This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/

Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Protegiéndote en una red pública inalámbrica pública

Hugo González
hugo.gonzalez@upslp.edu.mx

UNIVERSIDAD
POL
DE SA

http://creativecommons.org/licenses/by/2.5/mx/

Es seguro usar redes inalámbricas ????

Debilidades !!!

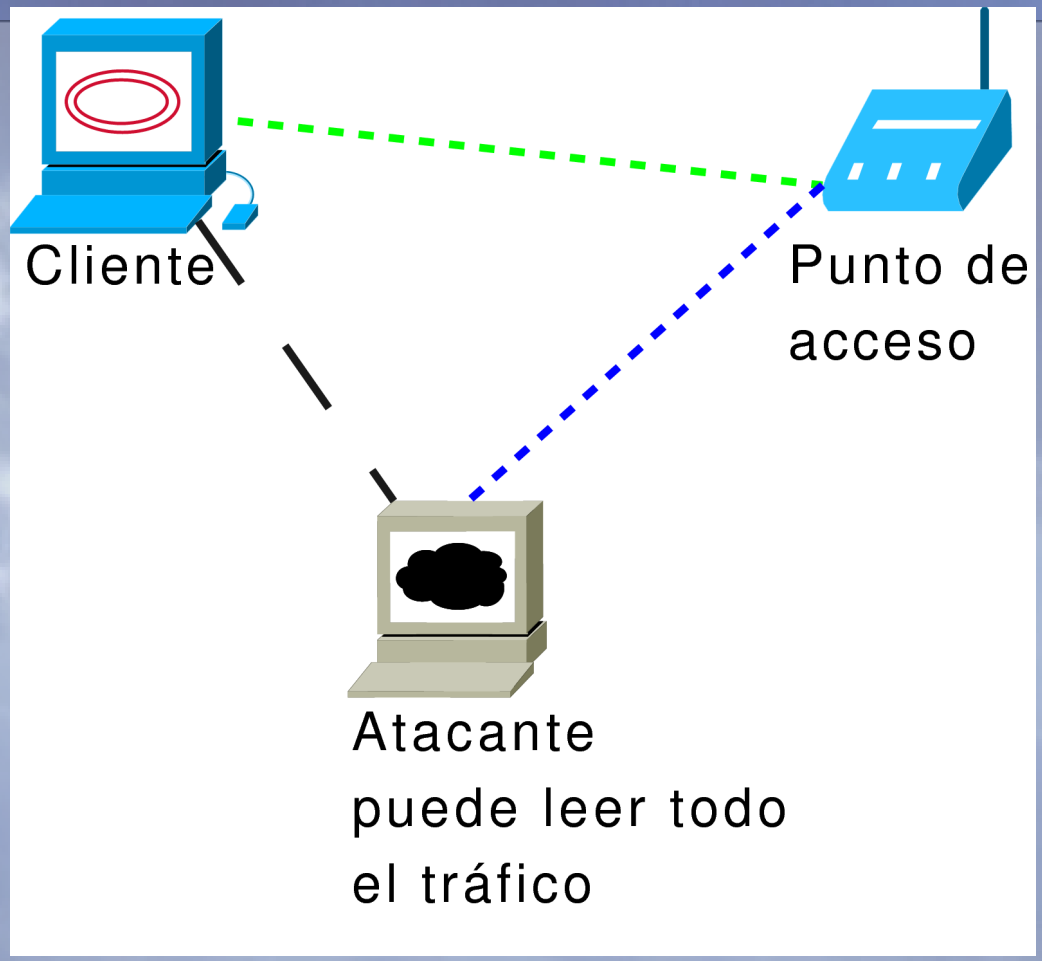
- Múltiples ataques, sin necesidad de CABLES
- El atacante se puede esconder !
- Técnicas fáciles, medias y MUY complejas
- Y si la red tiene contraseña ?? wep, wpa !!!

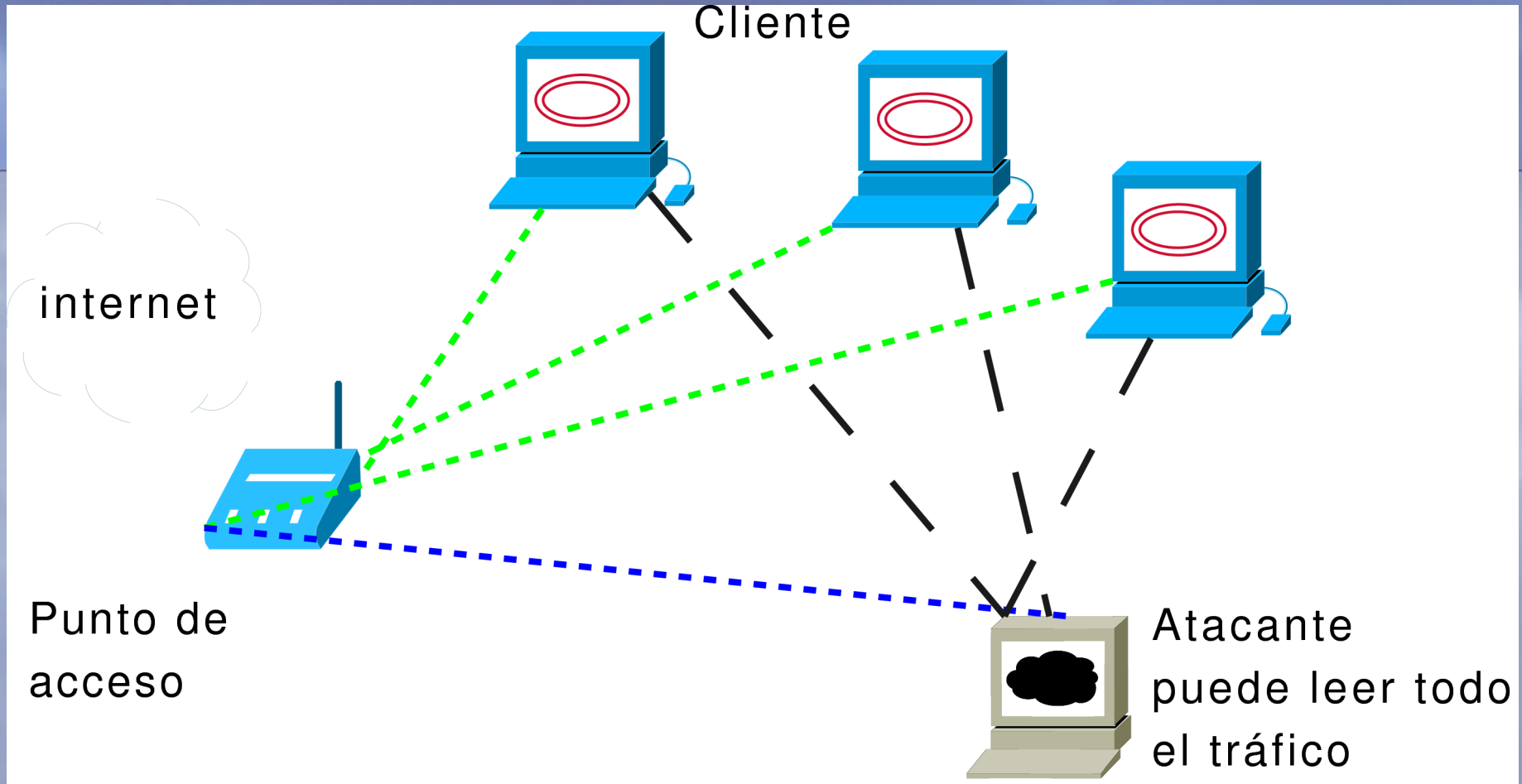
fácil

ARP

Envenenamiento de rutas arp

También funciona en redes cableadas


Cliente
Punto de acceso
Atacante puede leer todo el tráfico



Envenenamiento de ARP
Escucha de todo el trafico
en busca de Username/password
Captura de cookies para robar identidad.

Ataque fácil ARP

- **Envenenamiento de ARP ...**
  - **sudo arpspoof 192.168.9.254**

Detección !

- arp estática ....
- arpwatch (creo que para windows)
- Solución técnica 1 ...
  - ip r # para ver la ruta por defecto ...
  - traceroute www.google.com # vamos a ver por donde viajan nuestros paquetes ...
  - El primer salto debe coincidir con el gw por defecto
  - O tienen arp ....

Detección !!!

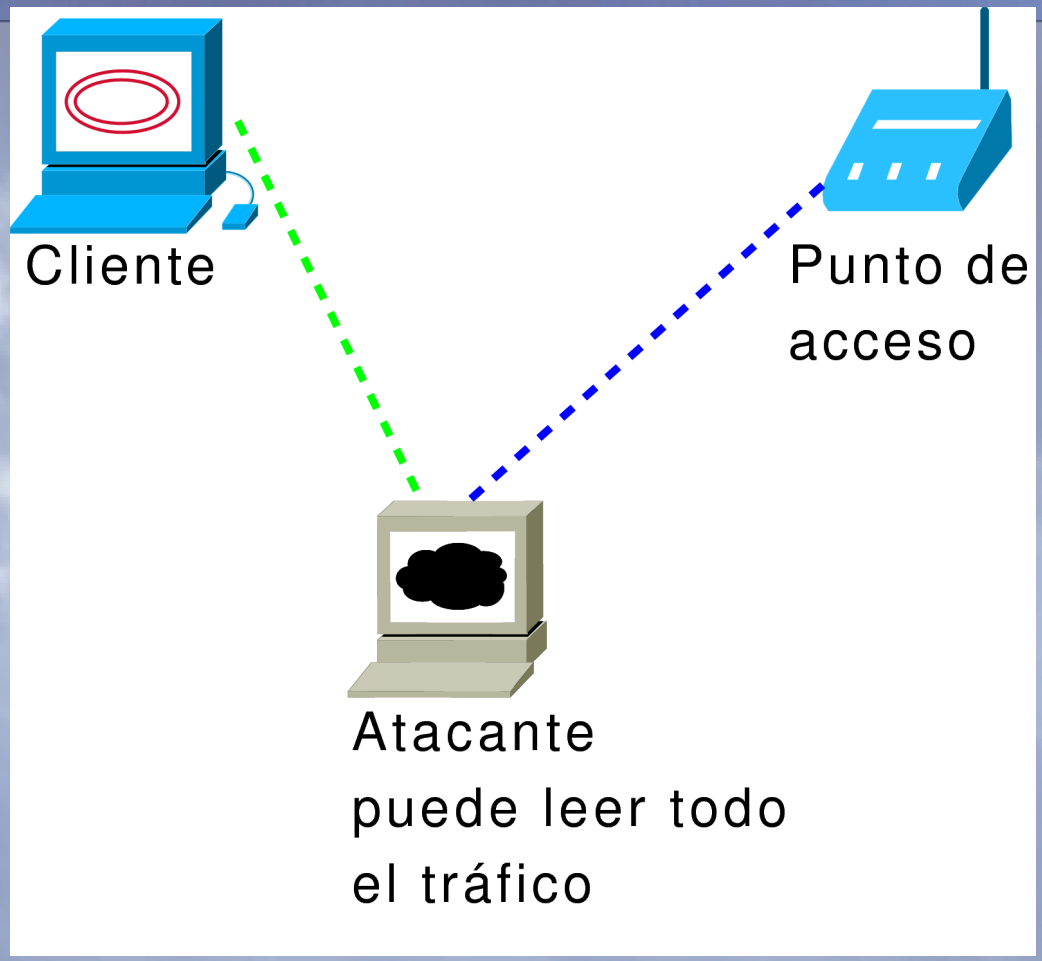
- **Solución técnica 2**
  - **Monitorear el tráfico arp**
  - **Tcpdump -nni wlan0 'arp'**
  - **Tráfico anómalo .... muchas respuestas arp**

Medio ?

_jack

Monkey jack

Solo para inalámbricas


Cliente
Punto de acceso
Atacante puede leer todo el tráfico

Un ataque más complejo

- Atacante necesita 2 tarjetas de red ...
- Interrumpe la comunicación entre el AP y el cliente
- Suplanta al AP y suplanta al cliente ...

Detección

- Es más compleja debido a la complejidad del ataque :)
- Escaneo de puertos de tu gw ..
- Tiempo de respuesta ..
- Canal de asociación
- MAC del AP ?!? macspoof

Avanzados !

Diversos

Falsos AP's
Sniffers en lo alámbrico
Otros ???

Detección ...

Alguna idea ????

Soluciones en general

- Rutas arp estáticas
  - Chamba extra pero te aseguras de que no te estén interceptando
- Uso de túneles
  - Puede ser tor, o vpn's
- Uso de https cuando sea posible
- No aceptar certificados en redes públicas (pueden ser falsos)
- Tu propia red ... BAM ?!?!?!

Agradecimientos !

- Organizadores del BugCON ...
- UPSLP $$$

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Datos de BugCON 09 !!!!

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

BugCon
security conferences

Preguntas ?!?!?!

hugo.gonzalez@upslp.edu.mx

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ