Part1

**Citala espartana**

Calendar

Description automatically generated with low confidence

Vinaigrette – tabela com letras

**Alberti cifer**

Text

Description automatically generated with low confidence

**Bellaso-Vigen`ere**

Key: “BELLASO”

A picture containing text, clock

Description automatically generated

modo ECB - Electronic CodeBook Mode;

modo CBC - Cipher Block Chaining Mode;

Text

Description automatically generated

modo OFB - Output Feedback Mode;

modo CFB - Cipher FeedBack Mode;

modo CTR - Counter Mode.

A picture containing text

Description automatically generated

**Padding**

OneAndZeros -> primeiro valor 1 (80 em hex) e resto é 0

Trailing Bit Complement -> complementa com o bit oposto

**Euler**

Text

Description automatically generated



aφ(n) ≡ 1(modn)



Se p, q são co-primos, φ(p · q) = (p − 1)(q − 1)

Se r ≡ s(modφ(n)) então ar ≡ as(modn)

r · t ≡ 1 modφ(n) então(xr)t ≡ x mod(n)

**Teorema RSA**

N=p\*q

A picture containing icon

Description automatically generated

Text

Description automatically generated

**Encriptar** -> rsa(x) = x^e \* mod(n)

**Desencriptar** -> rsa^−1(y) = y^d \* mod(n)

**Protocolo Diﬃe-Hellman**

•1 ≤ x ≤ p – 2

•1 ≤ y ≤ p – 2

•A = αx (mod p) - Alice envia A para Bob

•B = αy (mod p) - Bob envia B para Alice

•Alice calcula K = Bx = (αy)x

•Bob calcula K = Ay = (αx)y.

Cifra ElGamal

Text

Description automatically generated

Text, letter

Description automatically generated

Text

Description automatically generated with medium confidence

**Hash – Merkle-Damgard**

sequências de s bits -> sequências de n bits

com s > n e deﬁne-se L = s − n.

1.OneZeroesPadding

2.Adicionar bloco de comprimento

3. 

**SHA-256**

mensagem M de comprimento arbitrário r

**1.**OneAndZeroes padding, de modo a obter um comprimento que seja múltiplo de 512 bits mas reservando os últimos 64 bits para a representação binária de r

**2.**A mensagem é subdividida em blocos m = m 1 ||m 2 || · · · ||m N cada um com comprimento 512-bits

**3.**Os blocos são processados sucessivamente, iniciando com um hash value H 0 ﬁxo e gerando os valores hash intermédios H i (com 256-bits) através de uma cifra por blocos C especifica do SHA-2: Davies-Meyer

Part2

**Conceitos base de segurança**

• Confidencialidade

• Ausência de divulgação não autorizada de informação

• Garantida por meios criptográficos ou de controlo de acessos

• Integridade

• Ausência de alterações não autorizadas ao sistema ou à informação

• Verificada por meios criptográficos ou de controlo de acessos

• A política de segurança determina o que é autorizado ou não

• Disponibilidade

• Prontidão do sistema para fornecer o serviço ou disponibilizar a informação

**Classificação**

• Projecto

• Vulnerabilidade durante a fase de definição de requisitos e desenho da arquitetura.

• Ex.: Não ter em conta todos os cenários onde a comunicação pode ser observada

• Codificação

• Erro de código (bug) com implicações de segurança

• Ex: validação insuficiente do input

• Operacional

• Vulnerabilidade causada por erro de configuração ou pelo ambiente de execução

• Ex.: contas sem palavras-passe

**Lockheed Martin kill chain**

Table

Description automatically generated

**Avaliação de risco**

• É preciso avaliar o risco

• Risco = probabilidade x impacto

• Probabilidade de explorar o risco

• Exposição do sistema afetado, tipo de utilização

• Grau de vulnerabilidade: Erros de projeto, código ou configuração

• Impacto

• Impacto nas propriedades de segurança da informação: confidencialidade, integridade, disponibilidade

• Impacto na reputação da organização

**Grau de gravidade**

Common Vulnerability Scoring System (CVSS)

• Vetor de ataque (rede, rede adjacente, local, acesso físico)

• Complexidade do ataque (alta, baixa)

• Privilégios necessários (altos, baixos, nenhuns)

• Interação com o utilizador (nenhum, requerida)

• Âmbito (mesmo, outro)

• Impactos (confidencialidade, integridade, disponibilidade)

• Explorabilidade (código não disponível, prova de conceito, funcional)

• Nível de remediação (solução completa, correção temporária, não oficial)

**Propriedades do PEP (Policy Enforcement Point):**

• Isolamento: não deve ser possível alterá-lo.

• Completude: não deve ser possível contorná-lo.

• Verificável: deve ser pequeno e estar confinado ao núcleo de segurança do sistema

por forma a facilitar a verificação da sua correcção.

**Vulnerabilidade Shellshock**

• O Shell é um interpretador de linha de comando em sistemas operativos • Esta vulnerabilidade explora um erro no programa bash ao converter variáveis ​​de ambiente para definição de função • Processo pai pode passar uma função a um processo filho na forma de variável de ambiente• Devido a um erro na lógica de parsing, o bash executa commandos contidos na variável

**Fuzzing:** Técnicas para encontrar falhas, injetando dados mal formatados de uma

forma automática

**Varredores de vulnerabilidades**

• Os fuzzers e injetores de ataques procuram vulnerabilidades desconhecidas

• Varredores de vulnerabilidades procuram vulnerabilidades conhecidas

• Percorrem base de dados de vulnerabilidades

• Injetam ataques

• Monitorizam o efeito na aplicação tentanto detetar se contém a vulnerabilidade

• Requisitos gerais de um varredor de vulnerabilidades web

• Identificar conjuntos específicos de vulnerabilidades presentes em base de dados

públicas

• Gerar relatório para cada vulnerabilidade

• Ter uma taxa de falsos positivos aceitável

**ZAP – operation modes**

Passive – passively analyzes all requests passing through it or generated by crawling components

Active – actively tries to find vulnerabilities using known attacks on selected targets

• Attacks the website using known techniques to find vulnerabilities

• This mode modifies data and may insert malicious scripts on the website.

• You can only run this mode for sites that we have testing permission for.

**Análise manual de código**

• Estratégias de compreensão do código

• Seguir entradas maliciosas

• Analisar por módulo ou algoritmo

• Estratégias de pontos candidatos

• Estratégia genérica de procura de candidatos

• Identificar pontos candidatos simples com ferramentas como o grep ou findstr

• Seguir o resultado da injeção de ataques

**Static Aplication Security Testing (SAST)**

• O objectivo das ferramentas SAST é analisar código fonte e fornecer relatórios

• Quais os elementos detetados que não são vulnerabilidades

• Quais os elementos cujo risco é aceitável e por isso não são imediatamente abordados

• Quais os elementos a serem mitigados e como o fazer

• Falsos positivos

• Assinalam situações que não são vulnerabilidades

• Analisadores de léxico (simbólica)

• Operam sobre as palavras geradas pelo scanner

• Não confundem getshow com função gets

**CodeQL**

• A análise de variantes é o processo de usar como modelo uma vulnerabilidade conhecida e procurar problemas semelhantes no código:

• Modelar o problema de segurança de maneira a poder ser aplicado a uma representação do programa

• Varrer a base de código procurando instâncias do problema de segurança modelado

• Adicionar o modelo a um repositório e usá-lo no processo de compilação da aplicação (integração contínua)

• O sistema CodeQL é uma linguagem e uma plataforma para automatizar a análise de variantes

**Predicados:** Um predicado permite colocar em evidência parte da interrogação

**Classes:** As classes em QL estendem um ou mais tipos, representam um conjunto de valores e definem predicados; A definição do corpo da classe consiste num predicado de característica (opcional) e num ou mais predicados membros

**Predicados:** Um predicado permite colocar em evidência parte da interrogação

Part3

**Trust**

• Is about how you use something.

• A system can be trusted if it always behaves in the expected manner for the intended purpose. Even when an attacker gains control of the system (it cannot misbehave).

• Users are given no guarantees that the trusted components will not breach their security policies.

**Trustworthy**

• Is about whether it is safe to use something.

• Users are asked to trust a set of components, and the security of the system is no longer guaranteed if any of its components are breached.

• Provides users with proof that its trusted components will not violate security.

Graphical user interface, text, application

Description automatically generatedDiagram

Description automatically generated

Diagram

Description automatically generated

Trusted Execution Environments (TEEs)

Diagram

Description automatically generated

**Inter-Environment Communication**

• Defines an interface allowing the TEE to communicate with the rest of the system.

• Has numerous benefits, but also introduces new threats

• Message overload attacks

• User and control data corruption attacks

• Memory faults caused by shared pages being removed

• Unbound waits caused by the noncooperation of the untrusted part of system.

• 3 key attributes should be satisfied

• Reliability (memory/time isolation)

• Minimum overhead (unnecessary data copies and context switches)

• Protection of communication structures.

**Secure Scheduling**

• Assures a “balanced” and “efficient” coordination between the TEE and the rest of

the system.

• It should assure that the tasks running in the TEE do not affect the responsiveness of the main OS.

• Often, the scheduler is designed preemptive!

• The scheduler should take real-time constraints into consideration.

**Secure Boot**

• Assures that only code of a certain property can be loaded

• If a modification is detected, the bootstrap process is interrupted

• Involves establishing a chain of trust and a RoT

**Secure Storage**

• Storage where confidentiality, integrity and freshness of stored data are guaranteed,

and where only authorized entities can access the data

• A common way to implement secure storage is sealed storage.

• Sealed storage is based on three components

• Integrity-protected secret key that can be accessed only by the TEE

• Cryptographic mechanisms, such as authenticated encryption algorithms

• Data rollback protection mechanism, such as replay-protected memory blocks (RPMB)

**Trusted I/O Path**

• Protects authenticity, and optionally confidentiality, of communication between the

TEE and the peripherals, enabling broader functionality within the TEE

• Allows a human user to directly interact with applications running inside the TEE

• 4 classes of attacks are considered

• Screen-capture attack

• Key logging attack

• Overlaying attack

• Phishing attack

Diagram

Description automatically generatedPart4

## Onde estamos vulneráveis? Qualquer equipamento que processe pacotes

Privacidade

• Esconde o tamanho da organização, sistemas e serviços

Mitigação de riscos

• Serviços expostos são vulneráveis a ataques

• Permite uma primeira linha de defesa em situações de necessidade de resposta a novos ataques

Registo

• Mantém um registo dos acessos para permitir a auditoria aos ataques

**Ataques podem ser:**

O software não faz sanitização dos dados

Quantidade de dados inesperada (overflow)/ quantidade excessiva de dados

Pode levar a que obtenham os privilégios de administrador

Perímetro e um ponto único de falha onde filtra pacotes e faz deteção de instruções pois faz analise dos pacotes.

Pode ser usado para entrar na organização através da VPN (VPN Gateway).

E preciso fazer a manutenção do perímetro, onde desenhar e configurar e fácil, mas os perímetros falham devido a falta de manutenção (atualizações, sistemas expostos e falta de alertas).

**O perímetro de rede** pode ser escondido utilizando **decoys**, estas escondem a firewall, escondem os serviços expostos, um servidor ativo parece estar desligado, mas não previnem ataques. Estas decoys podem quase sempre ser descobertas, mas obriga o atacante a ter mais trabalho e ajuda descoberta de endereços hostis.

**Exploração do perímetro:** **nmap**(Portscan, múltiplas técnicas de portscan, deteção de aplicações e sistemas operativos), **hping3**(Permite a manipulação dos pacotes enviados com maior detalhe, permite testar a performance da rede, Avaliar a implementação da pilha TCP/IP, Gerar ICMP Redirects, ou outros pacotes especializados)

## Redes virtuais privadas (VPNs) VPNS são redes privadas com linhas dedicadas, têm um custo elevado que esta dependente da sua distância. • Tempos elevados para instalação de novas ligações. • Os dados apenas são decifrados quando chegam ao outro extremo, circulando cifrados sobre a internet. • Adicionam latência extra. Acesso remoto pode ser Client-to-site (transporte) ou Site-to-site (Tunel). • Ligações subutilizadas exceto durante picos

## Tipos de VPNS:

## • IPSec (Norma promovida pelo IETF, suportada pela maioria dos dispositivos, Fornece integridade dos dados, confidencialidade e autenticação, Modo túnel (Dois cabeçalhos IP, um externo e um interno à VPN), Modo transporte (Entre dois dispositivos, Só um único cabeçalho IP) , Internet Key Exchange (Protocolo utilizado para negociar parâmetros da sessão, certificados, chaves partilhadas),

## • L2TP/IPSec (Implementado na maioria dos sistemas operativos, O L2TP sozinho não fornece cifra ou autenticação forte, daí aconjugação com o IPSec, Normalmente IPSec em modo de transporte, Inicialmente é IPSec com IKE e de seguida estabelece o L2TP sobre otúnel IPSec, adiciona um cabeçalho IP/UDP, Fornece um serviço L2, pode-se usar com outros protocolos que não oIP)

## • SSL (Em larga expansão devido à dispensa de um cliente pré-instalado, De implementação mais simples que o IPSec mas igualmente segura, Muito prática, do lado do cliente apenas é necessário um browser capaz de executar conteúdo ativo (Java, JavaScript, Flash ou ActiveX), Usam tecnologia Web para transportar os dados)

## • OpenSSL (Baseada em tecnologias de código aberto e utilização livre, Usa qualquer porto, bastante configurável, É necessário algum esforço na configuração)

## Análise de tráfego

Ferramentas como o **Wireshark** devido ao seu ambiente gráfico, e um analisador de pacotes a correr no pc. A captura só e possível se as tramas chegarem fisicamente ao host.

## Tipos de ataques:

• ARP Poisoning, • ARP cache flooding, • ICMP Redirect, • DHCP/DHCPv6 spoofing,

• WPAD (Web Proxy Auto Discovery).

Medidas de prevencao:

• ARP inspection(os switches controlam o conteúdo dos pacotes ARP)

• DHCP snooping (os switches controlam o conteúdo dos pacotes DHCP)

• Port security (Limitar o número de endereços MAC numa porta)

• ICMP redirects (Configurar os clientes para ignorarem ICMP redirects)

## Firewalls Resumo :

• **Filtragem estática**: • Cada pacote e analisado isoladamente, • Apenas e verificado os campos dos cabeçalhos dos pacotes, • Bom para condições absolutas **• Faz filtragem na entrada/saída ou ambos.**

## • Problemas Filtragem estática:• Não inspeciona o conteúdo dos pacotes, • causa problemas em protocolos complexos.

• **Filtragem dinâmica** (com estado): • Adiciona a capacidade de se lembrar dos pacotes para mais tarde tomar decisões, • Melhor controlo do tráfego, • Não tem a capacidade de analisar o conteúdo (Exceto alguns protocolos)

**Filtragem dinâmica** guarda o tráfego de saída, permitindo assim a resposta passar na firewall. Enquanto se um atacante tentar passar pela firewall, e se este não tiver o tráfego na tabela de estado nem com as regras existentes, e bloqueado.

Quando as ligações TCP terminam a entrada de estado da tabela e removida. O mesmo acontece se o contador expirar (UDP)(Remove da tabela).

Os Firewalls têm limitações: não existe nenhuma verificação do conteúdo, ataques as aplicações podem não ser detetados, VPNs podem ultrapassar as firewalls.

Deteção e prevenção de Intrusões

**(NIDS)Sistema de Deteção de Intrusões (Network Intrusion Detection Systems)**

• Observam todo o tráfego que circula • Procuram ataques potenciais • Normalmente baseados em “assinaturas” • Quando existe uma suspeita é despoletado um alarme • Não substituem as firewalls, políticas de segurança, atualização e hardening de sistemas • Não são ferramentas de baixa manutenção • Não servem para detetar todas as intrusões

**Implementação**

• Introduzido como um analisador de tráfego passivo em pontos de agregação

de tráfego • Faz a identificação de padrões a partir da base de dados de regras e suas assinaturas • As regras são aplicadas aos pacotes e eventos gerados quando uma regras é aplicável • As regras identificam:

• Protocolo, endereços, portos • Payload • Sequências de caracteres • Análise do fluxo de tráfego • Flags dos cabeçalhos • Qualquer campo no pacote

• Normalmente estabelece-se um quadro de referência para o tráfego

numa rede• A partir desse ponto é possível detetar situações anómalas • Permite a deteção de ataques que exploram vulnerabilidades 0-day • Os IDS podem também detetar variações inesperadas em protocolos que sejam conhecidos

**Sistema de Prevenção de Intrusões(Network Intrusion Prevention Systems) NIPS**

• Tenta prevenir os ataques, em vez de apenas os detetar • Fusão entre uma firewall e um IDS • Inspeção de pacotes baseada em estados

• Como nas firewalls dinâmicas • Nova versão de algo que já existe

• Existem algumas variantes que enviam TCP-Resets mas são consideradas piores que versões que atuam como uma bridge • Não substituem as firewalls, políticas de segurança, atualização e hardening de sistemas • Não são ferramentas de baixa manutenção

**Implementação**

• Normalmente introduzidos no perímetro da rede, antes ou depois de

uma firewall • Se for entre o operador e a firewall protegem os dispositivos colocados na DMZ • Se for atrás da firewall protege a rede interna dos utilizadores da VPN e pode ajudar a identificar dispositivos internos que tenham sido comprometidos • Requer especial atenção uma vez que os NIPS não são passivos e intercetam o tráfego • Requerem hardware de alta performance que permita reduzir o impacto na comutação de pacotes

**NIDS vs NIPS?**

• NIDS é mais neutro

• Os falsos positivos do NIDS são alertas errados

• Os falsos positivos do NIPS provocam quebras de conectividade

## • O NIDS é melhor quando? Os hosts fazem parte da política de segurança: Atualizados e protegidos

**•** O NIPS é melhor quando? **Os hosts não fazem parte da política de segurança•** Procuramos uma solução completa

**Problemas**: Falsos positivos

## Segurança WiFi: Wireless formas de autenticação/ cifra: WEP (descontinuada, algoritmo RC4, pode ser Open e é a forma mais segura ou Shared permite deduzir facilmente a chave através de iterações ao AP), WPA/WPA2(WPA2 usa cifra CCMP uma cifra robusta baseada em AES, pode ser WPA-Personal também conhecido por WPA-PSK(pre shared key) ou WPA-Enterprise também conhecido com WPA-802.1X com chaves dinamicas), WPS(WiFi Protected Setup) (facilita os utilizadores residenciais)

**Riscos de uma rede Wifi:** Eavesdropping (escuta), Masquerading (disfarce), Denial of Service (negação de serviço), Rogue access points (pontos de acesso maliciosos)

## zonas de segurança

## • Uma zona é um segmento único segregado • Segregar os ativos baseados no seu valor • Segregar os ativos baseados no seu grau de confiança • Valor mais elevado leva normalmente a maiores graus de confiança • Atribuir um grau de confiança a cada zona

**Estratégia a Nível da rede**: • Router de fronteira • Firewall dinâmica

**Nível do cabo**: • Filtragem ao nível da aplicação(proxies, SMPT gateway, NIPS) • Monitorização da camada de rede (NIDS, Pode fornecer alertas)

**Switching**: • Tomar atenção às zonas de fronteira (Switches físicos diferentes quando; VLANS em zonas com graus de confiabilidade próximos) • Não criar caminhos alternativos à volta de uma firewall ou filtro

**Virtualização:** • Todos as máquinas virtuais devem ser da mesma zona de segurança • Evitar hosts que atravessem multiplas zonas de segurança (colocar uma zona virtual atrás de uma zona melhora a segurança)• Permitir que o host monitorize as máquinas virtuais

**VPNs e Cifra:** • Evitar VPNs a terminar em sistemas • Cifra para dados em circulação • Cifra para dados armazenados

**Logging:** • Quando for colocado em produção é preciso pensar na manutenção a

longo prazo • Isolar o equipamento • Cifrar registos que atravessem zonas de baixo grau de segurança • Focar na qualidade e não na quantidade

**Regime jurídico**

• NIS (Network Information Security)

• Segurança das Redes de Informação (Directiva SRI)

• Garantir um elevado nível comum de segurança das redes e da informação em toda a União (2016/1148)

• Cibersegurança das redes e sistemas de operadores de: Serviços essenciais (Água, Banca, Energia, Infraestrutura digital, Mercado financeiro, Saúde, Transportes), Serviços digitais (Mercados online, Motores de pesquisa, Serviços de computação na nuvem)

• Equipas de resposta a incidentes de segurança informática a nível

nacional (CSIRT)

• Centro Nacional de Cibersegurança (autoridade nacional de cibersegurança)

• Grupos de coordenação internacional

• Para coordenação estratégica e troca de informações

• Cada Estado-Membro define a estratégia de segurança em conjunto com os operadores através de medidas políticas e regulamentares

• Cada Estado-Membro designa as autoridades nacionais competentes, os pontos de contacto únicos e os CSIRT nacionais (CERT.pt)

• Obriga à notificação de incidentes

• Aplicação de boas práticas

**Quais as principais diferenças entre um Quadro Normativo (por exemplo, o Quadro Nacional de Referência para a Ciber segurança) e um Regulamento (por exemplo, o Regulamento Geral da Proteção de Dados)?**

Ambos são um Conjunto de políticas e procedimentos que regulam a implementação e gestão contínua da segurança de uma organização.

A utilização de um quadro normativo e considerado as melhores práticas da indústria. Permite que as organizações tenham a informação organizada de acordo com os requisitos de conformidade e consigam comunicar utilizando o mesmo vocabulário.

O Quadro Nacional de Referência para a Ciber segurança representa um conjunto de passos que organizações devem seguir. O quadro normativo e orientado a gestão do risco pois e gerido por um ciclo de vida de processo continuo de identificação, diagnóstico e resposta.

O regulamento representa um conjunto de regras e leis que têm de ser cumpridas. Um regulamento e composto por artigos que especificam Direitos e obrigações que precisam de ser cumpridas por parte da empresa.

O Regulamento Geral da Proteção de Dados e uma regulação europeia sobre proteção de dados e privacidade, é a lei de privacidade e segurança mais

resistente(toughest) do mundo. Impõe obrigações as organizações desde que direcionem ou recolham dados relacionados com pessoas na UE.

**NIST – National Institute of Standards and Technology**

**Cyber Security Framework**

• Encorajado pelo NIST a ser aplicado em organizações privadas e infraestruturas críticas

• Processo de 7 passos

• Prioridades e âmbito

• Orientação

• Perfil atual

• Levantamento de riscos

• Perfil alvo

• Determinar, analisar e priorizar lacunas

• Implementar um plano de ação

• Não considera a certificação

• Os controlos usados podem vir de outro quadro normativo: ISO 27000 por exemplo

**Risk Management Framework**

• Quadro normativo de gestão de risco

• Define a segurança de informação dos sistemas de informação desde a sua

conceção

• Foca-se na definição de controlos de segurança e na sua implementação

• Processo para atingir a segurança dos sistemas de informação:

• Categorização de segurança, baseada em análises de impacto

• Seleção dos controlos de segurança

• Implementação dos mecanismos de controlo

• Avaliação dos controlos

• Autorização do sistema de informação (para funcionamento)

• Monitorização dos controlos de segurança