Seguridad Redes Inalámbricas

Dr. Roberto Gómez Cárdenas

DCC del ITESM-CEM

rogomez@campus.cem.itesm.mx

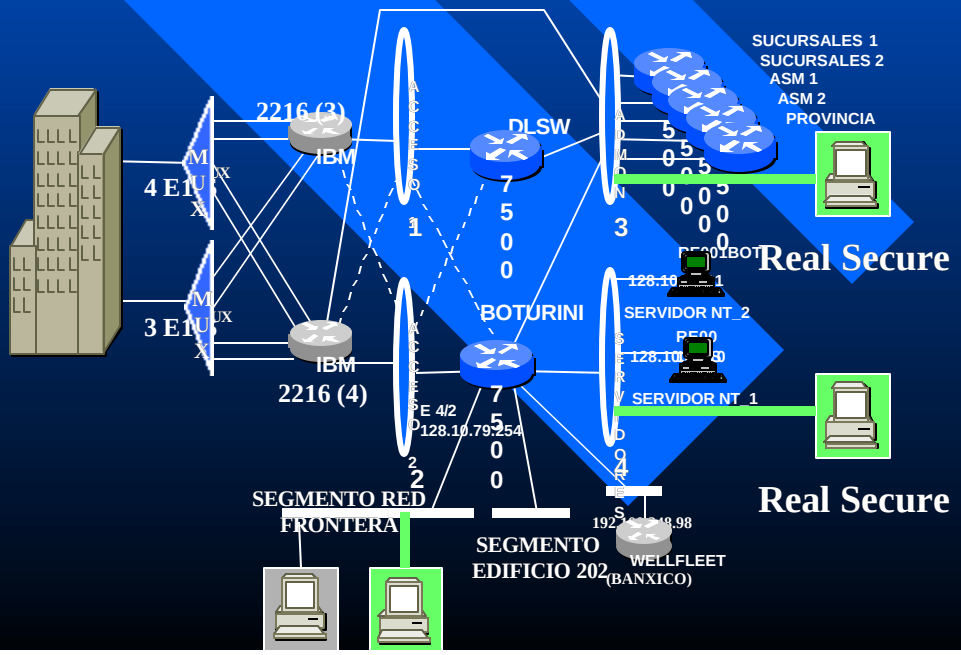
http://webdia.cem.itesm.mx/dia/ac/rogomez

Contenido

- Antecedentes
- Los ataquentes
- Tipos de ataques
- Defendiendo el sistema
- Redes inalambricas
- Seguridad redes inalambricas
- Atacando la seguridad de las redes inalambricas
- Conclusiones

Antecedentes

- Las redes fueron diseñadas para el intercambio de información y compartir recursos.
- La seguridad no era un factor tomado en cuenta en el diseño de las redes.



Haciendo cuentas ...

- Computación electrónica 50 años !
- Redes sólo tienen 30 años de vida !
- Seguridad 23 años !
- Internet 15 años !
- Web 6 años !
- Intranets 3 años...
- Extranets 2 años...

El Hacker: La Vieja Guardia

- Origen del término a finales de los 60.
- Programador con alto dominio de su profesión, capaz de solucionar problemas a través de hacks (segmentos de código muy ingenioso).
- Verdaderos conocedores de la tecnología de cómputo y telecomunicaciones (85-93).
- La búsqueda del conocimiento siempre fue su fuerza impulsora.

El cracker

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas computacionales. Una vez logrado el acceso produce daños a los recursos del sistema atacado.
- No necesariamente tiene el mismo nivel de conocimientos que el hacker

La nueva generación o los ¨Script-Kidies¨

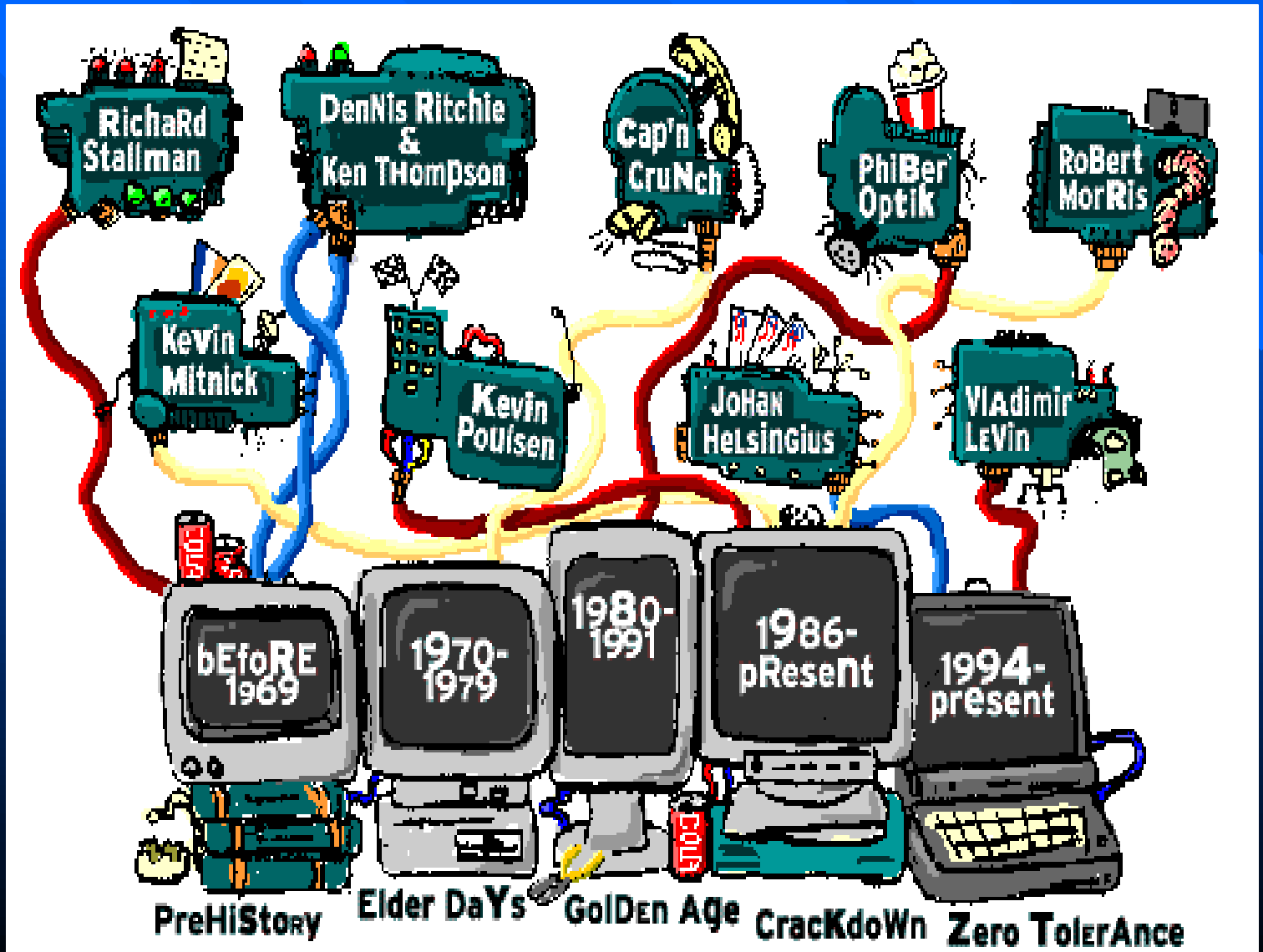
- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al inframundo.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy ¨cool¨.

El Hacker: La Visión del Resto de los Usuarios

- ¿Qué es eso?
- Eso pasa solo en las películas.
- Así como los de ¨The Net¨
- Yo soy hacker.
- Yo apenas sé como se usa una computadora.
- Bill Gates se va a encargar de ellos.

Hackers más Famosos.

(www.discovery.com/area/technology/hackers/hackers.html).



¿Qué es un ataque?

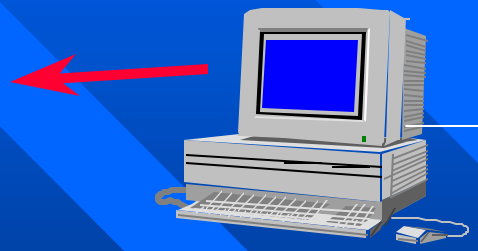
- Acción o acciones que previenen cualquier parte de un sistema de información automatizado, de funcionar de acuerdo con su propósito definido. esto incluye cualquier acción que causa la destrucción, modificación o retraso del servicio no autorizado.

Otra definición ...

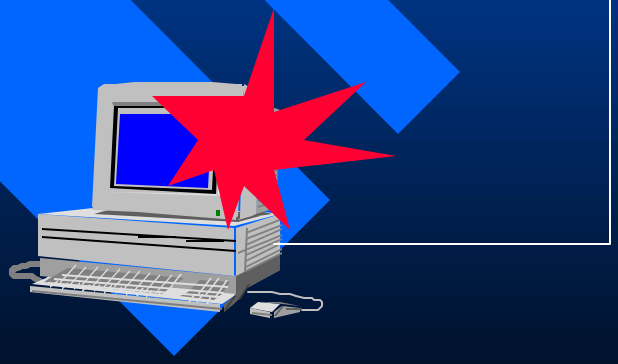
- El acto de tratar agresivamente, de evitar controles de seguridad de un sistema. el hecho de que se haga un ataque no necesariamente significa que tendrá éxito.
- El grado de éxito depende de la vulnerabilidad del sistema o actividad y la efectividad de las medidas de protección existentes.

Tipos de Ataques

Ataques Pasivos.



Ataques Activos.



Principales Ataques

- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Fuerza Bruta
- Basado diccionario
- Stack overflow
- Pepena
- Bombas lógicas
- Dedos inexpertos
- Falsificación
- Usurpación
- Sniffers
- Spam y hoaxes
- Grafiti
- Ingeniería Social
- Negación de servicio

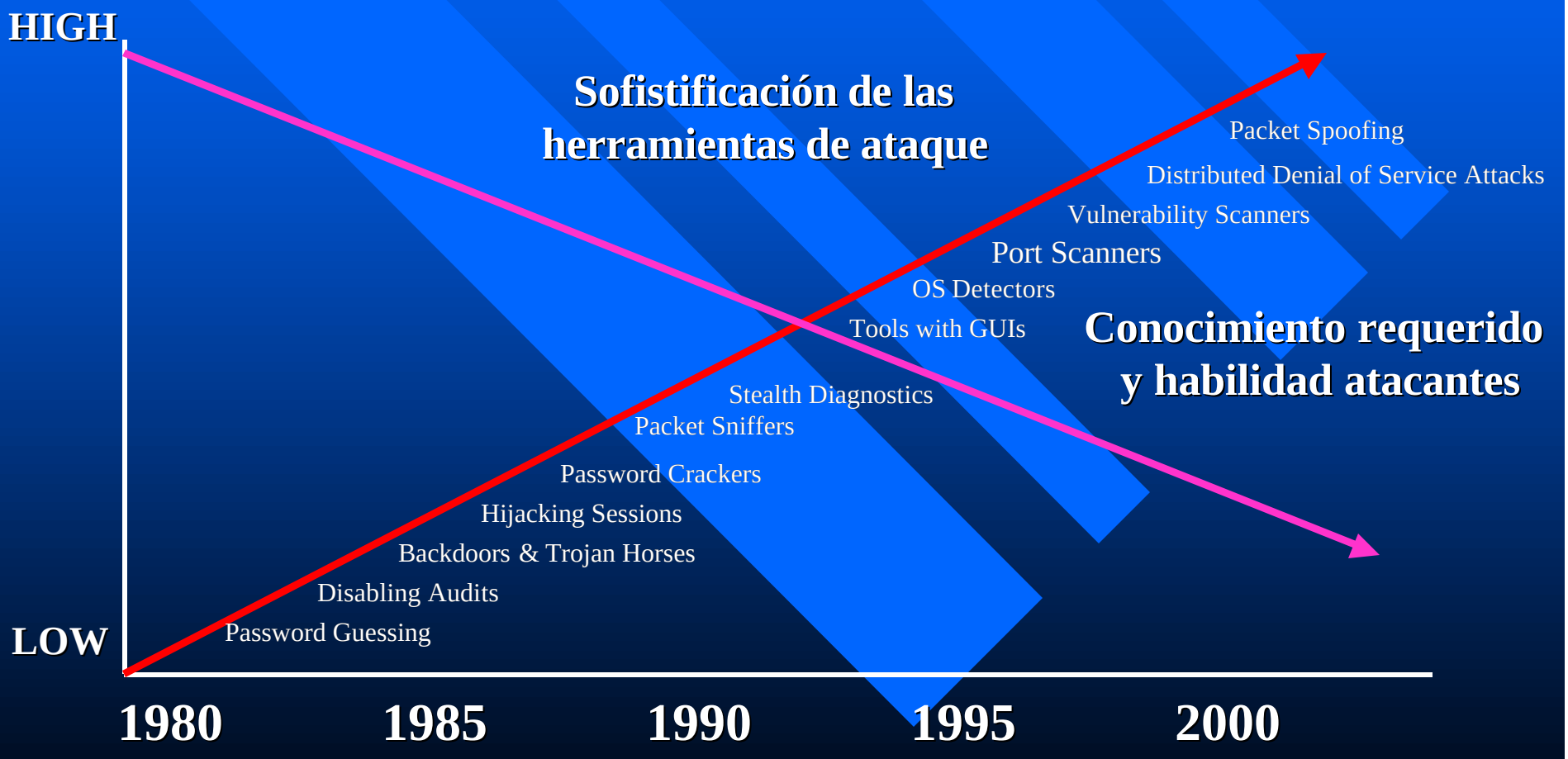
Sniffers

¿Cómo se comunican dos computadoras en una red local?

computadora en
modo promiscuo

snifeando (husmeando)

External Threats: Hacker Tool Explosion



Busqueda reciente en internet de “Hacker Tools” regresan cerca de 2100 hits

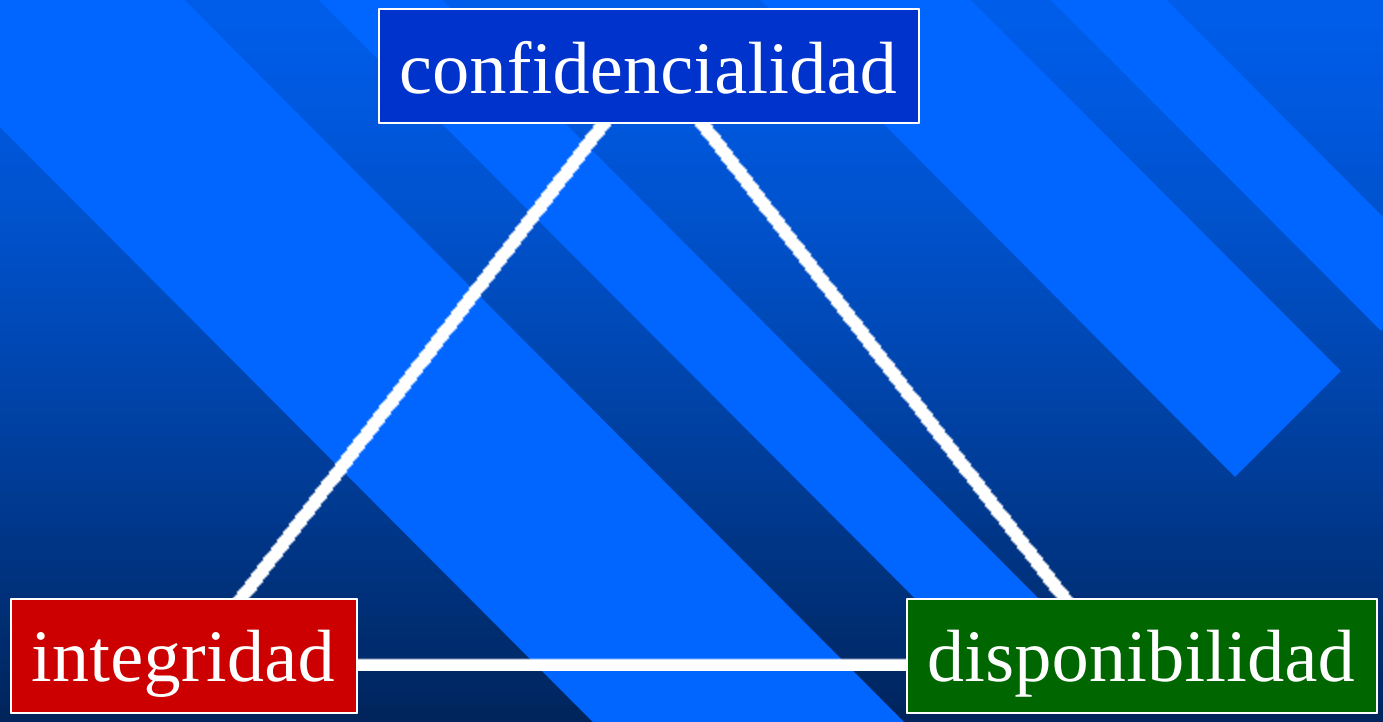
¿Cómo me protejo?

Dos aspectos a cubrir:
el administrativo y el técnico

¿Y qué es la seguridad computacional?

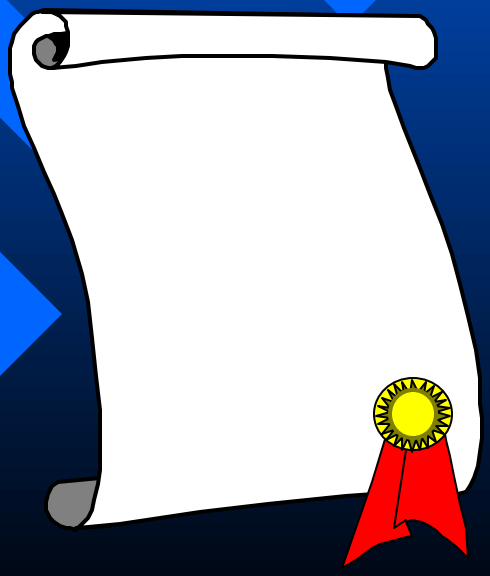
- Seguridad Computacional
  - conjunto de políticas y mecanismos que nos permiten garantizar la ***confidencialidad***, la ***integridad*** y la ***disponibilidad*** de los recursos de un sistema.

La seguridad computacional



Política de Seguridad

- Definición del conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Depende de los objetivos y metas de la organización.



Paradigmas

Existen varios paradigmas:

1) *Paranoico:* Nada está permitido.

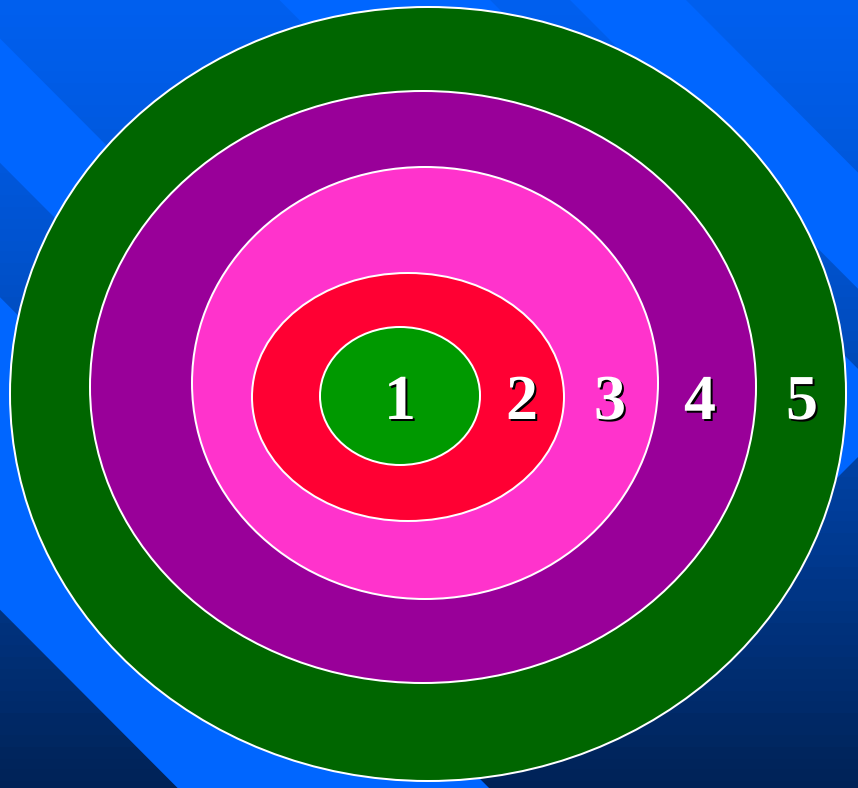
2) *Prudente:* Lo que no está expresamente permitido, está prohibido.

3) *Permisivo:* Lo que no está expresamente prohibido, está permitido.

4) *Promiscuo:* Todo está permitido.

Aspectos Técnicos
(definir perímetros)

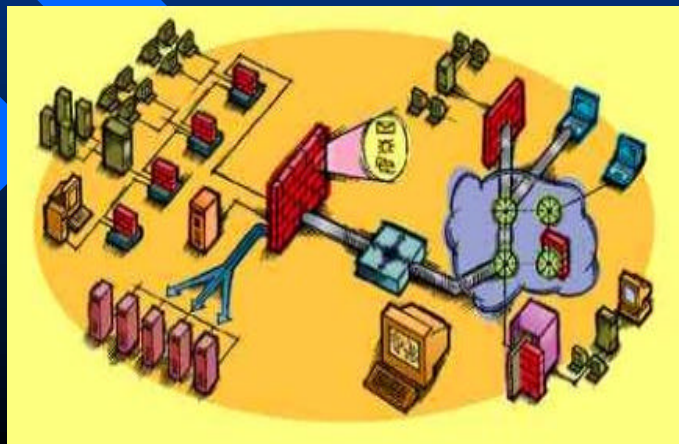
Los Perímetros



1. aplicaciones
2. almacenamiento
3. host
4. tránsito
5. perimetro exterior

Algunos mecanismos de seguridad

- Herramientas de prevención
  - firewalls
  - autenticación (biometricos, tjtas, inteligentes)
  - control de acceso
  - proxies, filtros
  - criptología
  - concientización de los usuarios
- Herramientas de monitoreo
  - IDS: Intruction Detection Systems
  - monitoreo del sistema (sniffers)



La criptologia

- Ciencia que estudia los aspectos y contenidos de información en condiciones de secrecía.
- Del griego: *criptos* oculto y *logos* tratado
- La Criptología se divide en:
  - *Criptografía*
  - *Criptoanálisis*

Criptografía

- Es el *arte* de construir códigos secretos.
- Es el conjunto de técnicas o procedimientos que alteran los símbolos de información sin alterar el contenido, convirtiendo a la información modificada en un conjunto de símbolos sin sentido para las partes que no disponen de las técnicas.

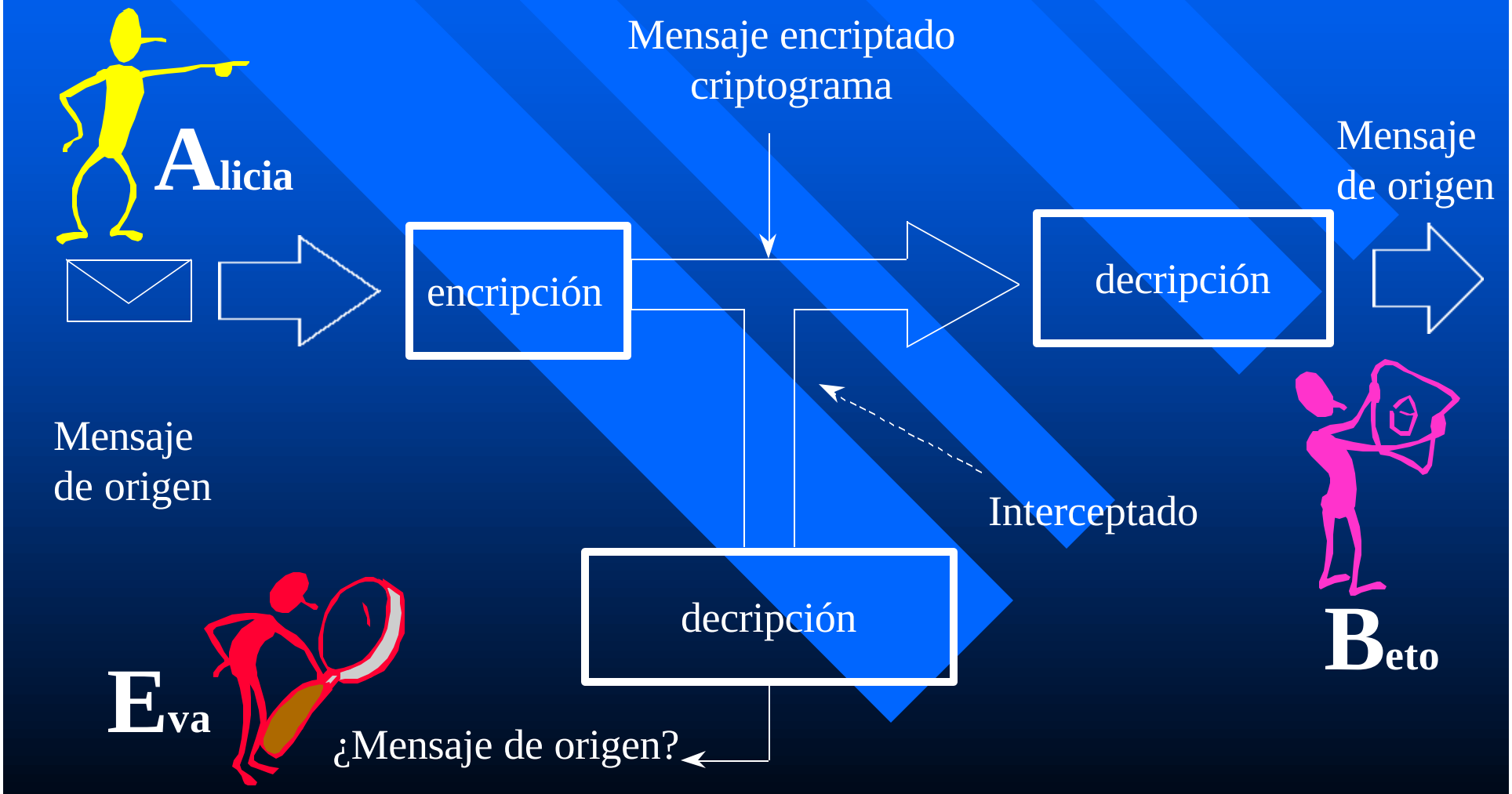
Criptoanálisis

- Metodologías y técnicas que permiten recuperar la información que ha sido previamente tratada por un procedimiento criptográfico, sin conocer *"a priori"* la técnica utilizada para la criptografia.

Criptosistemas

- Es el conjunto de procedimiento que garantizan la seguridad de la información y utilizan técnicas criptográficas.
- El termino en inglés es cipher.
- El elemento fundamental de un Criptosistema es la *“llave”*.
- En algunas referencias a la llave se le conoce como *clave*.

Elementos criptosistema



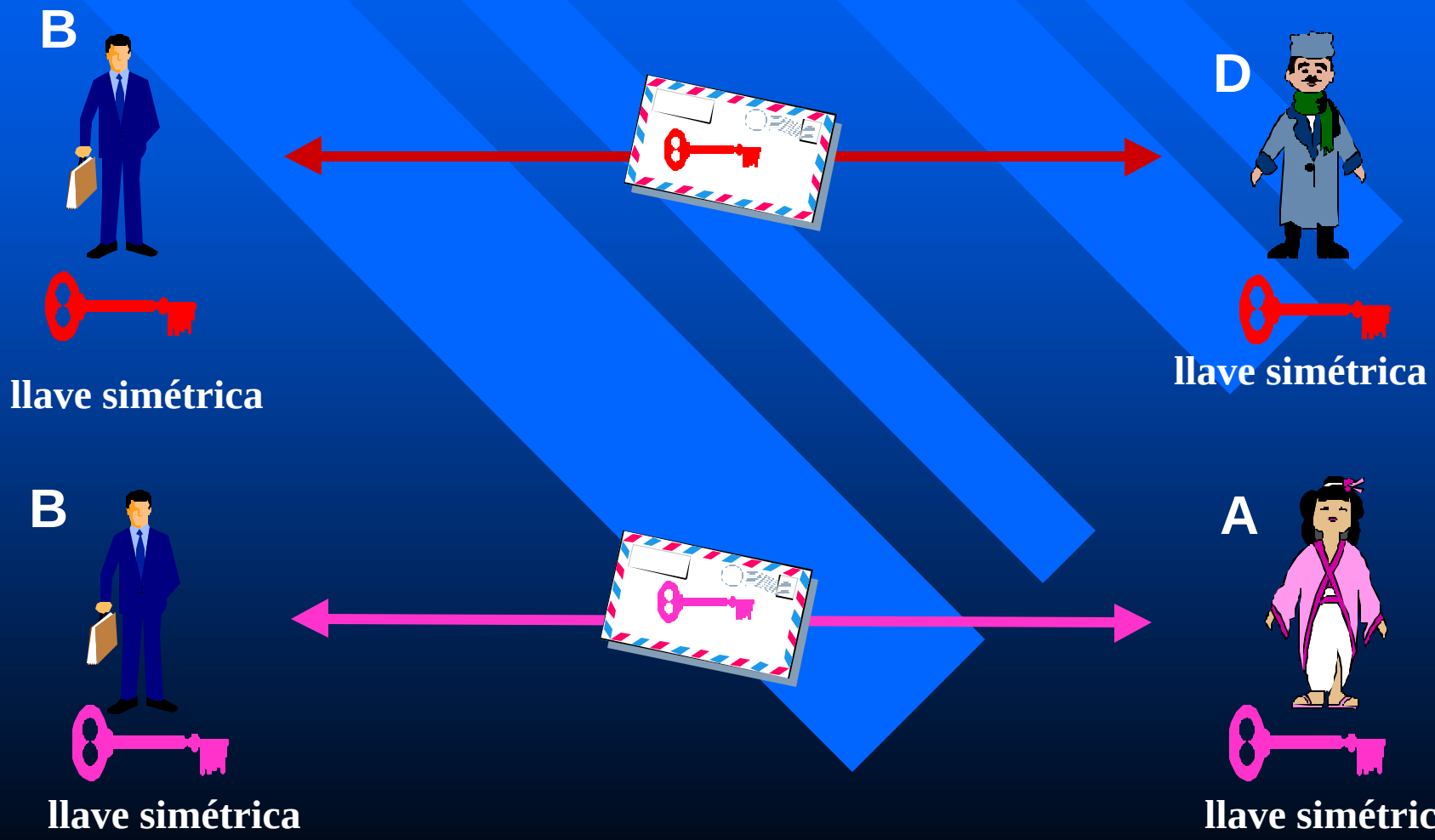
Métodos criptográficos modernos

- Métodos Simétricos
  - llave encriptado coincide con la de descifrado
  - la llave tiene que permanecer secreta
  - emisor y receptor se han puesto de acuerdo previamente o existe un centro de distribución de llaves
- Métodos asimétrico
  - llave encriptado es diferente a la de descriptado
  - llave encriptado es conocida por el público, mientras que la de decriptado solo por el usuario

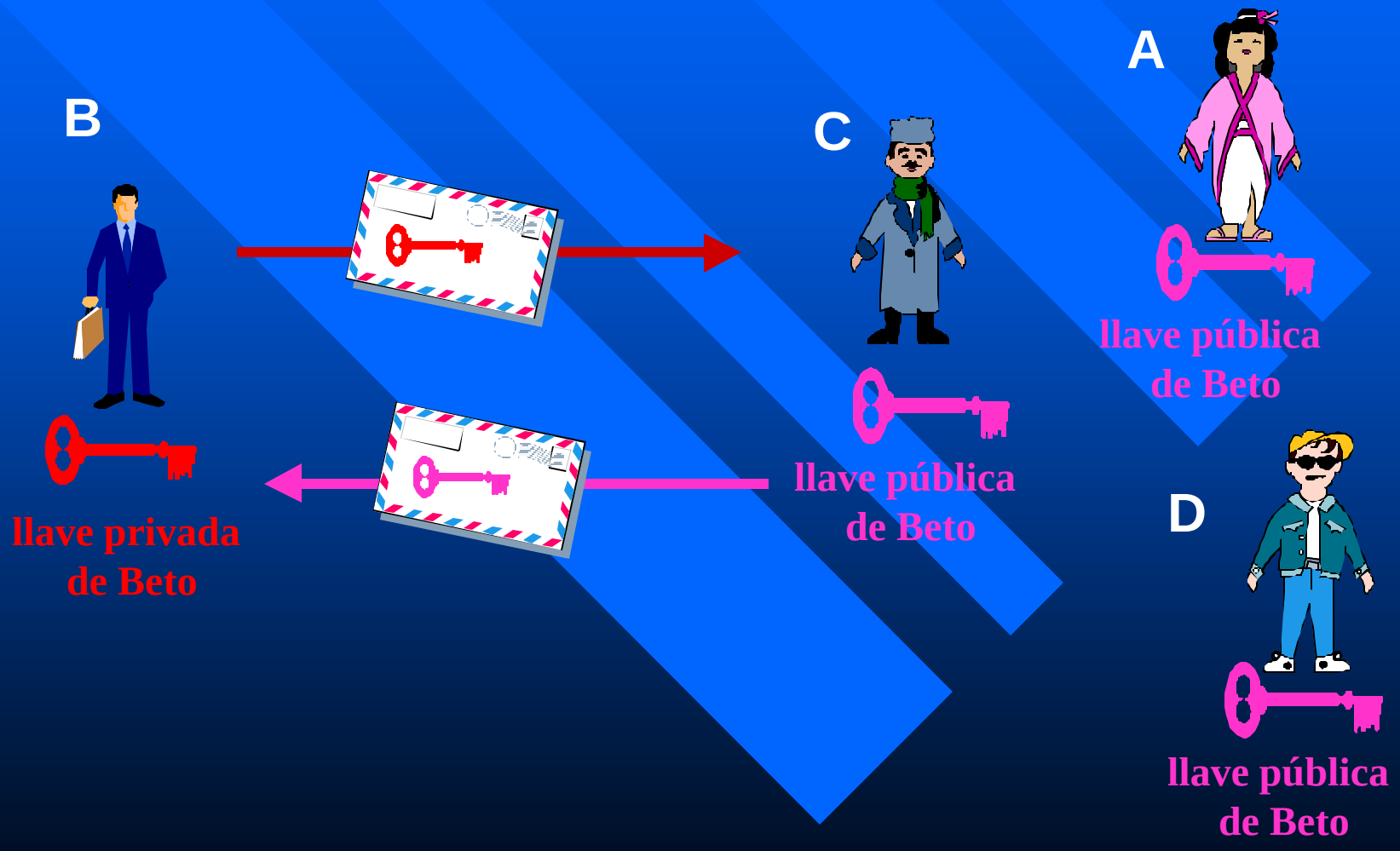
Sinonimos metodos

- Los métodos simétricos son propios de la criptografía clásica o criptografía de llave secreta.
- Los métodos asimétricos corresponden a la criptografía de la llave pública, introducida por Diffie y Hellman en 1976.

Encripción llave secreta (simétrico)



Criptograma llave pública (asimétrico)



Clasificación métodos encripción simetricos

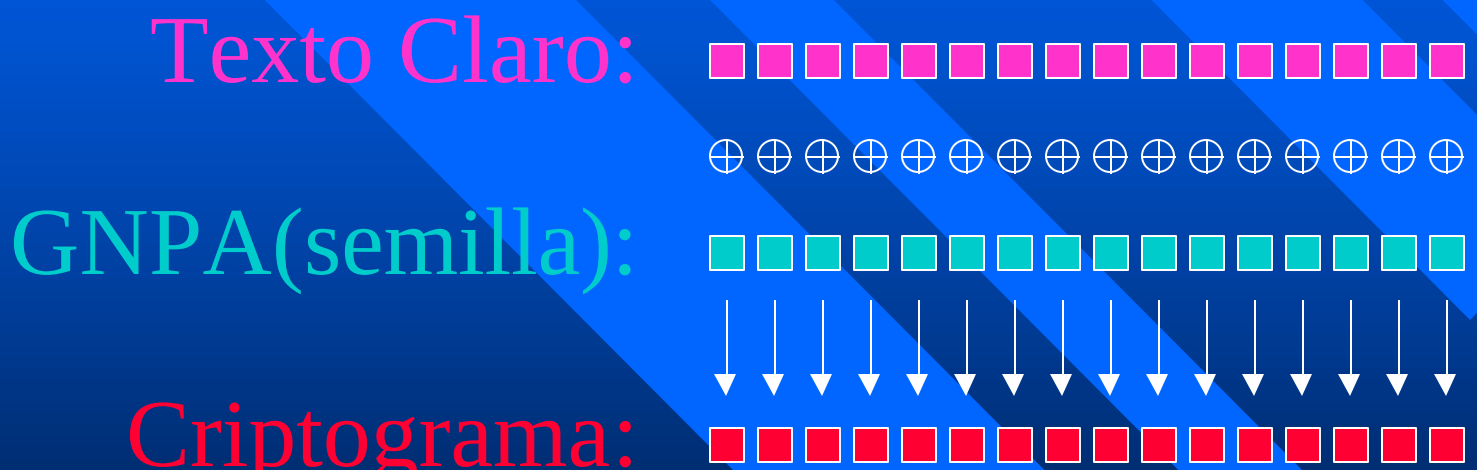
- Encripción en flujo

- Encripción en bloques

Encriptado en flujo

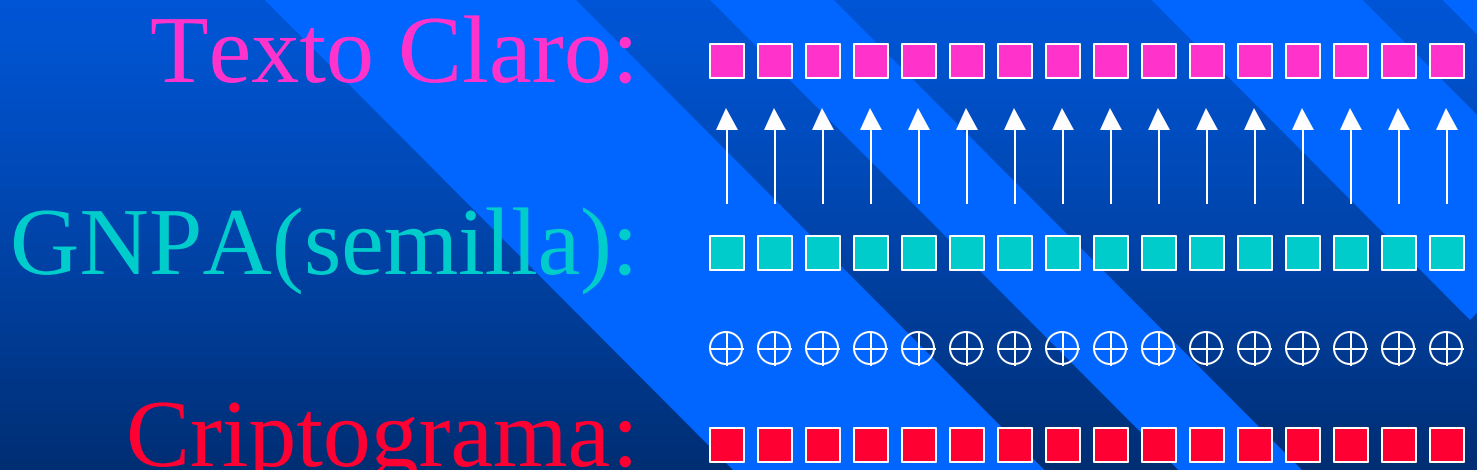
- En inglés: stream ciphers.
- Usa la llave como semilla de un generador de números pseudo-aleatorio.
- Toma el flujo de bits generado por el generador y realiza un XOR con el texto plano para construir un criptograma.
- Es más seguro conforme más se aproxima la secuencia binaria generada a una auténtica secuencia aleatoria

Encripción de criptosistemas de flujo



GNPA: Generador Números Pseudo-Aleatorios

Decripción de criptosistemas de flujo



GNPA: Generador Números Pseudo-Aleatorios

Las redes

- RED: unión de dos o más computadoras, para crear una comunicación entre ellas que les permita compartir información y recursos.
- Para realizar esta conexión se requiere de un medio físico, en el cual viajará la información.

¿Que es una red inalámbrica o WLAN?

- El medio de transmisión más utilizado es el cable, pero para el caso de una red inalámbrica ese medio físico es el aire.
- WLAN: Siglas en inglés de Wireless Local Area Network.

¿Que va a pasar con el cableado de red?

- Una red inalámbrica NO va a desplazar a una red por medio de cable.
- La red inalámbrica complementa a la red cableada en situaciones como
  - difícil montar una red,
  - realizar más conexiones
  - se requiere estar moviéndose de un área a otra sin necesidad de desconectarse de la red (computo móbil)

Ventajas

- Flexible
  - llega donde el cable no puede.
- Facilidad de instalación (simple y rápida).
  - no hay necesidad de cableado.
  - se evita tirar cables por muros y techos.
- Escalabilidad
  - el cambio de topología de red es muy sencillo.
- Movilidad
  - información en tiempo real en cualquier lugar con cobertura para todo usuario de la red.
- Integración a las redes tradicionales.

Limitaciones

- Potencia y distancias limitadas.
- Velocidad de transmisión limitada.
- Tecnología relativamente nueva.
- ***A mayor velocidad de transmisión, menor área de cobertura de la señal y viceversa.***

Aplicaciones

- LANs preinstaladas.
- Acceso a información de usuarios moviles.
- Entornos difíciles para el cableado.
- Entornos que cambian con frecuencia.

Tipos WLANS

- Ad-hoc
- Infraestructura permanente

WLAN Ad hoc

- Se juntan varios nodos móviles en una área reducida
- Se establece una comunicación entre ellos sin la ayuda de ningún tipo de columna (backbone).
- Para implementar redes ad hoc se tienen dos maneras:
  - Broadcasting/flooding
  - Infraestructura temporal

Broadcasting/Flooding

- Se tiene un protocolo de acceso múltiple como ALOHA ó CSMA.
- Un nodo con paquetes listos para enviar, los envía. Otro nodo los recibe, los checa y si no son para él lo retransmite sin leerlo.
- La desventaja radica en una pobre utilización del canal y la falta de garantía de una recepción óptima.
- La ventaja es su sencillez de implementación.

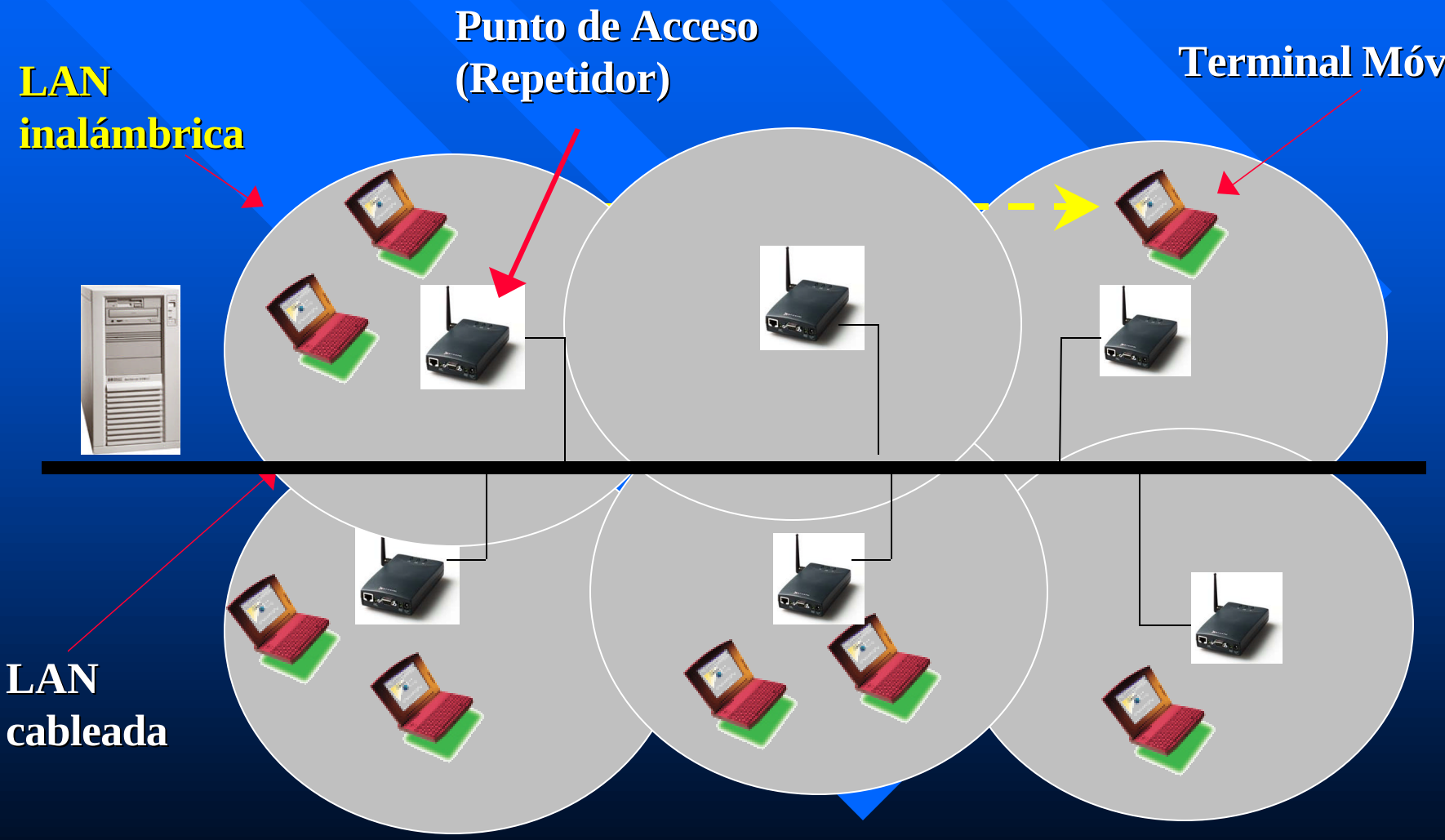
Infraestructura temporal

- Los nodos pueden establecen una infraestructura temporal
  - esta infraestructura jerárquica elige un nodo como estación base.
- Desventajas:
  - sólo sirve para una red con un número pequeño de nodos,
  - la estructura se tiene que actualizar periódicamente, lo que reduce la eficiencia del canal (disolvencia del mensaje)

WLAN con infraestructura permanente

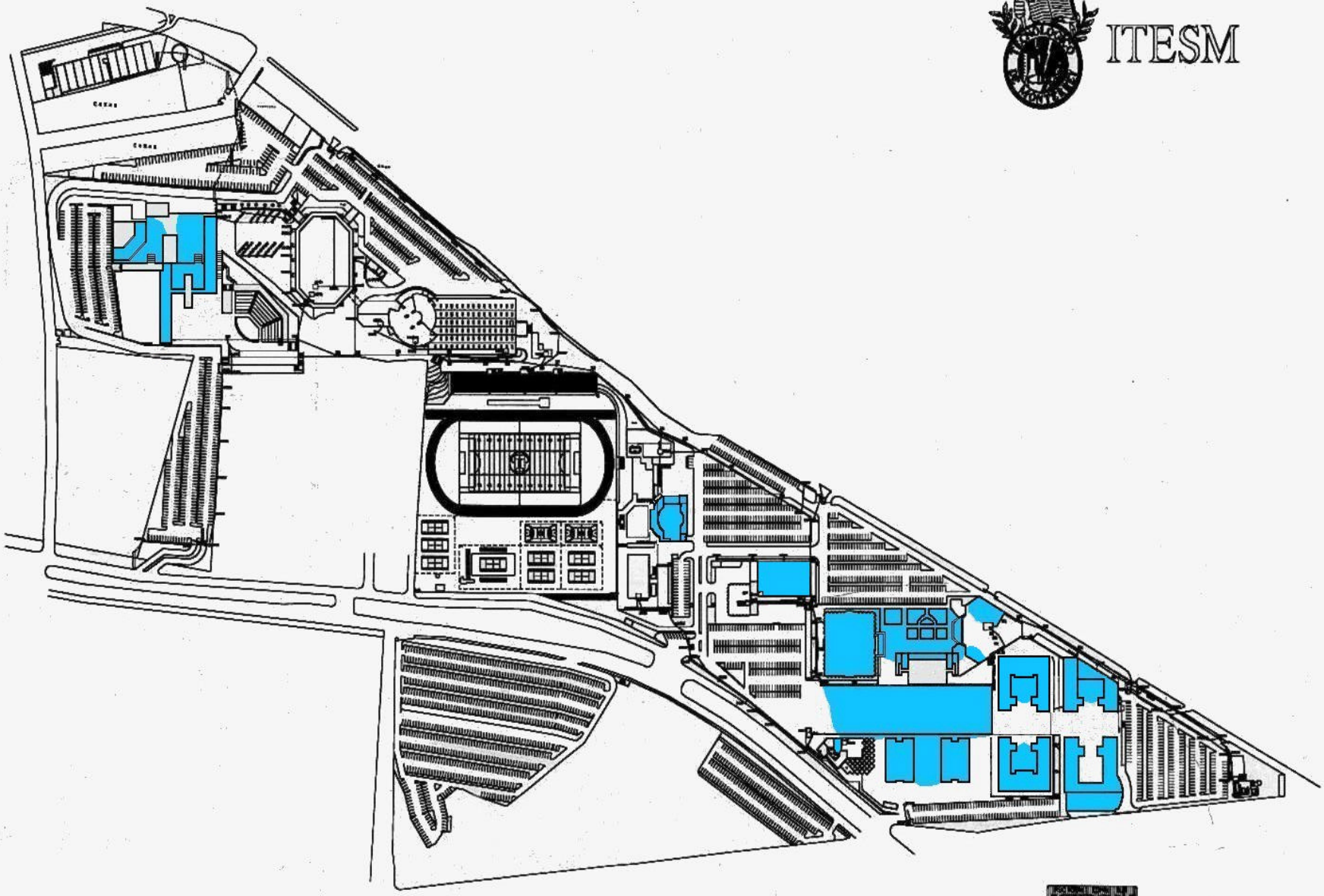
- Regularmente la infraestructura principal es una columna vertebral cableada (backbone).
- Esta estructura tiene puntos de contacto (puntos de acceso) con el medio inalámbrico.
  - estos pueden ser estaciones base o repetidores
- A partir del backbone existen dos tipos de comunicación
  - subida
  - bajada.

Ejemplo estructura WLAN



Elementos de una WLAN

ITESM



ITESM

CAMPUS ESTADO DE MEXICO

DIRECCION DE PROYECTOS

Instalacion Telefonica General

Riesgos de una WLAN

- Monitoreo de tráfico inalambrico
  - datos de usuarios
  - localización de usuarios
  - identidad de usuarios
  - análisis de tráfico
- Acceso no autorizado a una red a través de un enlace inalambrico
  - persona pasaendose en una bicicleta
- Corrupción de servicios inalambricos

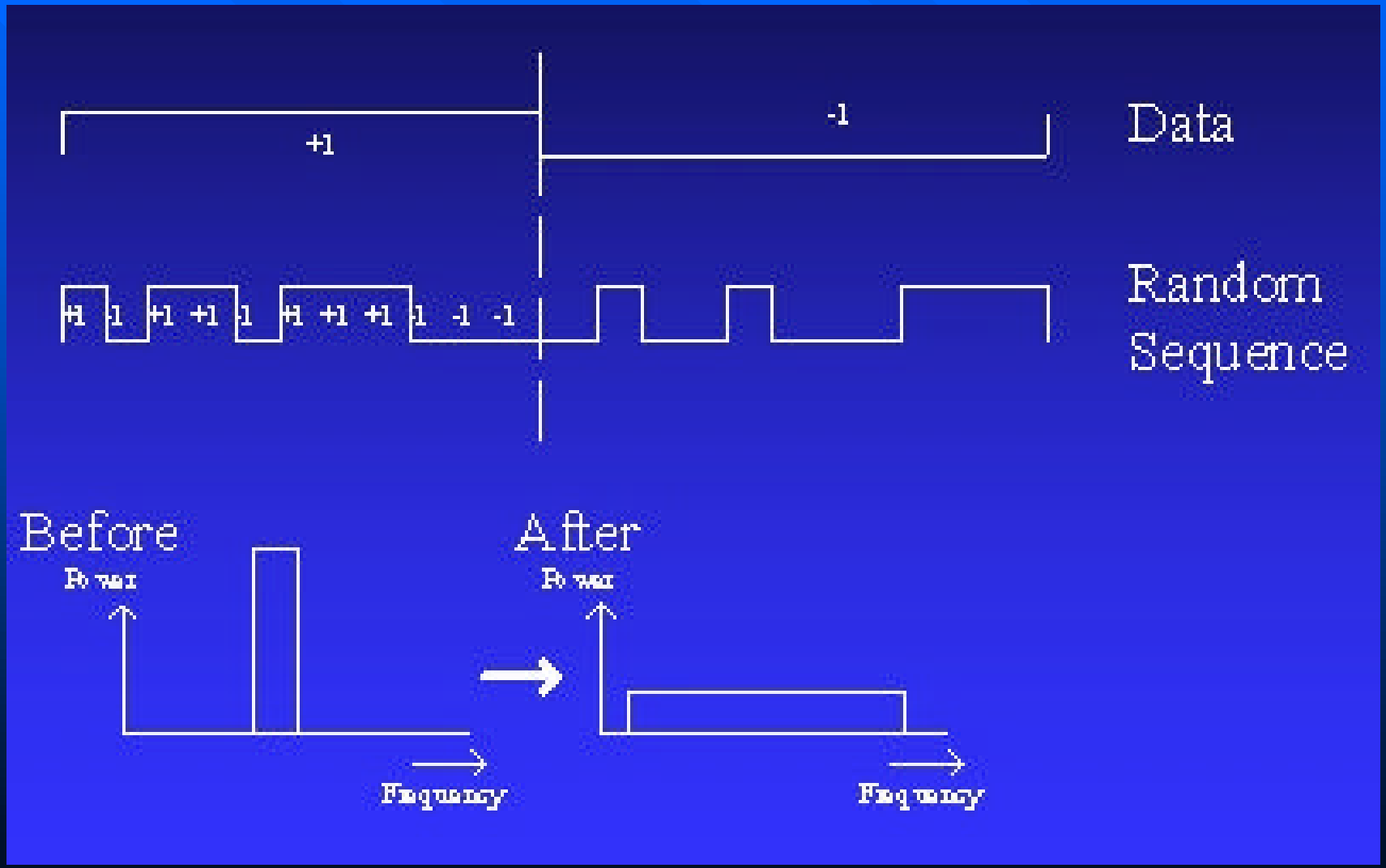
Servicios para evitar riesgos

- Limitar el ambiente inalambrico
  - anchos de banda
  - encripción/decripción realizada en tiempo real
  - sincronización
- El mismo metodo de acceso puede proporcionar un nivel de seguridad
  - DSSS: Direct Secuence Spread Spectrum
  - FH: Frecuency Hopping

Características DSSS

- Espectro disperso de secuencia directa
- La información se mezcla con un patrón pseudo aleatorio de bits, con una frecuencia mucho mayor que la de la información a transmitir.
- Aquel receptor que tenga el mismo código de extensión, será capaz de regenerar la información original.
- Menor alcance, mayor velocidad.
- Puede enviar mayor número de paquetes en un mismo tiempo.

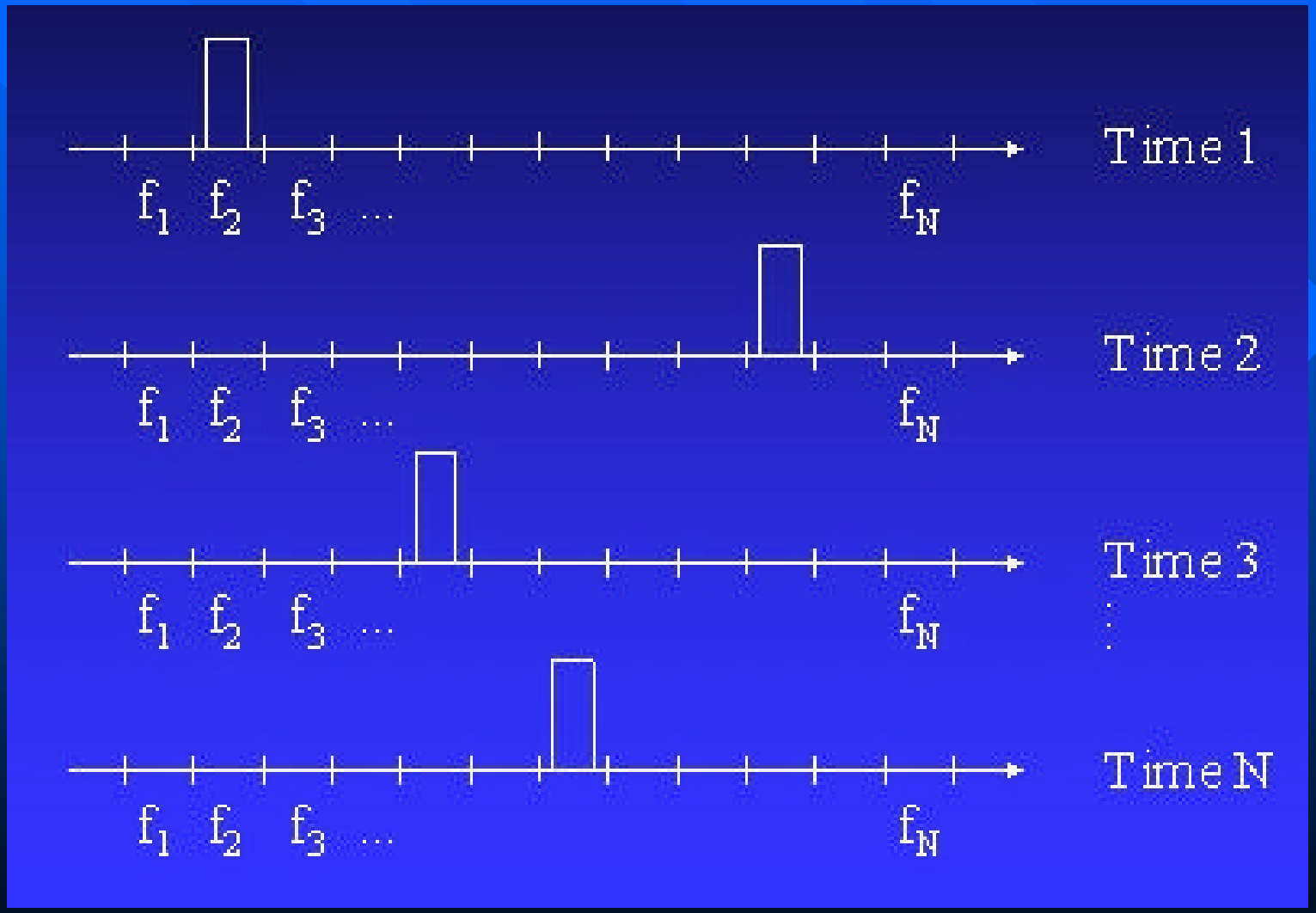
Esquema DSSS



Características FH

- Salto de frecuencia
- La información se transmite brincando de de manera aleatoria en intervalos de tiempo fijos, llamados “chips”, de un canal de frecuencia a otro en la banda total.
- Aquel receptor sincronizado con el transmisor y tenga exactamente el mismo código de salto podrá brincar a las frecuencias correspondientes y extraer la información.
- Menor inmunidad al ruido.
- Mayor alcance, menor velocidad

Esquema FH


Time 1
f1 f2 f3 ... fN
Time 2
f1 f2 f3 ... fN
Time 3
f1 f2 f3 ... fN
:
Time N
f1 f2 f3 ... fN

Otros servicios de seguridad

- Autorización a través de passwords y llaves para usuarios mobiles y puntos de acceso.
- Uso de la criptografia para protegaer los datos de los usuarios y su identidad

Estandares WLAN

- IEEE-811
  - el comité IEEE 802.11 estuvo trabajando en el desarrollo de un stándard para LAN´S inalámbricas desde 1990 y a mediados de 1996 concluyeron.
- El Europeo HIPERLAN (ETSI)
  - en 1991 se formó el standard HIPERLAN, desarrollado por el Instituto de Standards de Telecomunicaciones Europeo (ETSI).

Características IEEE-802.11

- Soporta velocidades de 2 Mbits/seg
- Soporta tanto redes tipo ad-hoc como de infraestructura
- Contiene estandares para los siguientes metodos de acceso:
  - DSSS: Direct Secuence Spread Spectrum (11 canales)
  - FH: Frecuency Hopping (79 canales, tres conjuntos de 26 saltos)
  - DSSS y FH operan en bandas de 2.4GHz ISM

Servicios Seguridad del IEEE 802.11

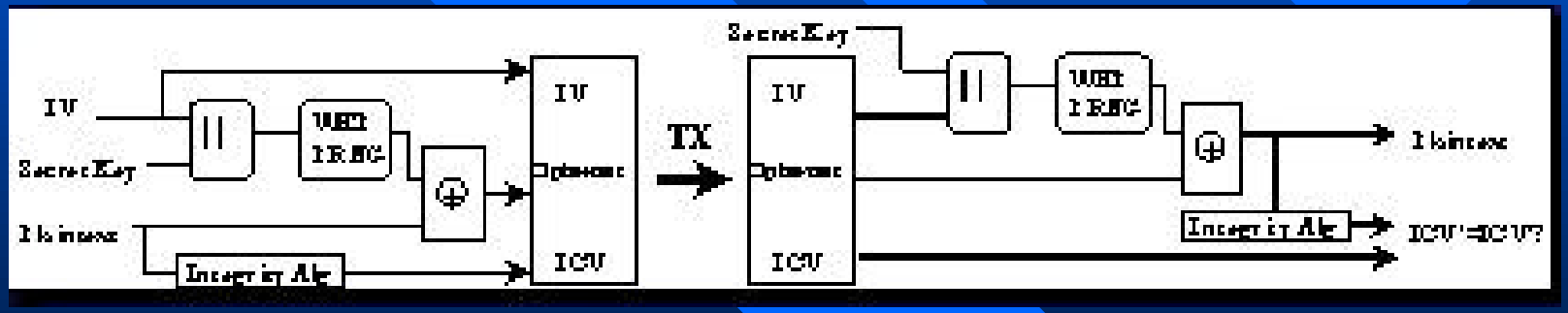
- WAP: Wired Equivalency Privacy (WEP)
  - Protección igual o mejor que las redes alambradas
  - Uso de llaves para autenticar cada estación
  - Puntos de acceso tambien requieren una llave para ser admitidos en la red
  - Desarrollo de rotocolos de autenticación y de distribución de llaves se les deja a los vendedores
  - Encripción *opcional* de datos entre estaciones usando algoritmo RC4

Algoritmo RC4

- Algoritmo propietario (RSA)
- Algoritmo de flujo
- Longitud llave variable (hasta 2048 bits)
- Algoritmo rápido
- Se dice que es un algoritmo muy fuerte
- Exportable fuera de US
- Algoritmo *dado a conocer* en internet en 1994

Encripción datos en IEEE 802.11

- La llave secreta es de 40 bits
- Se cuenta con un vector de inicalización de 24 bits



Comentarios sobre la seguridad IEEE 802.11

- Solo los datos de la estación estan encriptados
  - la identidad de la estación no se encripta
- El algoritmo se encuentra a nivel MAC (acceso) no actualizable
- Llaves de 40 bits
  - cortas para reducir overhead
  - que pasa con ataques de fuerza bruta

¿Y todo es seguro?

no totalmente...

Airsnort

- Herramienta para wireless LAN que recupera llaves de encriptación.
- Opera rastreando las transmisiones que pasan por la red inalámbrica.
- Una vez que han sido enviados suficientes bloques de información calcula la llave de encriptación utilizada.
- Todas las redes de 802.11b con 40/128 bit WEP (Wired Equivalent Protocol) son vulnerables, ya que tienen numerosas grietas de seguridad.

¿Cuanta información requiere?

- AirSnort, junto con WEPCrack son las primeras implementaciones públicas de este tipo de ataque.
- Requiere interceptar aproximadamente de 100MB a 1GB de datos, una vez que los tiene, AirSnort puede adivinar la llave de encriptación utilizada en menos de un segundo.

Prerequisitos de Airsnort

- Linux, wlan-ng drivers, 2.4 kernels.
- Para compilar AirSnort se requiere:
  - fuente del Kernel
  - paquete de PCMCIA CS.
  - paquete de wlan-ng
  - patch wlan-monitor-airsnort
- AirSnort requiere el juego de chips Prism2,
  - las tarjetas que lo poseen son las únicas capaces de llevar a cabo el sniffing necesario.

¿Es posible obtener tantos datos?

- Negocio con cuatro empleados que utilizan el mismo password.
- Estos empleados navegan por la red todo el día
  - generando alrededor de 1,000,000 de bloques de información al día,
  - de los cuales aproximadamente 120 de ellos son débiles.
- Después de 16 días es casi seguro que la red haya sido crackeada.
- En este ejemplo la red no esta saturada
  - en el caso de una red saturada generalmente este tiempo se reduciría a un solo día.

Algunas observaciones

- Se esta atacando un *protocolo* que utiliza un *algoritmo de encripción*, no al algoritmo en si.
- Posibles acciones a tomar:
  - encriptar a niveles más altos del protocolo
  - actualizar a los estandares 802.11 cuando estos estén disponibles
  - tener cuidado con la generación de llaves
- RC4 es utilizado en otros protocolos “sin problemas”.

Conclusiones

- No existe un 100% de seguridad.
- Tengo información sensible en mi institución/organismo
- Hay que definir políticas.
  - respetarlas y darle seguimiento
- Conforme la tecnología avanza se necesitan algoritmos más fuertes
- Sin embargo la tecnología de criptoanálisis tambien evoluciona.

La invencibilidad depende de uno mismo; la vulnerabilidad del enemigo, de él.

La invencibilidad reside en la defensa; la posibilidad de la victoria en el ataque.

Sun Tzu

¨El arte de la guerra¨

Dr. Roberto Gómez Cárdenas

DCC del ITESM-CEM

rogomez@campus.cem.itesm.mx

http://webdia.cem.itesm.mx/dia/ac/rogomez