ACTUALÍZATE.

www.cisco.com/edu/espanol

Academy Conference 2005

Cisco Systems

Seguridad en Wireless.

CCNP Everardo Huerta Sosa
ehuerta@uat.edu.mx

AGENDA

- **Controladores para WLAN.**
- **Vulnerabilidades y amenazas de la seguridad WLAN.**
- **Criterios de despliegue de seguridad WLAN.**
- **Ejemplos de despliegue WLAN.**
- **Mejores prácticas de seguridad WLAN.**
- **Wireless IDS.**
- **Mejores prácticas de integración Cableado/Inalámbrico**
- **Sumario**

¿Por qué la seguridad WLAN es importante?

- **Vulnerabilidades**

- **Lecciones.**
- No confiar en el encriptamiento básico WEP; requerimiento para seguridad de clase Empresarial (WPA, protocolos EAP 802.1x, Wireless IDS, VLANs/SSIDs, etc).
- Los empleados instalarán equipamiento WLAN por sí mismos (compromete la seguridad de toda tu red).
- Impacto empresarial debido al robo de datos: potenciales consecuencias financieras y legales (Leyes que protegen la confidencialidad de la Informácion; ejemplo: Cuidado de la Salud).

Requerimientos para desarrollos empresariales

- **Mayoría de aplicaciones de Datos e incremento en la tasa de Desarrollo VoIP.**

  Aplicaciones Típicas- Acceso Web/E-Mail, VoIP Inalámbrica, Mensajería instantánea y aplicaciones Cliente-Servidor

  - **Ambiente homogéneo > Cambiando poco a poco a ambiente heterogéneo.**

  Mayoría de dispositivos para Laptop estandarizados. (SO también estandarizados)

  Los dispositivos VoIP requieren de características de seguridad específicas.

  Crecimiento de las necesidades para soportar múltiples tipos de seguridad (Tipos EAP así como tipos de encriptación).

Requerimientos para desarrollos empresariales

- **Los empleados quieren redes inalámbricas.**

  Si IT no emigra a Wireless, los empleados instalarán Rogue AP's.

Requisitos para Desarrollos Verticales.

- **Soporte para Usuarios Móviles Activos.**
  Almacenamiento: Registro de Inventario.
  Cuidado de la Salud: Aplicaciones para monitoreo de pacientes

- **Herencia de Dispositivos.**
  Renta/Almacenamiento:Herencia del Código de Barras, Scanners,etc.

- **Clientes Heterogeneos.**
  Universidades: Los estudiantes pueden traer una laptop con una NIC de cualquier fabricante.
  Renta/Almacenamiento:Lectores de Código de Barras, Terminales Punto de Venta y Teléfonos VoIP muy comúnes.

Requisitos para desarrollos verticales.

- **Red WLAN desarrollada como red primaria para conectividad.**

  Considerar la disponibilidad como parte de los criterios de seguridad.

Agenda

- Controladores para WLAN.
- Vulnerabilidades y Amenazas de la seguridad WLAN.
- Criterios de despliegue de Seguridad WLAN.
- Ejemplos de despliegue WLAN.
- Mejores prácticas de seguridad WLAN.
- Wireless IDS.
- Mejores prácticas de integración Cableado/Inalámbrico
- Sumario

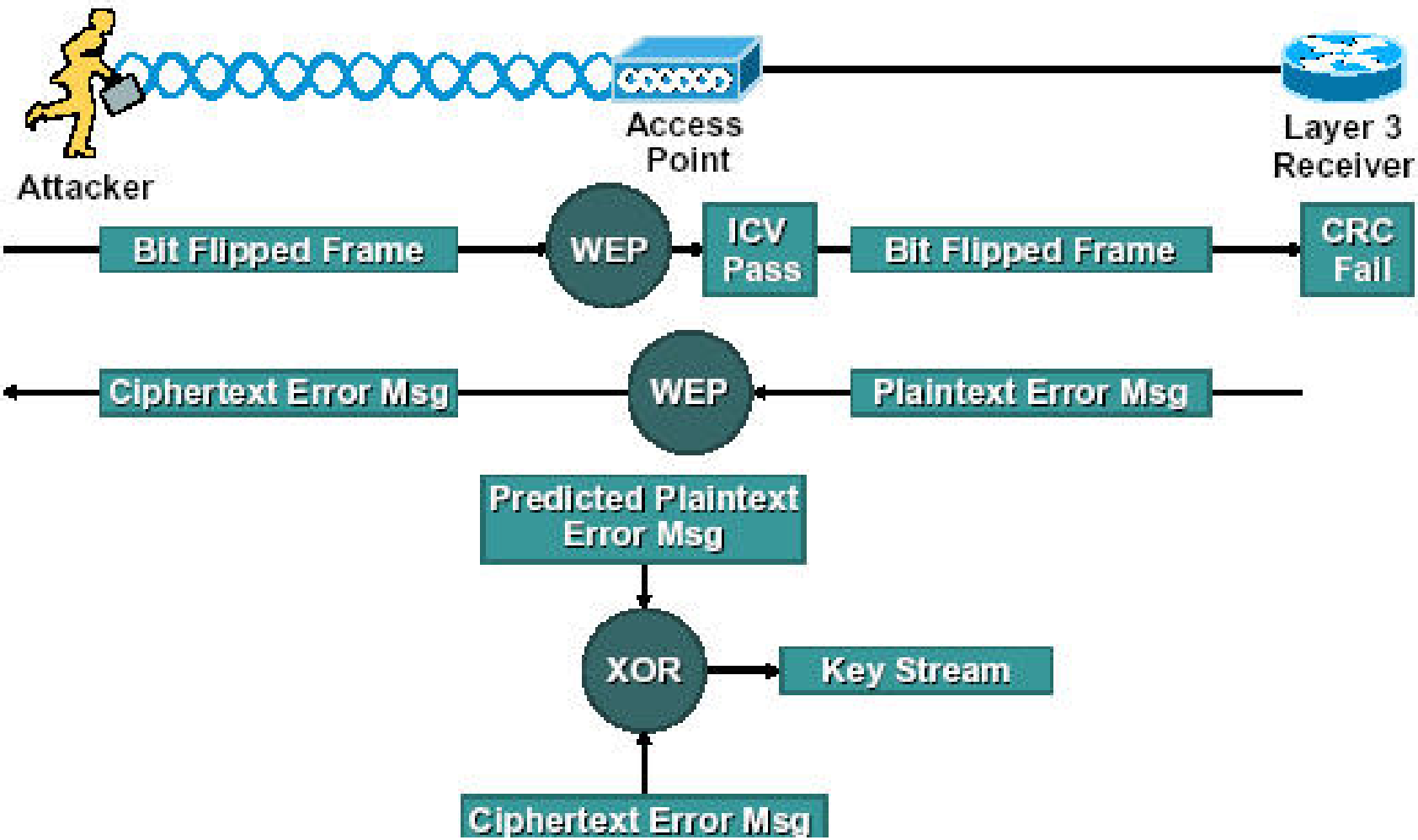
Vulnerabilidades y amenazas de la seguridad WLAN.

- **Existen diferentes formas de vulnerabilidades y amenazas.**
- Vulnerabilidades de encriptación
- Vulnerabilidades de autenticación: Autenticación de llave compartida, ataques diccionario y ataques MITM.
- ¿Habilitar ó deshabilitar el Broadcast SSID?
- Usurpación de direcciones: Usurpación de direcciones IP y MAC (ataques hostiles internos y externos).
- Access Points y clientes mal configurados.
- Ataques DoS utilizando de autenticación 802.11 y desasociación de tramas, Bloqueo RF, etc.

Vulnerabilidades WEP

- **WEP Estático 802.11 dañado: ataques pasivos.**
  - El algoritmo de programación de llave RC4 utiliza un vector de inicialización de 24 bits y no tiene llaves de encriptación rotativas.
  - Herramientas prácticas han implementado el ataque FMS (como AirSnort) y pueden descubrir la llave WEP después de capturar 1000 paquetes. Esto es menos de 17 minutos para comprometer La llave WEP en una red ocupada.
  - Este ataque es pasivo y las herramientas de ataque “sólo” requieren de escuchar a la red WLAN (como paquetes Sniff WLAN).
- **WEP Estático 802.11 dañado: ataquesactivos.**
  - No se protege la integridad de los datos del usuario WLAN.
  - Muchos ataques posibles: Ataques Replay y Bit Flipping.

Vulnerabilidad de Bit Flipping.



Vulnerabilidades de Autenticación

- **La llave de autenticación compartida está defectuosa.**
  - AP reta al usuario WLAN a asegurarse de la posesión de una llave de encriptación válida.
  - El atacante puede obtener una corriente de llave > Reto del Texto Plano XOR Texto Cifrado = Corriente de Llave.
  - No recomendable para despliegue.
- **Ataques diccionario.**
  - Ataques en Línea: ataques activos para comprometer passwords o frases de paso.
  - Ataques Fuera de Línea: ataques pasivos para comprometer passwords o frases de paso.
- **Ataques MITM.**
  - El atacante se inserta en el medio de la secuencia de autenticación.

¿Qué es un ataque de diccionario?

- **¿Qué es un diccionario?**
  Contiene variaciones de passwords.
  Passwords débiles pueden ser crackeados usando
  Diccionarios estándares.

- **Factores de éxito para esta herramienta.**
  - Variaciones del password del usuario se encuentran en el diccionario del atacante.
  - Experiencia del atacante para generar diccionarios.
  - Fuerza del Password.
    Un password de 6 caracteres será más fácilmente comprometido que un password de 10 caractéres.
    La fuerza del diccionario del atacante determina cuál es el password que puede ser comprometido.

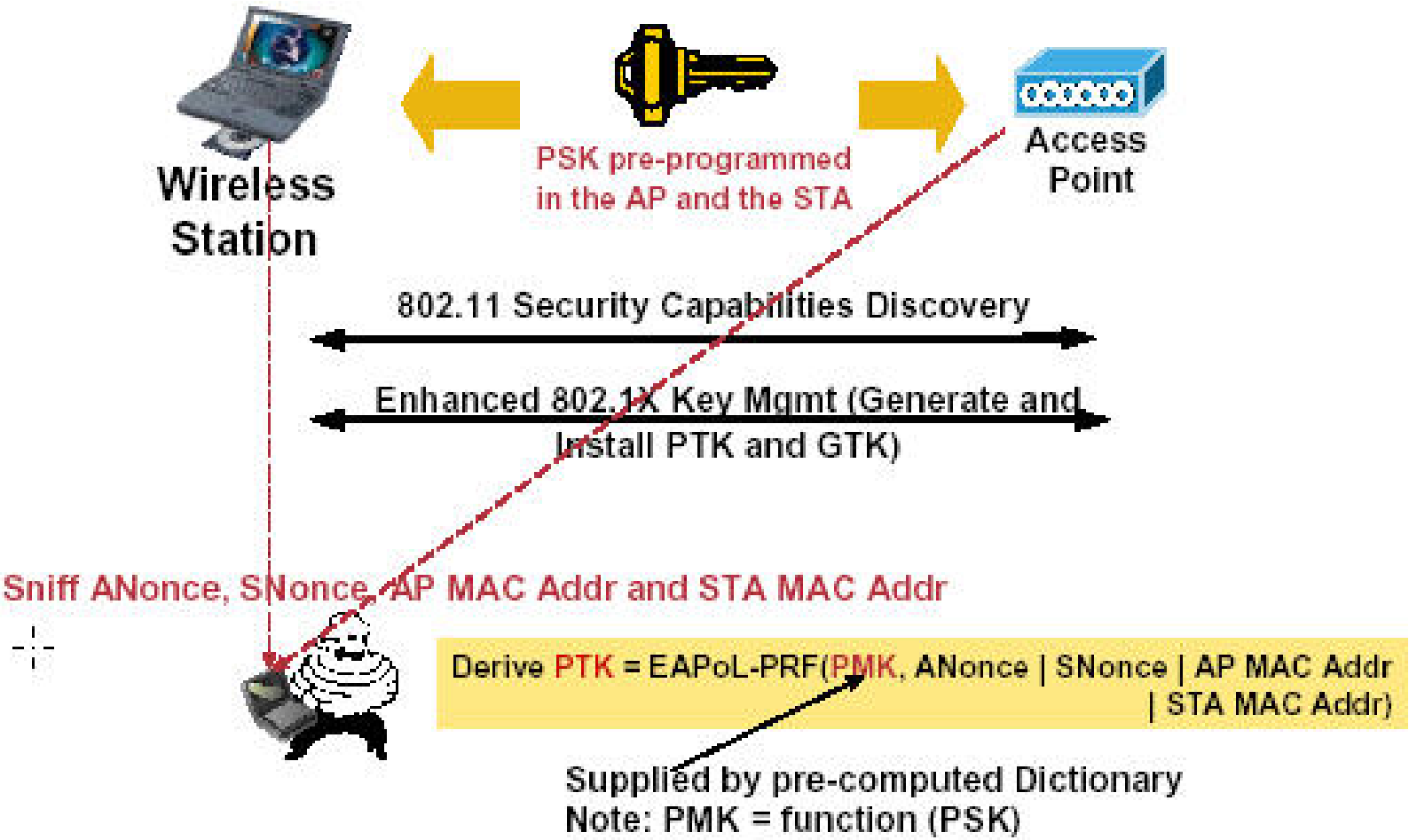
CISCO LEAP: ATAQUE DICCIONARIO OFFLINE

- **Cisco LEAP está basado en arquitectura MS-CHAP.**
  - No se usa un salto en el reto/respuesta(el proceso de encriptación no se realiza al azar).
  - Selección débil de llave DES en reto/respuesta.
  - Nombre de usuario enviado en claro.
- **Los ataques pasivos de diccionario son posibles:**
  - Consideraciones:
  - El atacante debe estar próximo a tu edificio.
  - El atacante es conocido por llevar a cabo ataques de diccionario avanzados.

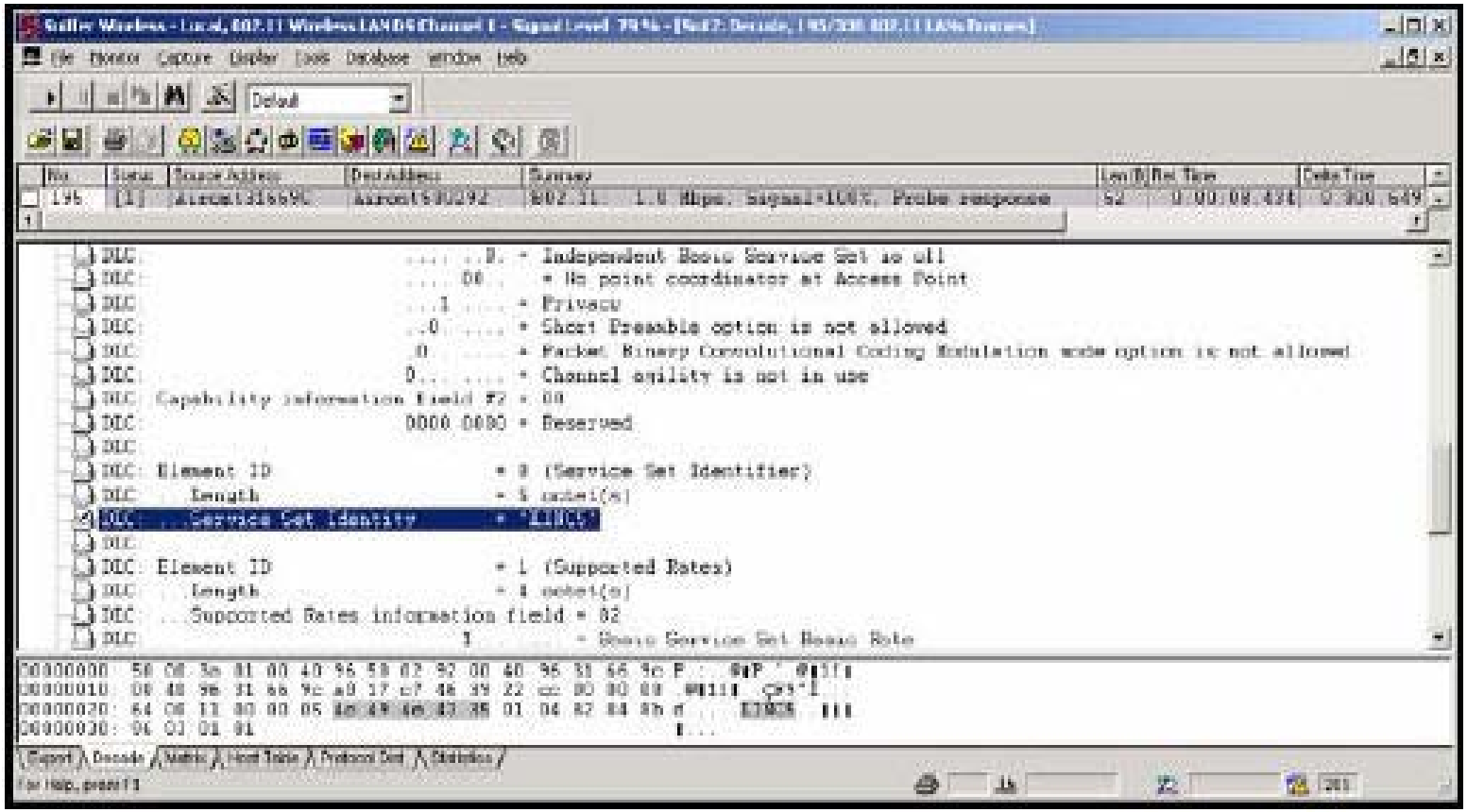
CISCO LEAP: ATAQUE DICCIONARIO OFFLINE

- **Los ataques pasivos de diccionario dependen de ciertas variables.**
  - Políticas de contraseñas.
  - Poder de procesamiento disponible para el atacante.
  - Eficiencia del algoritmo del atacante.

Autenticación de Llave Precompartida (PSK)

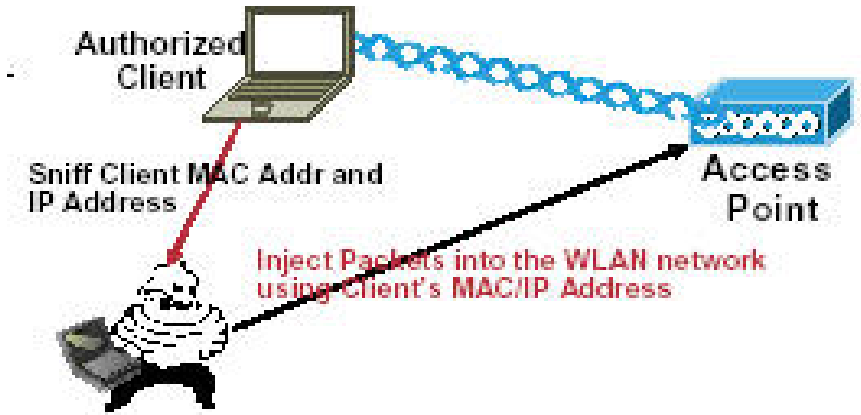


Habilitar o Desabilitar Broadcast SSID ?



En realidad no importa, El atacante puede descubrir tu SSID utilizando un sniffer

Usurpación de direcciones.



- **La usurpación de Direcciones IP y MAC es posible en redes WLAN.**
- **Escenario de atacante externo.**
  - La usurpación de IP no es posible si el encriptamiento está activado.
  - Sólo usurpación de MAC(No sirve de mucho sin la IP,si la encriptación está activada)
- **Escenario de atacante interno.**
  - La usurpación de IP y MAC no será exitosa si se usa autenticación EAP/802.1x

¿Quián instala AP's Rogue ?

- **Empleado frustrado.**

  Usuario que instala AP's inalámbricas para beneficiarse de la eficiencia y conveniencia que ofrece.

  Es común por la gran disponibilidad de AP's de bajo costo.

  Usualmente ignorante de la configuración de seguridad más común de AP.

- **Hacker**

  Penetra la seguridad física para instalar un Rogue AP.

  Puede personalizar la AP para ocultarla de las herramientas de rastreo.

  Difícil de rastrear; es más eficiente prevenir con 802.1x y seguridad física.

  Más probable instalar la caja de Linux que la AP.

Ataques DoS

- **Atascamiento de RF.**

  Un simple transmisor de atascamiento RF (Microondas o un teléfono a continuación de un AP)

- **Ataques DoS usando tramas de administración 802.11**

  Las tramas de administración 802.11 no son autenticadas entre AP y clientes. Cualquiera puede usurpar una dirección MAC y enviar una trama en favor de ese cliente.

- **Inundación de autenticación 802.1x**

  Un atacante puede enviar una corriente de requisiciones de autenticación 802.1x a las AP.

  Provoca que la AP procese tramas innecesarias de autenticación

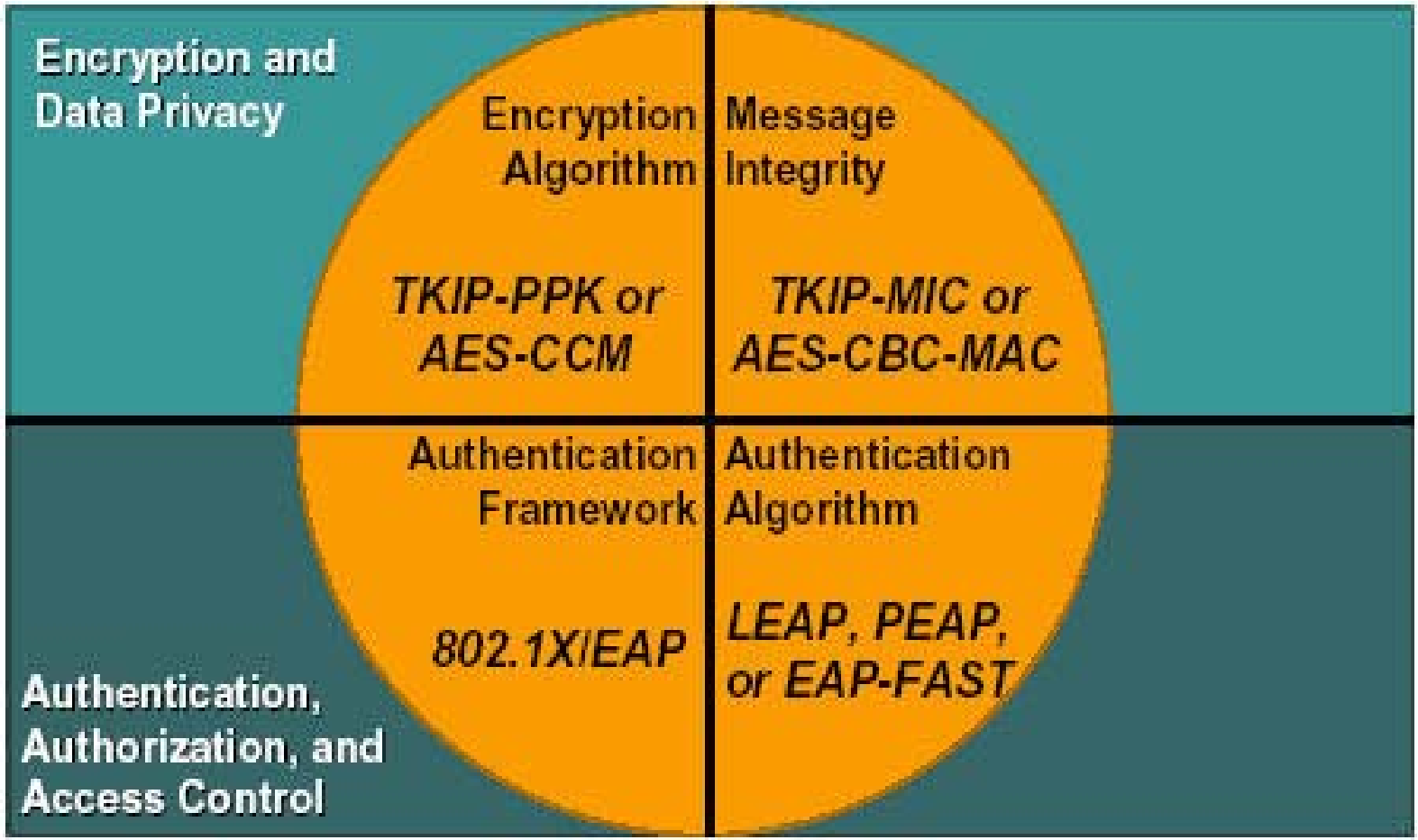
Agenda

- Controladores para WLAN.
- Vulnerabilidades y Amenazas de la Seguridad WLAN.
- Criterios de Despliegue de Seguridad WLAN.
- Ejemplos de Despliegue WLAN.
- Mejores Prácticas de Seguridad WLAN.
- Wireless IDS.
- Mejores Prácticas de Integración Cableado/Inalámbrico
- Sumario

Requerimientos básicos para asegurar las WLAN.

- **Algoritmo de Encriptación.**
  Mecanismo para proveer seguridad de los datos.
- **Integridad del Mensaje**
  Se asegura que las tramas estén libres de trampas y que
  Provengan realmente de la fuente.
- **Trama de Autenticación**
  Trama para facilitar los mensajes de autenticación entre
  Clientes, access points y servidor AAA.
- **Algoritmo de Autenticación.**
  Mecanismo para validad las credenciales del cliente.

Requerimientos básicos para asegurar las WLAN.



Requerimientos avanzados para asegurar las WLAN.

- **Políticas de administración de seguridad.**
  - Telnet Seguro, SSH, SNMP, FTP, TFTP, RADIUS y Tráfico WLCCP a todas las APs y Puentes.
- **IDs Inalámbricas.**
  - Proveen capacidad para detectar y eliminar AP no autorizadas
  - Detectar ataques activos y mejorar seguridad de capa 2.
- **Mejores prácticas de integración Cableado/Inalámbrico.**
  - Trazar las políticas de seguridad a la red alámbrica
  - Uso de múltiples grupos de Usuario/Servicio (Vía Túneles SSID's/ VLAN's/ mGRE)
  - Uso de características de seguridad cableada para desarrollo WLAN.

Agenda

- Controladores para WLAN.
- Vulnerabilidades y amenazas de la seguridad WLAN.
- Criterios de despliegue de seguridad WLAN.
- Ejemplos de despliegue WLAN.
- Mejores prácticas de seguridad WLAN.
- Wireless IDS.
- Mejores prácticas de integración Cableado/Inalámbrico
- Sumario

Ejemplo de desarrollo empresarial.

- **Escenario de desarrollo WLAN.**

  Aplicaciones típicas- Acceso Web/E-Mail, VoIP inalámbrica, mensajería instantánea y aplicaciones cliente-servidor.

  Cobertura en todas las áreas incluyendo salones de junta.

- **Metas específicas de desarrollo.**

  Autenticación y autorización de cada usuario.

  Proteger la integridad y confidencialidad de los datos.

  Ambiente estandarizado para el cliente.

  Escalabilidad y manejabilidad.

  Acceso a invitados.

  Alta calidad y desarrollo de acceso a oficinas remotas

  WLAN desarrolladas como alternativa(Redes cableadas como red Primaria.

Ejemplo de desarrollo educacional.

- **Aplicaciones de enseñanza que ayudan a alumnos y maestros.**
- **Staff : Requerimiento de acceder a registros de estudiantes y otra información sensible.**
- **Retos del desarrollo**

  Ambiente NO estandarizado para estudiantes

  Estudiantes: Sólo autenticación de usuario.

  Staff: Autenticación de usuario y confidencialidad de datos.

- **Ambiente NO estandarizado del cliente significa:**

  Los estudiantes pueden traer cualquier dispositivo.

  Los estudiantes pueden usar cualquier SO.

  Los estudiantes pueden usar NIC’s de cualquier fabricante.

- **Dispositivos estandarizados para staff (OS Y WLAN NIC).**

Ejemplo de desarrollo para cuidado de la salud.

- **Desarrollo WLAN entre múltiples clínicas y hospitales.**

  Información móvil de los pacientes en tiempo real.

  WLAN provee acceso a aplicaciones ricas en imágenes.

  Aplicaciones para cuidado y monitoreo de los pacientes.

- **Criterios de desarrollo.**

  Esfuerzo para estandarizar el ambiente del cliente.

  Desarrollo WLAN descentralizado: múltiples sitios;

  Múltiples modelos de desarrollo.

  Requerimiento para proteger la información relativa a los pacientes.

  WLAN es la red primaria, por eso importa la disponibilidad.

Agenda

- Controladores para WLAN.
- Vulnerabilidades y amenazas de la seguridad WLAN.
- Criterios de despliegue de seguridad WLAN.
- Ejemplos de despliegue WLAN.
- Mejores prácticas de seguridad WLAN.
- Wireless IDS.
- Mejores prácticas de integración Cableado/inalámbrico
- Sumario

Mejores prácticas para asegurar WLAN

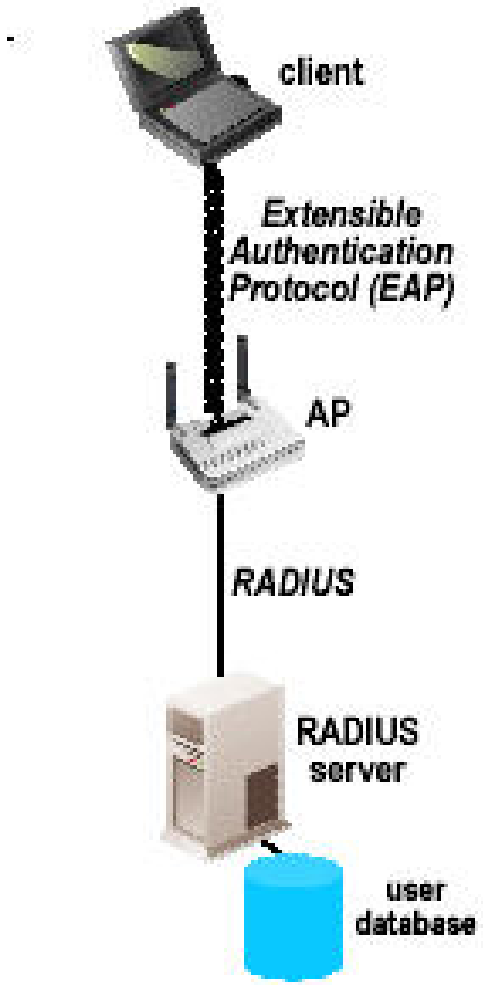
- **Tecnologías para asegurar las WLAN.**
  - Protocolos de Autenticación EAP/802.1x
  - Encriptación de Datos e Integridad de Mensajes: WPA, CKIP, WPAv2.
  - Desarrollo IPSec VPN .
- **Consideraciones de desarrollo EAP/802.1x con WPA/WPAv2**
  - Disponiblidad EAP
  - Disponibilidad y escalabilidad del servidor RADIUS.
  - Roaming rápido y seguro.
- **Mejores prácticas de administración segura.**

Vista general de autenticación 802.1x

- **Recomendación del grupo i de tareas 802.11 para autenticación WLAN.**
- **Soportada por Cisco desde diciembre del 2000.**
- **Extensible e interoperable**
  Soporta:

  Diferentes métodos o tipos de autenticación EAP.

  Nuevos algoritmos de encripción, incluyendo AES como reemplazo de RC4.



Vista general de autenticación 802.1x

- **Beneficios clave:**

Autenticación Mutua entre cliente y servidor RADIUS.

Llaves de encriptamiento después de la autenticación.

Control centralizado, donde la expiración de la sesión solicita re-autenticación y requiere una nueva llave.

Cisco LEAP

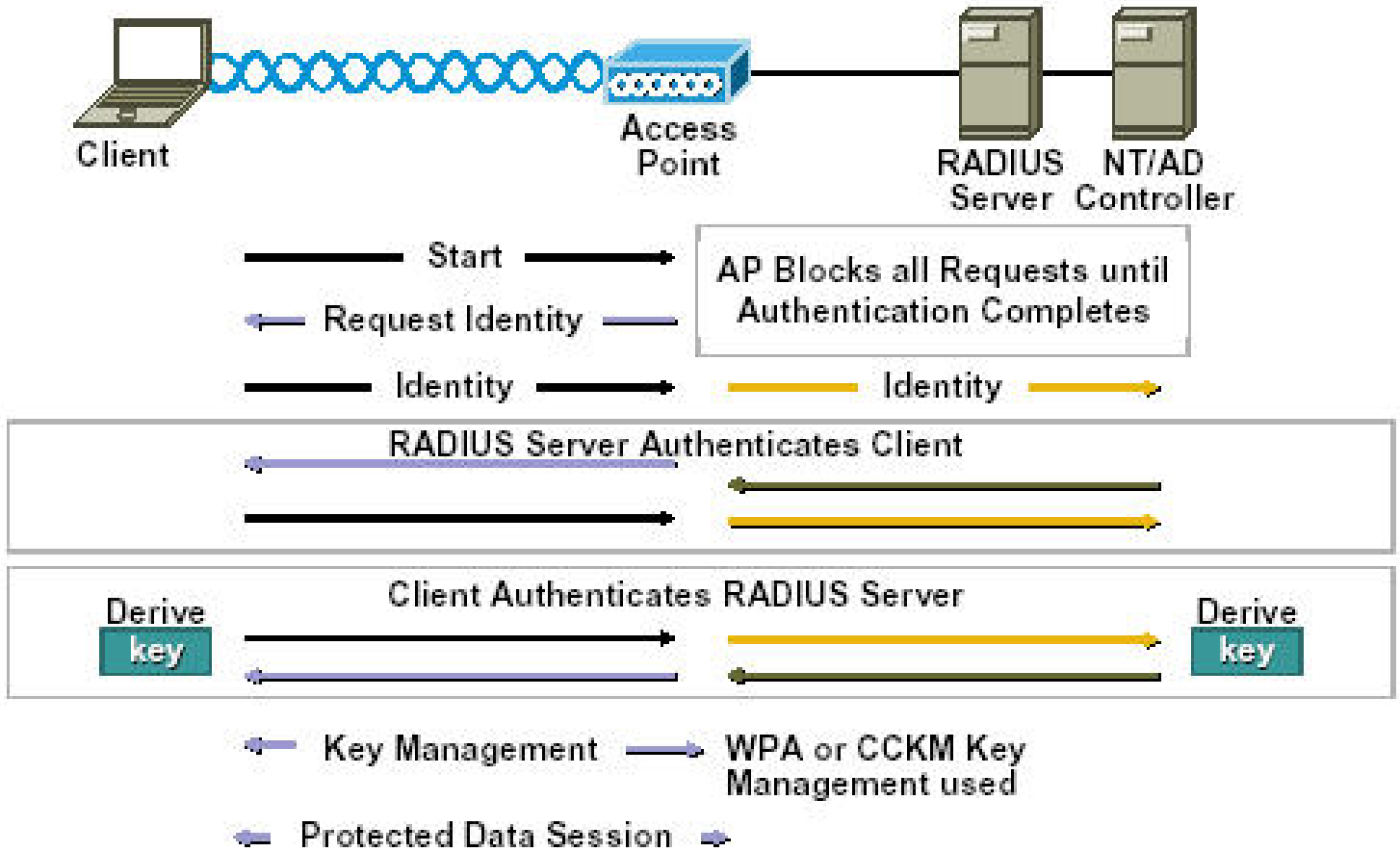
- **Soporte al cliente**

  Windows 95-XP, Windows CE, Macintosh OS 9.x, 10.x y Linux.
- **Servidor RADIUS**

  Cisco ACS y Cisco AR.
  Interlink Merit.
- **Dominio Microsoft o directorio activo para autenticación extrema.**

- **Soporte a dispositivos.**
  Puentes de grupo de trabajo
  Puentes (Series BR 350, BR 1400 y BR 1300)

Autenticación Cisco LEAP.



Mejores prácticas para desarrollo LEAP.

- **Ataques de Diccionario en Línea.**

  Políticas del Servidor RADIUS para bloquear a un usuario después de un número determinado de fallas al conectarse.

- **Ataques de Diccionario Fuera de Línea.**

  Uso de políticas de password fuerte(mínimo 10 caracteres).

  Posibles métodos para sobreponerse a las limitaciones humanas para políticas fuertes de passwords.

  Cuenta de Usuario MSFT AD separada y password para acceso WLAN.

  El Administrador debe generar un password sólido para autenticación WLAN para cada usuario.

  Autenticación WLAN con ID de Usuario y password sólido almacenado en el dispositivo.

Mejores prácticas para desarrollo LEAP.

- **Ejemplo de Políticas de Passwords Sólidos**
  - El password debe tener al menos 12 caracteres:
  - http://www.cisco.com/warp/public/707/cisco-sn/-20030802-leap.shtml
  - http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html
  - Una mezcla de mayúsculas y minúsculas.
  - Al menos un caracter numerico(0-9)ó caracteres No alfanumericos(¡#&)
  - Distinto al Nombre de Usuario
  - Una palabra que no exista en el diccionario(local o extranjero)
  - Passwords generados al azar
- **Ejemplo Passwords Sólidos**
  - W1r313ss1sG00d (Wireless is Good)
  - N3tw0rk3rsR0cks(Networkers rocks)

EAP-FAST autenticación flexible vía Tunneling

- **La autenticación EAP-FAST tiene 3 fases:**
  - PAC se genera en la fase 0 (Dynamic PAC Provisioning).
  - Un túnel seguro se establece en la fase 1.
  - El cliente se autentica mediante el túnel seguro en la fase 2.

- **Las credenciales de acceso protegido(PAC) pueden ser provistas dinámicamente en los clientes.**
  - PAC es una credencial única compartida para autenticar tanto al cliente como al servidor
  - PAC está asociado con un ID se usuario específico y un ID de autoridad
  - PAC no requiere PKI (Certificados Digitales).

EAP-FAST autenticación flexible vía Tunneling

- **PAC y el protocolo TLS son usadas para establecer un túnel seguro entre el usuario y el servidor RADIUS.**

  La autenticación del usuario es pasada en el túnel de encriptación hacia el servidor RADIUS

EAP-TLS

- **Soporte al vliente**
  - Windows 2000, XP, Windows CE, MeetingHouse y Funk
  - Cada Cliente requiere un certificado de usuario.
- **Requerimientos de infraestructura**
  - EAP-TLS que soporte servidor RADIUS.
  - El servidor RADIUS requiere un certificado de servidor.

Mejoras en la seguridad WLAN IEEE 802.11i

- **802.11.i es un subcomité de la IEEE 802.11 responsable de las mejoras de seguridad WLAN.**
- **Los componentes clave de 802.11i**

  Trama EAP/802.1x basada en autenticación de usuario.

  TKIP Alivia la vulnerabilidad RC4 y la vulnerabilidad contra ataques activos.

  Manejo de Llave: Aísla la administración de la llave de encriptación para la autenticación del usuario.

  AES: Protocolo de reemplazo para RC4.

Autenticación VPN

- **Es una alternativa a 802.1x en WLAN.**
- **IETF estandarizó la implementación IPSec.**
- **Soportada por Cisco en los concentradores y routers basados en Cisco IOS.**
- **Beneficios:**
  - Autenticación mutua entre cliente y concentrador VPN
  - Provee encriptación 3DES o AES.
  - Provee SHA/MD5 para una protección integral de los datos.
  - Provee autenticación centralizada del usuario.

Extensiones compatibles Cisco (CCX)

- **Existen 69 socios y más de 130 productos que han superado la prueba CCX v1.**

  Laptops de IBM, Dell, Toshiba.

- **Productos CCX v2**

  Seguridad

  - WPA
  - Pruebas de Interoperabilidad para 3 tipos de autenticación:
  - (LEAP, PEAP y EAP-TLS)

  Mobilidad

  Voz en WLAN

  Detección de AP Rogue.

Mejores prácticas de manejo de seguridad.

- **¿Cómo asegurar el tráfico hacia AP's, Puentes, WGB, etc?**

  Deshabilitar Telnet y usar SSH.

  Usar TACACS para administración de la autenticación.

  Deshabilitar o restringir el acceso vía interfaz radial al Access Point/Puente.

  Restringir el tráfico entre Access Point y red cableada.

Agenda

- Controladores para WLAN.
- Vulnerabilidades y amenazas de la seguridad WLAN.
- Criterios de despliegue de seguridad WLAN.
- Ejemplos de despliegue WLAN.
- Mejores prácticas de seguridad WLAN.
- Wireless IDS.
- Mejores prácticas de integración Cableado/Inalámbrico
- Sumario

¿Por qué son importantes los WLAN IDS?

- **Permiten la detección de:**
  - Access Points NO Autorizados.
  - Ataques Activos.
  - Access Points y Clientes mal configurados.

- **WLAN se ha convertido en una tecnología envolvente y cada vez más usada alrededor del mundo.**

  Requerimiento para monitorear herramientas de ataques y tipos específicos de ataques.

Agenda

- Controladores para WLAN.
- Vulnerabilidades y amenazas de la seguridad WLAN.
- Criterios de despliegue de seguridad WLAN.
- Ejemplos de despliegue WLAN.
- Mejores prácticas de seguridad WLAN.
- Wireless IDS.
- Mejores prácticas de integración Cableado/inalámbrico
- Sumario

Mejores prácticas de integración Cableado/Inalámbrico

- **Integrar las políticas de la red WLAN a la red cableada.**
- **Usar las características de seguridad de la red Cableada para la red WLAN.**
- **Usar Roaming Seguro (CCKM)**

Agenda

- Controladores para WLAN.
- Vulnerabilidades y amenazas de la seguridad WLAN.
- Criterios de despliegue de seguridad WLAN.
- Ejemplos de despliegue WLAN.
- Mejores prácticas de seguridad WLAN.
- Wireless IDS.
- Mejores prácticas de integración Cableado/Inalámbrico
- Sumario

Sumario

- Se recomienda usar como solución para seguridad en WLAN el protocolo WPA, WPAv2 o Cisco TKIP Integrado con EAP.
- Implementar características de seguridad avanzadas como Wireless IDS así como integración de Wireless con red alámbrica.
- Habilitar políticas de seguridad vía WLSE

Lecturas de referencia

- **Vulnerabilidades WEP.**

  http://www.cs.rice.edu/asstuble/wep/wep_attack.pdf

  http://airsnort.soundforge.net/

- **Respuesta de Cisco a ataques en Cisco LEAP.**

  http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml

- **Guía para desarrollos WLAN.**

  http://www.cisco.com/US/products/sw/secursw/ps2086/products_whitepaper09186a00801495a1.shtml