Part1

Citala espartana

texto limpo: acitalaeumsistemadecifrausadonaantigagrecia

distribuição dos caracteres na cítala:

a c i t a l a e u
m s i s t e m a d
e c i f r a u s a
d o n a a n t i g
a g r e c i a

texto cifrado:
AMEDACSCOGIIINRTSFAEATRACLEANIAMUTAEASIUDAG

Vinaigrette

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Alberti cifer

$\mathcal{A} = \{A, B, C, D, E, F, G, I, L, M, N, O, P, Q, R, S, T, V, X, Z, 1, 2, 3, 4\}$,

$\mathcal{A}' = \{a, b, c, d, e, f, g, h, i, k, l, m, n, o, p, q, r, s, t, v, y, x, z, \&\}$

Bellaso-Vigen`ere

Key: "BELLASO"

Chave :	B	E	L	L	A	S	O	B	E	L	L	A	S	O	B
Texto limpo :	a	c	i	f	r	a	d	e	b	e	l	l	a	s	o
Texto cifrado :	B	G	T	Q	R	S	R	R	F	F	W	L	S	G	P

modo ECB - Electronic CodeBook Mode;

modo CBC - Cipher Block Chaining Mode;

$$\begin{aligned} m &= m_0 m_1 \cdots m_r \\ c_0 &= e_K(m_0 \oplus IV) \\ c_i &= e_K(m_i \oplus c_{i-1}),\ i \geq 1 \\ c &= c_0 c_1 \ldots c_r \end{aligned}$$

modo OFB - Output Feedback Mode;

modo CFB - Cipher FeedBack Mode;
modo CTR - Counter Mode.

$$\begin{aligned} m &= m_0 m_1 \cdots m_r \\ c_i &= m_i \oplus e_K(IV + i) \\ c &= c_0 c_1 \ldots c_r \end{aligned}$$

Padding
OneAndZeros -> primeiro valor 1 (80 em hex) e resto é 0
Trailing Bit Complement -> complementa com o bit oposto

Euler

1. Se p é um número primo, então $\phi(p) = p - 1$;
2. Se p é um número primo, então $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$;
3. Se n e m são dois inteiros positivos primos entre sim, então

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$$

Em particular $a^{-1} \equiv a^{\phi(n)-1} (\bmod n)$

Teorema RSA
N=p*q

$$\phi(n) = (p-1)(q-1).$$

1. É calculado $\phi = \phi(n) = (p-1)(q-1)$ e escolhido $e \in \mathbf{Z}_\phi^*$;
2. É calculado $d = e^{-1} (\bmod \phi)$ e são destruídos os valores p, q, ϕ;
3. A chave pública é $k =< n, e >$, a chave privada é $K =< n, d >$

Encriptar -> rsa(x) = x^e * mod(n)
Desencriptar -> rsa^–1(y) = y^d * mod(n)

Cifra ElGamal

1. É calculado α um gerador do grupo multiplicativo $\mathbf{Z}_p^*$
2. É escolhido aleatoriamente um inteiro a, $2 \leq a \leq p-2$, e calculado $\alpha^a \bmod p$.
3. A chave pública é $k =< p, \alpha, \alpha^a >$, a chave privada é $K =< p, a >$

- Cifragem (com a chave pública):
  Para cifrar $x \in \mathbf{Z}_p^*$, é escolhido aleatoriamente r (**chave efímera**) tal que $2 \leq r \leq p-2$, e calculados

$$y = \alpha^r (\bmod p) \quad \text{e} \quad z = x \cdot (\alpha^a)^r (\bmod p)$$

  A encriptação de x é definida então por

$$\text{elgam}(x) = (y, z)$$

- Descifragem (com a chave privada) de um par (y, z), com $y, z \in \mathbf{Z}_p^*$:

$$\text{elgam}^{-1}(y, z) = (y^{-a})\, z (\bmod p)$$

Efectivamente, se $(y, z) = (\alpha^r (\bmod p), x \cdot (\alpha^a)^r (\bmod p))$ então

$$\begin{aligned} \text{elgam}^{-1}(y, z) &= (y^{-a})\, z (\bmod p) \\ &= (\alpha^r)^{-a} \cdot x \cdot (\alpha^a)^r (\bmod p) \\ &= x (\bmod p) \end{aligned}$$

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

Ordem	Fase	Descrição
1	**Reconhecimento** (*Reconnaissance*)	Procurar, identificar e selecionar os alvos.
2	**Armar** (*Weaponization*)	Ligação do malware com o payload que permite afetar o sistema alvo. Ex: Colocar em ficheiros PDF ou Word o código de ataque.
3	**Entrega** (*Delivery*)	Transmissão da "arma" para o alvo (Ex: Anexos email, Pen USB, Web sites visitados pelos alvos)
4	**Exploração** (*Exploitation*)	Uma vez entregue, a "arma" é ativada executando o código do atacante, explorando a superfície de ataque (sistema operativo, aplicações, utilizador, ...)
5	**Instalação** (*Installation*)	A "arma" instala um *backdoor* no sistema alvo, permitindo o acesso permanente ao mesmo
6	**Comando e controlo** (*Command & Control*)	A partir do exterior da organização passa a haver acesso aos sistemas dentro da rede alvo
7	**Ações para o objetivo** (*Actions on Objective*)	O atacante tenta atingir os seus objetivos, os quais podem incluir roubo e destruição de dados ou intrusão em outros alvos

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

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
- 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

Varredores de vulnerabilidades

Fuzzers and attack injectors look for unknown vulnerabilities
- Vulnerability scanners look for known vulnerabilities
- Run through vulnerability database
- inject attacks

They monitor the effect on the application trying to detect if it contains the vulnerability

General requirements of a web vulnerability scanner
- Identify specific sets of vulnerabilities present in public databases
- Generate report for each vulnerability
- Have an acceptable false positive rate

Proxies
Intersection of requests and responses

HTTPS connections must be transparently intersected with authorized man-in-the-middle

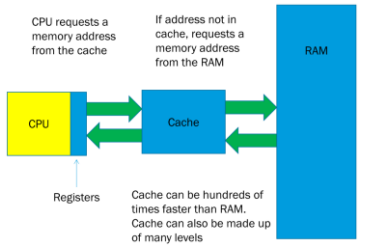
ZAP – operation modes
Passive – passively analyzes all requests passing through it or generated by crawling components
Active – actively tries to find vulnerabilities using known attacks on selected targets
- Attacks the website using known techniques to find vulnerabilities
- This mode modifies data and may insert malicious scripts on the website.
- You can only run this mode for sites that we have testing permission for.

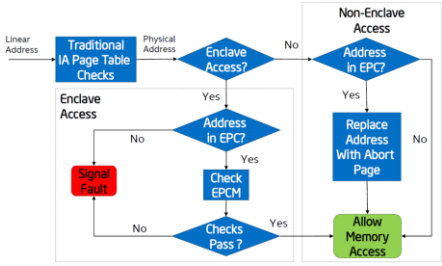
Part3

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.

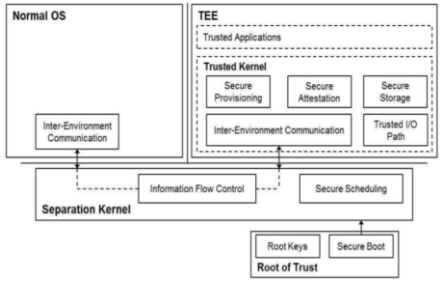
Trustworthy
- Is about whether it is safe to use something.
- Users are asked to trust a set of components, and the security of the system is no longer guaranteed if any of its components are breached.
- Provides users with proof that its trusted components will not violate security.

Example Side Channel
- Timing
- CPU Cache
- Power Usage
- Electromagnetic field
- Acoustic
- Thermal
- Speculation





Trusted Execution Environments (TEEs)



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

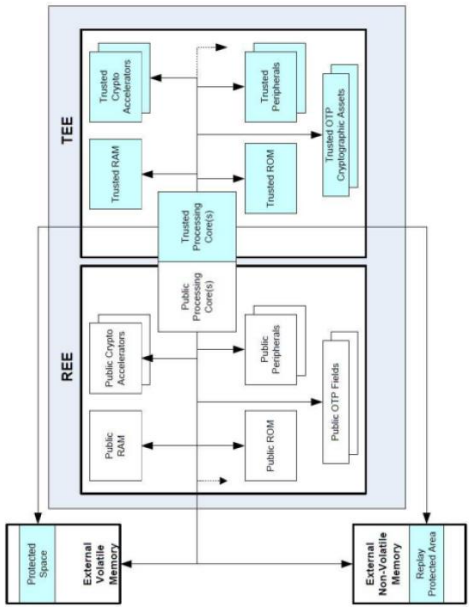
• Assures that only code of a certain property can be loaded
• If a modification is detected, the bootstrap process is interrupted
• Involves establishing a chain of trust and a RoT

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



Part4

Modulo 4 Segurança do perímetro da rede

Onde estamos vulneráveis?

Qualquer equipamento que processe pacotes

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).

Técnicas de ataque:

• ARP poisoning• ARP table flooding e ICMP redirect

• Port scanning, ataques a partir de terceiros (proxies abertos na Internet) …

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…

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. 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).

Tipos de VPNS: IPSec, L2TP/IPSec, SSL, OpenSSL

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,

• IPv6 Neighbour Advertisement/SLAAC spoof, • 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

• **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)

Firewalls Problemas da **filtragem estática**: • Não inspeciona o conteúdo dos pacotes, • causa problemas em protocolos complexos. • Faz filtragem na entrada, • filtragem na saída ou ambos.

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 • 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

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

Tenta prevenir os ataques, em vez de apenas os detetar

Fusão entre uma firewall e um IDS

Não substituem as firewalls, políticas de segurança, atualização e hardening de sistemas

Não são ferramentas de baixa manutenção

Resumo NIDS e NIPS

• O NIDS e o NIPS fazem deteção de intrusões a partir de padrões/assinaturas• Tanto os cabeçalhos como o conteúdo dos pacotes podem ser Analisados• NIPS é uma firewall dinâmica com uma base de dados de padrões/assinaturas • Na aquisição de um destes produtos é obrigatório exigir a linguagem das assinaturas e o conteúdo destas (• Para corrigir falsos positivos, • Para otimizar o dispositivo para o ambiente local)

Qual a diferença entre um Sistema de Deteção de Intrusões e um Sistema de Prevenção de Intrusões?

• 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

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)

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.