Projeto AirStrike:
Um Sistema com Acesso Seguro e Gerenciamento Integrado para Redes sem Fio Baseadas no padrão 802.11

Airon Fonteles da Silva
Bruno Astuto A. Nunes
Luciano R. de Albuquerque

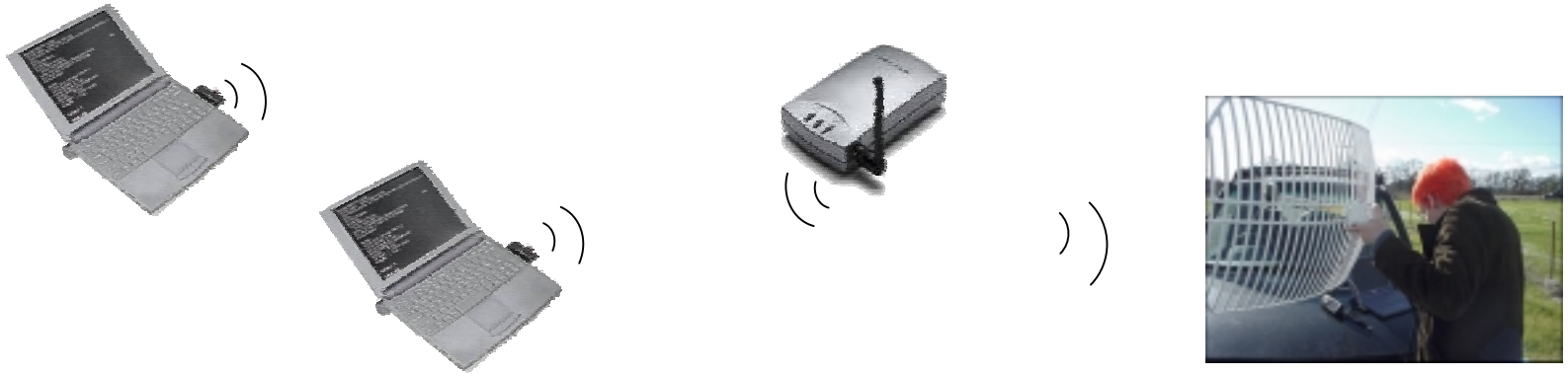
Sumário

- Aspectos importantes de segurança
- Soluções de segurança atuais
- Projeto AirStrike
  - Atual
  - Integração ICP
- Em desenvolvimento
- Considerações finais

Aspectos importantes de segurança

- Autenticação mútua
- Autorização
- Privacidade
- Integridade
- DPD (Dead Peer Detection)
- Tempo de resposta a falhas

Problemas da Segurança se Agravam num Meio Sem Fio



- Redes sem fio envolvem, de forma simples, a comunicação via rádio
  - Logo, qualquer um pode bisbilhotar e/ou injetar tráfego

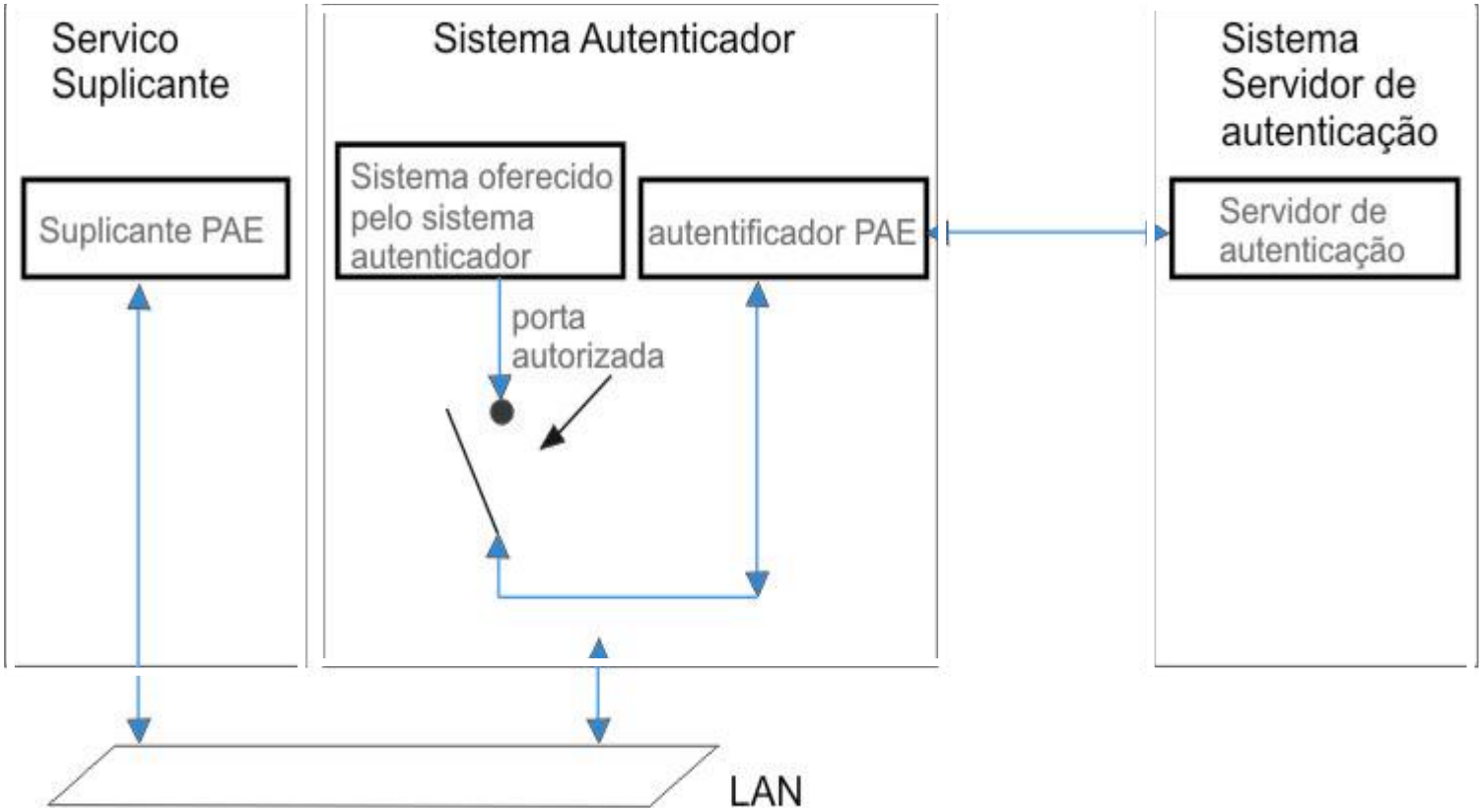
Soluções de Segurança Atuais

- WEP
- 802.1X
- WPA 1 e WPA 2
- Portais de captura
- DHCP Autenticado

Soluções de Segurança Atuais
WEP (Wired Equivalent Privacy)

- Utilização opcional
- Atua na camada de enlace
- Chaves de 40 e 104 bits
- VI de 24 bits
- Diversas falhas de segurança
  - Walker 2000
  - Borisov 2001
  - Fluhrer 2001

Soluções de Segurança Atuais
802.1X



- Possui falhas
  - Arbaugh, William 2002

Soluções de Segurança Atuais

WPA (Wi-Fi Protected Access)

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

- Possui falhas
  - Bob Moskowitz (ICSA Labs) 2003

Soluções de Segurança Atuais
Portais de captura

	Oasis	NoCat	NetLogon
Licença	BSD	GNU / GPL	GNU /GPL
Software cliente	Não	Não	Não
Autenticação	Através de PAM	Arquivo de senha local, BD MySQL	SSH, POP3, IMAP, NIS
Plataformas	Linux (FreeBSD)	UNIX	Linux
Control de acesso	Filtragem IP/MAC	Filtragem IP/MAC	Filtragem IP
DPD	ARP/ICMP ping, plug-in ou monitoramento de tráfego	Timeout	ARP ping, SNMP para SWITCH

AAIP : DHCP Autenticado

- RFC 3118
  - Não existem implementações
- Avaliação de segurança
  - Utiliza MD5
  - Não permite uso de outros algoritmos
  - Autenticação da STA somente
  - Suscetível a ataques DoS

Projeto AirStrike

AirStrike
Características

- Implementação de um PA em um PC
- Baseado na utilização de software livre
  - OpenBSD 3.6
- Mecanismos de segurança
  - Autenticação (login/senha e certificados)
  - Autorização (*firewall*)
  - Privacidade e integridade (*IPSec*)
  - Dead Peer Detection (*isAlive*)

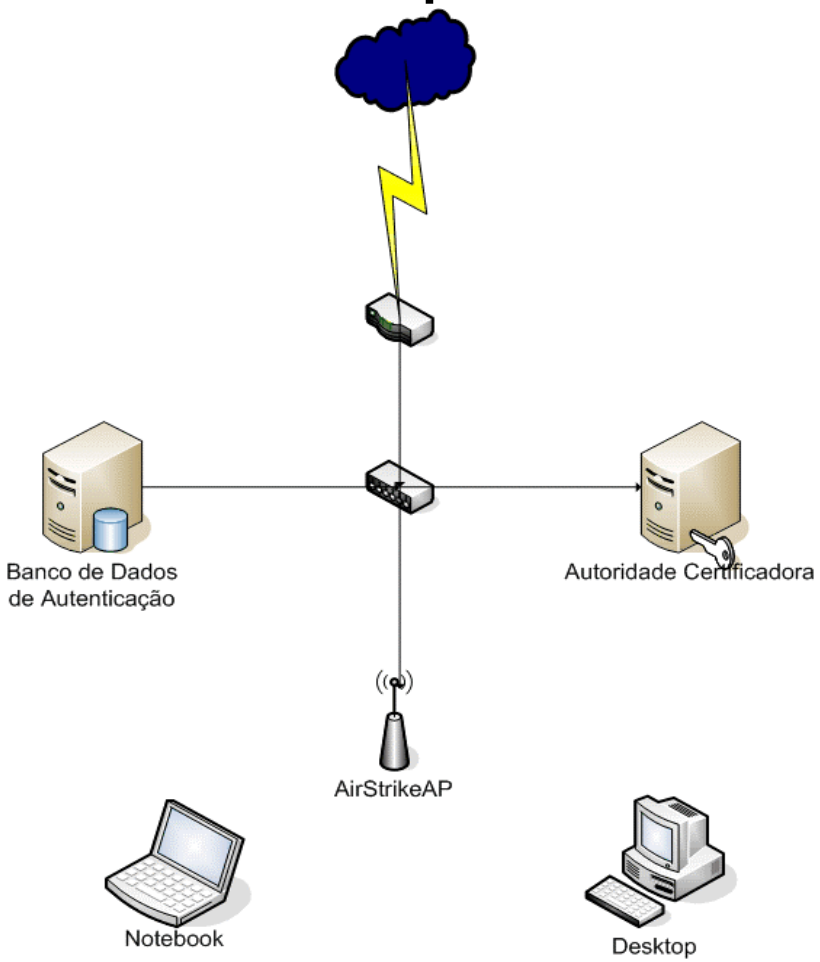
AirStrike
Mecanismos de segurança

- Autenticação mútua
- Autorização
- Privacidade
- Integridade
- DPD (Dead Peer Detection)
- Tempo de resposta a falhas

AirStrike
DPD (Dead Peer Detection)

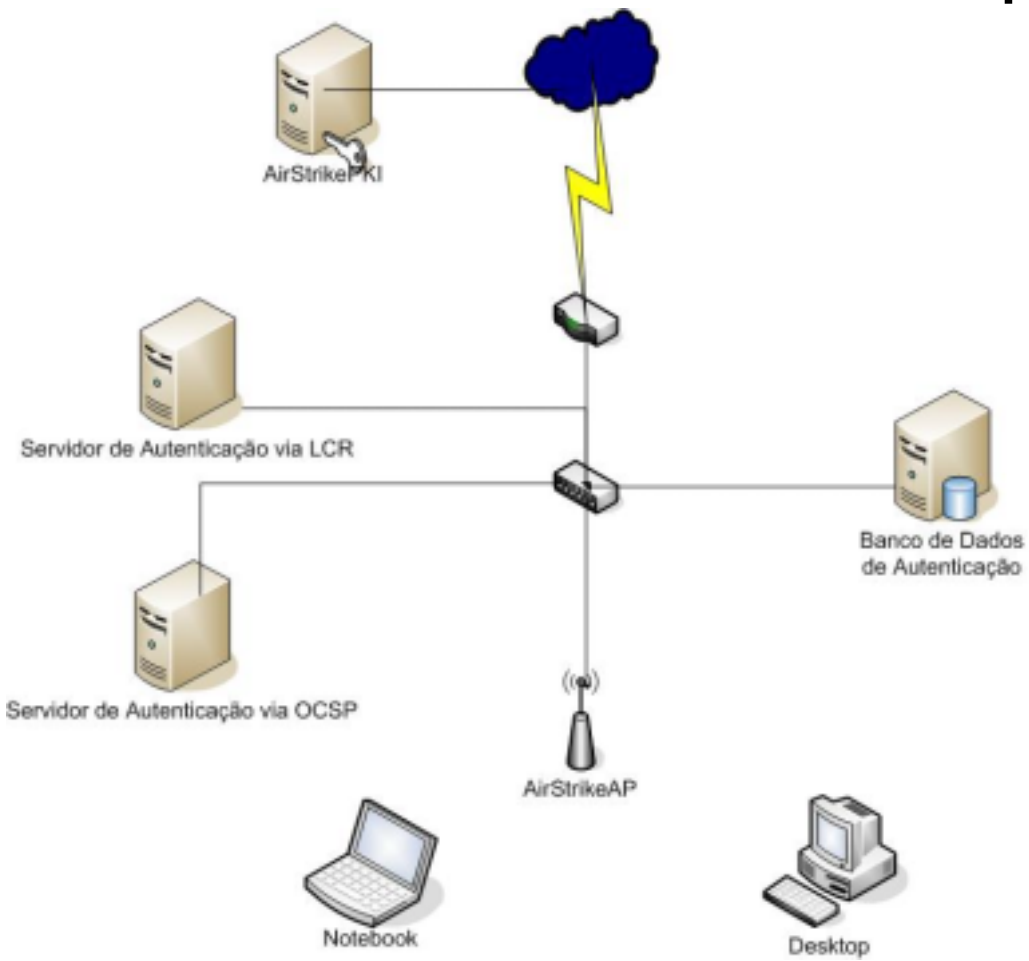
- isAlive
  - Garantia do controle de acesso
  - Tarifação por tempo de uso
  - Dead após K em N mensagens
    - (Time to Kill controlado)
  - Tratamento de mensagens falsas
  - Processamento em paralelo

AirStrike
Arquitetura



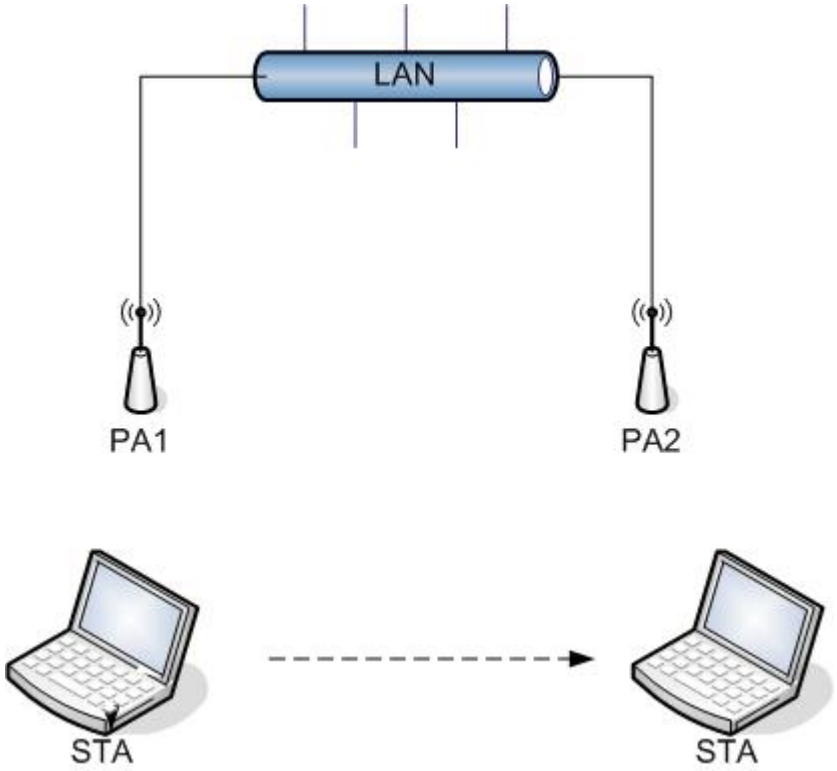
Integração

Integração com outros projetos
Infraestrutura de chave pública



Projeto AirStrike
em desenvolvimento

Integração com outros projetos
Handover



- Objetivos
  - Pré-alocação de recursos
  - Segurança

Integração com outros projetos
Handover

- Comunicação
  - STA → PA
    - Lista de PAs
  - PA → Entidade Central
  - Entidade Central → PAs
    - Histórico de movimentação
    - Predição de mobilidade
    - Pré-alocação de recursos

AirStrike
Em desenvolvimento

- Gerenciamento simplificado
  - Gerenciamento de segurança atuais usam paradigmas equivocados
  - Interface única e integrada entre os dispositivos de segurança
  - Manter a integridade entre os mecanismos de segurança

AirStrike
Em desenvolvimento

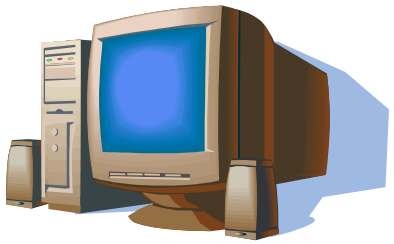
- Utilização simplificada
  - Cliente e servidor próprios
  - Interface única e integrada entre os dispositivos de segurança
  - Não utiliza servidor web
  - Não utiliza browser

AAIP: TLS Protocolo

Cliente

Handshake TLS baseado em CD

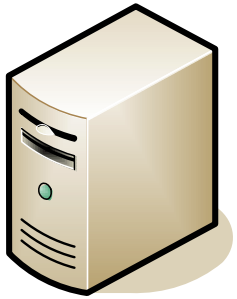
Servidor



.
.
.

isAliveProbe

isAliveResponse



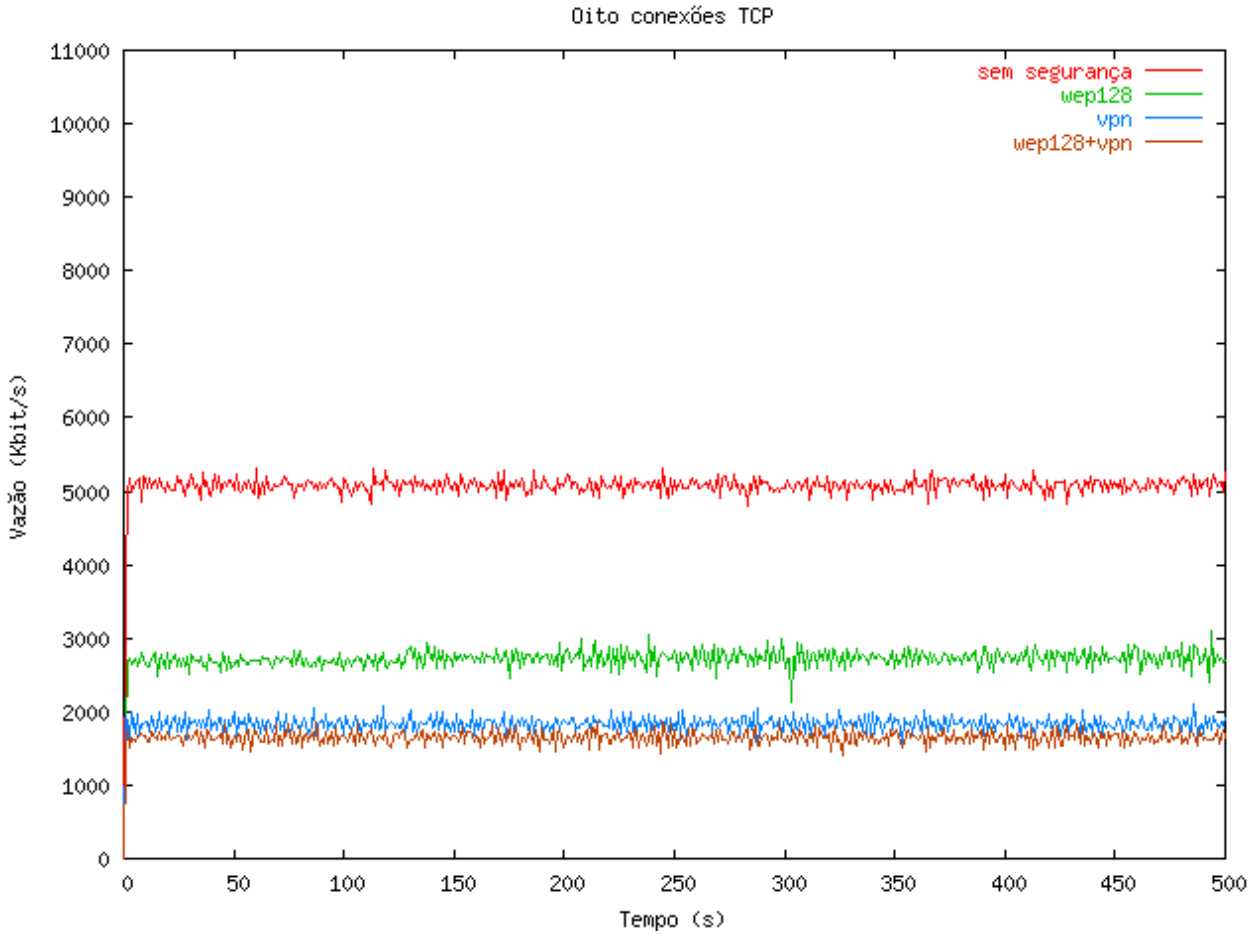
AAIP: TLS
Implementação

- 3 entidades: AP, STA, “ICP”
- Utilização do OpenSSL
- Autenticação mútua
- Utilização de certificados digitais
- Necessita de uma ICP

Considerações Finais

- Avaliar impactos causados pelos mecanismos de segurança
  - Mecanismos de segurança diminuem QoS
- Avaliar custo-benefício entre segurança e QoS

Considerações Finais



Avaliando a Sobrecarga Introduzida nas Redes 802.11 pelos Mecanismos de Segurança WEP e VPN/IPSec
[Ditarso,Arouche, de Moraes -- 2003]

Considerações Finais

- Mecanismos atuais não atendem todos os requisitos de segurança
- Constante busca de novas soluções que incrementem a segurança

Obrigado !