Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Capítulo 7

Segurança em Redes IEEE 802.11

As redes sem fios, em particular as redes 802.11, são também conhecidas como redes WLAN (*Wireless Local Area Network*) ou redes Wi-Fi.
Os problemas de segurança colocados pelas redes sem fios são:

- A autenticação entre um equipamento móvel (STA - *station*) e as redes sem fios a que acede
- O controlo de acesso de um STA a uma redes sem fios
- A confidencialidade das mensagens trocadas via rádio
- A autenticidade, ou controlo de integridade, das mensagens recebidas

Redes Cabladas e Wireless

- ***Elementos de prova***
  - Difícil aplicar limites físicos de propagação
  - Características físicas vulneráveis onde existe interferência nas comunicações e observação das comunicações

- ***Mitigação***

Mecanismos para reduzir interferências e observação	
Nível Físico	**Nível de Dados**
- Impossibilitar os atacantes de descodificar o canal onde a codificação necessita de usar um segredo partilhado e as condições de transmissão dependem deste segredo. - Prevenir transmissores de monopolizarem o canal (políticas de acesso ao meio físico)	- Prevenir que os atacantes identifiquem participantes da comunicação, é cifrado os cabeçalhos e criação de identificadores temporários - Prevenir que atacantes compreendam os dados transmitidos, os pacotes são cifrados - Prevenir que atacantes criem pacotes de dados válidos, os pacotes têm de ser autenticados (autenticação da origem ou do grupo)

Arquitetura

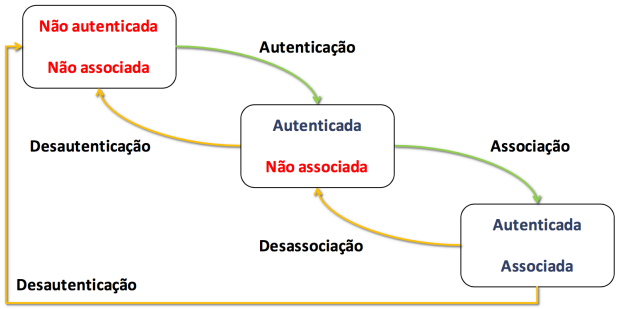
- ***STA (Station)*** - Dispositivo que se liga a uma rede sem fios. Possui um identificador único, como o endereço MAC.
- ***Access Point (AP)*** - Dispositivo que serve de ponto de coordenação para os dispositivos de uma rede.
- ***Redes sem Fios (Wireless)*** - Rede formada por um conjunto de STAs e APs que comunicam com sinais de rádio.

O padrão 802.11 permite duas arquiteturas de redes alternativas:
• ***ad-hoc*** - nesta arquitetura cada STA pode comunicar com outros, segundo um modelo P2P. O conjunto de equipamentos que constitui cada rede ad-hoc forma uma BSS.
• ***estruturado*** - nesta arquitetura os STA comunicam com os AP, apenas possuindo portas para comunicar com redes cabladas e antenas para comunicar com os STA.

Terminologia de uma Rede

• ***Basic Service Set (BSS)*** - Rede formada por STA associadas a um AP.
• ***Extended Service Set (ESS)*** - Rede formada por várias BSS ligadas por um sistema de distribuição.
• ***Service Set ID (SSID)*** - Identificador de uma rede servida num BSS ou ESS. A mesma infraestrutura pode usar vários SSID.

Máquina de Estados de Autenticação e Associação



Autenticação	- A autenticação é feita recorrendo a múltiplas trocas de pacotes *Authentication Request / Authentication Response*. - No processo de autenticação, o AP pode pedir ao STA que prove pertencer a um determinado utente.
Associação	- A etapa de associação, associa o STA a um AP, o que na prática significa que o AP reserva recursos para identificar o STA e para gerir a comunicação com o mesmo. -A associação normalmente é realizada com a troca de pacotes *Association Request* e *Association Response*.
Desautenticação	- A desautenticação entre um STA e um AP pode ser comunicada por qualquer um dos interlocutores através de um pacote *Deauthentication*. A desautenticação permite que sejam libertados recursos (chaves criptográficas partilhadas). - A desautenticação implica uma desassociação automática.
Desassociação	- A desassociação entre o STA e o AP pode ser comunicado por qualquer um dos dois interlocutores através de um pacote *Desassociation*.

Tipos de Pacotes

- ***Pacotes de Dados*** - Os pacotes de dados servem para efetuar uma troca de dados útil, nomeadamente datagramas IP, entre o STA e AP.
- ***Pacotes de Gestão*** - Os pacotes de gestão permitem que um STA e um AP negociem e mantenham uma ligação entre si.
  - *Authentication Request & Response;*
  - *Deauthentication;*
  - *Association Request & Response;*
  - *Reassociation Request & Response;*
  - *Disassociation*
- ***Pacotes de Controlo*** - Os pacotes de controlo servem para gerir a comunicação entre o STA e o AP. Estes pacotes são usados para gerir o acesso ao meio de comunicação e para evitar a ocorrência de colisões provocadas pro comunicações simultâneas.
  - *Request to Send*
  - *Clear to Send*
  - *Acknowloedgment*

Segurança do Nível dos Dados

Os problemas de segurança das redes WLAN, derivam do facto de ser complexo ou mesmo impossível limitar fisicamente o acesso de pessoas não autorizadas ao sinal de rádio usando nas redes WLAN ou aos AP que as suportam.

- Inicialmente, a segurança das redes estruturadas 802.11 era baseada no protocolo WEP. Este protocolo permite a autenticação unidirecional dos STA e a confidencialidade e o controlo de integridade dos dados trocados entre STA e os AP.
- O WPA tem a vantagem de permitir reutilizar os equipamentos de rede dos STA que suportam apenas WEP mas exige que os AP saibam operar com WPA. O WPA permite configurações de segurança mais simples, particularmente para ambientes SOHO.

Tipo de Rede / Funcionalidade		pré-RSN	RSN (Robust Security Network)	
		WEP	WPA	802.11i (ou WPA2)
Autenticação		Unilateral (STA)	Bilateral com 802.1X (STA, AP e rede)	
Distribuição de Chaves			EAP ou PSK, 4-Way Handshake	
Política de Gestão de IV			TKIP	AES-CCMP
Cifra dos dados		RC4		AES-CTR
Controlo de Integridade	Cabeçalhos		Michael	AES CBC-MAC
	Dados	CRC-32	CRC-32, Michael	

WEP

O WEP inclui duas funcionalidades distintas:

- autenticação do STA
- confidencialidade e controlo de integridade dos dados trocados

O WEP não permite distinguir utentes que acedem à rede.

- ***Autenticação***

OSA	SKA
- Não existe qualquer autenticação dos STA, logo a sua associação ao AP é sempre autorizada. Apenas ocorre o processo de associação e autenticação (do AP). - Este modelo de autenticação é útil em alguns cenários específicos, por exemplo, caso se pretenda fornecer um acesso totalmente público e livre a determinada rede.	- A autenticação é feita usando um processo simples de desafio-resposta, o AP envia um desafio ao STA e este deverá devolve-lo cifrado com a chave partilhada de autenticação. - A autenticação com SKA pressupõe uma pré-distribuição de chaves PSK ao STA e AP.

- SKA é completamente inseguro pois um atacante possui toda a informação para se fazer passar por uma vítima e não é necessário saber a chave, e os APs falsos não podem ser detetados.
- A mesma chave é usada para autenticação e confidencialidade, sem distribuição de chaves.
- Um dos problemas do WEP é a inexistência de políticas e mecanismos de geração de novas chaves WEP de cada vez que um dado utente se associa a um AP. A chave WEP é sempre a mesma - a pré distribuição entre o utente e o STA e os gestores do AP. Como o VI tem uma dimensão finita, tal significa que ao fim de algum tempo (ou tráfego) vão-se repetir as chaves contínuas geradas para cada utilizador.

- ***Confidencialidade e Controlo de Integridade***

  Para cada pacote é escolhido um vetor de iniciação (VI) que juntamente com a chave WEP, são usadas como chave do algoritmo RC4 para gerar uma chave contínua. Esta chave contínua é somada aos dados a enviar via rádio e à sua soma de controlo calculada com CRC-32, transformando-os num criptograma. A decifra do criptograma segue o processo inverso: o recetor retira o VI da mensagem que recebeu, usa-o juntamente com a chave WEP para gerar a chave contínua e soma-a ao criptograma recebido, de onde resultam os dados em claro inicialmente apresentados para cifa.

WPA

O WPA manteve toda a funcionalidade do WEP, tipicamente fornecida pelas interfaces de rede, e acrescentando-lhe funcionalidades ao nível de gestão de chaves de cifra e ao nível do controlo de integridade dos pacotes.

Com o WPA, cada pacote é cifrado com uma chave WEP diferente de forma a que não seja possível construir dicionários de chaves contínuas até mesmo quando se usa a mesma PSK repetidas vezes.

- A autenticação do WPA no acesso a um terminal móvel à rede permite o modelo *Enterprise* para redes de médio/grande dimensão.
- Permite a autenticação mas não a obriga

IEEE 802.11i ou WPA2

O 802.11i, também designado por WPA2, é um padrão complexo que define um modelo de segurança para redes 802.11.
O 802.11i usa o conceito de redes de segurança robusta, RSN (*Robust Security Network*). Uma rede diz-se RSN se suportar uma autenticação mais eficaz dos interlocutores, baseada em 802.1X.
São usados mecanismos mais avançados para proteção das tramas, ou seja, métodos que não implicam suporte do hardware existente, como AES-CCMP, AES-CTR, CBC-MAC.

AES-CCMP

O AES-CCMP é a combinação-base de mecanismos de segurança do 802.11i para proteger trama 802.11. Esta combinação tem por base o algoritmo criptográfico AES com chaves e blocos de dados 128 bits. Para controlo de integridade, o AES-CCMP usa o modo de operação CCM (*Counter with CBC-MAC*). Este é um modo de operação concebido para fornecer simultaneamente autenticação e controlo de integridade usando cifra por blocos de 128 bits.
A cifra do CCM é uma cifra contínua com base numa cifra por blocos operando em modo CTR. O controlo de integridade do CCM é realizado com CBC-MAC.
O modelo de operação AES-CCMP é muito semelhante ao do TKIP, mas usando apenas uma chave de sessão para cifra e controlo de integridade TK (*temporal key*).

O WPA assenta em dois pilares

TKIP	802.1x

- Lida com a autenticação e confidencialidade das tramas.
- O TKIP encapsula o WEP, usa-o mas de forma a não expor as vulnerabilidades.
- O TKIP corrige a deficiencia de chaves e do VI do WEP
- O TKIP usa três chaves partilhadas com o interlocutor
  - uma chave para confidencialidade, TK de 128 bits
  - duas outras para controlo de integridade (chaves MIC de 64 bits), uma para cada sentido da comunicação.
	- Lida com a autenticação entre interlocutores e distribuição de chaves de sessão após uma operação.
	- Este protocolo serve para efetuar a autenticação mútua entre interlocutores, STA e rede, aquando da ligação de um STA a uma rede sem fios. Este protocolo permite criar e distribuir chaves de sessão frescas aos equipamentos que efetuam a troca efetiva de mensagens via rádio, STA e AP.
	Três tipo de interlocutores:
	• **Suplicante** - equipamento (móvel) que se pretende ligar à rede
	• **Autenticador** - elemento que controla o estado do porto de acesso do suplicante à rede
	• **Servidor de autenticação** - servidor central gerido no âmbito do domínio de segurança da rede, que efetivamente conduz o processo de autenticação mútua entre os suplicantes e a rede

Um porto pode ser controlado ou não controlado. Um porto não controlado não impõe qualquer restrição à troca de dados através de si. Um porto controlado possui estados distintos e permite efetuar controlo de trocas de dados em cada estado
- “não autorizado” não permite a troca de dados, enquanto no estado “autorizado” permite.

Etapas do 802.1x

As operações realizadas no âmbito 802.1x em redes sem fios dividem-se em três etapas. Após a terceira etapa pode ter lugar a troca de dados segura entre o STA e a rede a que o AP está ligado. Os dados serão protegidos usando o material criptográfico e os algoritmos negociados entre o AP, servidor de autenticação e o STA.

- ***Primeira Etapa: Descoberta e Associação 802.11***

- O suplicante (STA) liga-se à rede sem fios. É efetuado o processo normal das redes 802.11 da descoberta da rede, autenticação do STA e de associação entre o STA e o AP.
- No final desta etapa o suplicante deverá estar autenticado e associado junto de um AP que irá supervisionar ou controlar as etapas seguintes. No final desta etapa o porto controlado está no estado "não autorizado".

- ***Segunda Etapa: Autenticação EAP***

- É realizada a autenticação mútua e uma distribuição de chaves de sessão entre o suplicante (STA) e o servidor de autenticação (SA). O autenticador supervisiona um diálogo entre o suplicante e o servidor de autenticação, o qual é o único permitindo através do porto não controlado.
- A troca de mensagens relativa à autenticação segue o metaprotocolo EAP. No final desta etapa o porto controlado continua no estado "não autorizado".

- **EAP (*Extensible Authentication Protocol*)**

  - O EAP é um metaprotocolo concebido para encapsular outros protocolos de autenticação.
  - No caso do 802.1x, o EAP é fundamental para libertar o AP (autenticador) da tarefa de gerir aspetos particulares do modelo de autenticação adotado. A autenticação é centralizada no servidor de autenticação e consegue-se alterar os paradigmas de autenticação da rede sem alterar o *software* dos AP.
  - A autenticação deverá ser mútua, resistente a ataques por interposição (*"man in the middle")* e resistente a ataques com dicionários.
  - Têm de gerar e distribuir aos interlocutores uma chave secreta simétrica. Essa chave deverá ter pelo menos 64 octetos e na sua geração deverão ser usados pelo menos 128 bits aleatórios e secretos.
  - Embora o EAP permita autenticações unilaterais, no caso do 802.1X normalmente usa-se com autenticação bilateral.

- ***Terceira Etapa: Acordo em 4 Passos***

- É realizada uma autenticação mútua e uma distribuição de chaves de sessão entre o suplicante (STA) e o autenticador (AP). A autenticação é fundamental para o suplicante garantir que está a interagir com um autenticador (AP) que pertence ao mesmo domínio de segurança do servidor de autenticação, e não a um impostor. A distribuição de chaves visa criar uma chave de sessão fresca entre o suplicante e o autenticador, que irá servir de base à proteção dos dados trocados entre ambos.
- No final desta etapa o porto controlado já está no estado "autorizado".

Todos os problemas estão resolvidos?

Não …

- O PSK e alguns métodos EAP vulneráveis a ataques por dicionário, continuarão a existir enquanto as passwords forem escolhidas pelos utilizadores
- Proteção apenas abrange tramas de dados:
  - Tramas de gestão
  - Atacantes podem desautenticar / desassociar STAs
  - Atacantes podem adivinhar o tipo de tráfego pelos tempos / tamanhos
  - Muitos protocolos expõem identidade do utilizador