Escola Superior de Ciências Empresariais
Instituto Politécnico de Viana do Castelo

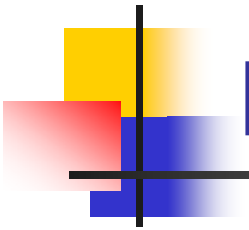
UNIVERSIDADE de AVEIRO

Avaliação do Desempenho de Sistemas de Segurança com Suporte WPA

Luís Barreto
Instituto Politécnico de Viana do Castelo

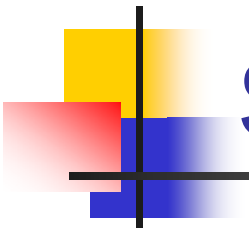
Susana Sargento
Universidade de Aveiro

8ª Conferência sobre Redes de Computadores, 29-30 Setembro, 2005



Motivação

- Popularidade das redes de computadores sem fios
  - *Hotspots*
  - Campus Virtuais
- Necessidades específicas ao nível da segurança
  - Ar é um meio partilhado
  - Não existe a necessidade de se estar fisicamente ligado
  - Facilidade de realização de ataques à segurança
    - Visualização de informação
    - Obtenção de palavras-chave
    - Etc.



Sumário

1. Redes sem fios e suas particularidades
2. WEP e seus problemas
3. Mecanismos de segurança WPA
4. Experimentação e resultados obtidos
5. Conclusões

Redes sem fios e suas particularidades

- Facilidade e flexibilidade de instalação
- Utilização de um meio partilhado, o ar, para a transmissão da informação
- É possível obter acesso a recursos e a informação de forma não autorizada
- Importante garantir os serviços de autenticação, confidencialidade, integridade e não-repúdio

Mecanismos de segurança nas redes sem fios

- Desde há algum tempo que tem havido necessidade de introduzir mecanismos de segurança, principalmente em redes sem fios
- Mecanismos como:
  - WEP (*Wired Equivalent Privacy*)
  - IPSec (*Internet Protocol Security*)
  - 802.1X (Autenticação Baseada em portas)
  - WPA (*Wi-Fi Protected Access*)
  - 802.11i / WPA2 / RSN (*Robust Security Network*)

WEP (*Wired Equivalent Privacy*)

- Primeira tentativa de implementação de um protocolo de segurança em redes sem fios
- Características:
  - Protocolo RC4 (*Rivest Code* 4)
  - Chave de 40 ou 104 *bits*
  - Vector de Inicialização (IV) de 24 *bits*
  - Verificação de integridade (*checksum* ou ICV) obtida de forma linear
- Apresenta, no entanto, muitas falhas:
  - Falsificações
    - Obtenção linear do ICV permite inserir e alterar informação
  - Ataques de repetição
    - ICV é anexado no final da trama e não é cifrado
  - Ataques de colisões ou de reutilização de IV
    - IV de 24 *bits* não é suficiente
    - Placas de rede que inicializam a zero o IV sempre que a placa é activada

WPA (*Wi-Fi Protected Access*)

- Forte substituto do WEP e interoperacional com o WEP
- TKIP (*Temporal Key Integrity Protocol*) para codificação dos dados
  - MIC (*Message Integrity Check*)
    - Obtido de forma não linear
    - Elimina ataques de falsificação
  - IV estendido/Novo contador de sequência IV
    - 48 *bits* - permite chaves dinâmicas por pacote
    - TSC (TKIP *Sequence Counter*) - elimina ataques por repetição
  - Chave de cifra de 128 *bits*
  - Protocolo criptográfico RC4
  - Autenticação através do 802.1X
    - Controlo de acesso centralizado

SS1

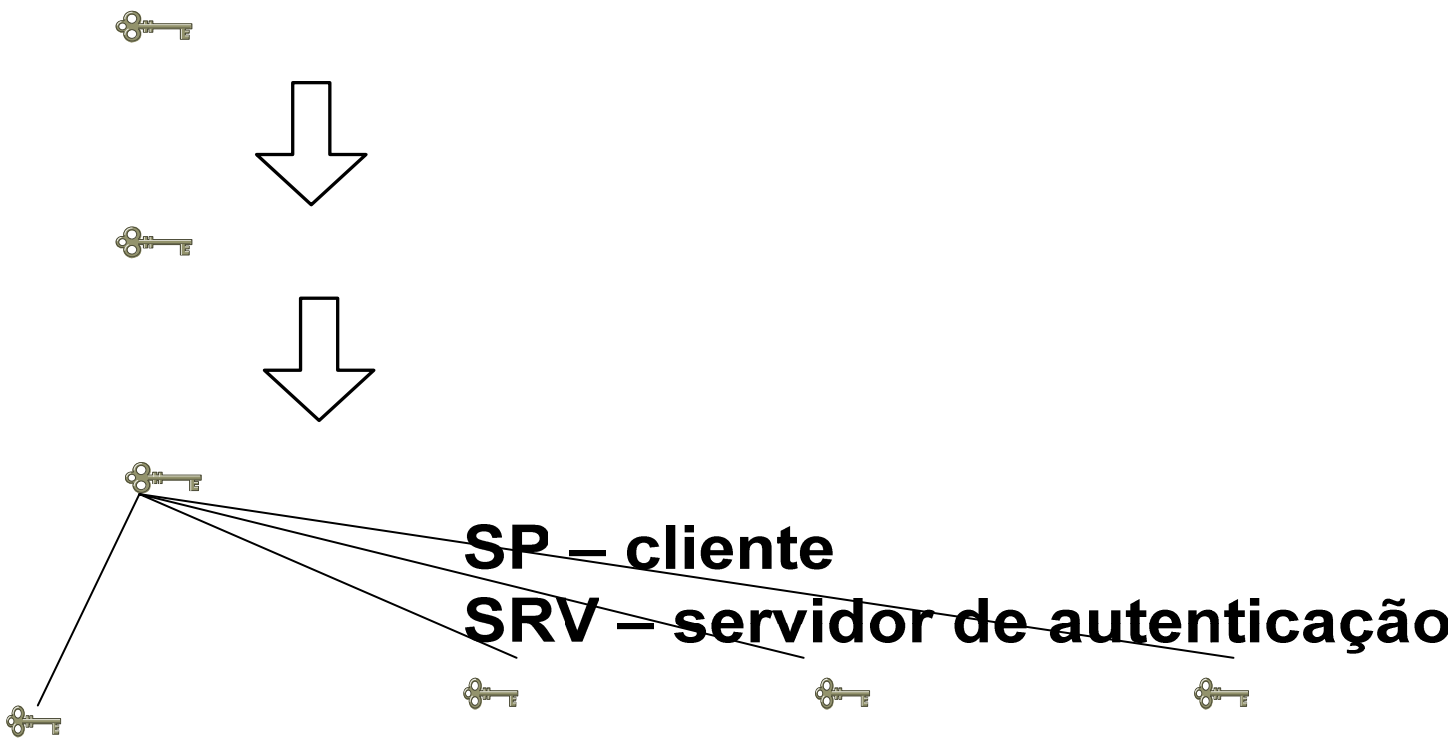
Slide 7

SS1 Depois dizer brevemente o que cada um destes mecanismos faz de especial e as suas diferenças em relação ao WEP

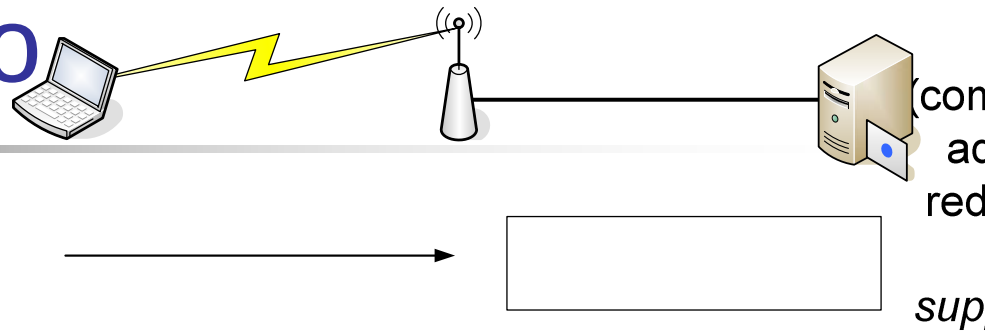
Susana Sargento; 13-07-2005

WPA (cont.)

- Hierarquia de chaves

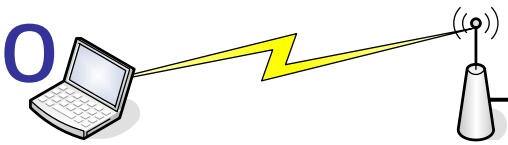


WPA
Funcionamento

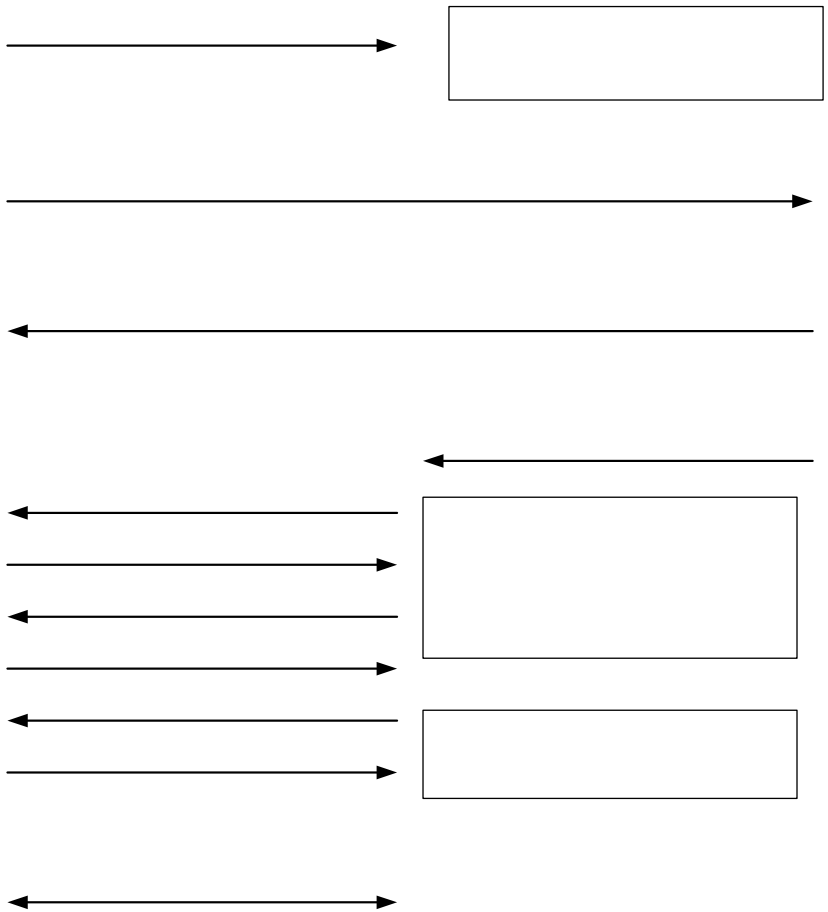


- Descoberta
  - Possíveis pares com quem comunicar
  - Anunciar as capacidades de segurança da rede aos clientes
- Autenticação 802.1x
  - Tornar o servidor num centro de decisão das políticas de acesso à rede
  - Autenticação mútua entre o cliente e o servidor (mensagens 802.1X)
  - Geradas as MK e a PMK
- Distribuição de chaves
  - Envio da PMK ao AP
- Gestão de chaves
  - AP e cliente confirmam que conhecem a PMK
  - PTK é gerada e sincronizada (*four-way handshake*)
  - Distribuição da GTK (*Group Key Handshake*)

WPA
Funcionamento



- WPA-PSK
  - Chave PMK pré-configurada
  - Fase de descoberta, autenticação e gestão de chaves não são realizadas
  - Fase de distribuição de chaves



Experimentação e Resultados

- WPA-EAP
  - Implementação do servidor de autenticação
    - *FreeRADIUS* numa máquina da rede
  - Implementação da Autoridade Certificadora
    - *OpenSSL* no servidor de autenticação
  - Cliente da rede sem fios com suporte EAP e WPA
    - *wpa_supplicant* num cliente da rede
  - AP da D-Link DWL 2000-AP+
- WPA-PSK
  - Cliente da rede sem fios com suporte EAP e WPA
    - *wpa_supplicant* num cliente da rede
  - AP da D-Link DWL 2000-AP+

Resultados obtidos

- Funcionamento dos mecanismos implementados
  - Visualização da informação trocada entre entidades (com a ferramenta *Ethereal*)
- Reacção a ataques de segurança
  - *Homem no meio*, Negação de serviço, Personificação, Repetição e Modificação da Informação
    - *Ettercap*, *Cain & ABel*
  - Ataque Passivo de Dicionário ao WPA-PSK
    - coWPAtty e *ptcrack*
- Desempenho da rede e dos seus equipamentos
  - Largura de Banda/ *Troughput*, *Jitter* e pacotes perdidos
    - IPERF
  - CPU, Memória, I/O, Processos
    - Vmstat & Sysstat

Funcionamento do WPA

WPA-EAP

- Mensagem de determinação da PTK (*four-way handshake*)
  - Tipo de chave a negociar PTK (*Key Type* : PTK)
  - Indicação de que ainda não é possível instalar as chaves (*Install flag:Not set*)
  - Indicação de que processo *four-way handshake* ainda não terminou (*Secure flag: Not set*)
  - MIC da chave (*Key* MIC *flag: Set*)
  - Protocolo de gestão de chaves TKIP
  - Protocolo de autenticação WPA

```
16 5.162645 192.168.120.2 D-Link_09:d3:ea EAPOL Key
▸ Frame 16 (137 bytes on wire, 137 bytes captured)
▸ Ethernet II, Src: 00:0c:41:17:50:b0, Dst: 00:0f:3d:09:d3:ea
▾ 802.1x Authentication
    Version: 1
    Type: Key (3)
    Length: 119
    Descriptor Type: EAPOL WPA key (254)
  ▾ Key Information: 0x0109
      .... .... .... .001 = Key Descriptor Version: HMAC-MD5 for MIC and RC4 for encryption (1)
      .... .... .... 1... = Key Type: Pairwise key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install flag: Not set
      .... .... 0... .... = Key Ack flag: Not set
      .... ...1 .... .... = Key MIC flag: Set
      .... ..0. .... .... = Secure flag: Not set
      .... .0.. .... .... = Error flag: Not set
      .... 0... .... .... = Request flag: Not set
      ...0 .... .... .... = Encrypted Key Data flag: Not set
    Key Length: 32
    Replay Counter: 1
    Nonce: 0452A5E30C669E4F2F014864DF9237EB7AD85F5FA364779B...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 04F62A6A2D4FF85418BD551B7DFD1539
    WPA Key Length: 24
  ▾ WPA Key: DD160050F20101000050F20201000050F20201000050F201
      Tag Number: 221 (Vendor Specific)
      Tag length: 22
      Tag interpretation: WPA IE, type 1, version 1
      Tag interpretation: Multicast cipher suite: TKIP
      Tag interpretation: # of unicast cipher suites: 1
      Tag interpretation: Unicast cipher suite 1: TKIP
      Tag interpretation: # of auth key management suites: 1
      Tag interpretation: auth key management suite 1: WPA
```

Funcionamento do WPA-PSK

WPA-PSK

- Mensagem do processo *four-way handshake*
  - *Nonce* é diferente
  - Protocolo de autenticação PSK

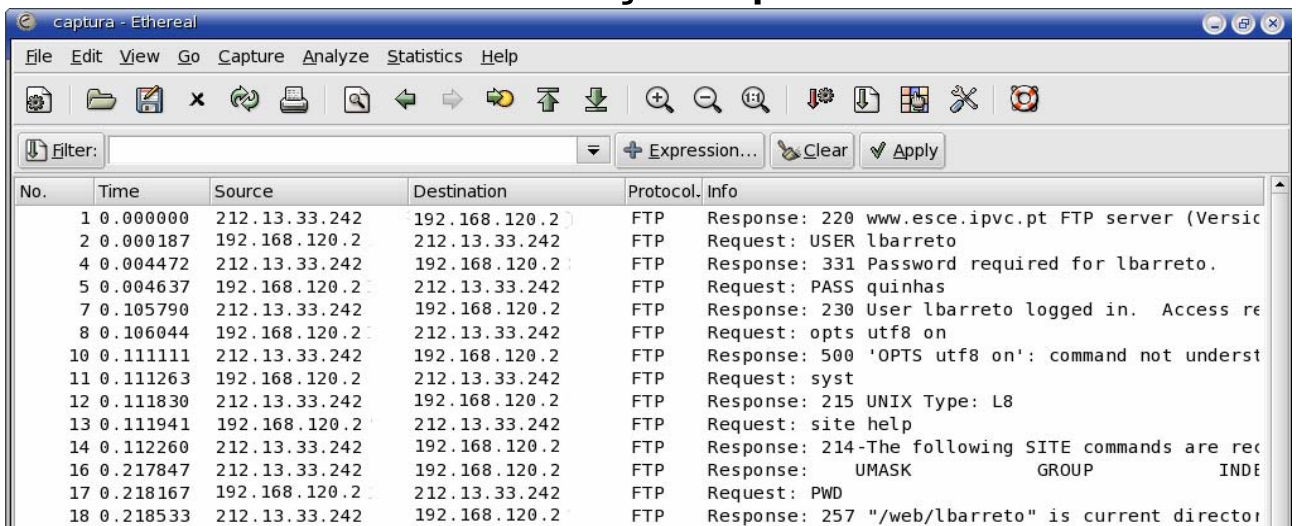
```
3 0.911900 192.168.120.2 192.168.120.1 EAPOL Key
Frame 3 (137 bytes on wire, 137 bytes captured)
Ethernet II, Src: 00:0c:41:17:50:b0, Dst: 00:0f:3d:09:d3:ea
802.1x Authentication
   Version: 1
   Type: Key (3)
   Length: 119
   Descriptor Type: EAPOL WPA key (254)
 Key Information: 0x0109
     .... .... .... .001 = Key Descriptor Version: HMAC-MD5 for MIC and RC4 for encryption (1)
     .... .... .... 1... = Key Type: Pairwise key
     .... .... ..00 .... = Key Index: 0
     .... .... .0.. .... = Install flag: Not set
     .... .... 0... .... = Key Ack flag: Not set
     .... ...1 .... .... = Key MIC flag: Set
     .... ..0. .... .... = Secure flag: Not set
     .... .0.. .... .... = Error flag: Not set
     .... 0... .... .... = Request flag: Not set
     ...0 .... .... .... = Encrypted Key Data flag: Not set
   Key Length: 32
   Replay Counter: 2
   Nonce: 1CB015635D7F0C795527D3575A170FC125425FF62D548BFE...
   Key IV: 00000000000000000000000000000000
   WPA Key RSC: 0000000000000000
   WPA Key ID: 0000000000000000
   WPA Key MIC: 0EAD61BB0BFD0CBE88C6B4139C245FAE
   WPA Key Length: 24
 WPA Key: DD160050F20101000050F20201000050F20201000050F202
     Tag Number: 221 (Vendor Specific)
     Tag length: 22
     Tag interpretation: WPA IE, type 1, version 1
     Tag interpretation: Multicast cipher suite: TKIP
     Tag interpretation: # of unicast cipher suites: 1
     Tag interpretation: Unicast cipher suite 1: TKIP
     Tag interpretation: # of auth key management suites: 1
     Tag interpretation: auth key management suite 1: PSK
```

Reacção a ataques de segurança

- Protocolo da camada de ligação de dados
- Ferramentas funcionam na camada de rede
- Não foi possível realizar ataques *homem no meio*, modificação, repetição
- Ataques de personificação também falharam
  - Mesmo IP, nome que um cliente autorizado
  - *wpa_supplicant* e certificados digitais com a mesma designação
- Ataques de negação de serviço
  - Intruso efectua de forma continuada pedido de autenticação
  - AP bloqueia impedindo a autenticação de clientes
- Ataque passivo de dicionário (WPA-PSK)
  - Registo das mensagens *four-way handshake*
  - Utiliza-se o *coWPAtty* ou *ptcrack* para se obter a PMK
  - Configura-se no intruso a PMK

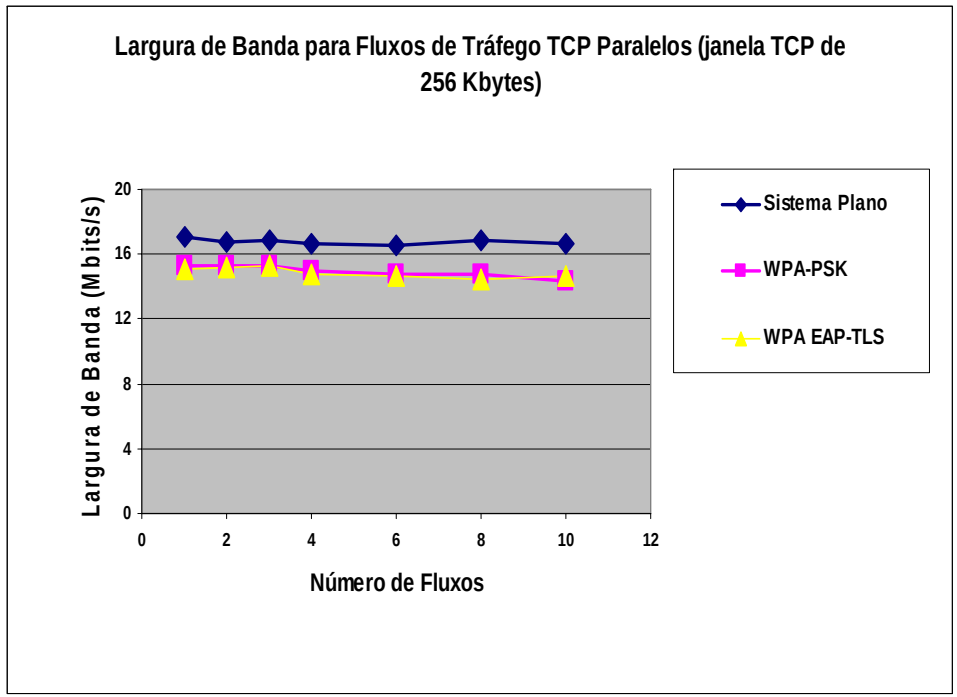
Reacção a ataques de segurança (cont.)

- WPA- PSK – ataque de dicionário
  - Com o coWPAtty obteve-se a PMK
    - # ./cowpatty -r eap-psk.dump -f dict -s wpa
    - The PSK is "thewindinthewillows".
  - Configurou-se a PMK no cliente e com o *ethereal* obteve-se a informação que circulava na rede



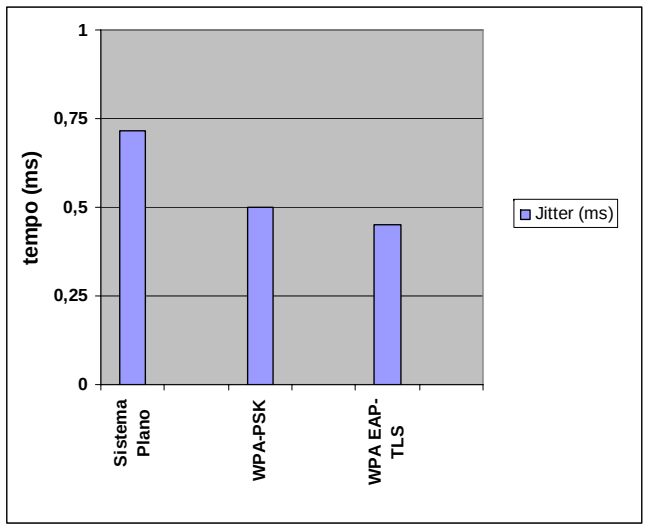
Desempenho da rede e dos seus equipamentos

- Largura de banda utilizada por vários clientes em simultâneo
  - Diminuição do desempenho com o aumento do número de clientes
    - Maior número de colisões
    - Menor capacidade do AP em processar as mensagens

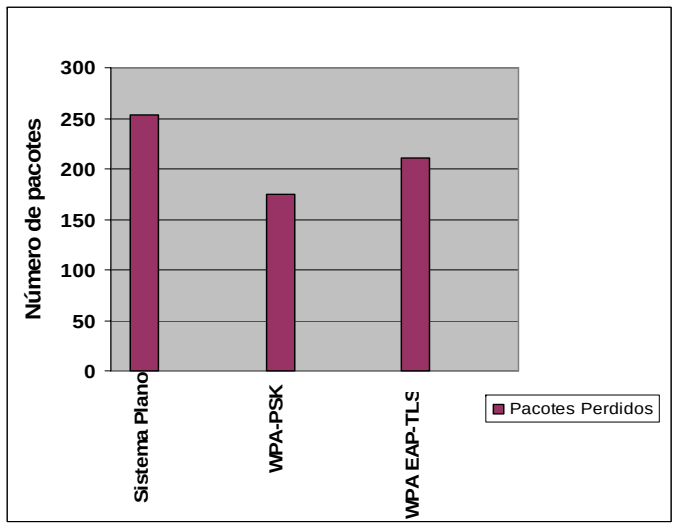


Desempenho da rede e dos seus equipamentos (cont.)

- *Jitter* e número de pacotes perdidos
  - Sistemas WPA apresentam menor número de pacotes perdidos
    - Menor número de mensagens a circular na rede
    - Menor número de colisões
  - WPA apresenta melhores valores de *Jitter*
    - Sistema plano, o *buffer* do AP está congestionado
      - Envio no mesmo espaço de tempo de maior número de mensagens



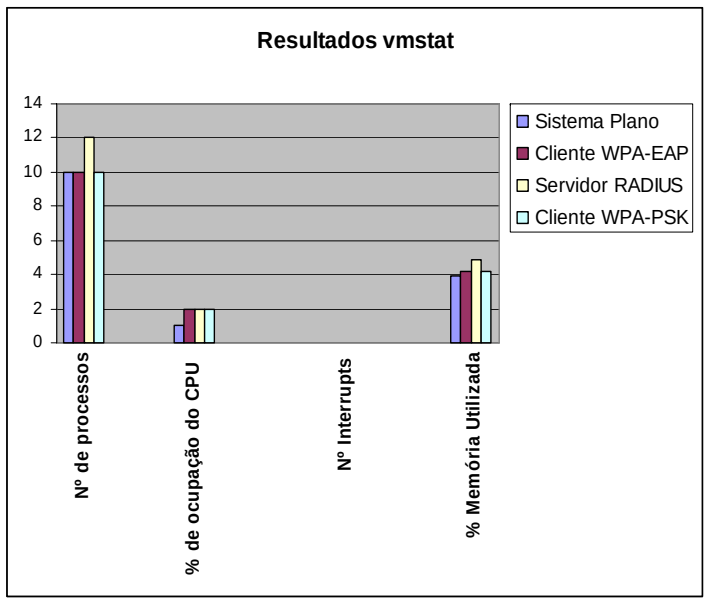
Jitter.



Pacotes perdidos.

Desempenho da rede e dos seus equipamentos (cont.)

- Avaliação do desempenho dos equipamentos
  - WPA não implica um aumento das necessidades dos sistemas



Conclusões

- Estudo do mecanismo de segurança em redes sem fios WPA
- Implementação e estudo experimental
  - Foi possível a implementação com ferramentas em código aberto
- O protocolo WPA é eficaz contra ataques de *homem no meio*, modificação de informação, falsificação e controlo de sessão
- Não protege contra ataques de negação de serviço
- WPA-PSK não protege contra ataques de dicionário
- WPA apresenta bons resultados de *troughput* e *jitter e* número de pacotes perdidos
  - Pacotes sofrem pequenas alterações
  - Algoritmo de cifra rápido
- WPA não exige sobrecarga dos equipamentos
  - CPU e de memória utilizada