

Redes Wireless 802.11b

Características y Securización

FIST Conferences 2003
October Edition

Javier Pascual Soriano “DaVinci”
CIUPS – Club de Informática de la UPSAM

E-Mail: jpascual@ciups.com

Web: <http://www.ciups.com>

¿Qué es una red inalámbrica 802.11b?

- Características Generales
 - Velocidad estándar de 1 a 11 Mbps
 - 11-15 Canales de emisión (depende del País)
 - Espectro de Frecuencia 2,4Ghz
- Elementos de la Red
 - Puntos de Acceso (AP)
 - Clientes (STA)
 - Antenas y Cableado
- Topologías y Funcionamiento
 - Punto a Punto: Ad-Hoc
 - Infraestructura: Managed y Master
 - Monitor

¿Por qué son inseguras estas redes? (I)

- La seguridad como fiabilidad del servicio
 - Degradación de la señal
 - Interferencias con Objetos y Personas
 - Colisión de frecuencias (Ej.: microondas)
 - Solapamiento entre canales
 - Limita el número de canales a utilizar
 - 3-4 canales sin solapamiento (1-6-11 ó 1-5-9-13)
 - Necesidad de *Roaming* entre APs
 - Distancia y dirección de la emisión
 - Adecuarlos a la necesidad (Ej.: Punto a Punto)
 - Restringir el campo de acción

¿Por qué son inseguras estas redes? (II)

- 802.11b: “Malformaciones de nacimiento”
 - Características del protocolo
 - Estándar IEEE 802.11b
 - Tipos de Tramas: Gestión, Datos y Control
 - Deficiencias innatas
 - Sistema de autenticación
 - Los problemas de la autenticación
 - *MAC Spoofing*
 - *Management Frames Spoofing*
 - Ataques de Disociación y Desautenticación
 - *Man-in-the-Middle*

¿Por qué son inseguras estas redes? (y III)

- WEP: “**W**ired **E**quivalence **P**rivacy”
 - Posible sinónimo: “**W**ireless, **E**nter **P**lease”
 - Características
 - Proporciona mecanismos de Autenticación y Cifrado
 - Cifrado mediante clave simétrica basado en RC4
 - Problemas
 - Claves estáticas. Fácilmente “crackeables”
 - Únicamente cifra las tramas de datos
 - Bits de encriptación no reales: 40 y 104 (-24 del IV)
 - Autentica dispositivos, no usuarios
 - ICV (*Integrity Check Value*) fácil de simular

Securización 802.11b. Nivel Físico (I)

- La elección del Punto de Acceso
 - Hardware:
 - ✓ Mayor eficiencia
 - ✓ Mayor cobertura (relativo)
 - ✗ Difícil actualización de prestaciones
 - ✗ Limitaciones del fabricante
 - Software:
 - **Linux** vs Windows... LINUX!!
 - ✓ Muy configurable y fácilmente actualizable
 - ✓ Menor coste (relativo)
 - ✓ Mejor Monitorización y Securización
 - ✗ Mantenimiento más complejo

Securización 802.11b. Nivel Físico (II)

- La elección del hardware cliente (STA)
 - Dispositivos *PCI*
 - ✗ Escasa Portabilidad
 - Dispositivos *USB*
 - ✓ Alta Portabilidad
 - ✗ Configuración en Linux y Consumo
 - Dispositivos *PCMCIA*:
 - ✓ Alta Portabilidad (relativa)
 - ✓ Extenso soporte en Linux
 - Conector de antena externo !!

Securización 802.11b. Nivel Físico (III)

- Seguridad en las Ondas: Antenas
 - La Ganancia
 - En qué influye la ganancia de la antena
 - Ajustar la ganancia a nuestras necesidades
 - La dirección y el radio de las ondas
 - Ajustar los solapamientos
 - Prevenir accesos no deseados
 - El alcance de las ondas:
 - Mantener constante el ancho de banda
 - Evitar el reenvío de tramas
 - Tipos de Antenas: Omni, Direccionales

Securización 802.11b. Nivel Físico (y IV)

- Donde y cómo situar nuestra red *wireless*
 - Puertas de Enlace
 - El AP como enlace entre redes
 - La importancia de un equipo dedicado a enlace
 - *Firewall* entre redes
 - *Netfilter, Iptables*
 - Filtrar la entrada y la salida
 - *Bridges* Inalámbricos (*WDS*)
 - Pérdidas de conectividad en el cambio de AP
 - Repetidores: mayor tráfico e interferencias
 - Misma red IP: problemas de encaminamiento

Securización 802.11b. Nivel Lógico (I)

- Mínima seguridad ofrecida
 - Listas de Control de Acceso
 - Ocultamiento y Redundancia de APs
 - *Beacon Frames*
 - Redundancia de Servicio
 - Falsos APs: *fakeAP*, *fakeAP-jack* (*discovery-jack*)
 - Utilización de *WEP*
 - Siempre con 128 bits (ó 256) de cifrado
 - Variar la clave frecuentemente
 - Evitar utilizar *DHCP*
 - Monitorizar el tráfico
 - Localizar flujos extraños de paquetes

Securización 802.11b. Nivel Lógico (II)

- Adoptar medidas generales de seguridad:
 - Concienciar a los usuarios de la red
 - Cumplimiento de la política de seguridad interna
 - Precaución ante la ingeniería social
 - Adoptar una política de contraseñas robusta
 - Utilización de protocolos seguros:
 - *SSH, HTTPS, POP-SSL, SMTPS...* etc.
 - Utilización de Redes Privadas Virtuales
 - *OpenVPN, IPSec*, Freeswan, CIPE*
 - Incorporar mecanismos de QoS
 - Garantizar el ancho de banda a los usuarios
 - Prevención de ataques *DoS*

Securización 802.11b. Nivel Lógico (y III)

- 3 en 1: Portales Cautivos
 - Proporcionan Autenticación, Privacidad y Cifrado*
 - Autenticación de usuarios a través de web
 - Usuario y Contraseña <> autenticación dispositivos
 - Conexiones seguras con SSL (*HTTPS*)
 - El AP se comunica con un *GW* y éste con el *Auth Server*, que accede a la base de datos de usuarios
 - Los mensajes de autorización se firman mediante *PGP/GnuPG*
 - Una vez autenticado, el *GW* redirige el tráfico al exterior (*LAN, Internet, etc*)
 - Proporciona mecanismos de *QoS*
 - Útiles para la implementación de “Nodos Libres”
 - ✗ No resuelven el problema del *Spoofing*

Nuevas necesidades, nuevas soluciones (I)

- Necesidad de un mecanismo robusto de autenticación de usuarios y estaciones
- Que permita utilizar distintos mecanismos de autenticación y cifrado
- Surge el *IEEE 802.11i*. Grupo de trabajo para desarrollar mejoras de seguridad para las redes *WLAN*:
 - Autenticación mutua: usuario – red, red – usuario
 - Autenticación de usuarios, no de dispositivos.
 - Generación de claves dinámicas y únicas para cada usuario.
 - Para ello, hace uso de *IEEE 802.11X*, *WPA* y *TKIP*

Nuevas necesidades, nuevas soluciones (II)

- Mecanismo *IEEE 802.11X*
 - Estándar basado en el protocolo de autenticación *EAP* (*EAPoL*)
 - Validación de usuarios centralizada
 - Servidor *RADIUS* con credenciales usuarios
 - Posibilidad de generar claves *WEP* dinámicas
 - Time-out de sesión con revalidación transparente
 - Implementación con *Linux*:
 - Driver *HostAP* (*EAP-TLS*)
 - Implementación con sistemas propietarios:
 - Soluciones *Cisco AP* (*LEAP*)
 - Surgen incompatibilidades
 - Variantes *EAP*:
 - *LEAP, EAP-TLS, EAP-TTLS, EAP-MD5, EAP-PEAP*

Nuevas necesidades, nuevas soluciones (y III)

- *WPA (Wi-Fi Protected Access) y TKIP (Temporal Key Integrity Protocol)*
 - Actualizable mediante software
 - Claves *WEP* dinámicas
 - Distribución automática de claves
 - Mejorar la seguridad del cifrado mediante *TKIP*:
 - ***MIC*** (*Message Integrity Check*) – Mejora el *ICV* para evitar ataques Man-in-the-Middle
 - **Per-Packet-Keying**: Clave *WEP* única para cada paquete
 - **Broadcast Key Rotation**: claves *WEP* dinámicas para el tráfico broadcast y multicast

 Implica modificaciones en el hardware

Conclusiones

- Planificar correctamente la topología y el alcance de la red
- Utilizar los mecanismos básicos de seguridad que ofrece el estándar 802.11b
 - ACLs* + WEP + Ocultamiento y Redundancia de APs + Monitorización
- Utilizar los mecanismos de seguridad en redes genéricos:
 - Concienciar a los Usuarios + Política de Contraseñas Robusta + Utilizar Protocolos Seguros + Utilizar VPNs + Implementar QoS
- Presupuesto limitado:
 - Utilizar portales cautivos (si procede)
 - Utilizar soluciones basadas en código libre
- Si el presupuesto lo permite:
 - Adoptar soluciones que implementen componentes *IEEE 802.11i*:
 - *IEEE 802.11X, WPA, TKIP*
 - Hacer uso de soluciones propietarias (fuera de estándares)

THE END

**FIST Conferences 2003
October Edition**

**Javier Pascual Soriano “DaVinci”
CIUPS – Club de Informática de la UPSAM**

**E-Mail: jpascual@ciups.com
Web: <http://www.ciups.com>**

