UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Comunicação Sem Fio (Wireless)

Aula 8 – Segurança em Redes Sem-fio

Prof. Fred Sauer

email: fsauer@gmail.com

http://www.fredsauer.com.br

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Base da segurança:
  - Confidencialidade
    - ✓ Controle de acesso
    - ✓ Não-repúdio
  - Integridade
  - Disponibilidade

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Confidencialidade:
  - A informação só deve ser acessada por quem for autorizado
  - Proteção de dados privados
  - Formas de obter confidencialidade
    - ✓Controle de acesso
    - ✓Controle das operações individuais de cada usuário (não-repúdio)

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Integridade:
  - – A informação não pode ser corrompida, e se for, isto precisa ser detectado
  - – Em alguns casos, a integridade pode ser mais importante do que a confidencialidade (por exemplo, escrituras de imóveis)
  - – Pode haver alteração dos dados na fonte, no destino ou durante o trânsito.

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Disponibilidade:
  - – A informação deve estar sempre disponível para uso
  - – Uma ruptura do sistema não deve impedir o acesso aos dados
  - – Impedir a disponibilidade é uma forma de ataque à segurança, pois isso pode impedir a verificação se os dados continuam confidenciais e íntegros

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Soluções para a segurança:
  - Autenticação
    - ✓ Autenticação de Usuários
    - ✓ Certificação Digital (PKI)
  - Confidencialidade
    - ✓ Controle de acesso
      - Na Estação e na Rede
    - ✓ Criptografia de Dados
      - Na Estação e na Rede (VPN, Criptografia de e-mail)

INTRODUÇÃO

- Soluções para a segurança:
  - Integridade
    - ✓ Assinatura digital
    - ✓ Anti-Virus / Anti-Trojan / Anti – Spyware
    - ✓ Controle de Conteúdo Ativo (ActiveX, Applets)
  - Monitoramento
    - ✓ Estático (análise/detecção de vulnerabilidades)
    - ✓ Dinâmico (Intrusion Detection / Intrusion Prevention)

INTRODUÇÃO

- Soluções para a segurança:
  - Controle Centralizado
    - ✓ Auditoria / Reporting
    - ✓ Instalação / Manutenção
    - ✓ Backup
    - ✓ Política de Segurança

INTRODUÇÃO

- Como se proteger:
  - Prevenção
  - Detecção
  - Resposta

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Plano de Segurança:
  - Planejamento e administração geral
    - ✓ Quais recursos devo proteger?
    - ✓ De quem/qual tipo de ameaça precisamos proteger?
    - ✓ Análise de custo e riscos
  - Segurança no dia-a-dia
    - ✓ Senhas, acessos, auditoria
  - Administração no dia-a-dia
    - ✓ Contas, manutenção, disponibilidade

INTRODUÇÃO

- Plano de Segurança:
  - Deve conter
    - ✓ Diretrizes
    - ✓ Normas
    - ✓ Procedimentos

Conceitos Sobre Segurança em Redes Sem Fio

INTRODUÇÃO

- Plano de Segurança:
  - Segurança Física
    - ✓ Relativo a proteção dos ATIVOS (ex: controle de acesso físico às instalações e CPD)
  - Segurança Lógica
    - ✓ Relativo a proteção das INFORMAÇÕES (ex: ataques e invasões)
  - Segurança Técnica
    - ✓ Relativo a falhas involuntárias (ex: pane em equipamentos)
  - Segurança Humana
    - ✓ Relativo ao despreparo de usuários e administradores

MOTIVAÇÃO

- Grande problema em redes sem fio.
- Muito suscetível a interceptações dos dados da rede
- Necessidade de protocolos de segurança para garantir a privacidade da rede

WEP

- Segurança em redes sem fio no padrão IEEE 802.11 original
  - Autenticação
    - ✓ Sistema Aberto (Open System)
    - ✓ Chave Compartilhada (Shared key)
  - Criptografia
    - ✓ Wired Equivalent Privacy (WEP)
  - Integridade
    - ✓WEP-encrypted Integrity Check Value (ICV)
      - Cyclical Redundancy Check (CRC)-32 checksum calculation

WEP

- WEP (Wired Equivalent Privacy):
  - Atua na camada de enlace entre estações e o Ponto de Acesso (AP)
  - Pode ser implementado em Software ou Hardware
  - Chaves de 40 bits ou 104 bits no RC4
  - Opcional
  - Foi projetado para oferecer integridade, confidencialidade e autenticação
  - Possui inúmeros problemas de segurança

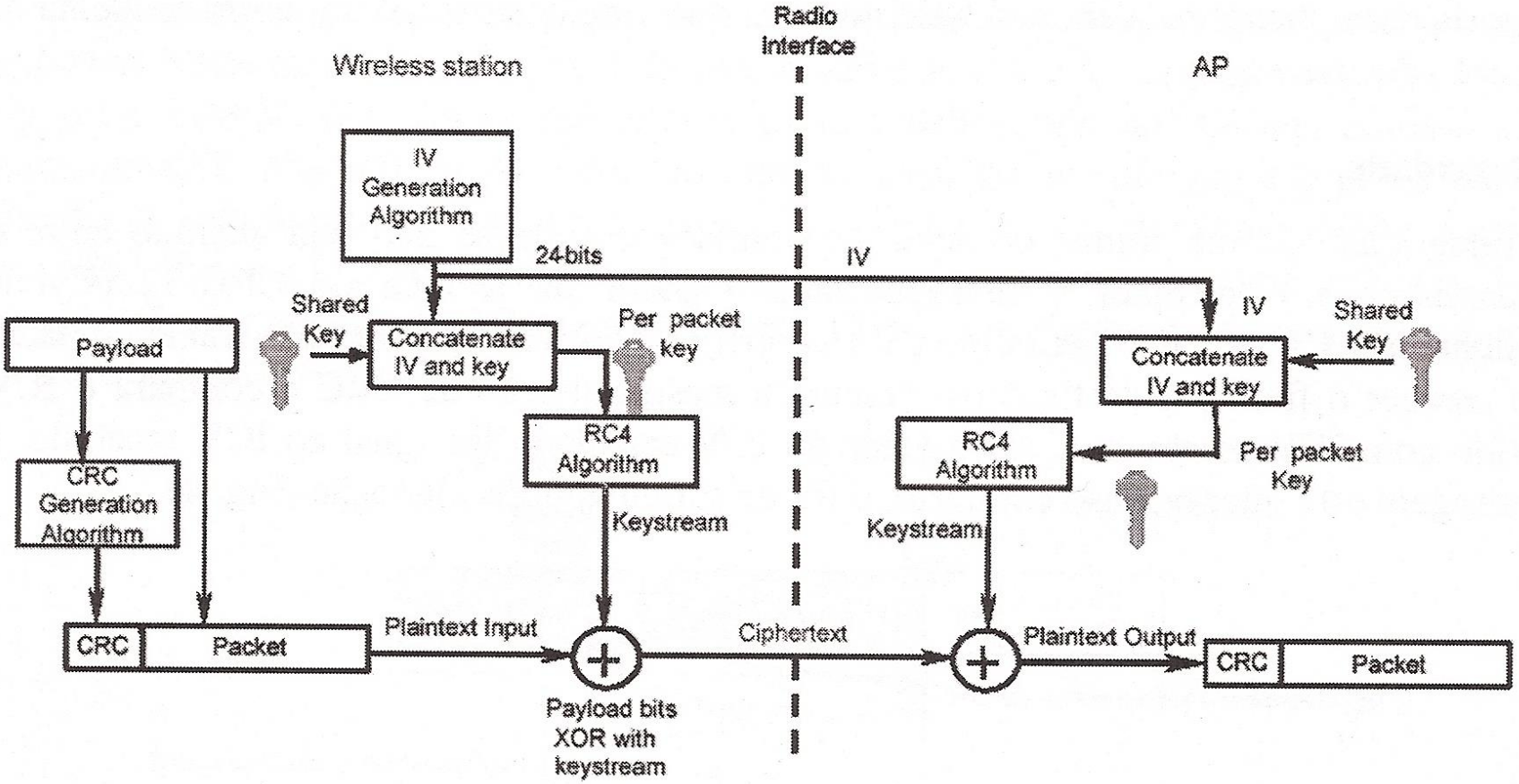
WEP

- Confidencialidade:
  - – Cada frame é criptografado independentemente dos demais
  - –Utiliza um vetor de inicialização (IV) para ampliar as chaves de 104 para 128 bits

IV	CHAVE SECRETA

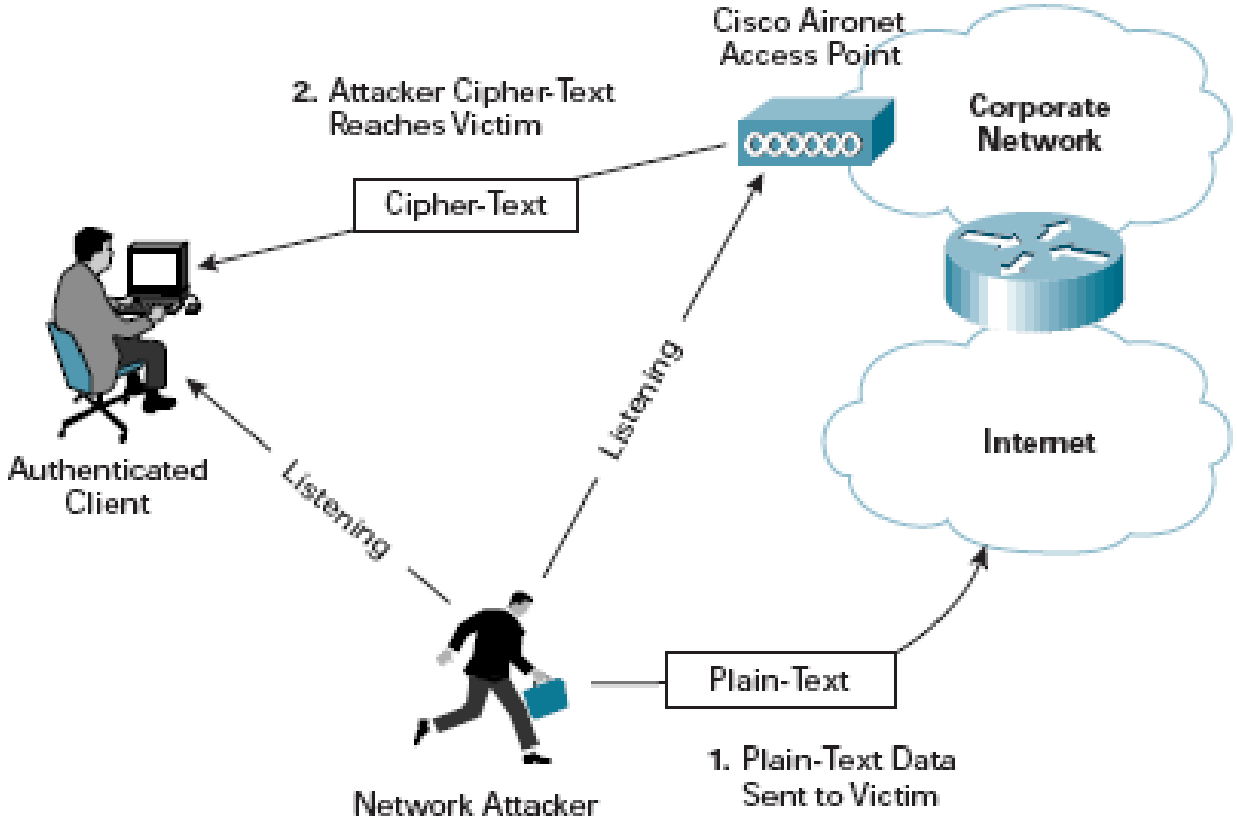
WEP

- Confidencialidade - Processo:



WEP

- Confidencialidade:
  - Problemas:
    - ✓ Não existe esquema de gerência de chaves. As estações e o AP compartilham a mesma chave
    - ✓ Existem diversos ataques que exploram o pequeno tamanho da chave de criptografia e a forma como é inicializada e incrementada.
    - ✓ O IV é transmitido em claro junto com a mensagem
    - ✓ Após pouco tempo monitorando o tráfego da rede em um celular é possível obter a chave de criptografia através de análise estatística dos textos cifrados
    - ✓ É possível obter-se a chave criptográfica a partir de uma mensagem conhecida e a respectiva mensagem criptografada

WEP

- Confidencialidade:
  - Problema: