**Ameaças à segurança**

**Motivação (3 - 46)**

- A segurança não é um estado, mas um processo de gestão do risco subjacente, onde engloba tecnologias, políticas e pessoas.

**Enquadramento histórico (47 - 59)**

- 1960: phone freaking (=phreaking). Clientes da AT&T começaram a explorar a comutação automática injetando vários tons para fazer chamadas interurbanas pelo preço de chamadas locais.

- Wardialing: Busca, com um modem, de números locais ligados cuja linha telefónica servia computadores. Depois aplicavam-se utilitários para quebra de passwords.

- Wardriving: Com um automóvel e um portátil ou PDA os utilizadores tentam detetar e comprometer redes wireless.

- 1984: Uma das primeiras ferramentas de defesa foi um IDS (intrusion detection system) – Permitem detecção rápida.

- 1988: DEC produz a primeira firewall stateless na forma de um filtro de pacotes IP

- 1989: A AT&T produz a primeira firewall stateful

- 1990s: As IDS começaram a ser substituídas por IPS (intrusion prevention systems/sensors) – Ao contrário dos IDS, os IPS são reativos.

**Ameaças externas vs Ameaças Internas:**

- As ameaças internas apenas começaram a ser mitigadas 20 anos depois de se dar atenção às ameaças externas

**Princípios Fundamentais da Segurança da Informação (60 - 69)**

**Objetivos típicos da segurança de informação:<**

- A segurança da informação manifesta-se de múltiplas formas, em função da situação e requisitos específicos da entidade ou entidades envolvidas na sua transação.

**Os três atributos fundamentais:**

- Confidencialidade

- Objetivo: Assegurar que o conteúdo da informação apenas está acessível às entidades autorizadas.

- Pode ser assegurado através de proteção física, algoritmos matemáticos

- Integridade

- Objetivo: assegurar que o conteúdo da informação apenas é alterado por entidades autorizadas.

- Para assegurar a integridade da informação são necessários mecanismos que possibilitem detetar a manipulação (adição, alteração, remoção) indevida de todo ou parte do conteúdo de forma intencional (fraude) ou acidental (negligência).

- Exemplos de violações de integridade:

- Alteração não solicitada da aparência de um web site

- Intercetar e modificar uma transação de e-commerce

- Alterar o conteúdo de uma ficha de informação num servidor

- Disponibilidade

- Objetivo: assegurar que os sistemas de informação e as respetivas infraestruturas permitem o acesso à informação na qualidade esperável quando este é solicitado.

- A disponibilidade é uma medida da acessibilidade da informação.

- Ex. Se um serviço fica off-line apenas 5 minutos por ano possui uma disponibilidade de 99.999 % (5 noves).

- Violações de disponibilidade

- O suporte digital da informação danifica-se (e.g., head crash)

- Uma ligação de acesso ao servidor fica saturada

- Um bug na codificação do servidor, estimulado natural ou maliciosamente, torna inacessível o serviço.

Modelo de segurança da informação:

- Atributos da segurança da informação (confidencialidade, integridade e disponibilidade)

- Estado da informação (Transmissão, processamento, armazenamento)

- Medidas de Segurança (Política e Procedimentos, tecnologia, educação e treinamento e conscientização)

- Suficiência dos três atributos fundamentais têm sido posta em causa diversas vezes.

- Autenticidade, titularidade e utilidade

- Accountability, Auditability, Authenticity/Trustworthiness, Non- repudiation, Privacy

**Instituições**

**Divulgação de alertas críticos:**

- A tecnologia RSS (Really Simple Syndication) é normalmente a preferencial para alojar feeds

- Capacidade de notificação activa (assíncrona)

- Capacidade de agregação local ou remota

**Gestão de Segurança da Informação**

**Normas publicadas:**

- Série ISO/IEC 27000 - Information Security Standards

- ISO/IEC 27002: Code of practice for information security management

- ISO/IEC 27033-1: Network security overview and concepts

- ISO/IEC 27032: Guideline for cybersecurity

- ISO/IEC 27037: Guidelines for identification, collection and/or acquisition and preservation of digital evidence

**Normas em preparação:**

- Organização

- Terminologia

- Requisitos Gerais

- Linhas de Orientação Gerais

**Domínios de gestão da segurança da informação:**

- A ISO/IEC 27002 organiza em 12 domínios os inúmeros aspetos relativos à segurança da informação

- Trata-se de um modelo de referência que nos ajuda a enquadrar qualquer discussão sobre a temática da Segurança

- Paralelo com o CISSP

**Risk Assessment (Avaliação do risco):**

- Primeira etapa do processo de gestão do risco

- Afere o valor quantitativo e qualitativo do risco relacionado com determinada situação específica ou ameaça identificada.

- Pressuposto: o risco pode ser miti gado, mas nunca evitado

- Estabelecesse um nível aceitável de risco para a organização

- Categorias dos bens

- Bens de Informação: pessoas, hardware, software, sistemas

- Bens de Suporte: infra-estruturas, serviços,

- Bens Críticos: qualquer um dos mencionados atrás

- Compilação dos atributos de cada bem identificado

- Determinação do valor relativo de cada bem

- Quanto retorno/lucro gera?

- Qual o custo de substituição associado?

- Quão difícil é a sua substituição?

- Quão rápido pode ser substituído?

- Ameaças

- Falhas de equipamentos, ataques estruturados, desastres naturais, vírus, e outros eventos causadores de danos

- Threat (Ameaça): perigo potencial levantado por uma vulnerabilidade.

- Threat agent (Atacante): entidade que explora a vulnerabilidade para atacar a vítima.

- Vulnerability (Vulnerabilidade): fragilidade de um sistema.

- Risk (Risco): potencial de sucesso do atacante e respetivo impacto no alvo.

- Exposure (Exposição): Volume potencial de dano causável pelo atacante.

- Countermeasure: Contramedidas adotadas para mitigar o risco potencial.

- Análise qualitativa do Risco

- Os valores da Exposição ao risco servem para priorizar a atenção dada a cada ameaça.

- Um novo worm -> probabilidade 7, severidade 7, exposição 49

- Sistema de armazenamento central avaria -> probabilidade 2, severidade 10, exposição 20

- Sistema de proteção contra incêndio inunda o datacenter -> probabilidade 1, severidade 10, exposição 10

- Análise quantitativa do Risco

- Aceitar – tomar consciência de que o risco existe mas aceitá-lo sem qualquer medida.

- Mitigar - Aplicar medidas de proteção que diminuam a exposição ao risco do bem em causa.

- Transferir - Entregar a terceiros a responsabilidade de gerir o risco.

- Evitar - Eliminar o bem do conjunto de bens da instituição ou eliminar a exposição ao risco do mesmo.

**Security Policy (Política de segurança):**

- Trata-se de um documento formal que clarifica como é que uma instituição planeia proteger os seus bens

- Define objectivos para a empresa, regras de comportamento para os utilizadores e requisitos para os sistemas, os quais coletivamente asseguram os níveis de segurança adequados.

- Exemplos:

- Todos os utilizadores devem possuir um par ID/password únicos em conformidade com a política de passwords local.

- A solução de antivírus da empresa para laptops deve efectuar atualizações diárias.

- Os maiores players (e.g. Cisco) possuem soluções ajustadas à implementação das políticas de segurança mais vulgares.

**Organization of Information Security (Organização da segurança de informação):**

- Procedimentos genéricos de base à segurança de informação que envolvem quer as políticas internas de coordenação da mesma quer as políticas externas de relacionamento.

**Asset Management (Gestão de bens):**

- Inventariação e classificação dos bens segurados, identificação dos seus legítimos proprietários e usufruto aceitável.

**Human Resources Security (Equipa técnica responsável pela Segurança):**

- Procedimentos de segurança relacionados com a admissão, manutenção e abandono de colaboradores.

**Physical and Environment Security (Segurança física e ambiental):**

- Segurança física da instituição, matriz de liberdade de acesso físico a locais e equipamento bem como políticas de reutilização do mesmo.

**Communications and Operations Management (Gestão de operações e comunicação)**

**Communications and Operations Management (Gestão de operações e comunicação)**

**Access Control (Controlo de acesso):**

- Direitos de acesso a redes, sistemas, aplicações, dados e funções por parte de cada entidade/colaborador.

**Information systems Aquisition, Development and Maintenance (Integração de segurança nas aplicações)**

**Information Security Incident Management (Gestão de incidentes de segurança):**

- Descrição de como antecipar e responder a cenários de insegurança manifestados (previstos ou não).

**Business Continuity Management (Gestão da ininterrupção de serviços):**

- Descrição de como proteger, manter e retomar processos e sistemas críticos aos negócios (disaster recover plans).

**Compliance (Conformidade):**

- Respeita aos cuidados de conformidade entre as medidas internamente adotadas e as disposições legais e normativas em vigor na zona geo-política em causa.

**ISO 27000: Metodologia de Implementação:**

- PLAN: Sistemas de Gestão de Segurança da Informação

- Definição da motivação e âmbito do SGSI a aplicar à organização

- Definição de uma política de segurança

- Definição da abordagem de análise/avaliação de riscos da organização

- Identificação dos riscos

- Análise e avaliação dos riscos

- Identificação e avaliação das opções para o tratamento de riscos

- Definição dos objetivos de controlo e controlos para o tratamento de riscos

- DO: Sistemas de Gestão de Segurança da Informação

- Formulação de um plano de tratamento de riscos (PTR)

- Implementação do plano de tratamentos de riscos

- Implementação dos controlos selecionados na 1ª etapa do SGSI

- Definição e especificação de como será feita a medição à eficácia dos controlos

- Implementação de procedimentos e outros controlos capazes de permitir a pronta deteção de eventos de segurança da informação e resposta a incidentes de segurança da informação

- CHECK: Sistemas de Gestão de Segurança da Informação

- Estabelecer procedimentos de monitorização/análise crítica

- Realização de análises de críticas regulares à eficácia do SGSI

- Medição da eficácia dos controlos para verificar se os requisitos de segurança da informação foram atendidos

- Analisar criticamente as avaliações de risco, riscos residuais e níveis de riscos aceitáveis

- Conduzir auditorias internas do SGSI em intervalos planeados

- Atualizar os planos de segurança da informação

- Registar ações e eventos que possam ter impacto na eficácia ou no desempenho do SGSI

- ACT: Sistemas de Gestão de Segurança da Informação

- Implementar as melhorias identificadas no SGSI

- Executar as ações preventivas e corretivas apropriadas

- Comunicar as ações e melhorias a todas as partes interessadas

- Assegurar-se de que as melhorias atinjam os objetivos pretendidos

**Ciber-Ameaças e Mitigação (115 -148)**

**As ameaças com efeitos mais nefastos:**

- Vermes

- Representam uma ameaça temível pelo seu impacto global.

- Executam e replicam-se de forma autónoma explorando vulnerabilidades protocolares e aplicacionais.

- Vírus

- Código malicioso integrado numa aplicação legítima. Quando ativado propaga-se.

- Podem ser inofensivos ou destrutivos.

- Meio preferencial de disseminação: email

- Cavalos Tróia

- Aparentemente inofensivos que escondem

código malicioso capaz de efectuar danos locais, aceitar comandos remotos (back doors), ou divulgar informação confidencial.

**Vírus:**

- Vírus biológico é um organismo infecioso que requer uma célula hospedeira para crescer e multiplicar-se.

**Cavalos de Tróia (Trojan Horses):**

- Apesar de não criarem réplicas de si próprios são de muito fácil elaboração (script kids) e operam em cliente/servidor.

- Em regra são de difícil detecção e por vezes autodestroem-se para impossibilitar/dificultar a deteção. Ex. Keylogger, Backdoor , Spammers, …

- Tipos comuns

- Remote-access Trojan Horse

- Data sending Trojan Horse

- Destructive Trojan Horse

- Proxy Trojan Horse

- FTP Trojan Horse

- Security software disabler Trojan Horse

- Denial of Service Trojan Horse

**Vermes (Worms) – Fases de propagação:**

- Muitos vermes caracterizam-se por explorar determinada vulnerabilidade, possuir um mecanismo de propagação em rede específico e um payload onde é alojado o códigoofensivo (e.g., uma backdoor)

**Vulnerabilidade típica: buffer overflows:**

- Cerca de um terço das vulnerabilidades do software dizem respeito a buffer overflows (CERT)

- Buffer é uma zona de memória reservada por uma aplicação para armazenar dados temporários

- Aplicações deficientes podem aceitar guardar dados de volume superior ao que na verdade suportam, corrompendo zonas de memória contíguas com outros dados ou código.

- Os Vírus e os Cavalos de Tróia tendem a explorar root buffers locais (espaços de endereçamento privilegiados)

- Vermes como o SQL Slammer e o Code Red exploraram root buffers remotos (i.e., não necessitaram de utilizadores locais nem dos seus privilégios para aceder a esses buffers)

**Mitigação:**

- Vírus e Cavalos de Tróia: antivírus locais e antivírus preparados para trabalhar conjuntamente com os servidores de email

- Vermes: Contenção (fechar portos explorados de forma maligna), aplicar *patches*, isolar e reparar sistemas infetados)

- Cisco Self-Defending Network é uma solução estrutural com diversas componentes que pretende resolver de forma integrada os desafios de segurança de uma rede.

- Cisco Security Agent (CSA): Um HIPS (host-based intrusion prevention system) integrável com um qualquer antivírus

- Cisco Network Admission Control (NAC): um dispositivo que restringe as admissões à rede a dispositivos que possúam um perfil de segurança adequado

- Cisco Security Monitoring, Analysis, and Response System (MARS): reporta eventos relevantes.

**Outra taxonomia possível:**

- Ataques estruturados

- Oriundos de hackers competentes e profundos conhecedores das vulnerabilidades, capazes de desenvolver ferramentas para o efeito. Tipicamente são movidos pelo intuito de realizar algum tipo de ilícito.

- Ataques não Estruturados

- Realizados por indivíduos inexperientes que possuem apenas a curiosidade de experimentar ferramentas existentes. Podem, no entanto, causar graves prejuízos.

- Ataques Externos

- Realizados por indivíduos estranhos à organização e conduzidos tipicamente de forma remota.

- Ataques Internos

- Perpetrados por indivíduos com acesso autorizado à infraestrutura de comunicação da empresa. Constituem entre 60 a 80% dos ataques. As motivações são diversas, mas normalmente estão relacionadas com a insatisfação dos seus autores.

- Ataques Passivos

- Captura e análise/interpretação/divulgação de conteúdo sensível presente tráfego.

- Normalmente este tipo de ataque tem pouca visibilidade mas é usado na preparação de ataques ativos.

- Ataques Ativos

- Entrar em sistemas através de credenciais obtidas de forma fraudulenta (obtidas por ataques passivos).

- Modificação de mensagens (MITM)

- DoS, …

**Metodologias de ataques em rede (149 - 167)**

**Metodologias de ataque:**

- Categorização (CCNA Security):

- Ataques por reconhecimento (Reconnaissance Attacks)

- Descoberta não autorizada de sistemas, serviços e vulnerabilidades. Ferramentas: sniffers e port scanners.

- Ataques de acesso a informação (Access Attacks)

- Exploração de vulnerabilidades de autenticação conhecidas em serviços disponíveis com o objetivo de aceder de forma ilegítima a informação sensível. Tipicamente usam-se ataques por força bruta apoiados por dicionários.

- Ataques de impedimento de prestação de serviço (Denial of Service Attacks - DoS)

- Este tipo de ataques visa consumir uma fração significativa de recursos (de servidores ou da rede) com prejuízos graves para o normal desempenho de serviços.

**Ataques por reconhecimento:**

- Precedem normalmente ataques de acesso ou DoS.

- Estratégia simples: ping sweep (ICMP Echo Req/Repl).

- Internet Information queries

- Descoberta de espaços de endereçamento (DNS/Whois)

- Para cada sistema descoberto inventariar os serviços alojados (e.g., Nmap).

- Para cada serviço identificar “assinaturas” (OS, version …)

- *Packet sniffers* (e.g. Wireshark)

- Em modo promíscuo podem capturar todo o tráfego *broadcast* e por vezes *multicast.*

- Nas redes comutadas (*switches*) o isolamento é apenas aparente quando comparado com a sua inexistência em segmentos partilhados (*collision domain*).

- Sistema de prevenção de intrusões (IPS) disparam alarmes a sinalizar alguns d estes ataques (e.g., IOS de *routers* Cisco ISR).

**Ataques de acesso:**

- Ataques a passwords (password attacks)

- Métodos: Ataques por força bruta (com ou sem apoio de dicionários), cavalos de Tróia (keyloggers), ou sniffers.

- Abuso de confiança (Trust exploitation)

- Exploram-se privilégios atribuídos indevidamente.

- Redireccionamento de portos (port redirection)

- É um tipo específico de ataque por abuso de confiança em que uma terceira máquina comprometida é usada como medidora do ilícito (por, por exemplo, usufruir de privilégios na firewall).

- Sistemas host-based IDS e antivirus ajudam na prevenção.

- Ataques por interposição (Man-in-the-middle attack-MITM)

- Tipicamente alteram conteúdo de mensagens que circulam entre um par de entidades legítimas.

**Ataques DoS:**

- Trata-se de um tipo de ataque de rede que pretende diminuir a disponibilidade de determinado serviço prestado a pessoas (e.g., sites web), equipamentos ou aplicações.

- São ataques simples, mas tipicamente os mais temíveis.

- Vulnerabilidades exploradas:

- Tratamento deficiente de determinada formatação específica de uma mensagem protocolar (e.g., Ping of Death).

- Limites dos recursos disponíveis nos próprios serviços (RAM/ CPU/ etc.) ou nas redes e equipamentos de acesso ao mesmo.

**Ataques DoS Exemplos:**

- Ping of Death

- Envio de um pacote IP maior que o tamanho máximo (65,535 bytes). A sua construção é possível através do envio de fragmentos. Bastavam 65,536 bytes para causar um buffer overflow na pilha do recetor e respetivo crash.

- Smurf Attack

- O atacante envia uma quantidade elevada de ICMP Echo Requests para o endereço de broadcast dirigido de uma rede, forjando o source address com endereços unicast locais.

- A rede destino rapidamente satura

- Hoje grande parte dos routers e dos sistemas operativos dos terminais já estão por omissão preparados para evitar ser alvos deste tipo de ataque.

- TCP SYN Flood

- Envio de muitos pacotes TCP SYN, tipicamente com o endereço SA forjado. Deste modo satura-se rapidamente o nº de sessões pendentes, ficando vedado o atendimento de clientes legítimos.

- Teardrop

- Envio de pacotes IP fragmentados com os campos protocolares usados no processo de reagrupamento povoados com valores fraudulentos de modo a provocar comportamentos erróneos no sistema atacado.

**Ataques DoS Consequências e Sintomas:**

- Consequências diretas comuns

- Consumo excessivo de recursos como largura de banda, espaço em disco, ou tempo de processador

- Danos na informação de configuração (e.g., encaminhamento)

- Danos na informação de estado (e.g., resets de sessões TCP)

- Danos em equipamentos físicos

- Impedimento de comunicação legítima com o sistema alvo.

- Sintomas possíveis

- Desempenho de rede abaixo do normal

- Indisponibilidade de determinado web site

- Indisponibilidade de todos os web sites

- Aumento desmesurado de spam (mail bombs)

**Ataques Distributed DoS (DDoS):**

- Semelhante ao DoS sendo no entanto que o tráfego malicioso é injetado a partir de múltiplos sistemas da rede

- Objetivo alcançado através da distribuição prévia de zombies (por vírus, vermes ou cavalos de tróia) que o atacante instrui posteriormente de forma remota.

- Em alternativa o ataque pode ser acordado através de redes sociais por grupos que partilham um mesmo objetivo (normalmente ideológico ou político)

**Botnets – Cibercrime e mercado negro:**

- O atacante compromete (através de vírus, vermes, cavalos de Tróia, etc.) um conjunto alargado de nós (denominados zombies), instalando nestes um robot.

- A rede (net) de bots, denominada botnet, aguarda de modo passivo por ordens/comandos emanados a partir do controlador central (command-and control(C&C) server).

- O potencial do botnet é então alugado para os mais diversos efeitos: envio de SPAM, DDOS (web sites e DNS root servers, extorsão por chantagem, etc.

- Estima-se que um em cada quatro computadores da Internet integrem um ou mais botnets.

- Os bots tipicamente recorrem a infra-estruturas de comunicação populares como o IRC, o twitter ou Instant Messenger para melhor camuflarem a comunicação com os Command & Control servers.

- As instâncias mais recentes têm evoluído para arquiteturas peer-to-peer(P2P).

- Os botnets mais modestos albergam 10.000 a 20.000 nós. Os maiores chegam a integrar vários milhões de terminais.

**Mitigação de ataques em rede (slide 168 - 175)**

**Mitigação de ataques de reconhecimento:**

- Defesas contra packet sniffers

- Mecanismos de autenticação robustos

- E.g., One-Time Password (OTP) recorre a autenticação de fator duplo (e.g., ATM: cartão + PIN)

- Encriptação da comunicação

- Adopção de infra-estrutura comutada (ajuda apenas)

- Antisniffer software (delays/CPU times anormais)

- Defesas contra Port scanning

- Não existe forma de mitigar estes ataques

- Os IPS e as firewalls podem limitar em muito a descoberta

- Os ping sweeps podem ser evitados filtrando tráfego ICMP na periferia da rede. Ainda assim é possível fazer port scanning!

- Os IPS (network e host-based) podem alertar o administrador para a realização de um ataque de reconhecimento

- O administrador pode tomar algumas medidas (e.g., alertar o ISP para a origem desses ataques).

**Mitigação de ataques de acesso:**

- Ataques por brute force podem ser desencorajados

- Desativando contas após tentativas consecutivas falhadas.

- Por adoção de política de escolha de passwords robustas.

- Usando OTPs ou passwords encriptadas

- A rede deve adotar o princípio da confiança mínima (minimum trust): um servidor seguro não deve confiar num servidor não seguro.

- Acessos remotos e tráfego de encaminhamento deve ser encriptado

**Mitigação de ataques DoS:**

- Ataques DoS

- A adoção de técnicas simples de proteção anti-spoofing no perímetro da rede elimina uma grande percentagem

- Firewalls e IPSs são das soluções mais efetivas, disponibilizando uma série de técnicas para o efeito (DHCP snooping, IP Source Guard, Dynamic ARP Inspection, ACLs.)

- Ataques DDoS

- A sua mitigação requer a cooperação com ISPs

- Mecanismo de Quality of Service (QoS) podem dar uma ajuda(limitada)

**Boas práticas:**

- Manter os sistemas atualizados diariamente (patches)

- Desativar serviços e portos desnecessários

- Usar passwords robustas e alterá-las com frequência

- Controlar o acesso físico aos sistemas

- Limitar ao estritamente necessário o input dos serviços de acesso remoto

- Realizar e testar backups com regularidade

- Educar os colaboradores para os riscos da engenharia social e desenvolver estratégias de apoio à validação de identidades através do telefone, email ou contacto pessoal

- Proteger com passwords e encriptação dados sensíveis

- Adotar soluções tecnológicas de apoio (firewalls, IPS, VPNs, antivírus, etc.)

- Redigir uma política de segurança para a empresa.

**Criptografia**

**O problema (slide 4)**

**Objetivo dos administradores de redes:**

- Proteger a infraestrutura (routers, switches, servers, terminais; configuração (hardening), controlo de acessos AAA, ACLs, firewalls, IPS/IDS)

- Assegurar que a informação viaja de forma segura entre os pares desejáveis (Autenticação, Integridade, Confidencialidade)

**Serviços de segurança (slide 6 - 9)**

**Autenticação:**

- Serviço e segurança que permite verificar se determinada mensagem provém de facto do emissor que a subscreve.

- Quando o canal de comunicação não é seguro (e.g., sujeito a spoofing) a autenticação deve ser sustentada por métodos criptográficos.

- É u um serviço suficiente quando não é suposto o recetor constituir uma ameaça à credibilidade da origem da mensagem.

- Exemplo: troca de mensagens dentro de sistemas informáticos de uma mesma instituição.

Não-repúdio:

- Serviço de segurança que garante que o emissor não pode negar ter enviado aquela mensagem em particular e/ou o recetor não pode negar tê-la recebido (envolve igualmente serviço de integridade).

- Sem esta garantia um cliente de um serviço de banca on-line poderia facilmente negar movimentos de sua autoria.

- A utilização deste serviço de segurança é necessária sempre que emissor e recetor possam ter conflitos de interesse (e.g., e-commerce) -> Certificados digitais.

**Integridade:**

- Serviço de segurança que permite ao recetor verificar se a mensagem recebida sofreu algum tipo de mutação em trânsito.

Confidencialidade:

- Serviço de segurança que permite ao emissor entregar uma mensagem cujo conteúdo apenas seja inteligível para o recetor.

- A privacidade da mensagem, mesmo que intercetada

ao longo do canal de comunicação que separa o emissor do recetor, não é comprometida.

- Técnicas de suporte:

- Criptografia: técnica destinada a baralhar a informação de uma mensagem para garantir a sua confidencialidade.

- Síntese criptográfica (hash function): Neste caso o conteúdo original perde-se, sendo produzida uma “síntese” única.

**Conceitos introdutórios (slide 10 - 28)**

**Criptologia:**

- Ciência que se dedica ao estudo da criptografia e criptanálise

**Criptografia:**

- Arte ou ciência que permite escrever uma mensagem de forma a tornar ininteligível o seu conteúdo a entidades não autorizadas.

**Criptanálise:**

- Ciência que permite tornar inteligível o conteúdo de mensagens criptografadas e/ou descobrir as técnicas de criptografia adotadas em certo contexto sem conhecer a(s) chave(s) usadas.

- Componente necessária à segurança pois não é possível provar formalmente a segurança dos algoritmos criptográficos. Testa-se antes a sua vulnerabilidade às várias técnicas criptoanalíticas.

**Tipos de Criptanálise:**

- Ataque de Força Bruta (Brute Force Attack)

- DES quebrado em 22 horas.

- O atacante tem acesso ao criptograma ou a parte dele.

- O atacante experimenta todas as chaves possíveis.

- Apenas criptogramas conhecidos (Ciphertext-Only Attack)

- A mensagem original é desconhecida.

- O atacante possui diversos criptogramas produzidos com o mesmo algoritmo.

- Objetivo: efetuar análise estatística da informação para recuperar a chave.

- Hoje não se usa, pois, as cifras são em geral resistentes à análise estatística.

- Mensagem e criptograma conhecidos (Known-Plaintext Attack/ Meet-In-The-Midle attack)

- O atacante possui os criptogramas e parte ou totalidade das mensagens

- Este ataque veio provar que a cifra dupla com chaves independentes não eleva ao quadro a dimensão do espaço de procura, mas apenas a duplica. O atacante usa todas as chaves possíveis até que haja coincidência com o texto em claro e usa todas as chaves possíveis até que haja coincidência com o criptograma. Se o criptograma conhecido coincide com o criptograma conhecido, a chave foi encontrada.

- Em média o atacante precisa de varrer por força bruta metade do espaço das chaves.

- Nos algoritmos de cifra modernos o espaço das chaves é de tal forma extenso que a força bruta não é vista como uma ameaça credível.

- Esta estratégia reduz imenso o espaço de pesquisa porque existe uma redução de combinações de pares de chaves possíveis.

- O espaço de armazenamento necessário é substancial, uma vez que é

necessário armazenar todos os criptogramas gerados a partir da primeira chave.

- Ataque com mensagens escolhidas (Choosen-Plaintext Attack)

- O atacante escolhe as mensagens a ser cifradas.

- Neste caso o sucesso pode ser maior pois a mensagem pode ser escolhida para revelar propriedades importante da chave.

- É um ataque difícil de executar pela dificuldade envolvida em ter acesso aos canais de entrada da mensagem e do criptograma associado

- Ataque com criptogramas escolhidos (Chosen-Ciphertext Attack)

- O atacante tem acesso a parte do criptograma e à respetiva decifra.

- Torna-se assim mais simples varrer o espaço de procura das chaves.

- Semelhante ao anterior mas com efeitos no sistema de decifra.

- Extorsão

- Conhecida por Rubber-hose cryptanalysis

- A estratégia mais simples de criptoanálise

- Ataque de Aniversário (Birthday Attack)

- O Paradoxo do Aniversário diz-nos que basta estarem reunidas 23 pessoas para, com 50% de probabilidade, duas delas partilharem o mesmo dia e mês de aniversário.

- Se uma função f(x) produz H resultados distintos com igual

probabilidade então é necessário em média varrer 1.25 ´ Ö(H) elementos para encontrar dois x1 e x2 tais que f(x1)=f(x2).

- Este resultado é especialmente importante no domínio das funções de síntese, provando que é necessário bem menos que a quantidade máxima de tentativas para, em média, encontrar uma colisão.

**Técnicas de Criptanálise:**

- Segurança por ocultação

- A segurança de um sistema de informação não deve assentar no secretismo do seu design ou implementação.

- Esteganografia

- Arte ou ciência que permite ocultar dentro de um conteúdo, aparentemente inocente, um segundo conteúdo sensível.

- Ao contrário da Criptografia, a Esteganografia não se revela. Pode

ser usada para manter uma comunicação secreta.

- Exemplos:

- Escrita com tinta invisível (watermarkets).

- Utilização dos bits menos significativos de cada pixel de uma imagem.

- Variação de parâmetros de transmissão de pacotes IP.

- Quem souber como a informação foi ocultada saberá recuperá-la.

Processo criptográfico (ciclo):

- Texto em claro (plaintext) - Mensagem original que se pretende transmitir.

- Cifra (encryption) - Técnica criptográfica de ocultação.

- Criptograma (ciphertext) - Texto cifrado que resulta de aplicação da cifra ao texto em claro.

- Algoritmo de cifra (encryption algorithm) - Define o modelo genérico de tratamento de dados. Atendendo aos perigos que a segurança por ocultação encerra deverá ser normalizado, implementado e de domínio público.

- Chave (key) - Parâmetro de entrada do algoritmo que permite variar o seu comportamento de forma complexa.

**Tecnologia de Cifra (slide 29 - 46)**

**Evolução:**

- Cifras de transposição - existem inúmeras variantes da cifra de transposição.

- Criptanálise das cifras de transposição

- Possuem um número muito limitado de chaves.

- Reproduzem os padrões estatísticos de frequência dos caracteres.

- No seu tempo serviram o propósito a que se destinaram, mas no domínio informático não têm qualquer utilidade quando usadas isoladamente.

- Cifras de Substituição

- As letras da mensagem original são substituídas pelas letras de um alfabeto deslocado n letras (n funciona como a chave do algoritmo)

- Cifra aditiva monoalfabéticas

- Cifras de substituição monoalfabéticas

- Cifra de substituição aditiva

-Cripto-letra = (letra + chave) mod #alfabeto

-Mod = Resto da divisão

- Número máximo de chaves = # alfabeto

- Como estruturalmente revelam padrões estatísticos estas cifras tornam-se frágeis.

- Além de revelarem frequências de letras revelam igualmente construções características da linguagem como digramas ou trigramas.

- Cifra de substituição multiplicativa

- Cripto-letra = (letra x chave) mod #alfabeto

- Chave tem de ser um n.º co-primo de # alfabeto

- Número máximo de chaves < # alfabeto

- Cifra de substituição polialfabética

- Resume-se a uma aplicação sucessiva e

cíclica de várias cifras monoalfabéticas.

- O número de cifras monoalfabéticas

define o período da cifra polialfabética.

- A Cifra de Viginère consiste na aplicação de N cifras monas alfabéticas aditivas.

- A chave de cada uma das cifras mono alfabéticas é o valor atribuído a cada letra de uma frase chave com N letras.

- As cifras polialfabéticas escondem melhor a frequência das letras individuais e mesmo dos digramas/trigramas.

- No entanto podem ser criptanalisadas conhecendo-se o seu período N (i.e., a extensão da chave). Sabendo-o, o problema reduz-se à criptanálise de N cifras monoalfabéticas normais.

- Teste de Kasiski

- A dimensão da chave é determinada através da procura de blocos idênticos no criptograma e da sua medição da distância (em número de letras).

- Efetuar a decomposição das distâncias em fatores primos

- O maior divisor comum revela o período N com alta probabilidade

- Algoritmo da Cisco

- Variante da Cifra de Vigenère - Por ser tão frágil não é difícil encontrar *on-line sites* com esse serviço disponível.

- Índice de coincidência (correlação)

- A criptanálise feita à cifra de Vigenère pela CryptTool baseia-se no estudo do Índice de coincidência (correlação).

- Facto: A probabilidade de existir, no texto em claro, o mesmo caractere separado por deslocamentos (offsets) múltiplos do tamanho da chave é razoável.

- Cifras de Transposição - E.g., Cifra dos Espartanos

- Cifras de Substituição - E.g., Cifra de César e de Vigenère

- Cifras multiplicativas (*product cipher*)

- Trata-se de uma combinação das anteriores e de outras operações simples:

- transposições, translações (e.g., XOR), transformações lineares, operações aritméticas, multiplicação modular e substituições simples.

- É aplicada (*round*) uma função composta por *nf* >= 2 funções

básicas de transposição e/ou substituição.

- Criam-se cifras de elevada qualidade (e.g., DES)

**Bases da Criptografia Moderna (slide 47 - 74)**

**Cifra perfeita:**

- Uma cifra diz-se perfeita quando, dado um criptograma c, a probabilidade de ele corresponder a um dado texto original m tendo sido gerado com uma dada chave k é igual à probabilidade de ocorrência do próprio texto m. Se o criptograma e o texto em claro são estatisticamente independentes a cifra oferece secretismo perfeito.

- Existe alguma chave que mapeia qualquer mensagem num criptograma qualquer com a mesma probabilidade.

- A chave tem que ser verdadeiramente aleatória para que todas as chaves possíveis sejam equiprováveis.

- A dimensão do espaço de chaves tem de ser superior à dimensão do espaço de textos em claro.

- Na verdade Shannon provou que a entropia do espaço das chaves deveria ser igual ou superior à entropia do espaço do texto original -> Requisito ideal mas impraticável. Por este motivo recorre-se muitas vezes a geradores pseudoaleatórios alimentados a partir de uma chave de tamanho razoável.

**Passwords:**

- Acredita-se que a melhor estimativa da capacidade de memória de um ser humano comum foi calculada por Paul Reber e cifra-se em 2.5 Petabytes = 2500 Terabytes.

- Paradoxalmente é difícil para pessoas comuns recordarem passwords com mais de 20 bits de incerteza

- Passwords alfanuméricas com 7 caracteres aleatórios são ummilhão de vezes mais fortes e bem mais fáceis de memorizar

- A nossa memória é um dispositivo de armazenamento gigante comuma capacidade de acesso ridiculamente baixa

- Por isto … são hoje propostos mecanismos de armazenamento de passwords sem consciência explícita do interveniente (Moodle)

**5 Critérios de Shannon para avaliar qualidade da cifra:**

- A quantidade de secretismo oferecida

- Aceitável quando: Tempo mínimo de segurança do criptograma (face ao esforço e montante envolvido na sua criptanálise) > Tempo de vida em que a informação deve permanecer secreta.

- A dimensão das chaves

- Quanto maiores e mais aleatórias mais seguras mas potencialemente mais dífíceis de gerir.

- A simplicidade de realização e exploração

- Não se aplica actualmente devido à existência de meios computacionais (na altura dominavam os meios mecânicos).

- A propagação de erros

- Pode ser desejável quando se pretende proteger a integridade de uma mensagem. Pode ser indesejável quando se pretende tornar robusto a erros de transmissão determinado protocolo de comunicação.

- A dimensão do criptograma

- Idealmente um criptograma deve possuir dimensão igual ou inferior ao texto original.

**Outros Critérios de Qualidade de uma cifra:**

- Assumir que o algoritmo é conhecido, bem como todas as suas fragilidades.

- Assumir que os criptogramas produzidos por uma dada cifra e chave podem ser todos capturados e analisados de forma eficiente em tempo útil.

- Assumir que são conhecidas porções do texto em claro, podendo as mesmas ser relacionadas

- Sucede por exemplo com documentos que são produzidos por determinados pacotes de software (e.g., Microsoft Word), que a par com o texto visível, incluem informação de formatação normalmente previsível/conhecida.

**Como projetar cifras com boa quantidade de secretismo:**

- Princípio da Confusão

- A relação entre o texto em claro, a chave e o criptograma deve ser o mais complexa possível porque:

- Por um lado pretende-se dificultar a descoberta de parte do texto original mesmo conhecendo alguns trechos do mesmo

- Por outro pretende-se dificultar a descoberta de parte ou totalidade da chave usada para produzir o criptograma

- Princípio da Difusão

- Cada porção pequena do criptograma deve depender de grande parte do texto em claro. I.e., cada bit do texto original deverá influenciar vários bits do criptograma.

- Deste modo a mais pequena alteração ao texto original provoca uma alteração significativa do criptograma.

**Taxonomia das cifras modernas:**

- As cifras usadas atualmente no universo dos sistemas de informação podem ser classificadas segundo dois vetores: tipos de chave (cifras simétricas e cifras assimétricas) e tratamento do texto (cifras por blocos e cifras contínuas).

- Serviços de integridade, autenticação e confidencialidade.

**Cifras contínuas:**

- Aproximações práticas

- As cifras contínuas existentes são aproximações práticas à cifra simétrica de Vernam.

- De uma chave finita é produzida, através de um gerador pseudoaleatório seguro, uma chave contínua (keystream).

- Exemplos:

- CFB: Cipher FeedBack

- OFB: Output FeedBack

- CTR: Counter

- Estes modos de operação que transformam cifras por blocos em cifras contínuas serão apresentados à frente.

**Cifras por blocos:**

- As cifras por blocos são funções que mapeiam blocos de *n* bits de texto em claro em blocos de *n* bits criptografados.

- O tamanho do bloco, *n*, pode ser um conjunto de dezenas, centenas ou mesmo milhares de bits (típico: *n*>=64).

- A informação é tratada como uma sequência de blocos.

- As funções são parametrizadas por uma chave K de *k* bits

- Podem ser vistas como simples cifras de substituição atuando sobre um único alfabeto (monoalfabéticas) caracterizado por um número extenso de caracteres (blocos).

**Cifras contínuas vs Cifras por blocos:**

- As cifras contínuas são, quando implementadas em hardware, mais rápidas

- As cifras contínuas requerem, quando implementadas em

hardware, componentes menos complexos (mais

económicas)

- As cifras contínuas são obrigatórias quando:

- Existem limitações de *buffering*

- Os caracteres têm de ser processados individualmente

- Os ambientes de transmissão são muito sujeitos a perturbações

- As cifras por blocos são usadas para recriar cifras pseudocontínuas

- As cifras por blocos são precursoras de imensas tecnologias: cifras contínuas, geração pseudoaleatória de números, funções de síntese, códigos de autenticação de mensagens (MACs), mecanismos de integridade, assinaturas digitais, etc.

**Cifras Simétricas (segredo/chave partilhada):**

- Usam uma chave comum ou duas chaves relacionadas em que uma é facilmente obtida a partir da outra.

- Garantem a confidencialidade de dados quando uma única entidade é detentora da chave secreta.

- Garantem a confidencialidade de dados trocados entre duas ou mais entidades que partilhem a mesma chave.

- Vantagem prática: São normalmente muito eficientes.

- Desvantagem: Em universos de N interlocutores são necessárias N x (N-1)/2 chaves diferentes ou o dobro se não forem usadas de forma bidirecional.

**Cifras assimétricas (chave pública/privada):**

- Recorrem a um par de chaves relacionadas: pública e privada.

- A chave pública é usada para cifrar, a privada para decifrar.

- Por vezes ocorre o oposto (e.g., garantia de autenticidade).

- Não é possível determinar a chave privada a partir da pública.

- O par de chaves é de uso individual (pessoas, servidor, serviço).

- Vantagem: São necessárias apenas N chaves públicas para uma comunicação segura entre N interlocutores.

- Desvantagem: muito pouco eficientes.

**Chaves híbridas:**

- Solução de compromisso.

- Reúne as vantagens das cifras simétricas e assimétricas.

- Combina as cifras simétricas e assimétricas durante as diversas fases do tratamento seguro da informação.

- Tipicamente são usadas:

- Cifras simétricas para segurar o grosso da informação (bulk encryption) por motivos de eficiência;

- Cifras assimétricas para segurar o processo de troca de chaves usadas nas cifras simétricas.

- Obtêm-se uma cifra assimétrica com uma eficiência muito próxima de uma cifra simétrica.

**Cifras por blocos (slide 75 - 87)**

**Cifras verdadeiramente aleatórias:**

- Condição:

- Uma cifra verdadeiramente aleatória de blocos de n bits deve poder conduzir a qualquer uma das possíveis permutações que os possíveis criptogramas possam assumir.

- Sendo que as funções de cifra são determinísticas, dependerá da chave essa riqueza.

- É, por conseguinte, necessário existirem (2^n)! chaves distintas.

- Consequentemente a chave deverá possuir n2^n bits o que se torna impraticável por exemplo quando n=64bits

- Solução: adotar função que aparente comportamento aleatório quando alimentada por uma chave aleatória de tamanho aceitável (que desincentive pesquisa exaustiva).

**Vulnerabilidade & Dimensão do bloco:**

- Blocos pequenos vs blocos grandes

- Bloco pequeno: Torna a cifra vulnerável a ataques baseados em análise estatística como a análise de frequência atrás apresentada para a Cifra de César. Este problema, no entanto, pode ser atenuado através da adoção de modos de aplicação inteligentes.

- Bloco grande: Aumenta a robustez da cifra, mas torna a implementação mais complexa (e.g., requer mais espaço de memória), sendo que esta complexidade cresce supralinearmente com n (tamanho do bloco).

**Modos de operação:**

- Como estruturar em blocos as mensagens a cifrar?

- Uma mensagem típica possui normalmente m >> n bits.

- Foram desenvolvidos diversos modos de cifra que permitem aplicar de forma segura e repetida a cifra por blocos recorrendo à mesma chave.

- Processamento genérico:

- O texto em claro é partido em diversos blocos de tamanho n

- O último bloco é completado através de um esquema de enchimento (padding) adequado, de modo a totalizar n bits.

- É aplicado um modo de operação (mode of operation) específico. Geralmente este processo recorre à aleatoriedade baseada num valor adicional: o vetor de inicialização.

- Modo ECB (Electronic Code Book)

- Trata-se do modo mais intuitivo: a cifra é aplicada a cada bloco individualmente.

- Uma fragilidade evidente: blocos iguais de texto original são transformados em blocos iguais no criptograma.

- A estrutura do texto é parcialmente revelada.

- Modo CBC (*Cipher Block Chaining*)

- Modo inventado pela IBM em 1976

- Cada bloco é somado, módulo 2, com o bloco anterior do criptograma.

- Cada bloco do criptograma depende dos blocos anteriores do plaintext

- O vetor de inicialização alimenta o bloco inicial.

- Ainda assim encontrando blocos iguais do criptograma é possível fazer alguma análise estrutural.

- Conclusão: a partir de dois blocos iguais do criptograma e conhecendo o plaintext de um deles é possível determinar o plaintext do outro sem conhecer a chave nem o algoritmo.

- É possível alterar de forma determinística todos os bits do bloco Pi+1 , alterando os mesmos bits do bloco Ci.

- Se não existir um controlo rigoroso de integridade do criptograma esta possibilidade abre portas a ataques MITM.

- O IPSec possui algumas vulnerabilidades deste tipo.

- Trata-se de uma fragilidade que o modo CBC introduz e de que o ECB não sofre.

- É o modo de operação mais usado com o DES (e é também o modo usado pela Cisco com o DES e 3DES no IPSec).

- Modo CFB (Cipher FeedBack)

- Transforma uma cifra por blocos numa cifra contínua.

- Cada bloco da keystream é produzido a partir da chave fixa (key) e do bloco do criptograma anterior.

- É possível usar valores distintas iniciais nos geradores de ambos os extremos, pois, o modo auto sincroniza-se.

- Modo OFB (Output FeedBack)

- Semelhante ao modo CFB.

- A diferença reside no facto de a realimentação ser feita a partir da saída do gerador (e não do criptograma, como sucede no CFB).

- Neste caso é necessário de ambos os lados usar os mesmos vetores de inicialização pois não há auto sincronismo.

- Modo CTR (Counter)

- Tal como o CFB e OFB o CTR transforma uma cifra por blocos numa cifra contínua.

- Cada bloco da keystream é produzido a partir da cifra dos sucessivos valores do contador.

- O valor inicial do contador funciona como vetor de inicialização.

- Resumo

ECB – mesma chave para dados diferentes, alteração determinística difícil, paralelização, acesso aleatório homogéneo, perda de blocos na recuperação de sincronismo.

CBC – não exposição de padrões de texto, confusão na entrada da cifra, mesma chave para dados diferentes, alteração determinística possível, paralelização na decifra, acesso aleatório homogéneo na decifra, propagação de erros no criptograma no bloco seguinte, perda de blocos na recuperação de sincronismo.

OFB – Não exposição de padrões de texto, confusão na entrada da cifra só com ctr, mesma chave para dados diferentes (V.I. diferente), alteração determinística fácil, pré-processamento, paralelização só com pré- processamento, acesso aleatório homogéneo só com pré- processamento.

CFB – não exposição de padrões de texto, confusão na entrada da cifra, mesma chave para dados diferentes (V.I. diferente), alteração determinística fácil, paralelização na decifra, acesso aleatório homogéneo na decifra, propagação de erros no criptograma apenas alguns bits seg., perda de múltiplos de n bits na recuperação de sincronismo.

CTR – não exposição de padrões de texto, confusão na entrada da cifra (ctr secreto), mesma chave para dados diferentes (ctr diferente), alteração determinista fácil, pré-processamento, paralelização, acesso aleatório homogéneo.

**Cifras simétricas por blocos (slide 88 - 114)**

**Cifras simétricas por blocos:**

- As cifras simétricas por blocos usam os princípios da difusão e confusão introduzidos por Shannon:

- Aplicação iterativa de uma operação complexa a um bloco grande (n >= 64 bits), operação esta normalmente controlada por uma chave

- Operações elementares:

- Permutação: troca de lugar dos diversos bits.

- Substituição: muda valores binários de acordo com determinada tabela de correspondência.

- Expansão: introduz novos bits, replicando alguns do bloco de entrada.

- Compressão: passa para a saída apenas alguns dos bits do bloco

- DES 64 bits bloco, 56 bits chave, 16 iterações internas

- CAST 64 bits bloco, 64 bits chave, 8 iterações internas

- IDEA 64 bits bloco, 128 bits chave, 8 iterações internas

- Blowfish 64 bits bloco, variável <= 448 bits chave, 16 iterações internas

- AES 128, 192 ou 256 bits bloco, 128, 192 ou 256 bits chave, 10,12 ou 14 iterações internas

- RC5 varável bits bloco, variável iterações internas

**DES – Origem:**

- DES – Data Encryption Standard - 1977

- Alto nível de segurança

- Algoritmo especificado e compreensível

- Algoritmo público

- Segurança devia assentar apenas no secretismo das chaves

- Suportar diversos cenários operacionais

- Economicamente realizável por hardware

- Suscetível de validação e exportação

**DES – Características:**

- Cifra simétrica por blocos de 64 bits

- Cifra multiplicativa: combina várias operações simples

- Chaves de 56 bits (8º bit de cada octeto da chave é de paridade)

- Previram-se quatro modos de operação: ECB, CBC, OFB, CFB

- Aplica 16 iterações na rede de Feistel

- Em cada iteração é usada uma chave própria derivada da chave inicial

- Provou-se mais tarde ser o melhor valor para resistir à criptanálise diferencial

- Possui 4 chaves fracas (resultam no mesmo criptograma), 12 semifracas (subchaves iguais) e 48 potencialmente fracas (4 subchaves distintas em vez das 16 necessárias)

**DES - input-output:**

- Os bits de paridade da chave são removidos desta

- A chave permite criar no máximo 2^56 bijeções das (2^64 !) possíveis perante cada bloco de 64 bits de texto em claro.

- Crê-se que foram introduzidos bits de paridade na chave para reduzir num fator de 256 a dimensão do espaço das chaves.

**DES – estrutura genérica:**

- O DES assenta numa rede de Feistel de 16 rounds

- Esta rede é precedida de um bloco de permutação inicial (IP).

- E terminada por um bloco de permutação final que mais não é que a permutação inicial invertida.

- A permutação inicial e final não possuem qualquer significado criptográfico. No entanto facilitavam o carregamento e descarregamento dos blocos nas arquiteturas de hardware da altura (mid 1970).

**DES - Permutação inicial do bloco de dados:**

- Permutação inicial do bloco de dados de 64 bits

- CrypTool: Indiv. Procedures > Visualization of Algorithms > DES…

- O bit 58 passa a ocupar a 1ª posição, o bit 50 a 2ª posição, …

**DES – Geração de 16 chaves (Key Schedule):**

- Remoção dos 8 bits de paridade da chave

- Permutação PC1 sobre a chave “efetiva” (56 bits)

- A chave permutada é desagregada em duas metades (L e R)

- Cada uma das 16 chaves resulta desta por rotação à esquerda n bits

- As duas metades L e R são reagregadas

- Aplica-se a permutação PC2: perdem-se 8 bits (48 bits)

- Fica gerada a primeira das 16 chaves k[1] … k[16] a aplicar no primeiro round da rede de Feistel

**DES – Função de Feistel:**

- Em cada um dos (i=1..16) rounds é aplicada a mesma função f estimulada por uma chave k[i]

- Primeiro estágio: Expansão

- A metade direita do bloco do estágio anterior (32 bits) é expandida para um bloco de 48 bits

- Segundo estágio: Mistura de chave (key mixing)

- A expansão é combinada por XOR com a chave derivada K[i]

- Terceiro estágio: Substituição (e compressão)

- O resultado do XOR é dividido em 8 grupos de 6 bits: B[i=1..8]

- Cada grupo de 6 bits estimula uma S-Box a produzir 4 bits através de uma transformação não linear que dá força à segurança do DES

- O valor decimal encontrado na matriz é agora representado no seu binário equivalente (representável por apenas 4 bits).

- Quarto estágio: Permutação

- Destinada a levar os 4 bits produzidos por uma S-Box do estágio atual a espalharem-se por 6 S-Boxes distintas do próximo passo.

**DES – Permutação final:**

- Na permutação final reverte-se a ordem criada durante a permutação inicial.

- Matriz de Permutação inicial vs. Permutação final

**DES – Aplicação em cifra por blocos:**

- Aplicação em modo de cifra por bloco

- Usada se dimensão do texto em claro >= 64 bits

- Modos de operação típicos: ECB, CBC

- Aplicação em modo de cifra contínua

- É aplicada a operação XOR entre o texto em claro e a sequência pseudoaleatória de bits criada através da chave e de parte do criptograma já produzido.

- Modos de operação típicos: CFB, OFB

**DES – Serviço e Robustez:**

- O DES oferece um serviço de confidencialidade

- Robustez

- Até hoje não foi encontrada nenhuma técnica de criptanálise mais eficiente que a própria pesquisa exaustiva.

- Porém, devido ao tamanho de 56 bits da chave, o poder computacional atual torna viável realizar ataques por pesquisa exaustiva em tempo útil, facto que fragiliza a aplicação do DES.

**Como aumentar a robustez da cifra:**

- Mantendo o DES

- Mudar a chave com regularidade

- Usar um canal seguro para o efeito

- Aplicar o modo de operação CBC

- Na verdade é o modo mais usado!

- Evitar usar uma das 64 chaves frágeis

- Aplicando a mesma cifra com novos métodos

- Cifra múltipla: e.g., Triple DES (pouco eficiente …)

- Branqueamento (whitening): e.g., DES-X

- Substituindo a própria cifra: AES

**Triple DES (slide 115 - 127)**

**Cifra múltipla:**

- Cifra múltipla

- O conceito é simples: cifrar o texto mais do que uma vez usando sucessivamente chaves diferentes

- Cifra dupla

- Apesar de ter sido originalmente proposta não reforça significativamente a segurança

- Em vez das intuitivas 2^2n tentativas, a força bruta requer apenas 2^n+1 tentativas

- Ataque Meet-in-the-midle (rever slides iniciais)

- Ainda assim, para ser exequível, a sua criptanálise requer quantidade substancial de armazenamento.

- Cifra tripla

- Aplicam-se sucessivamente três operações

- Cifra -> Decifra -> Cifra

- EDE: Encrypt, Decrypt, Encrypt

- Usa-se 1,2 ou 3 chaves distintas

- Um aspeto importante do modo EDE reside no facto de a utilização de uma só chave conduzir ao DES simples

- A primeira e segunda operações anulam-se.

- Este comportamento permite uma interação simples com equipamentos e aplicações antigos, mas é hoje obsoleto.

**Triple DES:**

- Triple Data Encryption Algorithm (TDEA)

- Também conhecido por 3DES

- Algoritmo

- Criptograma **= EK3(DK2(EK1(**Plaintext**)))**

-Plaintext **= DK1(EK2(DK3(**Criptograma**)))**

- Opções de chave

- Opção 1 (3TDEA): K1, K2, K3 independentes

- Dimensão efetiva da chave: 3 × 56 = 168 bits

- Opção 2 (2TDEA): K1, K2 independentes (K3=K1)

- Dimensão efetiva da chave: 2 × 56 = 112 bits

- Opção 3: K1=K2=K3

- Equivalente ao DES (não recomendada)

- Aplicações

- Pagamentos electrónicos (MasterCard, Visa, ...)

- Nos EUA foi dada ordem de substituição do DES pelo 3DES nos sistemas ATM (Automated Teller Machine) até 1-Janeiro-2007.

- O DES havia sido universalmente usado desde 1981 para cifrar o PIN (personal identification number) nas transações electrónicas.

- Protocolos seguros

- IPSec (RFC 2451)

- Aplicações (Microsoft Office 2007/2010, …)

- Sistemas operativos (IOS, …)

- Criptanálise

- Apesar da chave combinada (na opção 1) possuir 168 bits é conhecida e bem documentada uma variante do ataque Meet-in-the-Midle que reduz a complexidade da decifra a apenas 2112 (=opção 2)

- Nota: Este facto evidencia a diferença entre o tamanho da chave e a segurança dos algoritmos simétricos!

- Tipicamente os algoritmos de cifra por chave simétrica são desenvolvidos de modo a oferecer uma segurança igual ao tamanho da chave.

- Se o DES demorasse 1 segundo a quebrar seriam necessários 60 milhões de anos para comprometer o 3DES.

- Outro problema do 3DES prende-se com a herança que fez do DES em processar apenas blocos de 64 bits e que o torna mais permissível a ataques de aniversário.

**DES-X (slide 128 - 129)**

**DES-X:**

- O branqueamento da chave (Key whitening) é uma técnica mais simples que a cifra múltipla

- As chaves K1 e K2 possuem a dimensão do bloco

**AES (slide 130 - 156)**

**Advanced Encryption Standard (AES):**

- A norma prevê 3 cifras: AES-128, AES-192 e AES-256

- As chaves dos diversos tamanhos podem ser usadas para cifrar blocos de 128, 192 e 256 bits, sendo permitidas as 9 combinações possíveis.

- Durante a normalização fixou-se em 128 bits o tamanho do bloco

- O algoritmo pode futuramente evoluir para chaves múltiplas de 32

- Foi desenhado para ser eficiente (hardware /software)

- 5´ mais rápido que o DES

- Adequado a baixas latências / débito elevado

- Ainda é um algoritmo “jovem” (ao contrário dos 35 anos do DES/3DES) e, portanto, menos “credível”.

- Não se baseia numa rede de Feistel como o DES

- Opera sobre uma matriz de 4 ´ 4 bytes

- Denominada “estado” (state)

- Considera uma chave secreta

**AES - Algoritmo geral (chave/bloco: 128 bits):**

- “Rijndael key schedule”: K1…K10

- Última operação por round: state XOR Ki

- SubBytes

- Substituição

- ShiftRows

- Permutação

- MixColumns

- Combinação

**AES - Operação SubBytes (substituição):**

- Rijndael S-Box: Fonte de Confusão (ñ linearidade)

- A S-Box deriva de uma combinação do inverso multiplicativo de GF(2^8)-um corpo finito (ou corpo de Galois), com uma função afim invertível.

**AES - Operação ShiftRows (permutação):**

- A primeira linha do state mantêm-se, as restantes são deslocadas 1,2 e 3 bytes respetivamente (permutação).

- Deste modo cada coluna do estado de saída incorpora bytes de colunas distintas do estado de entrada.

- Junto com a operação MixColumns, constitui a principal fonte de difusão

- Cada bit do texto em claro influencia vários bits do criptograma

**AES - Operação MixColumns (combinação):**

- Cada coluna é tratada como um polinómio sobre o campo de Galois

- Como resultado … os bits de cada coluna são misturados, i.e. cada byte do novo estado passa a depender dos restantes bytes da mesma coluna do estado anterior.

**AES - Operação AddRoundKey:**

- O estado resultante é multiplicado de forma exclusiva (XOR) com a chave específica do round em causa.

**AES - Geração de chaves:**

- A chave expandida é uma matriz de 44 colunas de 32 bits

- As 4 colunas inicias são preenchidas c/ a chave original

- A partir destas geram-se as restantes colunas

- Cada uma das restantes três colunas resulta do XOR entre a respetiva coluna da chave anterior e a primeira coluna da chave do round atual.

- O par de procedimentos descritos repete-se para gerar cada uma das chaves usadas nos demais rounds

**AES - Número de rounds & robustez:**

- O Governo Norte-Americano (a NSA) anuncia que:

- O AES com chaves de 128, 192 e 256 bits é suficiente para proteger informação ao nível SECRET

- O nível de protecção TOP SECRET requer a utilização do AES com chaves de 192 e 256 bits

- O NSA é responsável por certificar produtos antes de serem usados para proteger informação nacional

- Os melhores ataques reportados até hoje dizem respeito a vulnerabilidades (side-channel attacks) que requerem a execução de código nos sistemas que processam a própria cifra/decifra.

**AES - A Decifra e os Modos de operação:**

- A decifra faz-se invertendo o processamento

- O AES tal como o DES deve ser conjugado com os modos de operação adequados

**AES - Desempenho & Aplicações:**

- Pentium Pro: 18 clks / byte

- Pentium 4: 3.5 clks / byte

- Aplicações: PCI, HIPAA, HITECH, GLBA

- Realizações / algoritmos validados e certificados

- Townsend: 10^6 cifras de cartões de crédito em 7s

**Como escolher um algoritmo de cifra:**

- Muitos algoritmos novos são quebrados rapidamente.

- Como neste âmbito não é possível formalmente demonstrar a segurança de determinado algoritmo de cifra só o tempo permite comprovar a sua robustez.

- Se os algoritmos forem robustos (i.e., apenas violáveis por ataques de pesquisa exaustiva) o fator imediato de escolha deve ser o tamanho da chave e as barreiras à exportação.