UNIVERSIDADE PORTUCALENSE

Segurança em Redes Wireless

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Segurança em redes sem fios

- As preocupações de segurança em redes sem fios são semelhantes aos encontrados em um ambiente com fios
- Os requisitos de segurança são os mesmos:
  - Confidencialidade, integridade, disponibilidade, autenticidade, auditoria
  - O risco mais significativo, é a forma de comunicação subjacente

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Segurança em redes sem fios

Wireless é um alvo popular

- Acesso adquirido com wireless
- Falta de segurança padrão
- Proliferação de dispositivos
- Anonimato
- Baixo custo

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Componentes de uma rede sem fios

Endpoint

Access point

DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Associação acidental

- Outra empresa nas proximidades disponibiliza redes sem fios o que pode criar sobreposição de faixas de transmissão. Um utilizador que se pretenda ligar a uma rede pode involuntariamente bloquear o ponto de acesso sem fio da empresa vizinha.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Associação maliciosa

- Nesta situação, um dispositivo sem fios está configurado para parecer ser um ponto de acesso legítimo, permitindo que o operador possa obter as contas de utilizadores legítimos e, em seguida, entrar na rede através de um ponto de acesso.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Redes ad-hoc

- São redes peer-to-peer entre computadores sem ponto de acesso entre eles. Essas redes podem representar uma ameaça de segurança devido à falta de um ponto central de controle.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Redes não tradicionais

- As redes não tradicionais e links, como dispositivos pessoais de rede Bluetooth, leitores de código de barras, e PDAs portáteis representam uma risco de segurança tanto em termos de espionagem e falsificação.

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Roubo de identidade (spoofing MAC):

- Ocorre quando um atacante é capaz de ler o tráfego de rede e identificar o endereço MAC de um computador com privilégios de rede.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Man-in-the middle

- Este ataque envolve convencer um utilizador e um ponto de acesso a acreditar que eles estamos falando uns com os outros, quando na verdade a comunicação está passando por outro dispositivo intermédio. As redes sem fio são particularmente vulneráveis a tais ataques.

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Negação de serviço (DoS)

- Um ataque de DoS ocorre quando um atacante bombardeia continuamente um ponto de acesso sem fios com várias mensagens de protocolo projetado para consumir recursos do sistema. O ambiente sem fios presta-se a este tipo de ataque, porque é muito fácil para o atacante dirigir várias mensagens sem fio para um alvo.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Injeção de rede

- Um ataque de injeção de rede tem como alvo os pontos de acesso sem fio que estão expostos ao tráfego de rede não-filtrado, tal como o protocolo de encaminhamento mensagens ou mensagens de gestão de rede. Um exemplo deste tipo é um ataque é aquele em que os comandos de reconfiguração falsos são usados para afetar os routers e switches para degradar o desempenho da rede.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Ameaças de redes sem fios

Associação acidental	**Associação maliciosa**	**Redes ad hoc**
Redes não tradicionais	**MAC spoofing**	**man-in-the**
DoS	**Injeção de rede**	

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Proteção de redes sem fios

- As principais ameaças são leitura não autorizada de mensagens (eavesdropping), alteração ou inserção de mensagens e perturbação
- Contramedidas para eavesdropping:
  - Esconder o sinal
  - Encriptação
- A utilização de protocolos de encriptação e autenticação é o método standard para contrariar as tentativas de alteração das transmissões.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Proteção de redes sem fios

- Medidas para esconder o sinal
  - Desligara transmissão por wireless do Service Set Identifier (SSID)
  - Pontos de acesso: Atribuir nomes crípticos aos SSIDs
  - Diminuir a intensidade do sinal ao mínimo necessário
  - Localizar os AP no interior do edifício e longe de janelas e paredes exteriores
  - Utilização de antenas direcionais

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Proteção de redes sem fios

- Medidas para esconder o sinal
  - Desligara transmissão por wireless do Service Set Identifier (SSID)
  - Pontos de acesso: Atribuir nomes crípticos aos SSIDs
  - Diminuir a intensidade do sinal ao mínimo necessário
  - Localizar os AP no interior do edifício e longe de janelas e paredes exteriores
  - Utilização de antenas direcionais

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Proteção de redes sem fios

- A principal ameaça envolvendo redes sem fios é o acesso não autorizado à rede
- A principal forma de prevenir estes acessos é o standard IEEE 802.1X para o controlo de acessos
  - fornece um mecanismo de autenticação para dispositivos que pretendem ligar-se a uma rede LAN ou wireless
- A utilização do 802.1X pode prevenir o acesso de pontos ilegais e de dispositivos não autorizados.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

Proteção de redes sem fios

UNIVERSIDADE PORTUCALENSE

Utilizar encriptação

- Os routers sem fios são tipicamente equipados com mecanismos incorporados de criptografia para o tráfego de router para router.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

Proteção de redes sem fios

UNIVERSIDADE PORTUCALENSE

Desligar a transmissão identificador

- Os routers sem fios são tipicamente configurados para transmitir um sinal de identificação para que qualquer dispositivo dentro do alcance pode saber da existência do router. Se a rede é configurada de modo que os dispositivos autorizados conheçam a identidade de routers, esta capacidade pode ser desativada, de modo a impedir os invasores.

Proteção de redes sem fios

UNIVERSIDADE PORTUCALENSE

Alterar o identificador padrão do router

- Alterar o identificador padrão do router. Esta medida contraria atacantes que tentem obter acesso à rede sem fios usando identificadores de padrão do router.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Proteção de redes sem fios

Alterar a password de administração do router

- Alterar a password pré-definida de administração do equipamento.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

Proteção de redes sem fios

UNIVERSIDADE PORTUCALENSE

Filtrar endereços MAC

- Permitir o acesso apenas computadores específicos à rede sem fio. Um router pode ser configurado para comunicar somente com endereços MAC aprovado.

UNIVERSIDADE PORTUCALENSE

Segurança de redes sem fio

- Wired Equivalent Privacy (WEP)
  - 802.11 privacy
- Wi-Fi Protected Access (WPA)
  - conjunto de mecanismos de segurança que elimina a maioria dos problemas de segurança do 802.11
- Robust Security Network (RSN)

UNIVERSIDADE PORTUCALENSE

Serviços 802.11i RSN

- Autenticação
  - Entre o utilizador e um servidor de autenticação que fornece autenticação mútua e gera chaves temporárias para serem utilizadas entre o cliente e o AP.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Serviços 802.11i RSN

- Controle de acessos
  - Impõe o uso da funções de autenticação, encaminha as mensagens corretamente e facilita a troca de chaves
  - Pode trabalhar com uma variedade de protocolos de autenticação

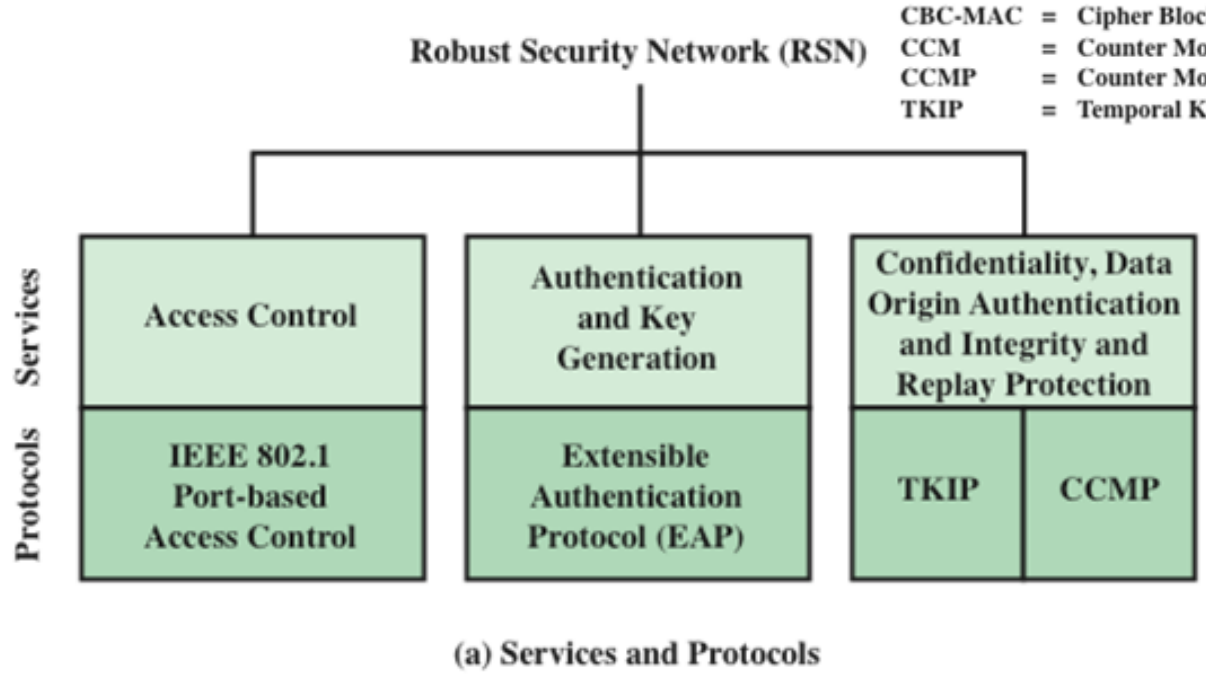
DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

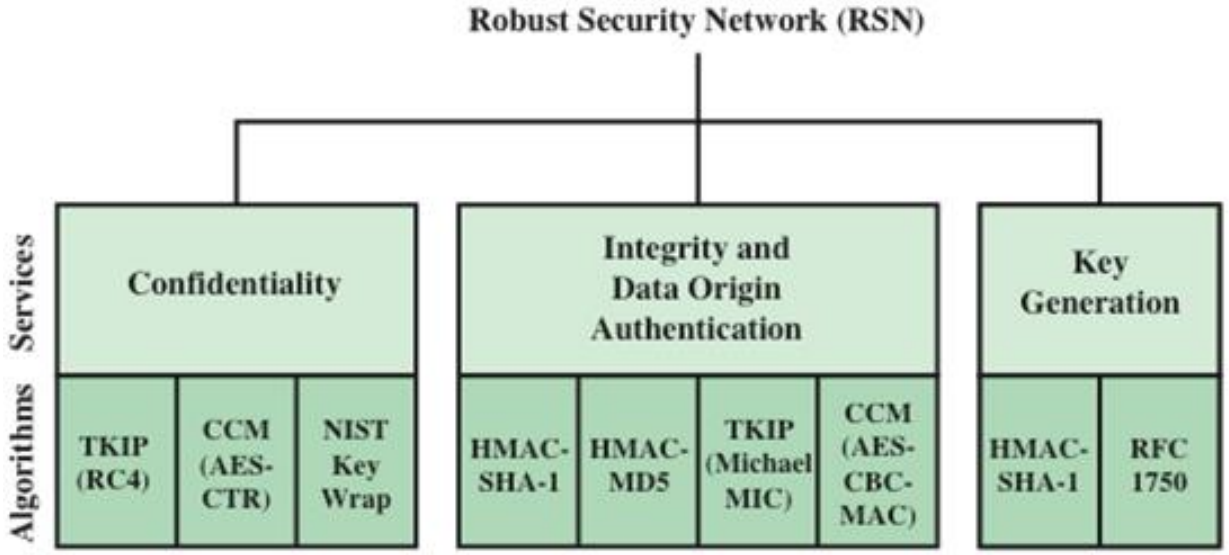
Serviços 802.11i RSN

- Privacidade com integridade da mensagem
  - Os dados a nível MAC são encriptados, juntamente com um código de integridade da mensagem que garante que os dados não foram alterados

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA



(a) Services and Protocols



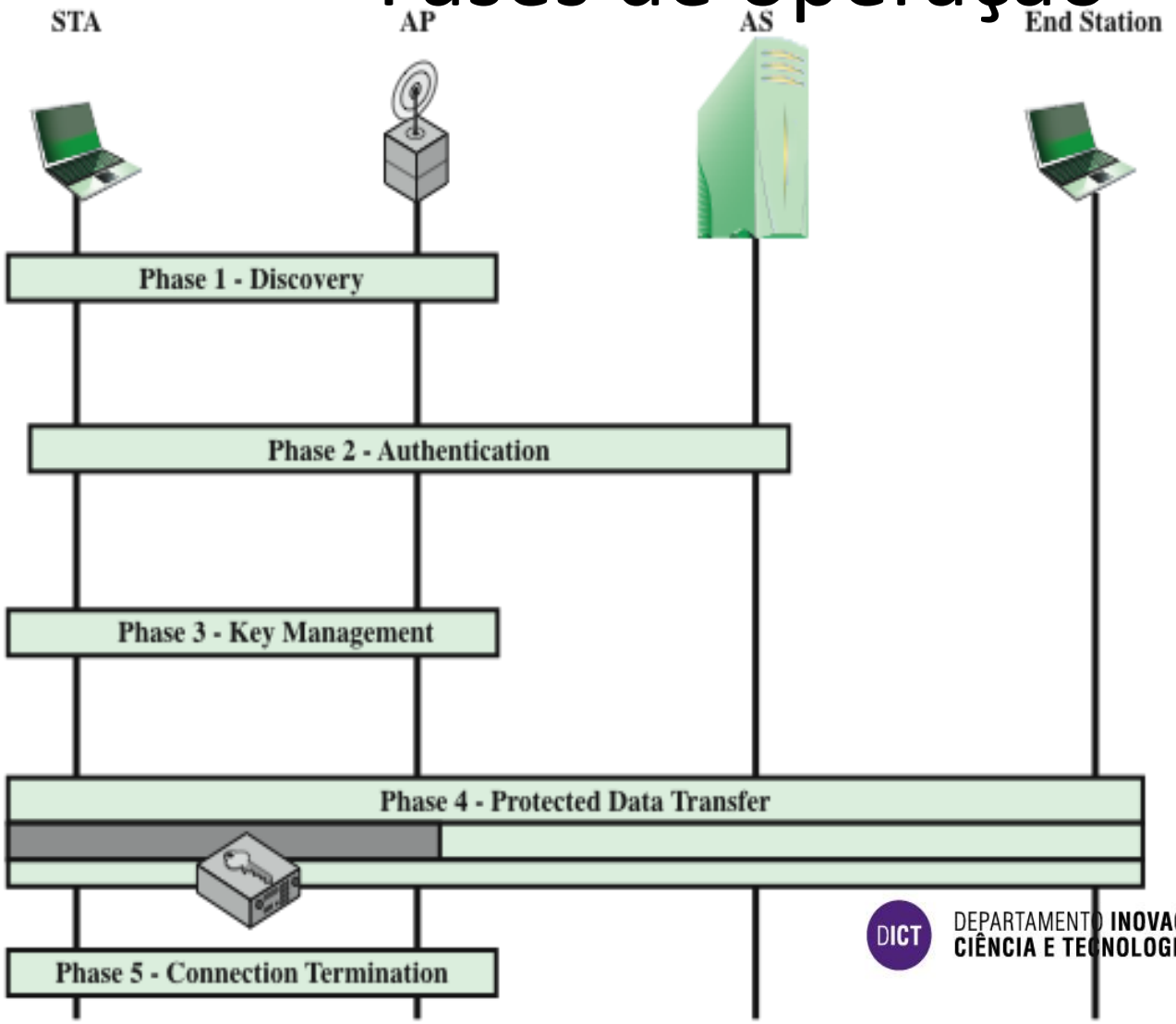
(b) Cryptographic Algorithms

Constituintes do IEEE 802.11i

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

IEEE 802.11i
Fases de operação



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA