Segurança Informática e nas Organizações - Resumos 2

José Mendes 107188

2023/2024

1 Criptografia Assimétrica

1.1 Criptografia Assimétrica (de blocos)

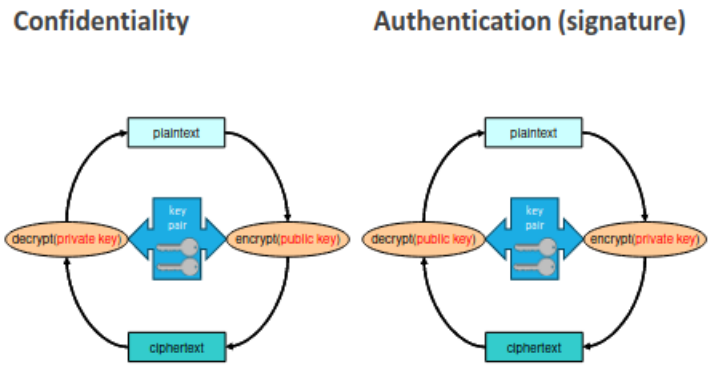
Usa um par de chaves:

- **Chave privada:** pessoal, não transmissível;
- **Chave pública:** disponível a todos;

Permite:

- Confidencialidade sem qualquer exchange of secrets prévia;
- Autenticação
  - De conteúdos (integridade dos dados);
  - De origem (atenticação da source, ou assinatura digital);

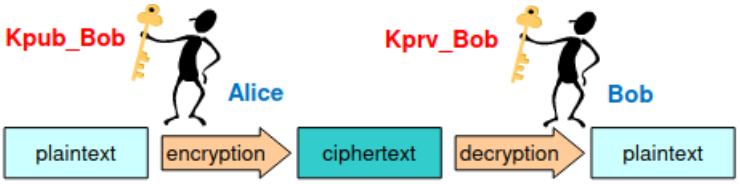
1.2 Operaçõees de uma Cifra Assimétrica



1.3 Use Cases: Comunicação Segura

Comunicação segura com um target (Bob)

- A Alice encrípta o plaintext **P** com a chave pública do Bob, **Kpub_Bob**
  - **Alice:** $C = \{P\}_{kpub\_bob}$
- O Bob decifra o ciphertext **C** com a sua chave privada, **Kpriv_Bob**
  - **Bob:** $P' = \{C\}_{kpriv\_bob}$
- P' deve ser igual a **P** (é necessário verificar)
- **Kpub_Bob** precisa de ser conhecida pela Alice



1.4 Cifras Assimétricas

Vantagens:

- São um mecânismo de autenticação fundamental;
- Permitem explorar caracteristicas que não são possíveis com cifras simétricas;

Desvantagens:

- Performance;
- Normalmente não são muito eficientes e consomem muita memória;

Problemas:

- Distribuição confiável de chaves públicas;
- O lifetime do par de chaves é limitado;

Abordagens: problemas matemáticos complexos

- Logaritmos discretos de números grandes;
- Factorização inteira de números grandes;

Algoritmos mais comuns:

- RSA;
- ElGamal;
- Eliptic Curves (ECC);

Outras tecnicas com pares assimétricos de chaves:

- Diffie-Hellman (key agreement);

1.5 RSA (Rivest, Shamir, Adelman, 1978)

Chaves:

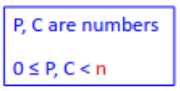
- **Privada:** (d, n)
- **Pública:** (e, n)

Encriptação da chave pública (confidencialidade)

- $C = P^e \mod n$
- $P = C^d \mod n$

Encriptação da chave privada (assinatura)

- $C = P^d \mod n$
- $P = C^e \mod n$



Complexidade Computacional

- Logaritmo discreto;
- Factorização inteira;

Seleção de Chaves

- **n** grande (centenas ou milhares de bits);
- $n = p \times q$ com **p** e **q** sendo números primos grandes (secretos);
- Escolher um **e** co-primo de $(p-1) \times (q-1)$;
- Computar **d** tal que $e \times d \equiv 1 \pmod{(p-1) \times (q-1)}$;
- Discartar **p** e **q**;
- O valor de **d** não pode ser facilmente computado a partir de **e** e **n** (apenas de **p** e **q**);

1.5.1 RSA - Exemplo

p = 5 q = 11 **(prime numbers)**

- n = p x q = 55
- (p-1) x (q-1) = 40

e = 3 **(public key = e, n)**

- Coprime of 40

d = 27 **(private key = d, n)**

- e x d ≡ 1 (mod 40) → d x e mod 40 = 1, (27 x 3) mod 40 = 1

For P = 26 **(notice that P, C∈ [0, n-1])**

- $C = P^e \bmod n = 26^3 \bmod 55 = 31$
- $P = C^d \bmod n = 31^{27} \bmod 55 = 26$

1.6 Encriptação Hibrida

Mistura criptografia simétrica com assimétrica

- Usa o melhor dos dois mundos, evitando os problemas;
- Cifra assimétrica: usa chaves públicas (mas é lenta);
- Cifra simétrica: Rápida (mas com métodos fracos de troca de chaves);

Método

- Obtém K_{pub} do destinatário;
- Gera uma chave simétrica aleatória K_{sym};
- Calcula $C1 = E_{sym}(K_{sym}, P)$;
- Calcula $C2 = E_{asym}(K_{pub}, K_{sym})$;
- Envia $C1 + C2$;
  - $C1$ é o texto encriptado com a chave simétrica;
  - $C2$ é a chave simétrica encriptada com a chave pública do destinatário (pode também conter um IV);

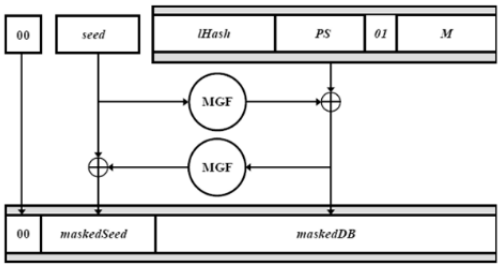
1.7 Randomização de encriptações assimétricas

Resultado de encriptações assimétricas não deterministico (não é previsível)

- **N** encriptações do mesmo valor, com a mesma chave, deve produzir **N** resultados diferentes;
- **Objetivo:** Previnir a descoberta de valores encriptados através de tentativa e erro;

Abordagens: Concatenação de um valor a encriptar com dois valores, um fixo (para controlo de integridade) e outro aleatório (para randomização);

1.7.1 OAEP (Optimal Asymmetric Encryption Padding)



lHash: digest over **Label**

seed: random

PS: zeros

M: plaintext

MGF: Mask Generation Function

- Similar to Hash, but with variable size

1.8 Diffie-Hellman Key Agreement (1976)

q (large prime)
α (primitive root mod q)

a = random

$Y_a = \alpha^a \bmod q$

$K_{ab} = Y_b^a \bmod q$

Y_a

Y_b

b = random

$Y_b = \alpha^b \bmod q$

$K_{ba} = Y_a^b \bmod q$

$K_{ab} = K_{ba}$

1.8.1 DH Key Agreement: MitM Attack

a = random

$Y_a = \alpha^a \bmod q$

$K_{ac} = Y_c^a \bmod q$

Y_a

Y_c

c = random

$Y_c = \alpha^c \bmod q$

$K_{ca} = Y_a^c \bmod q$

$K_{cb} = Y_b^c \bmod q$

Y_b

Y_c

b = random

$Y_b = \alpha^b \bmod q$

$K_{bc} = Y_c^b \bmod q$

1.9 Eliptic Curve Cryptography (ECC)

Curvas elipticas são funções específicas

- Têm um gerador **G**;
- Uma chave privada K_{priv}, é um inteiro com um máximo de bits permitidos pela curva;
- Uma chave pública K_{pub}, é um ponto $(x, y) = K_{priv} \times G$
- Dada K_{pub}, deve ser computacionalmente dificil determinar K_{priv};

Curves

- NIST curves (15)
  - P-192, P-224, P-256, P-384, P-521
  - B-163, B-233, B-283, B-409, B-571
  - K-163, K-233, K-283, K-409, K-571

Other curves

- Curve25519 (256 bits)
- Curve448 (448 bits)

1.10 ECDH: DH com ECC

ECC curve → G

a = random

$Y_a = a\ G$

$K_{ab} = a\ Y_b$

Y_a

Y_b

b = random

$Y_b = b\ G$

$K_{ba} = b\ Y_a$

$K_{ab} = K_{ba}$

1.11 Encriptação de chave pública com ECC

Mistura encriptação hibrida com EDHC

Método

- Obtém K_{pub_recv} do destinatário;
- Gera um random K_{priv_send} com um correspondente K_{pub_send};
- Calcula $K_{sym} = K_{priv\_send} \times K_{pub\_recv}$;
- $C = E(P, K_{sym})$;
- Envia $C + K_{pub\_send}$;
- Destinatário calcula $K_{sym} = K_{pub\_send} \times K_{priv\_recv}$;
- $P = D(C, K_{sym})$;

2 Assinaturas digitais

2.1 Cifras Assimétricas (de blocos)

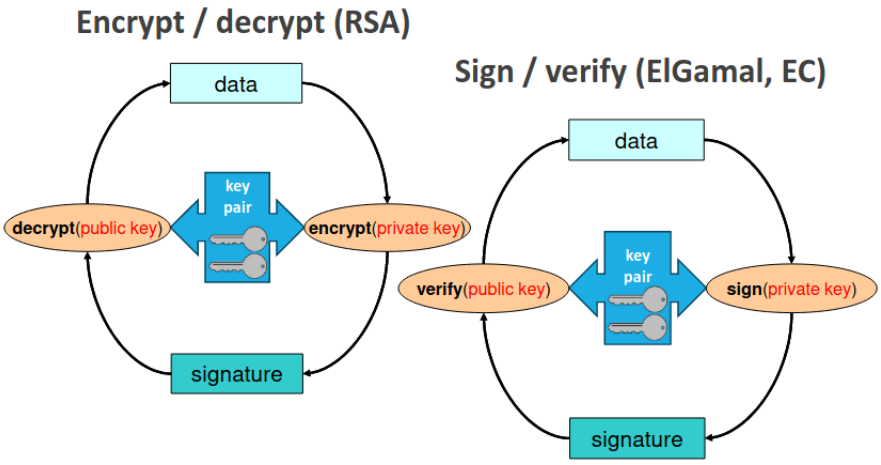
Usa pares de chaves:

- Uma **chave privada** (pessoal, não transmissível);
- Uma **chave pública** (disponível a todos);

Permite:

- Confidencialidade sem qualquer exchange of secrets prévia;
- Autenticação
  - De conteúdos (integridade dos dados);
  - De origem (atenticação da source, ou assinatura digital);

2.2 Assinaturas Digitais



Autenticação de conteúdos de um documento - Garante a sua integridade (não se alterou);

Autenticação do autor - Garante que a identidade do criador/origem;

Previnir repudiação de assinaturas

- Non-repudiation (o autor não pode negar a autoria);
- Autores genuínos não podem negar a autoria (apenas a identidade do autor pode gerar uma dada assinatura);

Abordagens

- Encriptação/Decifração assimétrica ou assinatura/verificação;
- Funções digest (apenas para performance);

$$\text{Signing: } A_x(\text{doc}) = \text{info} + E(K_x^{-1}, \text{digest}(\text{doc} + \text{info}))$$

$$A_x(\text{doc}) = \text{info} + S(K_x^{-1}, \text{digest}(\text{doc} + \text{info}))$$

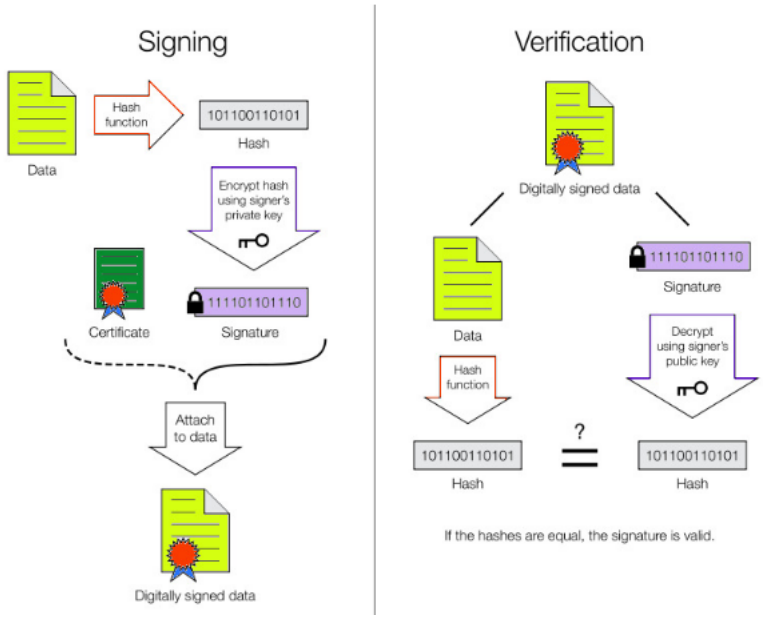
$$\text{info} = \text{signing context, signer identity, } K_x$$

$$\text{Verification:}$$

$$D(K_x, A_x(\text{doc})) \equiv \text{digest}(\text{doc} + \text{info})$$

$$V(K_x, A_x(\text{doc}), \text{doc}, \text{info}) \rightarrow \text{True / False}$$

2.2.1 Encriptação/Decifração signatures



2.2.2 Assinatura digital num email: Multipart content, signature w/ certificate

```
From - Fri Oct 02 15:37:14 2009
[…]
Date: Fri, 02 Oct 2009 15:35:55 +0100
From: =?ISO-8859-1?Q?Andr=E9_Z=FAquete?= <andre.zuquete@ua.pt>
Reply-To: andre.zuquete@ua.pt
Organization: IEETA / UA
MIME-Version: 1.0
To: =?ISO-8859-1?Q?Andr=E9_Z=FAquete?= <andre.zuquete@ua.pt>
Subject: Teste
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1; boundary="------------ms050405070101010502050101"

This is a cryptographically signed message in MIME format.

--------------ms050405070101010502050101
Content-Type: multipart/mixed;
 boundary="------------060802050708070409030504"

This is a multi-part message in MIME format.
--------------060802050708070409030504
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

Corpo do mail

--------------060802050708070409030504-
--------------ms050405070101010502050101
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIamTCC
BUkwggSyoAMCAQICBAcnIaEwDQYJKoZIhvcNAQEFBQAwdTELMAkGA1UEBhMCVVMxGDAWBgNV
[…]
KoZIhvcNAQEBBQAEgYCofks852BV77NVuww53vSxO1XtI2JhC1CDlu+tcTPoMD1wq5dc5v40
Tgsaw0N8dqgVLk8aC/CdGMbRBu+J1LKrcVZa+khnjjtB66HhDRLrjmEGDNttrEjbqvpd2QO2
vxB3iPTlU+vCGXo47e6GyRydqTpbq0r49Zqmx+IJ6Z7iigAAAAAAAA==
--------------ms050405070101010502050101--
```

3 Derivação de chaves

Algotitmos de cifras requerem chaves de tamanho fixo - 56, 128, 256,... bits;

Podemos derivar chaves de múltiplas origens- shared secrets, passwords geradas por humanos, PIN codes e secrets de tamanho pequeno;

Origem original pode ter baixa entropia - reduz a dificuldade de ataques de força bruta, no entanto, devemos ter uma relação forte para uma chave útil;

Por vezes percisamos de múltiplas chaves do mesmo material - enquanto não permite encontrar o material (a password, outra chave) de uma chave nova;

3.1 Prepósitos de derivação de chaves

Refroço de chaves: aumenta a segurança de uma password

- Nomralmente definido por humanos;
- Tornando ataques de dicionário nada práticos;

Expansão de chaves: aumenta o tamanho de uma chave

- Expande o tamanho que serve o algoritmo;
- Eventualmente deriva outras chaves relacionadas para outros algoritmos (ex: MAC);

3.2 Derivação de chaves

Derivação de chaves requer a existência de:

- Um **salt** que trona a derivação única;
- Um problema difícil;
- Um nível de complexidade escolhido;

Dificuldade de Computação

- A transformação requer recursos computacionais relevantes;

Dificuldade de Memória

- A transformação requer recursos de armazenamento relevantes;
- Limita os ataques usando aceleração de hardware;

3.3 Derivação de chaves: PKBDF2

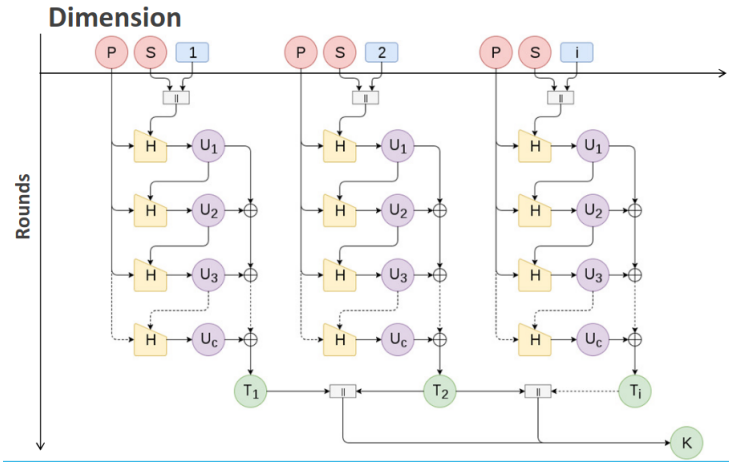
Password Based Key Derivation Function 2

Produz uma chave a partir de uma password, com uma dificuldade escolhida

$$K = PBKDF2(PRF, Salt, rounds, dim, password)$$

- **PRF** - Pseudo-Random-Function: função digest;
- **Salt** - Valor aleatório;
- **Rounds** - O custo computacional (dezenas ou centenas de milhares);
- **Dim** - Tamanho do resultado pretendido;

Operação: calcula operações ROUNDS x DIM a partir do PRF utilizando o SALT e a PASSWORD - um tamanho maior de rounds aumenta a custo;

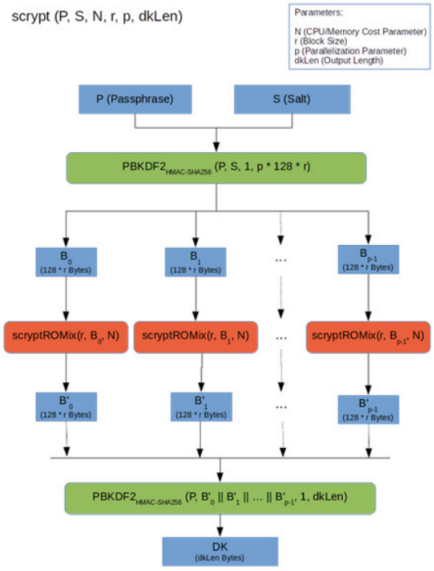


3.4 Derivação de chaves: Scrypt

Produz uma chave com um custo de armazenamento escolhido

$$K = scrypt(password, salt, n, p, dim, r, hLen, Mflen)$$

- **Password** - Um segredo;
- **Salt** - Valor aleatório;
- **n** - Parâmetro de custo;
- **p** - Parâmetro de paralelismo $p \leq (2^{32} - 1) \times hLen/Mflen$;
- **dim** - Tamanho do resultado pretendido;
- **r** - Tamanho do bloco a usar (default: 8);
- **hLen** - Tamanho do da função digest (32 para SHA256);
- **Mflen** - Bytes na internal mix (default: $8 \times r$);



4 Gestão de chaves assimétricas

4.1 Problemas a resolver

Garante um uso correto do par de chaves assimétricas

- **Privacidade das chaves privadas**
  - Garante a autenticidade;
  - Previne a repudiação de assinaturas digitais;
- **Distribuição correta de chaves públicas**
  - Garante confidencialidade;
  - Garante a correta validação de assinaturas digitais;

Evolução temporal da entidade $\longleftrightarrow$ mapeamento de pares chave

- **Para combater ocurrência catastróficas** (ex: perda de chaves privadas)
- **Para combater os requisitos de exploitations normais** (ex: refresh do par de chaves para reduzir riscos personificação)

Garante a correta geração de pares de chaves

- **Geração aleatória de valores secretos**, de forma a poderem ser facilmente previstos;
- **Aumentar a eficiência sem reduzir a segurança**
  - Tornar mecânismos de segurança mais eficientes;
  - Aumentar a performance;

4.2 Objetivos

- **Geração do par de chaves** - quando e como gerar;
- **Lidar com a chave privada** - como manter a chave privada;
- **Distribuição da chave pública** - como ditribuir corretamente as chaves públicas world-wide;
- **Tempo de vida do par de chaves** - quando vão expirar, até quando as usar e como verificar se esse par de chaves está obsuleto;

4.3 Geração de pares de chaves: Principais Designs

Usar bons geradores de números aleatórios para produzir segredos

O resultado é indestinguível de noise, isto é, todos os valores possíveis são igualmente prováveis e, não existem padrões resultantes do número da iteração ou de valores prévios;

Exemplo: Bernoulli 1/2 Generator

- Gerador sem memória;
- $P(b = 1) = P(b = 0) = 1/2$;
- Coin toss (atirar uma moeda ao ar);

Facilidade sem comprometer a segurança

Chaves públicas eficientes

- Algumas são 1 bits, tipicamente $2k + 1$ valores (3, 17, 65537);
- Acelerar o processo com chaves públicas (o custo é proporcional ao número de bits 1);
- Sem security issues;

Self-generation de chaves privadas

Maximiza a privacidade, uma vez que outros nunca vão conseguir usar a dada chave privada. Apenas o dono tem a chave, melhor ainda, o dono não tem a chave, mas pode usá-la;

Principio pode ser relaxado quando não involve a geração de assinaturas. Quando não existem issues relacionados com non-repudiation.

4.4 Lidar com chaves privadas

- **Correctness**
  - **A chave privada representa o sujeito** (i.e., um cidadão, um servidor, etc.). O seu compromise deve ser minimizado. Cópias físicas seguras (backups) podem existir em alguns casos;
  - **O caminho de acesso à chave privada deve ser controlado**. Proteção de acesso com password ou PIN code. Correctness das aplicações que usam;
- **Confinement**
  - **Proteção da chave privada dentro de um domínio seguro (reduzido) (ex: cryptographic token)**. O Token gera pares de chaves, exporta a chave pública mas nunca a privada, e, este Token encripta/decifra internamente com a chave privada.
  - **Exemplo: SmartCards**, podemos pedir ao cartão para cifrar/decifrar algo. A chave privada nunca sai do SmartCard.

4.5 Distribuição de chaves públicas

Distribuição a todos os senders de dados confidenciais. Processo manual, usando um shared secret. Ad-hoc usando certificados digitais;

Distribuição a todos os receivers de assinaturas digitais. Processo manual. Ad-hoc usando certificados digitais;

4.5.1 Problema

Como garantir a Correctness de uma chave pública?

Disseminação confiável de chaves públicas - Paths/Graphs confiáveis. Se **A confia em** K_X^+ e **B confia em A**, então **B confia em** K_X^+.

Hierarquias de certificação/grafos com as relações de confiança expressas entre entidades. Certificação é unidirecional!

4.6 Public key (digital) certificates

É um **documento digital issued por uma autoridade de certificação (CA)**

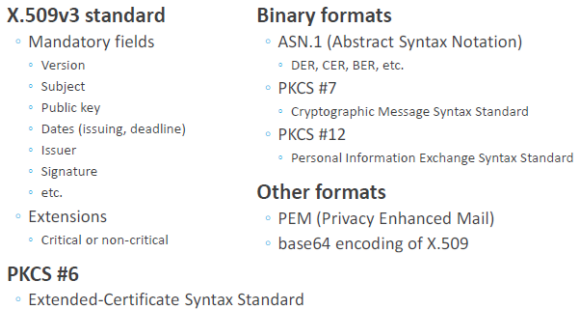
- **Liga a chave pública a uma entidade** (ex: pessoa, servidor ou serviço);
- **São documentos públicos**, não contêm informação privada, apenas pública. Pode ter informação adicional (ex: URL, nome, email, etc.);
- **São seguros criptograficamente**, digitalmente assinados pelo issuer, não podem ser alterados;

Pode ser usado para ditribuir chaves públicas de uma forma confiável

O certificate receiver pode ser validade de várias formas

- Com a chave pública do CA;
- Pode também validar a identificação;
- Validar a validade;
- Validar se a chave está a ser usada para o propósito correto;

O certificate receiver confia no comportamento do CA, pelo que confia os documentos que este assina. Quando o CA associa um certificado a A, se o receicer confiar no CA, então confia que a associação de A é correta.



4.7 Key pair usage

O certificado publico conecta o par de chaves a um perfil de utilização. As chaves privadas raramente são multifuncionais.

Perfil de utilização tipico

- Autenticação/distribuição de chaves (Digital signature, Key encipherment, Data encipherment, Key agreement)
- Assinar documentos (Assinatura digital não repudiável)
- Certificate issuing (exclusivo de CAs). Assinar certificados, assinar CRLs (Certificate Revocation Lists)
- Timestamping (exclusivo de Time Stamping Authorities TSAs)

Certificados de chaves públicas têm uma extensão para isto, key usage (critical) que indica o perfil de utilização da chave pública.

4.8 Assinatura de Certificados (CA)

Organizações que gerem certificados de chaves públicas. Companhias, não por lucro, governamentais, etc.;

Define politicas e mecanismos para:

- Issuing de certificados;
- Revoking de certificados;
- Distribuição de certificados;
- Issuing e distribuição das correspondentes chaves privadas;

Gerir a lista de certificados revogados (CRLs), interfaces programaticas para verificar o estado atual de um certificado;

4.9 Trusted Certification Authorities

CAs intermediários - CAs certificados por outras CAs confiaveis. Usando um certificado, permitindo a criação de uma hierarquia de certificação;

Anchor confiavel (ou root CA) - Um tem uma chave pública confiavel, normalmente implementada por certificados self-certified, ou seja, issuer e subject são o mesmo. Distribuição manual (ex: dentro do código do browser, OS, distribuição, etc.).

Ver Exemplo de certificado nos slides 19-23.

4.10 Refreshing of asymmetric key pairs

O par de chaves deve ter um tempo de vida limitado - uma vez que, as chaves privadas podem ser perdidas ou descobertas, e para implementar uma politica de update;

Problema - Os certificados podem ser copiados e distribuidos. O universo de donos de certificados é desconhecido, pelo que, não podemos contactá-los para eliminar certificas específicos;

Solução - Certificados com um periodo de validade (nem antes, nem depois). Listas de certificados revogados, para revogar certificados antes da validade expirar;

4.11 Certificate Revocation Lists (CRLs)

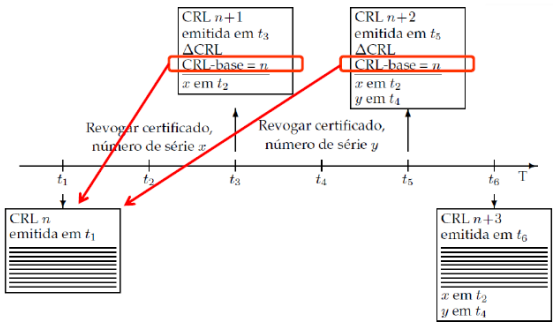
Base ou delta - Completa / diferenças

Listas de certificados assinados (identifiers) prematuramente invalidados

- Devem ser regularmente visitado por donos de certificados
- Protocolo OCSP para verificar a validade de um certificado (RFC 2560)
- Pode dizer a razão da revogação (slide 31)

Publicação e distribuição de CRLs - Cada CA mantém a sua CRL e permite o acesso publico da mesma.

4.12 CRL e Delta CRL



4.13 Online Certificate Status Protocol (OCSP)

Protocolo baseado em HTTP para dar assert ao estado de um certificado

- **Request** - Inclui o serial number do certificado;
- **Response** - Inclui se o certificado está revoked, é enviado pela CA e não possui validade;
- Uma verificação por certificado;

Requer menor largura de banda para clientes - uma verificação por certificado em vez que fazer download de uma lista de certificados revogados (CRL);

Involve maior largura de bannda para CAs - uma verificação por certificado, problemas de privacidade uma vez que um CA saberá que um certificado está a ser usado;

OOCSP stapling - Inclui um timestamp recentemente assinado na resposta do servidor para dar assert à validade. Reduz a demora da verificação e carregamento no CA. Previne problemas de privacidade.

4.14 Distribuição de certificados de chaves públicas

Transparente (integrado com sistemas ou aplicações)

- Direcory systems, larga escala (ex: X.500 através de LDAP), organizacional (ex: Windows 2000 Active Directory), etc.;
- On-line: sem protocolos que usam certificados para autenticação peer (ex: protocolos de comunicação segura (TLS, IPSec, etc.), assinaturas digitais, dentro de MIME mail messages ou dentro de documentos);

Explicito (voluntáriamente ativado pelos users)

- User faz request de um serviço para obter um certificado necessário (ex: pedido mandado por email, acesso a uma página HTTP pessoal).

4.15 PKI (Public Key Infrastructure)

Infrastrutura para permitir um uso correto de chaves assimétricas e de certificados de chave pública.

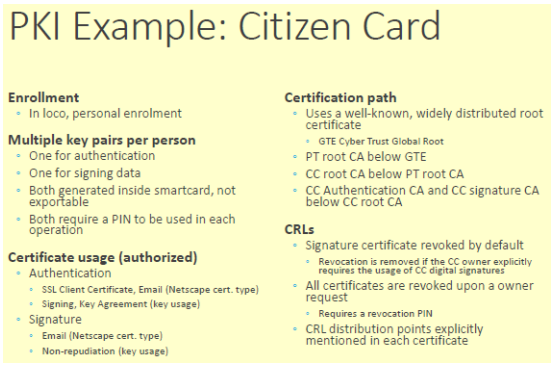
Criação do par de chaves assimétricas para cada entidade que participa. Politicas de participação, ploiticas de geração do par de chaves.

Criação e distribuição de certificados de chaves públicas. Politicas de participação, definição de atributos de certificados.

Definição e uso de certification chains (ou paths). Inserção numa hierarquia de certificação, certificação de outros CAs.

Atualização, publicação e consulta de CRLs. Politicas de revogação de certificados, serviços de distribuição de CRL, serviços OCSP.

Usa estruturas de dados e protocolos permitindo inter-operabilidade entre componentes/serviços/pessoas.



4.16 Certificate Pinning

Se um atacante tem acesso a uma Root confiavel, pode fingir ser qualquer entidade. Manipula um CA confiavel em dar issue ao certificado (pouco provável). Injetar um CA costumizado na base de dados da vitima (mais provável).

Certificate Pinning: adiciona a fingerprint do PubK (public key) ao código fonte. A fingerprint é uma hash (ex: SHA256).

Validação do processo: O certificado deve ser válido a regras locais, deve possuir uma chave pública com a dada fingerprint.

4.17 Certificate Transparency (RFC 6962)

Problemas

- CAs podem ser comprometidos (ex: DigiNotar) por atacantes, governo, etc.
- Comprometer é dificil de detetar. Resulta na mudança de suposições associadas com o comportamento do CA. O proprietário saberá sozinho.

Definição: um sistema global que regista todas as informações sobre certificados públicos criados

- Garante que apenas um certificado tem as roots corretas;
- Guarda a chain de certificados inteira para cada certificado;
- Apresenta esta informação para auditoria (organizações ou ad-hoc por end users);

5 Mecanismos e Protocolos de Autenticação

5.1 Autenticação (Authn)

Prova de que uma entidade tem um atributo que diz ter

5.2 Authn: Tipos de Prova

- **Algo que a entidade sabe**: Um segredo memorizado (ou escrito . . .);
- **Algo que a entidade tem**: Um objeto/token apenas possuído pela entidade;
- **Algo que a entidade é**: A Biometria da entidade;

5.2.1 Autenticação Multi-factor

Usar simultaneamente diferentes tipos de prova. 2FA = Two Factor Authentication.

5.2.2 Risk-based MFA

MFA variável. Maior risco de ataque, mais fatores ou menos fatores risky. Menor risco de ataque, menos fatores ou fatores mais simples.

5.3 Authn: Objetivos

- **Autenticar interactors**, pessoas, serviços, servidores, hosts, redes, etc.;
- **Permitir o reforço das politicas e mecanismos de autorização**,
  - Autorização $\neq$ Autenticação;
  - Autorização $\rightarrow$ Autenticação;
- **Facilita o abuso (exploitation) de outros protocolos security-related**. Ex: distribuição de chaves para comunicação segura.

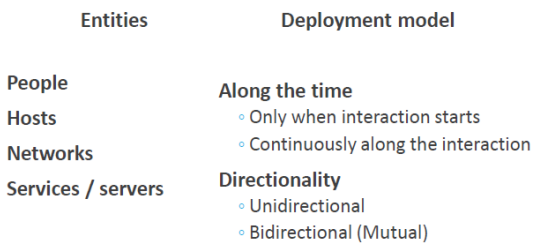
5.4 Authn: Requisitos

- **Confiança (Trustworthiness)**
  - Quão bom é em provar a identidade de uma entidade?
  - Quão dificil é de ser enganada?
  - Level of assurance (LoA) - Nível de confiança;
- **Segredos (Secrecy)** - Nenhuma divulgação de credenciais secretas usadas por entidades legítimas.

NIST 800-63				
LoA	DESCRIPTION	TECHNICAL REQUIREMENTS		
		IDENTITY PROOFING REQUIREMENTS	TOKEN (SECRET) REQUIREMENTS	AUTHENTICATION PROTECTION MECHANISMS REQUIREMENTS
1	Little or no confidence exists in the asserted identity; usually self-asserted; essentially a persistent identifier	Requires no identity proofing	Allows any type of token including a simple PIN	Little effort to protect session from off-line attacks or eavesdropper is required.
2	Confidence exists that the asserted identity is accurate; used frequently for self service applications	Requires some identity proofing	Allows single-factor authentication. Passwords are the norm at this level.	On-line guessing, replay and eavesdropping attacks are prevented using FIPS 140-2 approved cryptographic techniques.
3	High confidence in the asserted identity's accuracy; used to access restricted data	Requires stringent identity proofing	**Multi-factor authentication**, typically a password or biometric factor used in combination with a 1) software token, 2) hardware token, or 3) one-time password device token	On-line guessing, replay, eavesdropper, impersonation and man-in-the-middle attack are prevented. Cryptography must be validated at FIPS 140-2 Level 1 overall with Level 2 validation for physical security.
4	Very high confidence in the asserted identity's accuracy; used to access highly restricted data.	Requires in-person registration	**Multi-factor authentication** with a hardware crypto token.	On-line guessing, replay, eavesdropper, impersonation, man-in-the-middle, and session hijacking attacks are prevented. Cryptography in the hardware token must be validated at FIPS 140-2 level 2 overall, with level 3 validation for physical security.

- **Robustez (Robustness)**
  - Previnir ataques ao protocolo de troca de dados;
  - Previnir cenários de ataques on-line DoS;
  - Previnir ataques de off-line dictionary;
- **Simplicidade (Simplicity)** - Deve ser o mais simples possível para prevenir as entidades escolherem caminhos alternativos perigosos.
- **Lidar com vulnerabilidades introduzidas por pessoas**
  - Têm uma tendencia natural a facilitar ou escolher atalhos;
  - Lidar com phishing;

5.5 Authn: Entidades e Modelo de Deployment



5.6 Authn interactions: Abordagens Básicas

Abordagem Direta

- Fornecer credenciais;
- Esperar o veredito;

A vantagem desta abordagem: **não é preciso computação** por parte do presenter. A desvantagem: as credenciais podem ser **expostas** a validadores maliciosos.

Abordagem Challenge-Response

- Obter o desafio;
- Fornecer uma resposta computada a partir do desafio e das credenciais;
- Esperar o veredito;

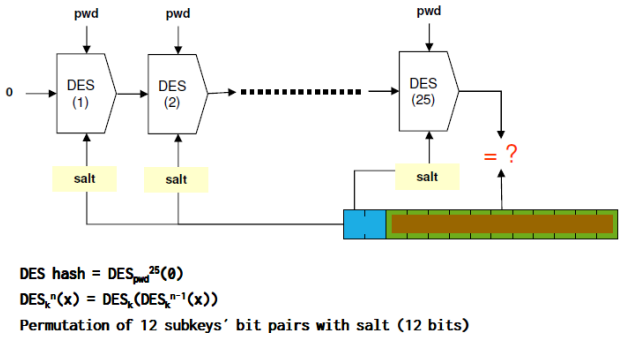
A vantagem desta abordagem: as credenciais **não são expostas** a validadores maliciosos. A desvantagem: requere **computação** por parte do presenter.

5.7 Authn of subjects: Direct Approach w/ known password

Uma password é verificada comparando com valores previamnete armazenados, para uma dada identidade (ex: username).

Valor pessoal armazenado: É transformado por uma função unidirecional. Em Windows, uma digest function, em UNIX, DES hash + salt, em Linux, MD5 + salt (hash é configurável).

Melhor: PBKDF2, Script with high complexity.



Vantagem: Simplicidade;

Problemas:

- A utilização de passwords fracas (permitindo dictionary attacks)
- Transmissão da password atraves de canais de comunicação inseguros, Eavesdroppers podem obter a password facilemnete (ex: Unix remote services, PAP);

5.8 Authn of people: Direct Approach w/ biometrics

As pessoas são autenticadas usando partes do corpo, como biometric samples, fingerprints, iris, face geometry, voice timber, manual writing, vein matching, etc.

Estas medidas são comparadas com registos pessoais (referencias biometricas (templates)), registadas no sistema com um procedimento prévio de enrollment.

Identificação vs Autenticação

- **Identificação** - 1-to-many verificações para match;
- **Autenticação** - 1-to-1 verificações para match;

Vantagens:

- As pessoas não precisam de memorizar ou ter a password consigo;
- As pessoas não podem escolher passwords fracas;
- As credenciais de autenticação não podem ser transferidas a outros;

Problemas:

- Métodos biométricos ainda são pouco fiáveis, em muitos casos podem ser enganados facilmente (ex: fingerprint, face recognition, etc.);
- As pessoas não podem mostrar as credenciais (em caso de roubo);
- Credenciais não podem ser transferidas entre individuos (casos extraordiários);
- Podem causar perigos a inidivuos, a integridade física pode ser comprometida para obter as credenciais;
- Não é facil de ser implementada em sistemas remotos, pois é obrigatório ter dispositivos biométricos seguros e confiaveis;
- Biometrias podem revelar segredos de outras pessoas (doenças);

5.9 Authn of subjects: Direct Approach w/ one-time passwords

One-Time passwords = segredos que podem ser usados apenas uma vez, pre-distribuidos diretamente, ou o resultado de uma função geradora. Exemplo: Códigos do banco, Google Backup Codes, etc.

Vantagens:

- Podem ser eavesdropped, permitindo o seu uso em canais sem encriptação;
- Podem ser escolhidas pelo authenticator, o que pode colocar uma dada complexidade;
- Pode depender de uma password partilhada;

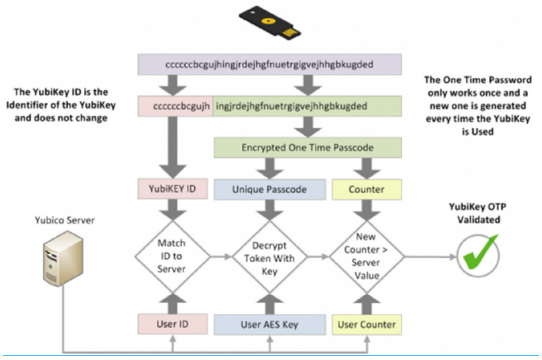
Problemas:

- Entidades a interagir precisam de saber qual password usar em cada ocasião;
- Individuos podem querer recursos adicionais para guardar/gerar passwords;

5.9.1 YubiKey

Dispositivo pessoal de autenticação: USB, Bluetooth e/ou NFC.

Ativação gera uma chave de 44 caracteres, emula um teclado USB, suporta HOTP (events) ou TOTP (temporal). Se um desafio é fornecido, o user toca no botão e obtem a resposta. Possui vários algorimos, incluindo AES 256.



5.10 Challenge-Response Approach

O authenticator fornece um desafio, um nonce (value not once used), normalmente random, pode ser um contador.

A entidade autenticada transforma o desafio, o método de transformação é partilhado pelo authenticator.

O resultado é enviado de volta ao authenticator

O authenticator verifica o resultado. Calcula o resultado utilizando o mesmo método e desafio, ou produz um valor do resultado e avalia se é igual ao desafio, ou a algum valor relacionado.

Vantagens:

- As credenciais de autenticação não são expostas;
- Um Eavesdropper vai ver o desafio e a resposta, mas não consegue calcular a resposta sem o método de transformação;

Problemas:

- Entidades autenticadas devem ter a capacidade de calcular resultados de desafios (hardware token ou software application);
- O authenticator deve precisar de manyer segredos partilhados (em clear text). Estes podem ser roubados, os users podem reutilizar segredos noutro sistema, permitindo ataques;
- Pode ser possível calcular todos os resultados para um (ou todos) desafio(s) (revelando o segredo usado);
- Pode ser vulneravel a dictionary attacks;
- O authenticator NUNCA deve enviar um mesmo desafio a um mesmo user;

5.11 Authn of subjects: Challenge-Response w/ Smartcards

Credenciais de autenticação:

- Ter um smartcard (ex: cartão de cidadão);
- A chave privada guardada no smartcard;
- O PIN de acesso à chave;

O authenticator sabe a chave pública;

Robusto contra:

- Dictionary attacks;
- Ataque offlince a uma base de dados;
- Canais inseguros;

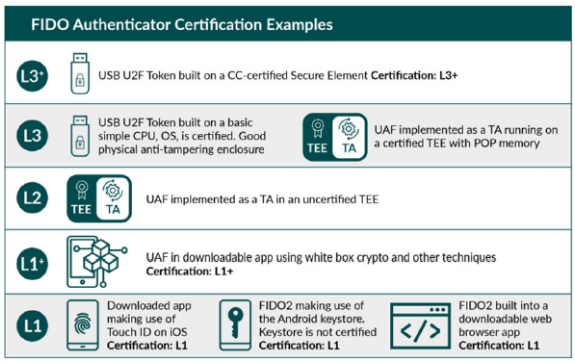
Prorocolo Challenge-Response:

- O authenticator gera o desafio;
- O dono do smartcard cifra o desafio com a chave privada (guardada no smartcard, protegida pelo PIN). Em alternativa pode assinar o desafio;
- O authenticator decifra o resultado com a chave pública. Se o resultado da decifra corresponder ao desafio, a autenticação é bem sucedida. Em alternativa, pode verificar a assinatura (que é o mesmo processo);

5.12 Authn of subjects: Challenge-Response w/ Other Tokens

Tokens FIDO2 (FIDO Alliance)

- Para ambientes desktop e mobile;
- WebAuthn, especificação para web authentication;
- Client-to-Authenticator Protocol (CTAP);
- Segurança
  - Credenciais nunca deixam o dispositivo do user e unca são guardadas num servidor;
  - Sem risco de phishing, sem roubo de passwords (mesmo assim, o token pode ser roubado);
  - Sem ataques de replay;
  - Token certification levels;
- Privacidade
  - Credenciais são únicas por website;
  - Tracking não é ppossivel (diferentes web sites, diferentes chaves públicas para um mesmo token);
  - Dados biométricos, quando usados, nunca saem do dispositivo do user;



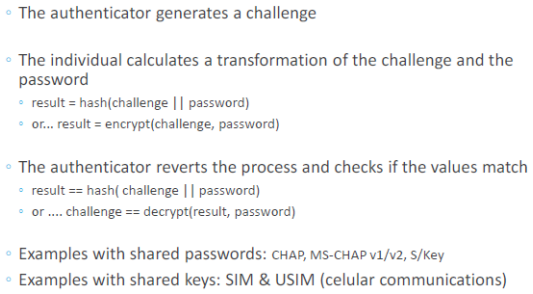
5.13 Authn of subjects: Challenge-Response w/ Shared Secret

Credenciais de autenticação: Password selecionada pelo user;

O authenticator sabe:

- Péssima abordagem: a shared password;
- Melhor abordagem: Uma transformação da shared password. A transformação deve ser unidirecional;

Protocolo Básico Challenge-Response:



5.14 PAP e CHAP (RFC 1334, 1992, RFC 1994, 1996)

Protocolos utilizados para PPP (Point-to-Point Protocol). Autenticação unidirecional. O authenticator autentica users, mas os users não autenticam o authenticator.

PAP (PPP Authentication Protocol): Representação simples de um par de UID/password. Transmissão insegura (em clear text).

CHAP (Challenge-response Authentication Protocol):

- Aut → U: authID, challenge;
- U → Aut: authID, MD5(authID, secret, challenge), identity;
- Aut → U: authID, OK/NOT OK;

O authenticator pode pedir mais autenticações a qualquer momento.

5.15 Authn of subjects: Challenge-Response w/ Shared Key

Utiliza uma chave criptografica em vez de uma password. Robusto contra dictionary attacks. Requer um dispositivo para armazenar a shared key.

5.16 GSM Subscriber Authentication

Usa um segredo partilhado entre o HLR e o telemovel subscrito

- Utiliza uma shared key de 128-bit (não é um par de chaves assimétricas);
- A chave é armazenada no SIM card;
- o SIM card é desbloqueado com um PIN;
- O SIM card responde a desafios usando a shared key;

Utiliza (initially unkonwn algorithms): A3 (autenticação), A8 (geração de session key), A5 (stream cipher para comunicação).

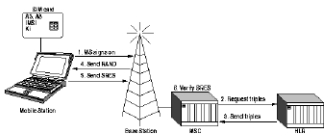
A3 e A8 são executados pelo SIM, A5 é executado pela baseband. A3 e A8 podem ser escolhidos pelo operador.

MSC requests triples from HLR/AUC

- RAND, SRES, Kc
- It can ask one or several

HLR generates RAND and the triples using the subscriber Ki

- RAND, random value (128 bits)
- SRES = A3 (Ki, RAND) (32 bits)
- Kc = A8 (Ki, RAND) (64 bits)



Frequently uses COMP128 for the A3/A8 algorithms

- Recommended by the GSM consortium
- [SRES, Kc] = COMP128 (Ki, RAND)

5.17 Autenticação de Sistemas

Por nome (DNS) ou MAC/IP address: Muito fraco, sem prova criptografica. Mesmo assim é usado em alguns serviços (ex: NFS, TCP wrappers).

Com chaves criptograficas: Secret keys partilhadas entre entidades que comunicam frequentemente. Par assimétrico de chaves, um por host. Chaves públicas pre-partilhadas com entidades que comunicam frequentemente. Chaves públicas certificadas por umas third-party (um CA).

Autenticação de um host: Todos os serviços co-localizados num mesmo host são automaticamente e indiretamente autenticados.

Credenciais exclusivas para cada serviço

Autenticação:

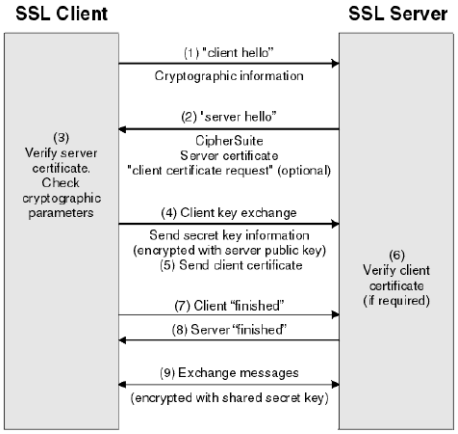
- Secret keys partilhadas com clientes (quando estas precisam de autenticação dos clientes);
- Par de chaves assimétricas por host/service (certificado por outros ou não);

5.18 TLS (Transport Layer Security, RFC 2246)

Protocolo de segurança para comunicação em TCP/IP. Evoluiu do SSL V3 (Secure Socket Layer). Gere sessões seguras sobre TCP/IP, individuais a cada aplicação. Inicialmente usado para o trafego de HTTP.

Mecanismos de segurança:

- Confidencialidade e integridade da comunicação entre entidades (distribuição de chaves, negociação de cifras, digests e outros mecanismos);
- Autenticação das entidades envolvidas
  - Servers, serviços, etc.
  - Clients (não tão comum)
  - Ambos utilizando chaves assimétricas e certificados X.509;



5.19 TLS Ciphersuites

Se um servidor suporta um único algoritmo, não pode experar que todos os clientes suportem o mesmo algoritmo (mais poderoso/limitado, velho/novo).

O conceito de ciphersuite permite a negociação de mecanismos entre cliente e servidor. Ambos mandam os seus ciphersuites suportados, e escolhem um que ambos suportem. O servidor escolhe no caso.

Exemplo: ECDHE-RSA-AES128-GCM-SHA256

- **ECDHE** - Ephemeral Elliptic Curve Diffie-Hellman, é o algoritmo de negociação
- **RSA** - Algoritmo de autenticação;
- **AES-128 GCM** - Algoritmo de cifra e modo de cifra
- **SHA256** - Algoritmo de controlo de integridade

5.20 SSH (Secure SHell)

Gere sessões seguras da consola sobre TCP/IP. Inicialmente desenhado para substituir o Telnet application/protocol. Atualmente utilizado em muitas outras aplicações

- Execução de comandos remotos de forma segura (rsh/rexec);
- Cópia segura de conteudos de/para hosts remotos (rcp);
- Transferência segura de ficheiros (sftp) (Secure FTP);
- Secure (Generic) communication tunnels (carry standard IP packets);

Mecanismos de segurança:

- Confidencialidade e integridade das comunicações (distribuição de chaves);
- Autenticação das entidades envolvidas
  - Servidor/Hosts;
  - Users;
  - Os dois atingidos através de vários mecanismos diferenciados;

5.21 SSH: Mecanismos de Autenticação

Servidor: Par de chaves assimétricas

- As chaves são distribuidas durante a interação (not certified!);
- Os clientes guardam as chaves públicas de interações previas. A chave deve ser guardada em ambientes confiados. Se a chave mudar o cliente deve ser avisado (ex: servidor reinstalado, key regenerou, etc.).

Clientes: Autenticação é configuravel

- Default: username + password;
- Outra: username + chave privada (a pública deve estar pré-instalada no servidor);
- Outra: itegração com PAM para mecanismos de autenticação alternativos;

5.22 Centralized network authentication

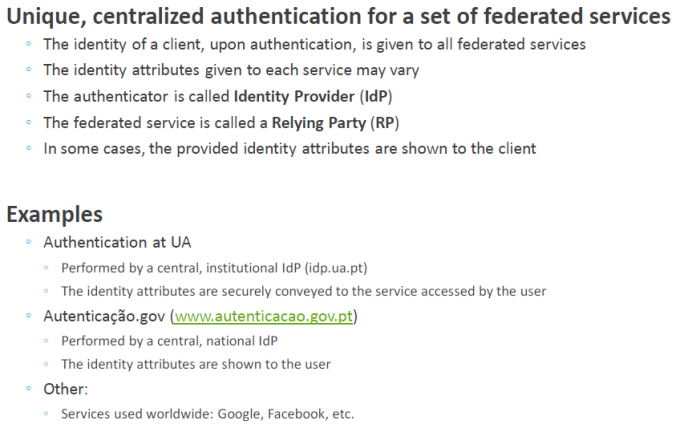
Usada para restringir o acesso à rede a clientes conhecidos

- Redes de cabo;
- Redes wireless;
- Em VPNs (Virtual Private Networks);

Geralmente implementado por um serviço central

- Servidor AAA (Authentication, Authorization, Accounting), ex: RADIUS e DIAMETER;
- O servidor define quais serviços de rede o user pode usar;

5.23 Autenticação por um IdP



5.24 Autenticação Centralizada

Vantagens:

- Pode reutilizar as mesmas credenciais sobre múltiplos sistemas/serviços;
- Repositório único e seguro para as credenciais (mais dificil de roubar Credenciais quando utilizado em varios serviços);
- Pode implementar restrições para serviços/sistemas;

Desvantagens:

- Requer servidores adicionais;
- Single point of failure: sem sistemas de autenticação, ninguém pode ser autenticado (importante deploy a credenciais para admins);
- Introduz delays no processo de autenticação;

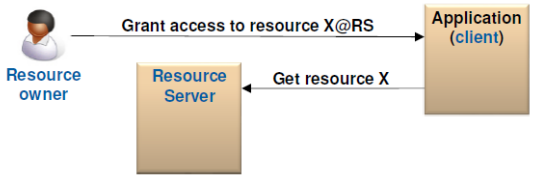
5.25 Single Sign-On

Uma facilidade normalmente associada com IdP. Ambos não obrigatório e nem sempre apropriado.

SSO existe para simplificar a vida dos users. Eles fazem login apenas uma vez para acessar vários serviços durante um periodo de tempo.

5.26 OAuth 2.0: delegação (RFC 6749)

Uma framework para permitir aos users delegar acesso aos seus recursos pela sua conta.



5.27 OAuth 2.0 roles

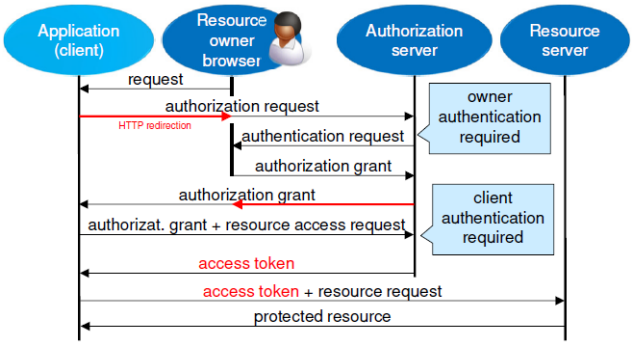
Resource Owner: Uma entidade capaz de conceder acesso a um **recurso protegido**.
End-user: um Resource Owner que é uma pessoa.

Resource Server: O servidor que hospeda os recursos protegidos. Responde a pedidos de acesso a recursos protegidos utilizando **tokens de acesso**.

Client: Uma **aplicação** que realiza requests por recursos protegidos em nome do Resource Owner e com a sua autorização.

Authorization Server: O servidor que emite tokens de acesso para os clientes após **autenticar o Resource Owner** com sucesso e obter a sua **autorização** para os clientes acederem a um dos seus (users) recursos.

5.28 Protocol Flow



5.29 OpenID Connect (OIDC)

Uma camada de identificação em cima do OAuth 2.0. OAuth 2.0 fornece a autenticação centralizada fundamental. Os recursos protegidos são os atributos da entidade, empacotados em **scopes**, os atributos são designados por (identity) **claims**.

6 Armazenamento confiável

6.1 Problemas

Os dispositivos de armazenamento desenvolvem falhas

- As falhas devem ser minimizadas previnindo a perda de dados;
- As falhas acontecem de certeza, não podendo ser ignoradas;

Acesso a discos pmecânicos é lento (hard disks (discos rigidos))

- Tempo de acesso = tempo de translação + tempo de rotação;
- Mais informação → maior impacto na storage media;

Solid State Devices (SSDs) têm um número limite de escritas

- 2.000-3.000 escritas por MLC (2 bits por célula);

Eventos especificos podem resultar na perda de dados

- Incêndios, roubos, "picos de energia", inundações, erros humanos, ataques, ...

Pode ser necessário distribuir dados de uma forma inteligente

- Maximizar a perfornance;
- Reduzir custos;

6.2 Soluções

Backups de dados

- Local
- Remoto

Armazenamento redundante

- RAID (Redundant Array of Independent Disks)
- Other: ZFS

Melhores dispositivos de armazenamento, ambientes com maior controlo

- SLED (Single Large Expensive Disk)
- Enterprise Grade Devices
- Temperature and humidity controlled environments

Infrastruturas dedicadas para armazenamento

- Single policy control point

6.2.1 Backups

Copiar os dados periodicamente

- Snapshot do estado do armazenamento num momento específico;
- Cópias vão permitir recuperar versões anteriores de ficheiros;
- Podem ser encriptados;

Full: Snapshot completo do volume de dados

- Recuperação rápida;
- Requer muito espaço;

Diferencial: Diferenças desde o último backup completo (full)

- Recuperação mais lenta, mas também requer menos espaço;
- Este tipo de backups diariamente aumenta com o número de mudanças;

Incremental: Diferenças desde o último backup

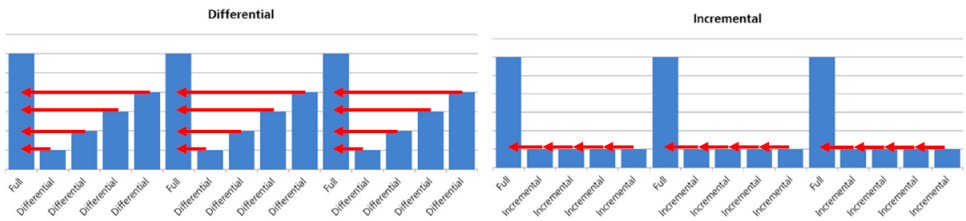
- Recuperação ainda mais lenta;
- Requer reconstrução de todos os backups intermédios desde o úçtimo full backup;
- Mais eficiente em termos de espaço;

Um backup não é um disco adicional com dados, externo ou remoto. **Considera políticas, mecanismos e procedimentos para fazer, manter e recuperar cópias dos mesmos dados**. Deve resistir a situações especificas, deve ser usado apenas em situações de emergência. É importante considerar a cópia, armazenamento e recuperação!

Legal framework implies a special care:

- Quando lidamos com dados pessoais;
- Impôr uma politica de retenção frequentemente, os backups devem expirar após um certo tempo;

6.2.2 Backups - Types



6.2.3 Backups: Compressão

Usa algoritmos e soluções de compressão sem perdas

- Ex: ZIP

Copiar algumas partes da informação

- Apenas ficheiros modificados;

Deduplicação (deduplication)

- Apenas guarda ficheiros/blocos únicos;
- Normalmente utiilizando full copy with deduplicação offline;
  - De blocos do disco utilizando formatos de imagem especificos;
  - De ficheiros utilizando hard links;

6.2.4 Backups: Níveis

Aplicações

- Extrair dados de aplicações (ex: mysqldump);
- Representar uma vista consistente da aplicação. Pode ser necessário bloquear o estado da aplicação (ex: mudanças na BD);
- Pode ser repetido para cada aplicação individual;

Ficheiros

- Copia de ficheiros individuais;
- Pode dar backup a qualquer sistema de ficheiro das aplicações;
- Estado pode ser inconsistente (ex: ficheiros abertos sem dados escritos, ou as aplicações mudam vários ficheiros de uma vez);

Sistema de Ficheiros

- Funcionalidades internas fornecidas pelo sistema de ficheiros de cada individuo;
- Criação de snapshots periodicos com registos de todas as mudanças ou estado atual;
- Pode permitir a recuperação de ficheiros individuais, ou do sistema de ficheiros por completo;

Blocos do Dispositivo

- Copia de todos os blocos de um storage medium;
- Independente do sistema de ficheiros ou de sistema de operações me uso;
- Pode ser implementado pela Infrastrutura de Armazenamento (transparente e sem qualquer impacto para as aplicações);

6.2.5 Backups: Localização dos dados

No mesmo volume ou o mesmo servidor

- Permite aos utilziadores recuperar a informação rapidamente;
- Protege contra mudanças/deleções feitas pelos utilizadores;
- Pode não proteger contra mau funcionamento do hardware (ex: macOS Time Machine);

Num sistema de localização na mesma infrastrutura

- Também com acesso rápido;
- Protege contra falhas de armazenamento isoladas;
- Não protege os dados contra eventos como incêndios, inundações, roubo, ...
- Ex: Most enterprise storage solutions, backuppc, TimeCapsule, Borg, Kopia

Remoto (off-site)

- Implementado para um sistema fora do datacenter local, serviço dedicado ou atraves da internet
  - Ex: Amazon S3, ou servidores em datacenters dedicados;
  - Encriptação se recomendado (ou obrigado) em caso de serviços externos;
- Implementado com transporte seguro especializado (carro blindado transportando backups para um sitio seguro);
- Permite recuperação mesmo se eventos far-reaching aconteçam (ex: terrorismo, terremotos, ...);
- Recuperação é mais lenta (limitada pela velocidade da rede ou do transporte fisico);

6.3 Escolhendo Dispositivos de Armazenamento

Different device grades: Enterprise vs Desktop

- Diferentes qualidades de construção e funcionalidades de recuperação;
- Diferentes MTBF (Mean Time Between Failures)
  - Enterprise HDD: 1.2M horas a 25ºC, trabalhando 24/7, 100% use rate;
  - Desktop HDD: 700K horas a 25ºC, trabalhando 8/5, 10-20% use rate;

Ajustar a cada use case

- Write intensive vs read intensive;
- NAS vs Video vs Desktop vs Cold Storage vs Data Center (diferenças no consumo de energia, fiabilidade e performance);

Ajustado a um nível especifico de performance

- Tier 0: Melhor performance, baixa capacidade (PCIe NVME SLC SSD);
- Tier 1: Alguma performance, alta capacidade e disponibilidade (M2 SATA SSD);
- Tier 3: Baixa performance, alta capacidade, baico preço (SATA HDD);

6.4 RAID (Redundant Array of Inexpensive Drives)

Melhora a subrevivência da iniformação

- Os dados são apenas perdidos depois de múltiplos dispositivos serem perdidos;
- O número de dispositivos perdidos é configurável;

Baixo preço e solução eficiente

- Pode usar hardware barato e de qualidade mais baixa;
- Podem melhorar a performance de leitura e escrita;

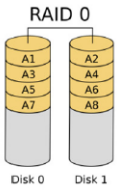
RAID não substitui backups

- Apenas tolera a falha de um número limitado de dispositivos;
- Não consegue lidar com erros humanos (mudificação/deleção de ficheiros);

RAID pode até aumentar a probabilidade de falha

- Uma vez que pode ser ajustado para obter melhor performance;

6.4.1 RAID 0 (Striping)



Objetivos:

- Acelerar o acesso aos dados;

Abordagem:

- Acessar os discos em paralelo;
- Striping
  - Os dados são divididos em pequenos pedaços (stripes);
  - Estes stripes são armazenados ao longo de todos os discos de uma forma distribuída;

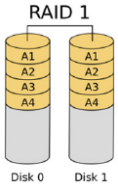
Vantagens:

- Pode acelerar a performance como fator do número de discos;

Desvantagens:

- Aumenta a probabilidade de perder dados (se **Pf** é a probabilidade de falha de um único disco, um volume RAID 0 com **N** discos tem uma probabilidade de falha de $1 - (1 - Pf)^N$);
- aumenta o número de dispositivos (pelo menos duplicando o número);

6.4.2 RAID 1 (Mirroring)



Objetivos:

- Tolerância à falha de discos;

Abordagem:

- Duplicação dos dados (mirroring)
  - Escrita sincronizada;
  - Leitura desitribuida de qualquer disco com ou sem comparação com outro disco;

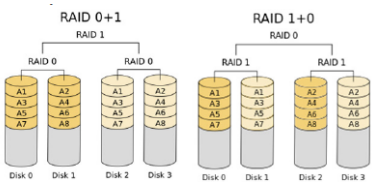
Vantagens:

- Diminui a probabilidade de perda de dados (se **Pf** é a probabilidade de falha de um único disco, um volume RAID 1 com **N** discos tem uma probabilidade de falha de Pf^N);

Desvantagens:

- Armazenamento ineficiente (vai perder pelo menos 50% da capacidade total, para 3 discos vai perder 66% $\ldots (N-1)/N$);
  - Aumenta o número de dispositivos (pelo menos o dobro);

6.4.3 RAID 0+1 e 1+0 (Nested)



Objetivos:

- Beneficios de RAID 0 (performance);
- Beneficios de RAID 1 (resiliência);

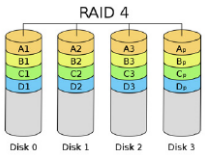
Abordagem:

- 0+1: Um volume RAID 1 utilizando volumes RAID 0 (mirroring of striped volumes);
- 1+0: RAID 0 sobre volumes RAID 1 (striping over mirrored volumes);

Desvantagens:

- Desperdicio da capacidade de armazenamento (pelo menos 50%);
- Aumenta o número de dispositivos;

6.4.4 RAID 4



Objetivos:

- Ter alguma resiliência como RAID 1;
- Com uma performance perto de RAID 0;

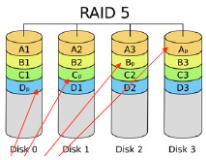
Abordagem:

- Guardar dados em N-1 discos;
- Guardar dados de paridade num disco adicional
  - Total waste é dependente da capacidade e número de discos;
  - Dados dos N-1 discos podem ser usados para recriar outro;

Desvantagens:

- Necessita de pelo menos 3 discos;;
- Das update aos dados de paridade é complexo e requer hardware específico;
- Impõe a necessidade de ler antes de escrever
  - Ler dados de blocos existentes (ex: C1) e do correspondente disco de paridade (Cp);
  - Compara os blocos de dados antigos com os novos, e alterando o bloco de paridade (Cp');
  - Escreve o novo bloco de dados (C1') e o novo bloco de paridade (Cp');
- As escritas devem ser serializadas devido à existênciade um disco de paridade;
- A recuperação é bem mais complexa do que RAID 1;

6.4.5 RAID 5



Objetivos:

- Parecido com RAID 4;
- Mas com maior eficiência nas escritas;

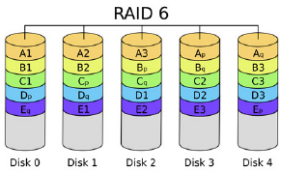
Abordagem:

- Distribuir os blocos de paridade por todos os discos;
- Desperdicio (waste) é parecido com RAID 4;
- A concurrencia de escritas é melhorada

Desvantagens:

- Mais complexo de implementar;

6.4.6 RAID 6



Objetivos:

- Melhorar a fiabilidade de RAID 5;

Abordagem:

- Usar 2 blocos de paridade, distribuidos por todos os discos;
- Desperdicio (waste) de capacidade vai ser mais alto do que no RAID 5 (igual a 2 discos);
- Concorrência é um bocado pior do que RAID 5;

Vantagens:

- Permite a falha de 2 discos sem perder dados;

Desvantagens:

- Ainda mais complexo do que RAID 5;

6.5 NAS e SAN

NAS: Network Attached Storage

- Sistema de armazenamento disponível na rede;
- Frequentemente criado com discos RAID;
- Custo: centenas a milhares de euros;

SAN: Storage Area Network

- Conjunto de sistemas disponiveis na rede;
- Implementa armazenamento distribuido com redundância;
- Custo: milhares a milhões de euros;

Vantagens:

- Permite centralizar as politicas de armazenamento;
- Fornece uma interface normalizada, independente de armazenamento real;
- Pode ser usado para implementar backups distribuidos;

7 Armazenamento confidencial

7.1 Problemas

As proteções fornecidas por sistema de ficheiros tradicional são limitadas

Proteções Fisicas

- O sistema de ficheiros é limitado a um dispositivo fisico;

Proteções Lógicas

- Controlo de acesso a ficheiros, controlado pelo sistema operativo;
- Utilizando ACLs e outros mecanismos de confinamento;

Existe um número relevante de situações onde proteções tradicionais são irrelevantes

Quando existem um acesso direto ou físico a dispositivos

- Acesso a dispositivos host (laptopts, smartphones, servers);
- Acesso a dispositivos de armazenamento externos (Tapes, CDs, DVDs, SSDs, NAS);

Acesso pelo sistema com os direitos corretos

- Acesso não-ético por administradores de sistemas;
- Com ataques de impersonificação;

Existe uma prevalência de armazenamento distribuído. Impõe confiar em múltiplos administradores, por vezes desconhecidos

Autenticação é feita remotamente

- Por vezes não é claro qual é o nível da segurança dos métodos;
- O fornecedor de armazenamento pode ter integrações desconhecidas;
- Modelos de interação são complexos, através de redes externas;
- Múltiplas entidades envolvidas;

A informação é transmitida através de canais de comunicação

- Pode violar a confidencialidade, integridade e criar problemas de privacidade;

7.2 Solução: Encriptação de dados

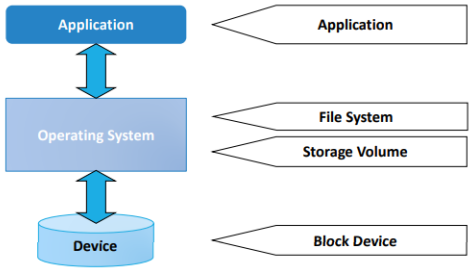
Encriptação/Decifração de conteúdos de ficheiros

- Permite transferencia segura através de redes inseguras;
- Permite armazenamento seguro em localizações inseguras (gerido por entidades externas, ou armazenamentos partilhados);

Problemas com a encriptação

- Acesso à informação. O user pode perder as suas chaves (key loss = data loss), o armazenamento das chaves pode reduzir a segurança num todo;
- Partilha de ficheiros (partilhar dados implica partilhar chaves);
- Pode interferir com a gestão tradicional e tarefas de recuperação (content analysis, deduplication, indexing, ...);

7.3 Abordagens



7.3.1 Encriptação nas Aplicações

Informação é transformada por cada aplicação

- Pouca ou nenhuma integração com outras aplicações;
- Normalmente é claro o que é seguro e o que não é (ficheiros especificos com extensão de ficheiros conhecida);

Apresenta janelas de vulnerabilidade

- Os dados devem ser desencriptados para outros ficheiros antes de serem acessados;

Informação pode ser processada por diferentes algorimos/chaves

- Adaptado a um sistema operativo especifico ou ao nível de segurança;
- Pode complicar os processos de recuperação de dados;

Pode dificultar a partilha de dentro do mesmo pacote encriptado

- Pode implicar extrair dados que estão guardados em clear format;

Exemplos: PGP, AxCrypt, TrueCrypt, VeraCrypt, RAR, ZIP, 7Zip, LZMA, ...

7.3.2 Encriptação nos Sistemas de Ficheiros

Informação é transformada quando é enviada da memória para o sistema de ficheiros

- Pode ser amplo, desde todo o sistema de ficheiros até o cache de memória global. Sem proteção em servidores partilhados onde os dados estão disponíveis para todas as aplicações. O mecanismo de segurança é dificil de implementar em ambientes distribuidos (coordenação de ACLs);
- Pode ser específico ao cache de um processo específico. Proteção no caso de servidores partilhados, uma vez que o acesso aos dados é context-bound. A API do cliente decifra os dados;

Exemplos: EncFS, EXT4, NTFS, CFS, ...

7.3.3 Encriptação no nível do Volume

Informação é transformada pelo driver do volume

- Transparente para a aplicação e quase transparente para o OS (requer suporte através de uma driver específica);
- O volume inteiro vai estar disponivel (partition);

Politicas definidas através das aplicações ou do controller

- Agnóstico ao sistema de ficheiros atual (protege tudo incluindo metadados);
- Mas não diferencia entre users individuais;

Não é capaz de resolver problemas relacionados com os sistemas distribuidos, mas soluciona aqueles relacionados com dispositivos móveis

- Sistemas distribuidos expõe o sistema de ficheiros depois da decifração;
- Dispositivos móveis: dispositivos roubados ou perdidos vão manter os dados seguros;

Exemplos: LUKS, BitLocker, FileVault, PGPDisk, ...

7.3.4 Encriptação no nível do Dispositivo

Dispositivos de blocos aplicam politicas de segurança internamente

- No boot, o dispositivo deve ser desbloqueado (depois de fornecer as credenciais corretas);
- Encriptação é implementada no hardware/firmware;

Vantagens:

- Sem perda de performance;
- Acesso aos dados não é trivial como as chaves são internas;
- Pode ser coordenado com aplicações (ex: dispositivos USB);

Desvantagens:

- Depois do dispositivo ser desbloqueado, os dados estão disponíveis;
- Segurança é limitada pelo algoritmo presente;
- A possível existência de backdoors é dificil de encontrar e corrigir;

Os dispositivos têm duas areas distintas

- Shadow Disk: Read-only, 100MB com software para desbloquear;
- Real Disk: Read/Write. Contém os dados do user;

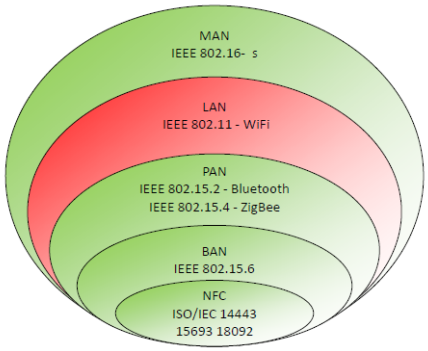
Duas chaves são utilizadas

- KEK: Key Encryption Key (Authentication Key) (fornecida pelo user, e armazenada com digest no Shadow Disk);
- MEK (ou DEK): Media (Data) Encryption Key (encriptada com o KEK);

Processo de Boot:

- BIOS vai acessar ao Shadow Disk e boots;
- Aplicação no Shadow Disk requer password, decifra KEK e verifica hash(KEK);
- Se corresponder, MEK é decifrado, e a geometria do disco é atualizada;

8 Comunicação segura em redes Wi-Fi (802.11)



8.1 Wireless vs Cabled Communications: Problemas de Segurança

Comunicação Broadcast

- Dificil de impor barreiras físicas de propagação;
- Barreiras físicas tipicamente não são suficientes para previnir:
  - Interferencia com comunicações;
  - O eavesdropping (escuta) de comunicações;

Mitigação:

- Reduzir as capacidades de interferencia e escuta (na camada fisica e de data link);

8.1.1 Reduzir as capacidades de interferencia e escuta: Camada Fisica

Previnir eavesdropping através de descodificar o canal, a codificação do canal precisa de usar algum segredo partilhado.

Exemplo: Bluetooth FHSS (Frequency Hopping Spread Spectrum)

- O carrier muda a frequência num padrão conhecido pelo transmissor e recetor:
  - Os dados são divididos em pacotes e são transmitidos por 79 frequências hop num padrão pseudo-aleatório;
  - Apenas transmissores e recetores que estão sincronizados no mesmo padrão de frequências hop, vão ter acesso aos dados transmitidos;
- FHSS parece ser um impulso de ruído de curta duração para eavesdroppers. O transmissor muda de frequências hop 1600 vezes por segundo, para assegurar um elevado nível de segurança dos dados;

Monopolização do canal atual pelos transmissores. Physical Medium access Policies

Exemplos:

- Bluetooth FHSS - Transmissores não sincronizados raramente colidem;
- Wi-Fi - Cada rede é instânciada por cima de uma frequência específica;
- GSM - Cada terminal transmite sobre uma estçaõ móvel específica;

Interferência ainda é possível a partir de fontes externas ou canais sobrepostos

8.1.2 Reduzir as capacidades de interferencia e escuta: Camada de Dados

Previnir atacantes de identificar os participantes da comunicação. Headers t em de ser encriptados, e identificadores temporários devem ser usados.

Previnir eavesdroppers de entender os payloads de data link. Frames precisam de ser encriptados. Normalmente, apenas o payload é encriptado.

Previnir atacantes de forjar data link frames aceitáveis. Frams precisam de ser autenticados (autenticação original, freshness)

8.2 IEEE 802.11: Arquitetura (em redes estruturadas)

Station (STA)

- O dispositivo que pode conectar à rede sem fios;
- Tem um identificador único (MAC (Media Access Control) address). Hoje em dia é popular ser aleatório (para permanecer anónimo);

Access Point (AP)

- O dispositivo que permite a interconecção entre a rede sem fios e outros dispositivos da rede ou redes;

Wireless network

- Rede formada por um conjunto de STAs e APs que comunicam utilizando sinais de rádio;

8.3 IEEE 802.11: Terminologia de uma rede estruturada

Basic Service Set (BSS)

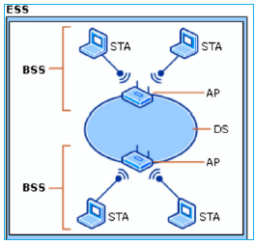
- Rede formada por um conjunto de STAs associadas a um AP;

Extended Service Set (ESS)

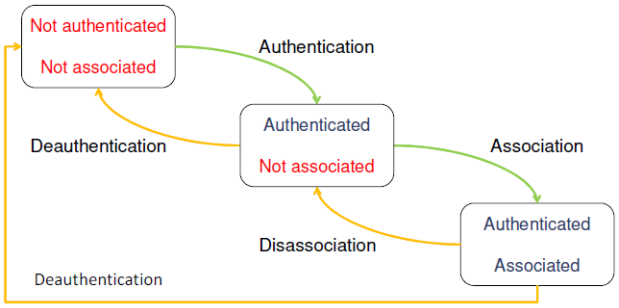
- Rede formada por vários BSSs interconectados por um Distribution System (DS);

Service Set ID (SSID)

- Identificador de uma rede sem fios servido oir um BSS ou ESS;
- A mesma infrastrutura pode usar vários SSIDs;



8.4 IEEE 802.11: Máquina de Estados de Autenticação e Associação



8.5 IEEE 802.11: Tipos de Frames

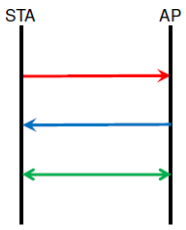
Management frames

- Beacon
- Probe Request & Response
- Authentication Request & Response
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation

Control frames

- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledgment (ACK)

Data Frames



8.6 IEEE 802.11 segurança data link: Overview

Functionality \ Network Type		pre-RSN	RSN (Robust Security Network)	
		WEP	WPA	802.11i (ou WPA2)
Authentication		Unilateral (STA)	Bilateral with 802.1X (STA, AP and network)	
Key Distribution			EAP ou PSK, 4-Way Handshake	
IV Management Policy			TKIP	AES-CCMP
Data Cipher		RC4		AES-CTR
Integrity Control	Headers		Michael	AES CBC-MAC
	Payload	CRC-32	CRC-32, Michael	

Other

- SSID hiding (on beacons)
- MAC address filtering (on associations)
- (Privacy) MAC client randomization before association

8.7 IEEE 802.11 WEP (Wired Equivalent Privacy)

Autenticação Opcional e unilateral, pode suportar múltiplos tipos simultânemente.

OSA: Open System Authentication, sem autenticação, apenas para o modelo de transação de estados.

SKA: Shared Key Authentication

- Desafio/Resposta entre STA e AP;
- Key (password) por pessoa (MAC address) ou rede;
- Autenticação STA unilateral (sem AP / autenticaçao da rede);

Frame payload encryprion, com RC4, usando chaves de 40 ou 104 bits.

Frame payload authentication w/ CRC-32

8.7.1 WEP: Vários problemas de segurança...

SKA é completamete inseguro

- Um eavesdropped tem tudo o que precisa para fingir ser uma vítima (não precisa de saber a password);
- Rogue APs não podem ser detetados;

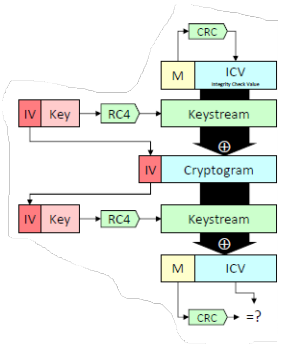
A mesma chave para autenticação e confidencialidade do payload, sem distribuição de chaves, chaves demasiado usadas.

Controlo de integridade é fraco

- CRC-32 é linear;
- Frame deterministic modification é trivial;

Gestão de IVs é mediocre

- IVs são muito pequenos (24 bits), fácil obter criptogramas com o mesmo IV. Tendo o mesmo IV e a mesma chave, obtemos o mesmo keystream, a criptoanálise fica muito fácil;
- IV não é gerido de todo, a reutilização não é controlada/previnida;



8.7.2 Mitigação dos problemas do WEP: WPA (Wi-Fi Protected Access)

WPA utiliza WEP de uma forma segura

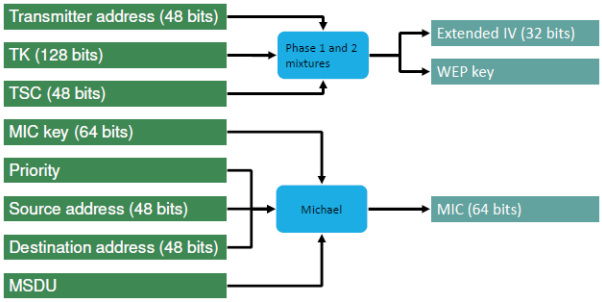
- Uma chave diferente RC4 por frame;
- Chaves RC4 fracas são evitadas;
- Controlo de integridade criptográfica extra w/ Michael;
- Sequência de IVs estrita para prevenir a reutilização de frames;

Implementada primeiro por drivers de dispositivos, mais tarde em firmware.

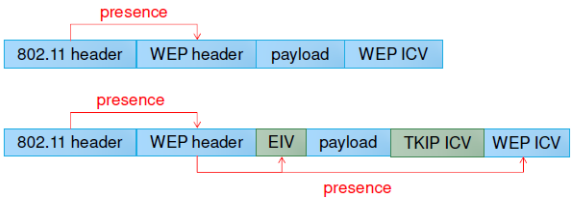
Inline w/ 802.11i

- O verdadeiro padrão de segurança 802.11;
- WPA pode ser usado com 802.1X para autenticações mutuas mais fortes;

WPA: TKIP (Temporal Key Integrity Protocol)



TKIP: Frame layout



8.8 IEEE 802.1X: Autenticação Port-Based

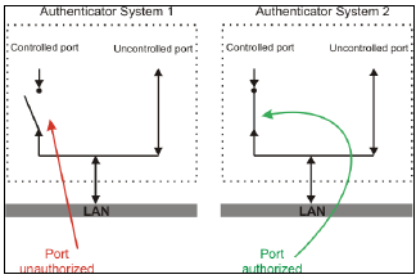
Modelo de autenticação para todas as redes IEEE 802, autenticação mutua na camada 2.

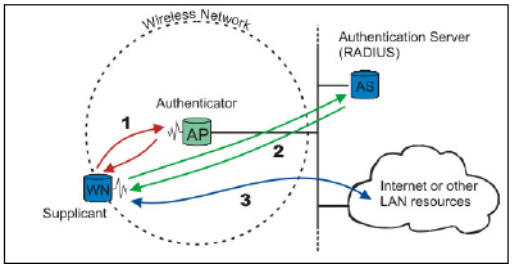
Originalmente desenvolvido para redes grandes

- Campus universitários, empresas, . . . ;
- Modelo foi extendido para redes sem fios;

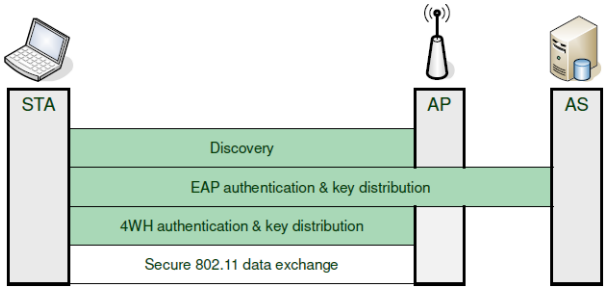
Realiza distribuição de chaves, protocolos adicionais focados nos processos restantes;

8.8.1 IEEE 802.1X: Arquitetura

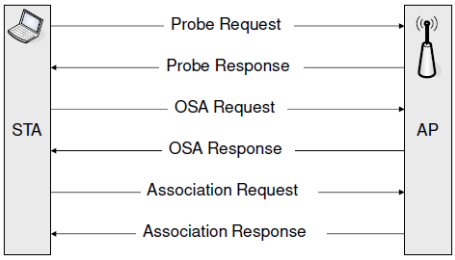




8.8.2 IEEE 802.1X: Fases Operacionais

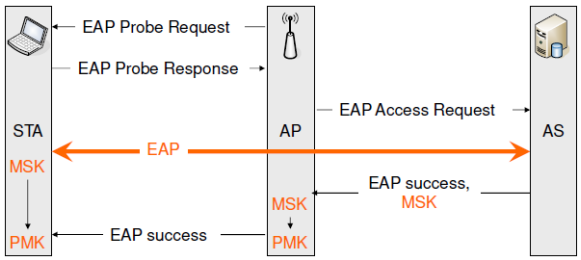


Fase 1: Discovery (mensagens 802.11)



STA apenas teve acesso ao AP (a porta controlada pelo 802.1X ainda está fechada)

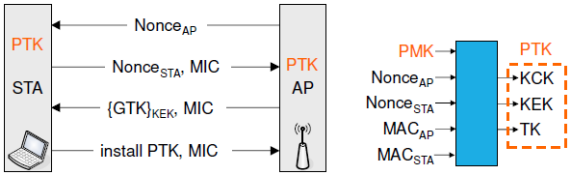
Fase 2: Authentication (mensagens EAP)



No final desta fase, AP e ATA partilham dados crypto

- PMK (Pairwise Master Key)
- Mas a porta controlada pelo 802.1X ainda está fechada;

Fase 3: 4-Way Handshake (mensagens EAPoL)



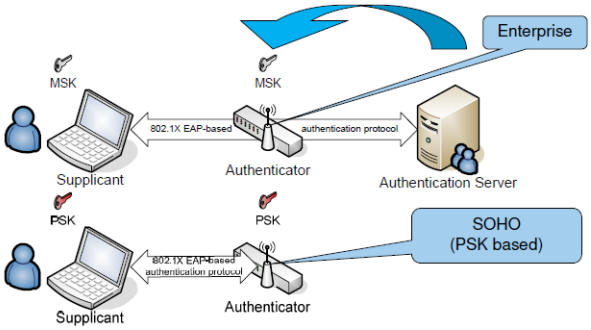
No final AP e STA partilham novos dados crypto

- PTK (Pairwise Transient Key)
- GTK (Group Transient Key)

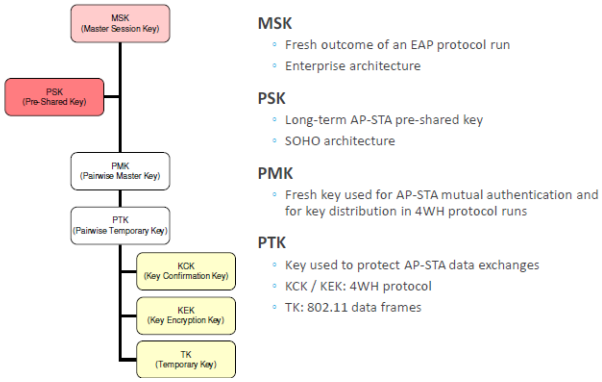
Ambos estão convencidos que o par conhece PMK e PTK, devido ao uso de MICs.

A porta controlada pelo 802.1X está agora aberta para tráfego unicast.

8.8.3 IEEE 802.1X: Opções Arquiteturais



8.8.4 IEEE 802.1X: Hierarquia de Chaves Completa



8.9 EAP (Extensible Authentication Protocol)

Inicialmente desenvolvido para PPP (Point-to-Point Protocol), adaptado para 802.1X.

AP não se envolve

- Retransmitir tráfego EAP;
- Protocolos EAP diferentes não umplicam mudanças em APs;

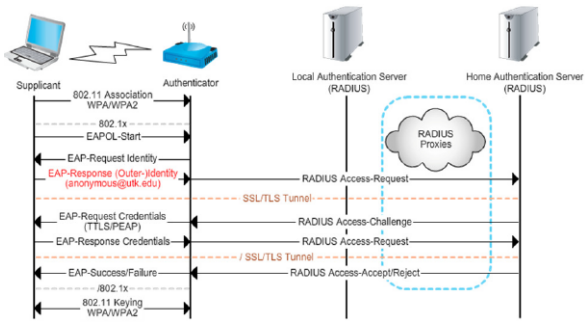
Não concebido para redes sem fios

- Tráfego EAP não é protegido;
- Autenticação mutua não é obrigatória (um STA pode ser enganado por um rogue AP mais forte (nível de rádio));

8.9.1 Alguns protocolos EAP para 802.1X

	LEAP	EAP-TLS	EAP-TTLS	PEAP
AS authentication	digest (challenge, password)	Public Key (certificate)		
Supplicant authentication	digest (challenge, password)	Public Key (certificate)	EAP, Public Key (certificate)	PAP, CHAP, MS-CHAP, EAP
Risks	Identity exposure Dictionary attacks Host-in-the-Middle attacks	Identity exposure		Possible identity exposure in phase 1

8.9.2 Eduroam: 802.1X w/ PEAP + MS-CHAPv2



Disponível na maioria das universidades do mundo. Servidores de Autenticação Local (usando RADIUS) para acesso roaming.

8.10 IEEE 802.11i (WPA2)

Define Redes de segurança robustas (RSN). São as que suportam WPA e 802.11i.

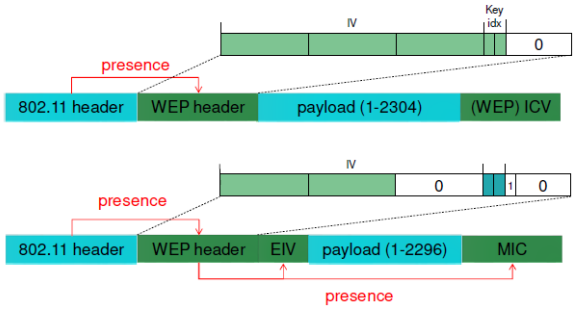
Utiliza mecanismos de segurança avançados para proteção de frames

- Advanced Security Algorithm (AES) para encriptação do payload e controlo de integridade de frames;

Utiliza 802.1X para autenticação mutua
Utiliza 802.1X para autenticação de acesso à rede

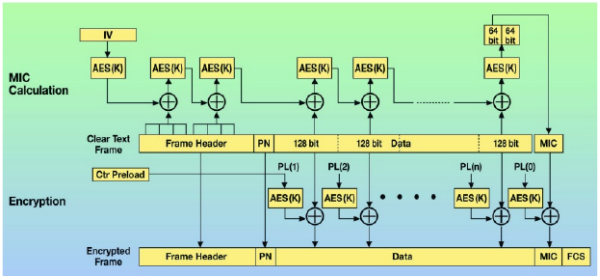
- Simplified Pre-Shared Key (PSK) mode for SOHO (Small Office, Home Office) environments;
- EAP-based protocol for enterprise environments;

8.11 WEP vs AES-CCMP: Frame Layout



8.12 WPA2 proteção de frames

CCMP - Counter CBC-MAC Protocol



8.13 802.11w: Proteção de Gestão de Frames

Gestão de frames que podem ser usados para ataques de DoS são autenticados

- Pedidos de deautenticação e desassociação;
- Outros frames de gestão são unicasted ou broadcasted por um AP;

BIP (Broadcast Integrity Protocol)

- IGTK (Integrity GTK (Group Temporal Key))
- Para proteger parte do tráfego de Broadcast do AP;

Security Association Query Request / Response

- Ajuda a lidar com problemas de desincronização;

8.14 IEEE 802.11 segurança: Todos os problemas resolvidos? NÃO!

Ataques de dicionário ainda são possíveis com autenticações baseadas em PSK ou EAP

- E estas vão continuar, enquanto os humanos continuarem a escolher passwords fracas;

Ainda existem alguns frames não protegidos

Algumas weaknesses ao nível do CSMA

- Low Congestion Window (CW) values permitem aos atacantes obter toda a largura de banda;