Resumo Geral Segurança Informática e nas Organizações Defesa contra catástrofes físicas Conseguir que um sistema computacional, ou o serviço que esse sistema presta, consiga sobreviver a catástrofes onde existam consequências a nível físico.

Catástrofes ambientais

Tremores de terra, incêndios, inundações, quedas de raios, tempestades magnéticas

Catástrofes políticas Ataques terroristas, motins

Catástrofes materiais

Degradação irreparável ou perda ou roubo de equipamentos computacionais, como: discos magnéticos, computadores portáteis Todas estas catástrofes são potenciais causas de dano físico irreparável de equipamentos informáticos e potenciais causas de perda irreparável de informação armazenada. Para que a sobrevivência dos dados seja assegurada, pode-se usar hardware com redundância ou equipamentos redundantes com informação replicada.

Solução

Realização periódica de cópias de dados (backup) Prevenção realista: para catástrofes mais prováveis Replicação da informação e dos recursos computacionais

Defesa contra falhas previsíveis A defesa contra falhas previsíveis visa sobretudo minimizar o impacto de problemas que ocorrem com uma frequência maior.

Falha Solução

Quebra no fornecimento de energia elétrica Sistemas de alimentação alternativo (baterias,

geradores)

Bloqueio na execução de aplicações ou

Sistemas transacionais sistemas operativos (blue-screen)

Falhas temporárias de conectividade em troços de rede (falhas de comunicação)

Defesa contra atividades não autorizadas Defesa de sistemas computacionais face a iniciativas tomadas por indivíduos contra o funcionamento normal destes. As atividades não autorizadas podem ter origem em sujeitos que pertencem à organização (mais difícil de detetar, uma vez que possuem habitualmente privilégios acrescidos) ou que não pertençam a ela.

Atividades Ilícitas

Acesso a informação Alteração da informação Utilização de recursos (CPU, memória, impressora) Alteração de permissões Vandalismo - Interferência com o normal funcionamento do sistema

Encaminhamento alternativo, garantindo que mais tarde a informação consiga chegar ao destino pretendido

Vulnerabilidades, Ataques, Riscos e Defesas Defesa de sistemas computacionais face a iniciativas tomada

• Vulnerabilidade: É uma característica de um sistema que o torna sensível a certos ataques. Fontes de Vulnerabilidades: - Aplicação com bugs; - Utilizadores descuidados ou desconhecidos - Má administração - Comunicação sobre redes não controladas

• Ataque: Conjunto de passos executados no âmbito da exploração de vulnerabilidades e que permite concretizar uma ação ilícita.

• Risco: É um dano que pode resultar da execução bem sucedida de um ataque

•Defesa: Conjunto de políticas e mecanismos desenhados, concretizados e implementados para:

- Diminuir as vulnerabilidade de um sistema - Detetar e contrariar/anular ataques passados/atuais - Minimizar os riscos de ataques bem sucedidos

Políticas

• Políticas de Segurança: Definem o princípio do privilégio mínimo, procedimentos de segurança e os requisitos de segurança de um domínio que devem ser respeitados.

• Princípio do privilégio mínimo: Este principio 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: Domínios de segurança: Definição do conjunto de máquina e redes de domínio, definição do universo de utentes válidos, definição do universo de atividades lícitas

Mecanismos As políticas de segurança são colocadas em prática recorrendo a mecanismos de segurança. Os mecanismos de segurança são a forma prática como as políticas são aplicadas em cenários concretos. Ex: Confinamento, Autenticação, Controlo de Acesso, Execução Privilegiada, Filtragem

Desencorajamento Ilusão

• Punição

- Restrições legais - Evidências forenses

• Barreiras de Segurança

- Firewalls, autenticação, comunicação segura, sandboxing

• Honeypots / Honeynets - simular falhas de sistemas e colher informações sobre invasores (não oferece nenhum tipo de proteção)

• Acompanhamento forense

Prevenção Deteção

• Políticas restritivas (ex: princípio do privilégio mínimo)

• Pesquisa de vulnerabilidades

• Eliminação de vulnerabilidades (ex: atualização regular)

• Sistemas de detenção de intrusões (ex: Snort)

• Auditorias

  • Análise forense de penetrações

Recuperação

• Backups

• Sistemas redundantes

• Recuperação forense

-

O desencorajamento, a ilusão e a deteção servem sobretudo para lidar com problemas conhecidos (tentativas de reconhecimento; ataques genéricos; ataques específicos) -

As medidas de prevenção protegem de vulnerabilidades conhecidas ou desconhecidas

Ataques do Dia Zero Este tipo de ataques são chamados de “zero-day attacks” uma vez que o autor da aplicação tem zero dias para planear qualquer forma de evitar esse ataque (como por exemplo: aconselhamento de soluções). Ou seja, quando este ataque é tornado público não existem quaisquer soluções conhecidas para por fim a este, possibilitando assim o acesso a dados e a informações confidenciais da aplicação. Este ataque explora assim vulnerabilidades que são desconhecida das vítimas, dos seus fabricantes e dos organismos que apoiam a defesa contra ataques. Existem muitas técnicas para limitar a eficácia das vulnerabilidades de corrupção de memória de dia zero, tais como buffer overflows.

CVE - Common Vulnerabilities and Exposures Dicionário público de vulnerabilidades e exposições de segurança para gestão de vulnerabilidades, gestão de correções e deteção de intrusões.

Vulnerabilidade Exposição

é um estado de um sistema computacional que: - permite que uma atacante execute comandos em nomes de terceiros - permite que um atacante se apresente como outrem.

CWE - Common Weakness Enumeration Linguagem comum para discutir, encontrar e lidar com as causas das vulnerabilidades de segurança. Os CWE são catalogados segundo uma estrutura hierárquica

SQL Injection É uma ameaça de segurança que se aproveita de falhas em sistemas que interagem com a base de dados via SQL. Formas de eliminar vulnerabilidades: desencorajamento, prevenção, ilusão, deteção e recuperação. - Parametrização de consultas - Usar “stored-procedures” - Limitar privilégios de acesso

Criptografia: Arte ou ciência de escrever de forma escondida. O objetivo da criptografia é permitir que um conjunto limitado de entidades, tipicamente duas, possam trocar informação - garantir a privacidade da informação. Criptanálise: Arte ou ciência de violar sistemas criptográficos ou informação criptográfica. Criptologia: Ramo que se dedica ao estudo da criptografia e da criptanálise.

é um estado de um sistema computacional que: - permite que um atacante realize recolhas de informação - permite a um atacante esconder as suas atividades

Benefícios

Fornece uma linguagem comum para referir problemas Facilita a partilha de dados entre investigadores e base de dados de vulnerabilidades

Operação de uma cifra

Cifra: texto em claro -> criptograma Decifra: criptograma -> texto em claro Algoritmo: modo de transformação de dados Chave: parâmetro do algoritmo

Tipos de Cifra

• Cifra de transposição - Opera baralhando caracteres do texto original.

• Cifra de substituição - Opera substituindo caracteres do alfabeto usado no texto original por caracteres de um alfabeto de substituição.

1) Cifras Monoalfabéticas - Usam apenas um alfabeto de substituição. Um caracter do alfabeto original é sempre substituído pelo mesmo caracter do alfabeto de substituição numa operação de cifra.

Problema: Possibilidade de reprodução de padrões estatísticos dos caracteres usados no texto original. Ou seja, se num texto 23% dos caracteres forem um A, então no criptograma 23% dos caracteres serão o substituto de A obtido através do alfabeto de substituição. Da mesma forma, podem-se detetar construções características da linguagem, como diagramas (consoantes dobradas RR e SS em português). ➡ A análise estatística facilita a criptanálise. Solução: Usar línguas pouco divulgadas, como fizeram os americanos na Segunda Guerra Mundial.

2) Cifras Polialfabéticas - Aplicação cíclica de várias cifras monoalfabéticas. Um caracter do alfabeto original pode ser substituído por diferentes caracteres dos alfabetos de substituição numa operação de cifra/decifra.

Problema: As cifras polialfabéticas podem ser criptanalisadas tal como as monoalfabéticas se souber-se o seu período N. O número de cifras monoalfabéticas define o período da cifra polialfabética.

Exemplo:

Cifra de Vigenère: Consiste na aplicação de N cifras monoalfabéticas. Teste de Kasiski: Consiste em medir as distâncias entre blocos idênticos do criptograma. Assim, o maior divisor comum de todas as distâncias indica o período da cifra polialfabética. Índice de Coincidência: Consiste em avaliar a percentagem de letras iguais em criptogramas idênticos sobrepostos com um deslocamento progressivo.

Criptografia: Aproximação Teórica vs. Aproximação Prática

Aproximação Teórica Aproximação Prática

Cifra Perfeita: A cifra é perfeita quando o criptanalista que capturar o criptograma não conseguir de modo algum concluir qual o texto original correspondente, porque para cada texto candidato existe sempre uma chave pode ter efetuado a transformação.

Classificação das Cifras

• *Modo de Operação*

- Cifra por blocos - São cifras monoalfabéticas onde cada caracter do alfabeto original e do resultante é formado por conjuntos de imensos bits (64, 128, 256). - Cifra contínuas - São cifras polialfabéticas constituído por um gerador pseudo- aleatório. O texto a cifrar deverá ser inferior ao período da chave contínua.

• *Tipo de Chave*

- Cifras simétricas (segredo partilhado) - Chave secreta partilhada por 2 ou mais interlocutores. Permite a confidencialidade para todos os conhecedores da chave e autenticação de mensagens (cifra por blocos). Apenas os detentores de uma chave secreta podem decifrar a informação cifrada com a mesma.

Vantagens: Normalmente muito eficiente Desvantagens: Num universo de N interlocutores, se pretender-se ter uma chave secreta partilhada por cada interlocutor são necessárias ((NxN(N-1))/2). Problemas: Distribuição segura ou chaves secretas.

- Cifras assimétricas (par de chaves) - Usam um par de chaves distintas - uma pública para cifrar e uma privada (pessoal e intransmissível) para decifrar. Não é possível dada uma chave pública, calcular a correspondente chave privada. 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 poder ser usada por qualquer entidade.

Vantagens: N interlocutores, N pares de chaves Desvantagens: Pouco eficiente - operações matemáticas complexas Problemas:

- Confinamento rigoroso das chaves privadas aos legítimos detentores - Distribuição fidedigna de chaves públicas a todos os que as pretendes usar - Gestão de tempo dos pares de chaves

A cifra diz-se segura na prática se cumprir o objetivo para que é usada.

Critérios de avaliação da qualidade Shannon: - Quantidade de secretismo oferecido - Complexidade das chaves - Simplicidade de realização - Propagação de erros - Dimensão do criptograma

Confusão: Complexidade na relação entre o texto em claro, a chave e o criptograma. Esta deve ser o mais complexa possível para dificultar a descoberta de partes do texto e/ou chaves. Difusão: Alteração no texto original leva a grandes alterações no criptograma.

Cifras Modernas

• Cifras simétricas por blocos Usam princípios básicos de difusão e confusão. Tal é feito recorrendo às seguintes operações:

- Aplicação iterativa de uma operação complexa a um bloco de grande dimensão (>64bits) - Operações elementares de perturbações

- Substituição, expansão e compressão de blocos

- DES - Cifra simétrica por blocos que usa blocos de 64 bits e chaves de 56 bits. Segue os princípios da confusão e difusão usando unidades elementares de permutações, substituição, expansão e compressão de blocos. O DES só pode ser atacado usando pesquisa exaustiva, o que hoje em dia é viável

- AES - Utiliza operações algébricas de forma inteligente: a segurança é conseguida através de operações complexas. O seu funcionamento baseia-se no processamento de um estado 4*4 bytes. Blocos variáveis com chaves de 128, 192 ou 256 bits.

• Cifras simétricas contínuas Aproximações realistas à cifra de Vernan (a chave tem de ter comprimento maior ou igual à mensagem a cifrar). A maioria das cifras contínuas são síncronas, ou seja, a operação do seu gerador é independente dos dados cifrados e decifrados, o que obriga os dois extremos da comunicação, o que cifra e o que decifra, a gerirem o sincronismo.

- A5 - Algoritmo de cifra usado em comunicações GSM e usa internamente três LFSR. O A5 permite usar diretamente chaves até 64 bits, o número de bits que se pode introduzir como estado inicial dos três LFSR, e produz chaves contínuas com comprimento máximo de 2^64 bits.

• Cifras assimétricas por blocos Não usam os princípios de difusão e de confusão. Usam, problemas matemáticos complexos. Até agora foram usados fundamentalmente três tipos de problemas:

- fatorização, cálculo de logaritmos discretos, knapsacks

- RSA - Baseia a sua segurança na complexidade de fatorização e cálculo de logaritmos modulares.

Cifra: C = Pe mod n Decifra: P = Cd mod n Para decifrar um valor cifrado com chave pública e, é preciso conhecer a chave privada d. O RSA pode igualmente ser usado como algoritmo de assinatura

- ElGamal - Baseia a sua segurança na complexidade no cálculo de logaritmos modulares. É mais lento nas operações de cifra relativamente ao RSA.

Confidencialidade Autenticidade

Ciframos com a chave pública de X e deciframos com a privada de X. Aqui a mensagem fica codificada e ninguém pode ter acesso ao conteúdo.

Aplicações das Cifras por Blocos: Modos de Cifra

• ECB - método mais simples e intuitivo de usar uma cifra por bloco Consiste em dividir o texto a cifrar em blocos independentes e contíguos de igual dimensão, que são cifrados independentemente.

Fraquezas: Reprodução de padrões do texto original Solução: Uso de blocos de maior dimensão ou outro modo de cifrar CBC

• CBC Operação semelhante ao ECB. Na cifra de cada bloco é introduzida realimentação. O texto em claro a cifrar é previamente somando ao módulo 2 com o bloco anterior do criptograma. Na decifra, cada bloco decifrado é somado com o bloco anterior do criptograma para recuperar o bloco de texto original.

Problema: Facto de permitir alguma alteração determinista do texto original recuperado após a decifra. Solução: Uso de blocos de maior dimensão ou outro modo de cifrar CBC

• OFB e CFB Transformam uma cifra por blocos numa cifra continua. Modo de Funcionamento: O gerador de cifra contínua é constituído por uma função de cifra por blocos, por 2 registos com comprimento do bloco, ri e ro, e por uma função de realimentação. A função cifra com o conteúdo de ri e guarda o resultado em ro. Desse resultado, os n bits mais significativos são usados para cifrar os dados. Diferenças: No OFB a realimentação é feita a partir do gerador.

No CBC a realimentação é feita a partir do criptograma.

• CTR A cifra do i-ésimo bloco Pi é feita somando-o, bit a bit e módulo 2, com o resultado da cifra de VI + i com a chave K, onde VI é o valor inicial de um contador. A decifra faz-se somando novamente o mesmo valor.

Reforço de Segurança

Cifra Dupla Cifra Tripla Branqueamento

A cifra múltipla consiste em cifrar um texto mais do que uma vez, usando em cada cifra uma chave diferente. A segurança será, à partida, tanto maior quanto maior for o número de cifras independentes aplicadas, mas também o desempenho será menor.

A cifra tripla usa três operações de cifra ou decifra e uma a três chaves distintas. É atrativo uma vez que permite compatibilizar cifras simples com cifras triplas usando uma única chave, o que facilita a interação com aplicações ou equipamentos antigos.

Consiste em usar duas chaves extra, do comprimento do bloco usado pelo algoritmo de cifra, que se somam módulo 2 à entrada e à saída da cifra.

Ciframos com a chave privada e deciframos com a chave pública, o que não tem qualquer interesse para esconder a informação, mas é importante para garantir a autoria.

Funções de Síntese As funções de síntese não são propriamente funções criptográficas, uma vez que não servem para cifrar ou decifrar dados, mas são úteis para complementar, com segurança criptográfica, outros mecanismos de segurança. São úteis para gerar e validar assinaturas digitais. As funções de síntese produzem valores de dimensão constante a partir de textos de dimensão variável.

Características: -Não é possível reverter o processo de síntese e descobrir o texto original -Não permite que se descubra um texto que gere a mesma síntese que outro -Não permite que se descubram quaisquer dois textos que gerem a mesma síntese. Sem estas três características não poderá ser classificada como função de síntese.

MAC - Autenticador de Mensagem Um autenticador de mensagem é um valor produzido a partir da síntese uma mensagem e de uma chave simétrica partilhada pelo emissor e pelo recetor da mesma. O MAC autentica uma mensagem por forma a garantir a integridade (alteração da informação) e autenticação (validar o emissor). Um MAC apenas pode ser gerado e validado por duas entidades.

• HMAC É semelhante ao Keyed-MD5, mas mais robusto e versátil porque pode ser usado como diversas funções de síntese. Gera um MAC aplicando a função de síntese 2 vezes, uma dita interior (inner) onde são processados a chave e a mensagem e outro exterior (outer) onde se processam a chave e a síntese interior.

HMAC = h [k⊕opad | h (k⊕ipad | mensagem)]

Assinaturas Digitais A assinatura digital de um documento consiste em autenticar o conteúdo do documento, e autenticar o seu assinante. Para este fim, a criptografia assimétrica é a que melhor se adequa a este fim, uma vez que os pares de chaves têm um cariz pessoal. A assinatura digital de um documento consiste na cifra do mesmo com a chave privada do autor. O criptograma resultante não serve para esconder o documento original mas sim para garantir, a quem o decifrar com a chave pública correspondente, que o texto recuperado, esteja igual ao original, está correto e foi assinado pelo detentor da chave pública. Uma mensagem assinada digitalmente deverá ser associável a uma e uma só entidade.

Gestão de Chaves Assimétricas As chaves devem ser geradas pelos próprios, guardadas por eles em suporte de armazenamento seguro e usadas por si em ambientes seguros onde seja improvável a divulgação para terceiros.

• Distribuição de Chaves Públicas - Manual - Usando um segredo partilhado - Distribuição ad-hoc

Certificados Digitais de Chaves Públicas A certificação digital consiste na emissão de certificados digitais de chaves públicas. Os certificados são documentos com uma estrutura predefinida que possuem, entre outros elementos, uma chave pública de uma dada entidade e uma assinatura digital do certificado feita pela entidade emissora do mesmo. Os certificados são documentos com um tempo de validade limitado (através do prazo indicado no próprio certificado ou através de certificados de revogação).

CRL - Lista de Certificados Revogados Criado para facilitar a renovação de pares de chaves assimétricos. É uma lista disponibilizada publicamente por uma PKI X.509v3 com todos os certificados que foram revogados e cujo prazo de validade ainda não expirou. Esta lista contém para cada certificado revogado, uma entrada que possui informação relevante sobre o mesmo, a razão para a sua revogação e a data da mesma. Distribuição integral: Uma CRL mais recente anula completamente uma CRL mais antiga Distribuição parcial: São fornecidas CRL parciais, denominadas Delta CRL, criadas com base num CRL completo de referência. Delta CRL: Possuem apenas entradas relativas a certificados que entraram ou sairam da CRL de referência.

OCSP - Online Certificate Status Protocol OCSP é um protocolo de teste de revogação de um certificado. É um protocolo simples de pergunta-resposta, onde o OCSP Responder é questionado sobre a existência de um certificado de revogação para um determinado certificado, dado o seu número de série.

PKI - Public Key Infrastructure Infraestrutura (hardware, software, pessoas, políticas, planos) cujo objetivo é fazer um bom uso de chaves assimétricas e certificados de chaves públicas. Para esse bom uso é necessário: - Criação de um par de chaves assimétricas para cada entidade envolvida (definição de

políticas de criação 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 certificação, certificados de

outras CA’s); - Atualização, publicação e consulta de CRLs (políticas para anular certificados); - Uso de estruturas de informação e protocolos que permitam a cooperação entre

componentes, serviços e pessoas.

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

Cartão de Cidadão O cartão de cidadão é um smartcard, porque possui um microcomputador embebido (chip).

• Funcionalidades - Guardar informação pessoal - Guardar informação privada - Guardar informação reservada - Guardar informação pública de grande dimensão, não memorizável - Guardar informação observável no CC - Efetuar operações criptográficas usando chaves que fazem parte da sua informação privada

• Assinaturas Digitais com o Cartão de Cidadão O cartão de cidadão possui um par de chaves assimétricas de assinatura digital qualificada, para assinar documentos. O smartcard possui e disponibiliza um certificado X.509v3 com a chave pública de validação da assinatura digital qualificada do titular.

• Objetivos dos Certificados do Cartão de Cidadão - Possibilita autenticar o dono do cartão - Possibilita o dono autenticar outras pessoas com cartões semelhantes - Possibilita o cartão autenticar clientes com certificados semelhantes