e pessoas.

→ Uma PKI define relações de confiança de duas formas diferentes: emitindo certificados para chaves públicas de outras CAs que estejam abaixo de si na hierarquia ou não relacionados entre si na hierarquia, requerendo o certificado de chave pública da sua root, caso esteja acima na hierarquia, ou não relacionados entre si na hierarquia.

10. Porque uma entidade certificadora expõe informação semelhante via CRL, delta-CRL e OCSP?

a. Refira o propósito de cada método.

O CRL é uma lista de certificados revogados. Tal define uma lista disponibilizada publicamente por uma PKI X.509 v3 com todos os certificados que foram revogados e cujo prazo de validade ainda não expirou e onde cada entrada da lista é apresentada informação relevante do mesmo, como a razão para a sua revogação e data.

A informação pode então ser apresentada a partir do CRL, como a partir de delta-CRL, onde só irá constar informações de entrada e saída de um CRL de referência.

- A principal desvantagem do CRL é que pode criar uma grande sobre carga enquanto o cliente pesquisa sobre a lista de revogações.

Por último, a informação ainda pode ser consultada por OCSP, ou seja, um protocolo simples de pergunta e resposta onde é questionado o certificado o consultor através do seu número de série.

- A principal vantagem é o cliente poder consultar o estado de um único certificado, em vez de ter de descorregar e analisar uma lista inteira (maior sobre carga para o cliente e rede).

- A principal desvantagem é que os pedidos são enviados para cada certificado, devido a isso pode haver uma sobre carga sobre o OCSP Responder (CA) para sites de alto tráfego.

11. no contexto da tentativa de descoberta de uma chave WEP, descreva o processo de reinjeção de tramas e o que motiva esse processo.

A cifra de dados da trama é feita através de RC4, chave de 40 bits ou 104 bits.

Existe um problema crítico de segurança, foi descoberta uma vulnerabilidade no RC4.

É um algoritmo não público mas bem conhecido e foram descobertas chaves fracas, onde alguns bits da keystream refletem bits da chave.

Isto causou impacto no WEP, pois os atacantes escutam as tramas com IV apropriado para uma chave fraca, onde os atacantes podem acelerar o processo enviando tramas adicionais.

As tramas são recolhidas, permitindo-se encontrar a chave secreta e o tempo do ataque cresce de forma linear com o tamanho da chave.

Em suma, quanto mais tramas os atacantes apurarem, mais depressa descobrem a chave.

12. Considerando a autenticação direta com senha partilhada e a autenticação por desafio-resposta, ambos com segredos escolhidos pelos utilizadores:

a. Descreva com detalhe e compare os métodos.

b. Como pode um atacante no canal de comunicação descobrir o segredo partilhado?

c. Na autenticação direta com senha partilhada, os utilizadores enviam os dados e este verifica a sua veracidade.

No caso da autenticação por desafio-resposta, o sistema (autenticador) envia um desafio ao utilizador, este crie a sua resposta em função do desafio e das suas credenciais e envia o resultado. O autenticador verifica o resultado, produzindo um resultado próprio usando a mesma aproximação e verifica a igualdade, ou seja, produz um valor a partir do resultado e verifica se iguala o desafio ou algum relacionado.

A autenticação por desafio-resposta deve ser usada sempre que o meio de transmissão possa ser escutado, porque este método é mais complexo. Quando o meio de transmissão é relativamente seguro, a aproximação direta de credenciais pode ser usada.

A autenticação por desafio-resposta é a mais segura pois não há passagem de credenciais em plaintext (como na autenticação direta), apenas há a passagem de um desafio e de uma resposta que se forem interceptados pelo atacante não fazem sentido.

b. Visto que é um segredo partilhado entre todos os utilizadores do canal é normal que se um atacante escutar o canal de transmissão pode guardar a chave.

Outro exemplo: Caso um valor de desafio-resposta seja repetido um indivíduo mal intencionado que monitora o canais de transmissão pode guardar todos os pares (desafio, resposta) e tentar autenticar-se até lhe ser pedido um desafio cuja resposta já conheça.

13. No contexto de chaves ^{de} utilização única (OTP)

a. Explique o conceito, vantagens e desvantagens.

b. Descreva a sua utilização com equipamentos SecurID.

a. As chaves de utilização única, também conhecidas como chaves descartáveis (one-time-password) são senhas que só se podem usar uma vez, as credenciais nunca se repetem.

A vantagem da sua utilização é que podem ser escutadas, pois isso não adianta a quem a fizer para personalizar o dano uma vez que todo é descartável.

As suas desvantagens são que as entidades interactantes precisam de saber que senhas devem usar em diferentes ocasiões (necessário algum sistema de sincronização) e, as pessoas podem precisar de recursos extras para manter ou gerar as senhas descartáveis - como é o caso do cartão de matrizes do banco ou equipamentos SecurID.

b. O SecurID é um equipamento que gera chaves descartáveis (OTP) normalmente em intervalos de tempo de um em minuto. É um sistema de autenticação com senhas descartáveis que usa chaves secretas, partilhadas entre autenticado e autenticador. É gerado uma OTP associada a uma pessoa (UserID) com o número apresentado no aparelho, hora, etc. No RSA ACE server faz o mesmo, dado o UserID verifica a igualdade.

Este sistema é robusto contra ataques de dicionário, uma vez que o utilizar não escolhe as chaves.

14. Descreva o funcionamento de modo AES-CCMP e qual o seu propósito no contexto de redes de comunicações sem fios (IEEE 802.11i)

O seu propósito é proteger as transmissões com mecanismos mais avançados.

O CCMP é o protocolo mais usado pelo WPA pela encriptação das mensagens transmitidas. Ele é totalmente independente do funcionamento WEP, diferentemente do WPA, pelo facto de não usar o algoritmo RC4. Ao invés disto, a mensagem é codificada antes de ser transmitida com o uso do AES. Porém, o conceito de chaves temporárias e código de integridade de mensagens introduzido pelo WPA continuou a ser usado, só que funcionando de maneira diferente. Além disto, a parte de autenticação é bem semelhante à do último e, portanto, será omitida.

15. No contexto da associação a uma rede sem fios IEEE 802.11:

- Quais as fases que compõem a norma IEEE 802.11x
- Qual o propósito de cada fase
- Quais os elementos participantes em cada fase e que informações estão associadas

As operações realizadas no âmbito do 802.11x em redes sem fios divide-se em 3 etapas:

- ① Descoberta e Associação (mensagens 802.11)
- ② Autenticação (mensagens EAP)
- ③ Acordo em 4 passos "4 Way Handshake"

① Nesta etapa, o station liga-se à rede sem fios. Consequentemente, é efetuado o processo normal das redes 802.11 de descoberta de rede, autenticação do STA e de associação entre o STA e AP.

No final desta fase, o STA deverá estar autenticado e associado junto de um AP que irá supervisionar ou controlar as etapas seguintes. No final desta etapa o porto controlado está no estado não autorizado.

② Nesta etapa, é realizada a autenticação mútua e uma distribuição das chaves de sessão entre o STA e o servidor de autenticação. Nesta etapa, o porto controlado continua no estado não autorizado.

③ Nesta etapa, é realizada uma autenticação mútua e uma distribuição de chaves entre o STA e o autenticador.

A autenticação é fundamental para o STA garantir que está a interagir com um autenticador (AP) que pertence ao mesmo domínio de segurança do servidor de autenticação, isto é, um impostor.

No final desta etapa o porto controlado já se encontra em estado "autorizado". Nesta etapa é também efetuada uma validação dos valores RSN IE trocados entre o STA e o autenticador quando a associação do cliente à rede.

Os elementos participantes são:

- Etapa 1: Descoberto e Associação → STA e AP
- Etapa 2: Autenticação → STA, AP e servidores de autenticação
- Etapa 3: Acordo em 4 passos → STA e AP

16. Explique como funciona uma firewall do tipo Stateful Packet filter.

Uma firewall de filtro de pacotes é dito um firewall seu estado, isso porque ele trata cada um dos pacotes que atravessam a interface de forma independente.

Ou seja, é realizado um stateful Packet Inspection que analisa completamente incluindo o seu contexto, determinando e caracterizando a aplicação em causa e aplicando regras de filtragem/limitação.

Esse filtro é feito através da base nos IPs.

17. Distinga controlo de acesso mandatório (ou obrigatório) de controlo de acesso discricionário e forneça alguns exemplos da existência de ambos os modelos no contexto de um sistema operativo.

As técnicas de controlo de acesso são normalmente em discricionários e obrigatórios.

No controlo de acesso obrigatório, a política é determinada pelo sistema e não pelo proprietário do recurso. Este controlo é utilizado em sistemas onde os dados são altamente sensíveis, como sistemas governamentais e militares.

O controlo de acesso discricionário é uma política de controlo de acesso determinada pelo proprietário (owner) do recurso (um ficheiro, por exemplo). O proprietário do recurso decide quem tem permissões de acesso em determinado recurso e qual o privilégio ele tem.

18. Descreva os mecanismos de elevação de privilégios existentes nos sistemas Linux e controlados através das permissões de um ficheiro.

a. Qual a utilidade desse mecanismo?

b. Quais os riscos deste mecanismo?

Esta funcionalidade serve para fazer uma alteração do UID do processo que executa um determinado programa. Se um programa possui o UID X e o bit set-UID ativo na sua ACL então ele será executado num processo com o UID X independentemente do UID de quem o mandar executar.

No prática, estas funcionalidades servem para disponibilizar acesso a operações privilegiadas a utentes em que não se confia, diariamente.

Este mecanismo é perigoso porque desta maneira pode-se atribuir permissões para realizar operações perigosas a uma aplicação maliciosa.

Trabalhar em modo super-utizador (root nos sistemas Linux) obtémos omnipotência sobre o sistema o que não é aconselhável para pessoas sem formação técnica, uma vez que a introdução errada, propositalmente ou não, pode conduzir a um fim não desejado.

16. Explique como funciona uma firewall do tipo stateful packet filter.

Uma firewall de filtro de pacotes é dito um firewall seu estado, isso porque ele trata cada um dos pacotes que atravessam a interface de forma independente.

Ou seja, é realizado um stateful Packet Inspection que analisa completamente incluindo o seu contexto, determinando e caracterizando a aplicação em causa e aplicam regras de filtragem/limitação.

Esse filtro é feita através com base nos IPs.

17. Distinga controlo de acesso mandatório (ou obrigatório) de controlo de acesso discricionário e forneça alguns exemplos da existência de ambos os modelos no contexto de um sistema operativo.

As técnicas de controlo de acesso são normalmente em discricionários e obrigatórios.

No controlo de acesso obrigatório, a política é determinada pelo sistema e não pelo proprietário do recurso. Este controlo é utilizado em sistemas onde os dados são altamente sensíveis, como sistemas governamentais e militares.

O controlo de acesso discricionário é uma política de controlo de acesso determinada pelo proprietário (owner) do recurso (um ficheiro, por exemplo). O proprietário do recurso decide quem tem permissão de acesso em determinado recurso e qual o privilégio ele tem.

18. Descreva os mecanismos de elevação de privilégios existentes nos sistemas Linux e controlado através das permissões de um ficheiro.

a. Qual a utilidade desse mecanismo?

b. Quais os riscos deste mecanismo?

Esta funcionalidade serve para fazer uma alteração do UID do processo que executa um determinado programa. Se um programa possuir o UID X e o bit set-UID ativo na sua ACL então ele será executado num processo com o UID X independentemente do UID de quem o mandar executar.

Na prática, estas funcionalidades servem para disponibilizar acesso a operações privilegiadas o utentes em que não se confia, diariamente.

Este mecanismo é perigoso porque desta maneira pode-se atribuir permissões para realizar operações perigosas a uma aplicação maliciosa.

Trabalhar em modo super-utizador (root em sistemas Linux) obtémos omnipotência sobre o sistema o que não é aconselhável para pessoas sem formação técnica, uma vez que a introdução errada, propositalmente ou não, pode conduzir a um fim não desejado.

19. Descreva os tipos de cópias de ficheiros (backups) vulgarmente realizados e as medidas que permitem reduzir as necessidades de armazenamento das cópias efetuadas.

Backup Completo ou Normal - É realizada a cópia de todos os ficheiros que estão no disco. É efectuada para o primeiro backup uma cópia total e nas posteriores as opções diferenciais ou incrementais.

- Vantagens:
- Fácil de localizar ficheiros (pois estão sempre no último backup realizado)
 - Recuperação mais simples (recupera apenas o conteúdo do último backup)

Desvantagens:

- Elevado tempo de recuperação e elevado espaço na local de destino da cópia, uma vez que copia sempre todos os arquivos, com isso ocorre muito desperdício de armazenamento pois faz backup de arquivos que não foram alterados após o último backup realizado.

Backup Diferencial - Apenas são copiados os arquivos que foram alterados/ adicionados após o último backup completo ou incremental.

- Vantagens:
- A recuperação é mais fácil, pois exige apenas o último backup completo e o último diferencial que foram atualizados

Desvantagens:

- Os backups diferenciais são mais lentos e maiores que os de tipo incremental.

Backup Incremental - Copia somente os ficheiros criados ou alterados desde o último backup completo ou incremental.

Vantagens:

- Requer menor quantidade de armazenamento para os dados (eficiência de espaço)

Desvantagens:

- Recuperação muito mais lenta (pode levar mais tempo do que se for usado o backup completo ou diferencial)

Os métodos que permitem reduzir as necessidades das cópias são a compressão por algoritmos sem perdas (zip), cópias seletivas de informações (apenas os ficheiros que foram alterados) e deduplicação.

20. Considere que se pretende criar um sistema de armazenamento composto por 10 discos de 1TB cada, com a capacidade de suportar a falha de um qualquer disco.

a. Descreva como se pode construir este sistema e quais as características operacionais final (desenvolvimento, espaço disponível, falhas suportadas).

b. Como é possível suportar a falha simultânea de dois discos, ou mesmo de quase todos os discos, e que desvantagens têm de ser considerados para cada um dos casos?

No RAID 5, a redundância é considerada de maneira diferente: em vez de existir uma unidade de armazenamento inteiro como réplica, os próprios discos servem de proteção.

Deste modo, pode-se inclusive montar um sistema com um número maior de unidades. Neste método de proteção, os dados estão divididos em pequenos blocos - cada um deles recebe um bit adicional, o bit de paridade.

- se a quantidade de bits '1' do bloco for par, seu bit de paridade é 0
- se a quantidade de bits '1' do bloco é ímpar, seu bit de paridade é 1

As informações de paridade, assim como os próprios dados são distribuídos entre todos os discos do sistema.

Para o caso de ter de suportar a falha simultânea de dois discos o ideal é o RAID 6.

O RAID 5 é uma operação bastante interessante para sistemas que precisam aliar redundância com custos relativamente baixos, mas tem uma limitação considerável - consegue proteger o sistema se apenas um disco apresentar falha.

Outra alternativa é o uso do RAID 6, tratando-se de uma especificação mais recente e parecida com o RAID 5, mas oferece uma importante diferença - trabalha com dois bits de paridade - com isto é possível oferecer redundância para dois HDs no sistema em vez de apenas um.

Para o caso de ter de suportar a falha de quase todos os discos, o ideal é o uso do RAID 1. O RAID 1 é, provavelmente, o modelo mais conhecido. Nele, uma unidade duplica a outra, isto é, faz uma cópia do primeiro. Com isto, se o disco principal falhar, os dados podem ser recuperados imediatamente porque existe uma cópia integral num outro disco.