Seguridad en Redes Universitarias 802.11

Carlos Vicente
cvicente@ns.uoregon.edu

Amenazas

- Uso ilegítimo del ancho de banda
- Violación de privacidad
- Tráfico ofensivo o delictivo por el que somos responsables (AUP)
- Acceso a recursos restringidos por rangos IP

WEP

- Wired Equivalent Privacy
  - Parte de la especificación 802.11 original
  - Pensado para proveer
    - Confidencialidad
    - Integridad
    - Autenticidad
- No es satisfactorio en ninguna de ellas

WEP

- Serias fallas de diseño
  - Cifrado utiliza RC4
    - Algoritmo seguro, pero mala implementación
      - Gestión manual de claves
      - Claves de 40 bits muy cortas
      - Initialization Vector (IV) muy corto (24 bits)
      - Aleatorización deficiente
  - Chequeo de Integridad con CRC
    - Puede fácilmente generarse un mensaje distinto que produzca la misma secuencia
    - Lo ideal es un hash (Ej: MD5)

WEP

- Herramientas para descubrir la clave
  - Disponibles gratuitamente
  - Recolectar entre 5 y 10 millones de frames
    - 2 a 6 horas en una red corporativa
    - Semanas en una red doméstica
  - Una vez recolectado tráfico suficiente, romper la clave es cuestión de segundos

AirSnort

- http://airsnort.shmoo.com
  - Tarjetas Aironet, Orinoco y Prism2
  - Versión de Windows en Alpha

Nuevos desarrollos

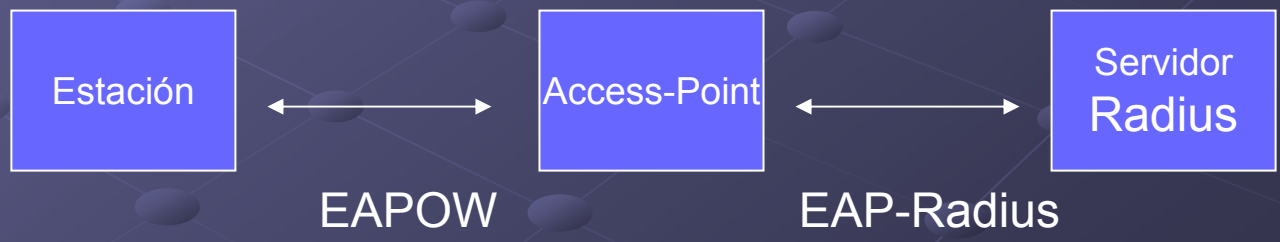
- Aprender de los errores:
  - Necesidad de un esquema más flexible
- 802.1x
  - Control de acceso a puertos (capa 2)
  - IEEE tomó EAP (del IETF) y lo adaptó para redes locales
  - Evolucionando hacia 802.1i en entorno wireless
  - Cliente ya incluido en Windows XP
  - Paso intermedio: WPA

EAP

- Extensible Authentication Protocol
  - Estándar del IETF (RFC-2284)
  - Inicialmente para PPP (enlaces dial-up), pero puede operar sobre cualquier protocolo de capa de enlace (802.3, 802.11, etc)
  - Realmente una envoltura
    - No especifica el método de autenticación, de ahí lo de “extensible”

EAP-Radius

- RFC-2869
  - Define modificaciones para RADIUS que permiten su utilización dentro de EAP
  - Radius ya es muy utilizado para autenticación de dial-up via PPP
  - EAPOL/EAPOW (EAP over LANs/Wireless)



EAP-TLS

- TLS: Transport Layer Security
  - Es SSL hecho estándar por el IETF
  - También una envoltura: Permite negociar algoritmos
- En este caso no utilizado al nivel de transporte
  - Puede utilizarse dentro de EAP
- Implementa esquema PKI
  - Utilización de algoritmos de clave pública para negociación de clave secreta
- Permite autenticación en ambos sentidos
- Necesidad de gestión de certificados!

LEAP

- Lightweight EAP
  - Desarrollado por Cisco
  - Buscando una solución al problema de distribución de certificados
    - Intercambio de claves WEP utilizando passwords
  - Problema: Propiedad de Cisco
    - Actualmente licenciando su uso a varios fabricantes

PEAP y TTLS

- También evitan la utilización de certificados de cliente
- Sí utilizan certificados para autenticar la red wireless
- Proceso en dos pasos:
  - Autenticar el servidor y negociar claves de cifrado para crear un túnel
  - Utilizar el túnel para negociar la autenticación del cliente

802.11i

- Implementación de 802.1x con cifrado AES
  - Pero las tarjetas 802.11b más viejas no contienen el algoritmo AES
  - Por eso se incluyó la alternativa de TKIP (Temporal Key Integrity Protocol)
    - También basado en RC4, pero con implementación corregida:
      - Clave de 128 bits
      - IV de 48 bits
      - Las claves no son permanentes sino que se pueden negociar
  - Nuevo algoritmo para control de integridad

WPA

- Wi-Fi protected Access
- Es básicamente 802.11i con la opción TKIP (RC4)
- Promovido por la Wi-Fi alliance (www.wi-fi.org)
  - Los fabricantes no pueden esperar la finalización de 802.11i

Otras opciones

- VPN (Virtual Private Network)
  - Cifrado es extremo a extremo
    - Túneles IPSEC
  - Requiere la instalación de clientes en cada estación
    - No escalable y no siempre posible cubrir todas las plataformas (PC, Unix, MAC, PalmOS, etc…)

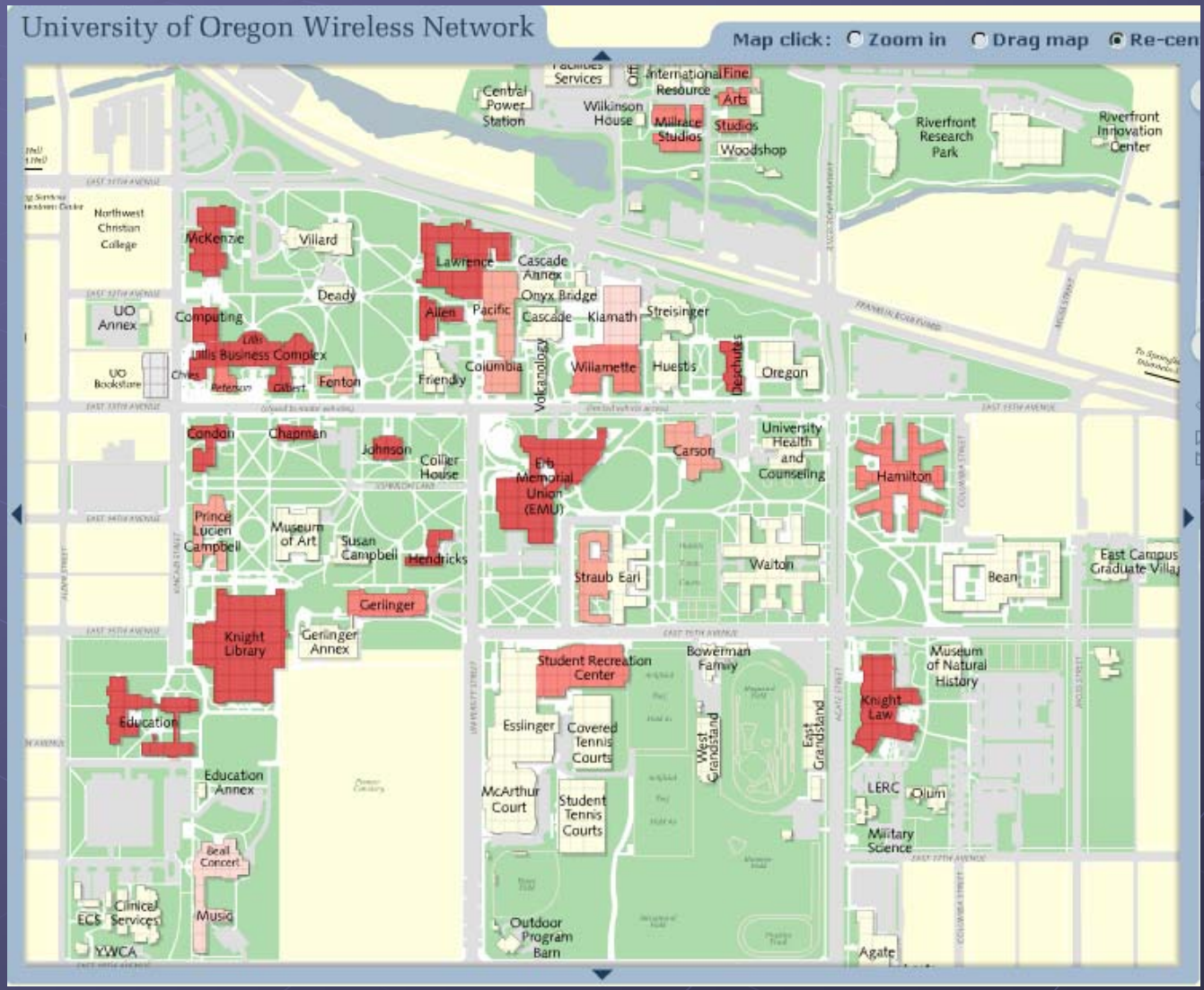
Limitaciones de un entorno Campus

- Variedad de proveedores de equipos
  - Necesidad de Estándares y simplicidad
- Volumen de usuarios
  - Soporte muy laborioso
    - Variedad de sistemas operativos
    - Usuarios con poco nivel de familiaridad con tecnologías
- Gestión y distribución de claves y certificados: Poco práctico

Wireless Gateways

- Solución “hecha en casa”
  - Caso UO:
    - ~20,000 estudiantes
    - ~200 access points y creciendo
    - Variedad de sistemas operativos
    - Claves ‘en claro’ no permitidas
      - No más Telnet, ahora SSH
      - Webmail sobre SSL
      - SPOP, SIMAP, etc

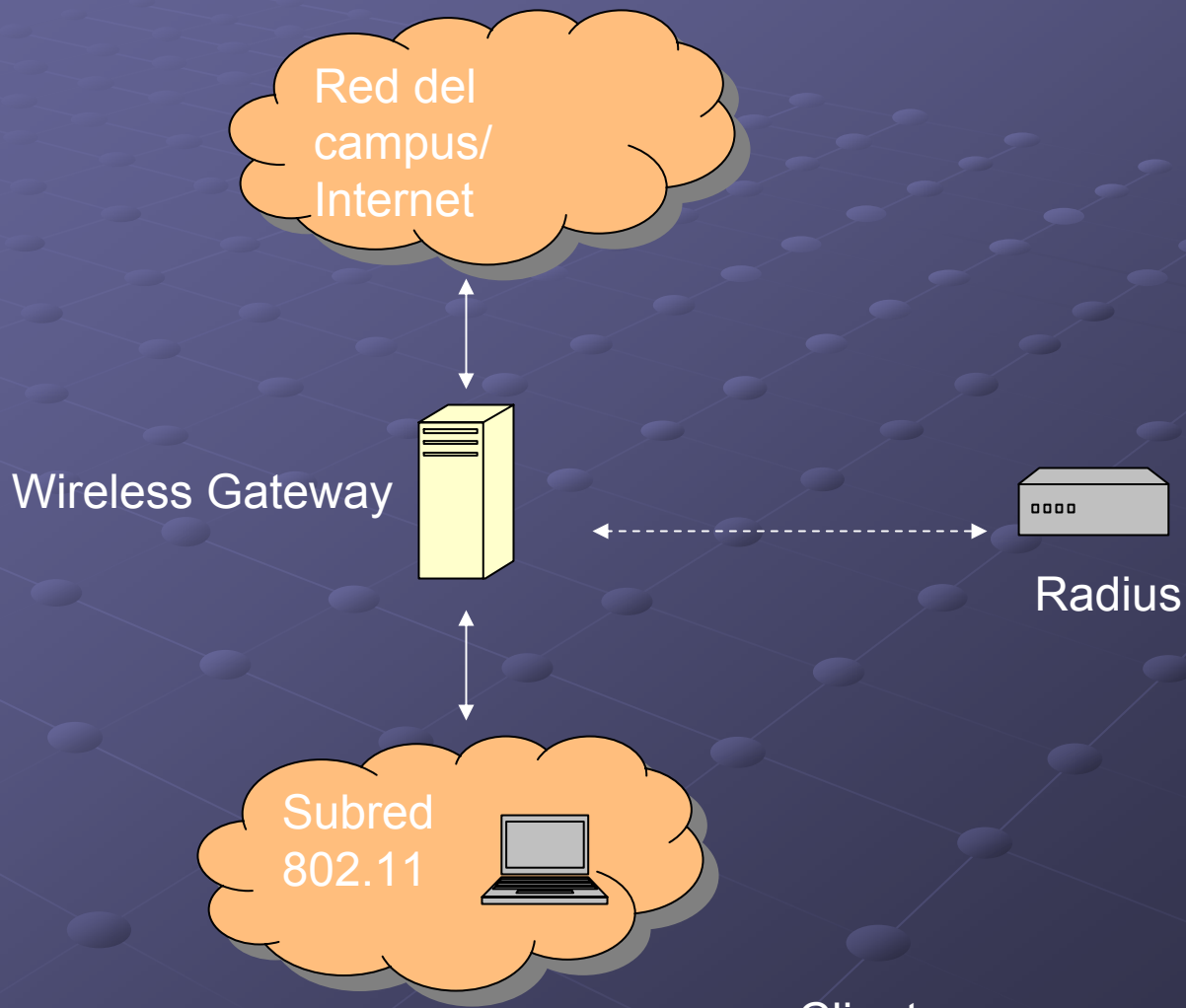
Cobertura 802.11 en UO



UO Wireless Gateway

- Componentes Open Source
  - Linux (con iptables)
  - Apache con SSL
  - Bind
  - ISC DHCP
  - Cliente Radius
  - CGI scripts en Perl y C
- Una sola subred (/22)

UO Wireless Gateway



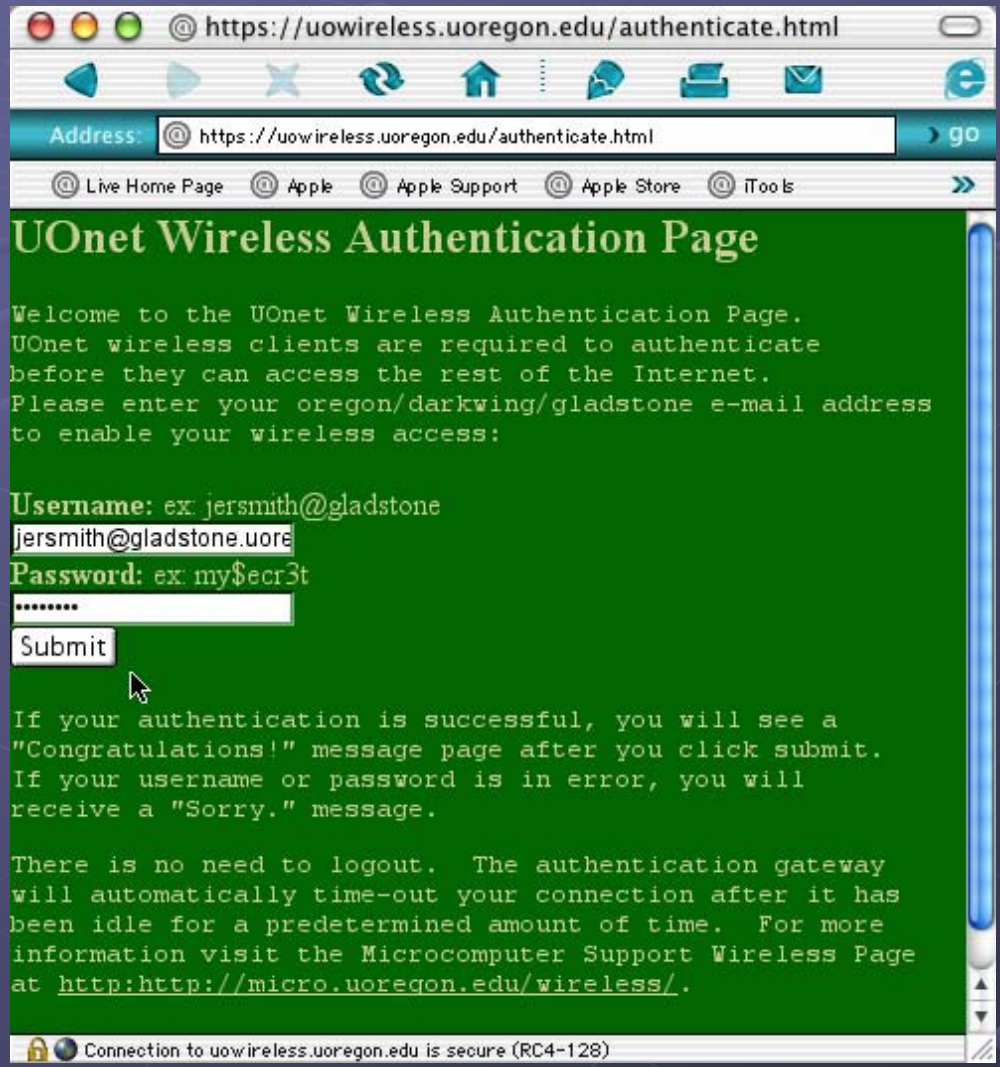
UO Wireless Gateway

- La estación hace una petición DHCP
- EL WG le asigna una dirección IP
  - También le asigna DNS y Default Gateway (él mismo)
- El usuario abre el navegador y escribe una dirección
- La máquina hace una petición DNS
- El WG responde con su propia dirección para cualquier nombre

UO Wireless Gateway

- La estación recibe la dirección y hace una petición HTTP
- El servidor web del WG recibe la petición y devuelve una página de login

UO Wireless Gateway



UO Wireless Gateway

- Una vez autenticado el usuario via Radius, el WG agrega una entrada en *iptables* permitiendo la dirección MAC de la estación
- Cómo evitar que la tabla crezca indefinidamente?
  - El WG envía pings cada x minutos para mantener la tabla al día
  - También los 'leases' de DCHP expiran en un tiempo relativamente corto
  - El usuario puede ir a la página de inicio y hacer un 'logout' explícitamente

Filtros basados en MAC

- Principales limitaciones
  - Algunos sistemas operativos permiten cambiar la dirección MAC
  - La estación puede comunicarse dentro de la subred inalámbrica aún sin estar autenticado
    - Hace a la subred insegura a ataques
  - Necesidad de una sola subred
    - Cableado independiente (más fibras)
      - Puede resolverse con troncales VLAN
    - Cierta cantidad de usuarios puede justificar la necesidad de subdividir la red

Wireless Gateways

- Soluciones Comerciales
  - ReefEdge
  - Blue Socket
  - Vernier
  - Ventajas comunes:
    - Funcionalidad distribuída (Connect Server, Edge Controller, etc)
    - Posibilidad de separar en subredes
    - Movilidad
      - Establece túneles IP/IP para mantener direcciones
    - Muchas más funciones
      - Autorización, Accounting, etc.
      - Interfaz web, DB backend
- Soluciones Open Source
  - NoCat (http://nocat.net)
    - Dos componentes:
      - NoCatSplash (redirección)
      - NoCatAuth (AAA)

Más información

- IETF
  - RFC-2284: PPP Extensible Authentication Protocol (EAP)
  - RFC-2869: RADIUS Extensions
  - RFC-2716: PPP EAP TLS Authentication Protocol
- Wireless LANs: Freedom vs. Security? (http://www.networkmagazine.com/showArticle.jhtml?articleId=10818265)
- Roadblocks for War Drivers: Stop Wi-Fi from Making Private Networks Public (http://www.networkmagazine.com/showArticle.jhtml?articleId=8703478)
- Georgia Tech LAWN Project (http://www.stonesoup.org/Meetings/0201/network.pres/lawn-overview.pdf)
- Blue Socket (http://www.bluesocket.com)
- ReefEdge (http://www.reefedge.com)
- Vernier Networks (http://www.verniernetworks.com)
- NoCat (http://nocat.net)