

PROGRAMACIÓN DE SISTEMAS TELEMÁTICOS

Msig. Adriana Collaguazo Jaramillo
Docente FIEC-ESPOL

TABLA DE CONTENIDOS

UNIDAD 4. INTEGRACIÓN DE SISTEMAS TELEMÁTICOS



SERVICIOS DE LOCALIZACIÓN



SISTEMA DE MENSAJERÍA



PRINCIPIOS DE SEGURIDAD EN RED



ASEGURAMIENTO DE SISTEMAS TELEMÁTICOS



OBJETIVO DE APRENDIZAJE



Aplicar servicios de localización, mensajería usando servicios en red para el manejo de notificaciones al usuario.

Servicios telemáticos móviles

- Telematics es en realidad la versión inglesa del término francés telematique, que fue acuñado por Simon Nora y Alain Minc en el libro L'informatisation de la Societe (La Documentation Francaise, 1978).
- La *telemática* a menudo se usa indistintamente con los servicios móviles basados en la ubicación.
- Recientemente la telemática se usa cada vez más para referirse a la telemática automotriz o los servicios de ubicación móvil para uso en vehículos.



Servicios de localización móvil

- Las tecnologías de análisis espacial desarrolladas en GIS (Geographic Information Systems) se han reutilizado para lograr la velocidad y la escalabilidad necesarias para los servicios de ubicación móvil.
- Las redes de datos inalámbricas de los operadores móviles se utilizan para la implementación de aplicaciones.
- Las tecnologías de posicionamiento aprovechan las tecnologías inalámbricas y satelitales para realizar mediciones complejas para identificar la ubicación de un usuario móvil, una información crítica en muchas aplicaciones móviles basadas en la ubicación.

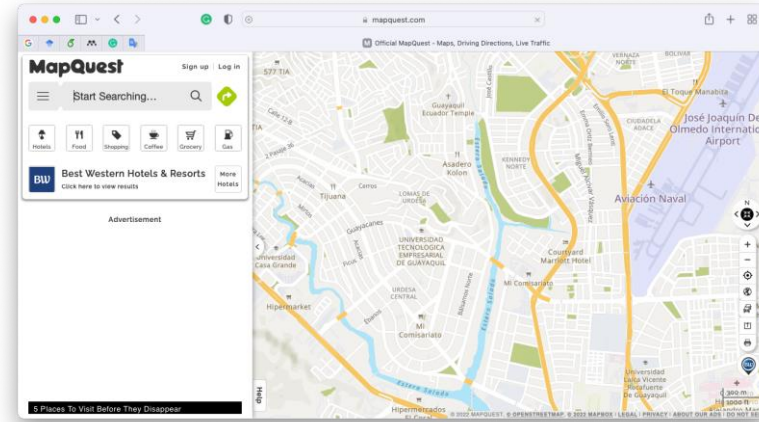


Servicios de localización móvil

- La información y el análisis basados en la ubicación permiten herramientas valiosas para la toma de decisiones en una variedad de aplicaciones.

Preguntas de evaluación:

- *¿En qué se diferencian los servicios móviles basados en la ubicación?*
- *¿Cuáles son las restricciones que tienen los servicios de localización móvil?*
- *Entonces, ¿Qué son exactamente los servicios de localización móvil?*



Referencias:

<https://www.mapquest.com/>

Artículo: M2M technology for bus fleet management. Case study: A college transportation system

<https://ieeexplore.ieee.org/document/9140131>

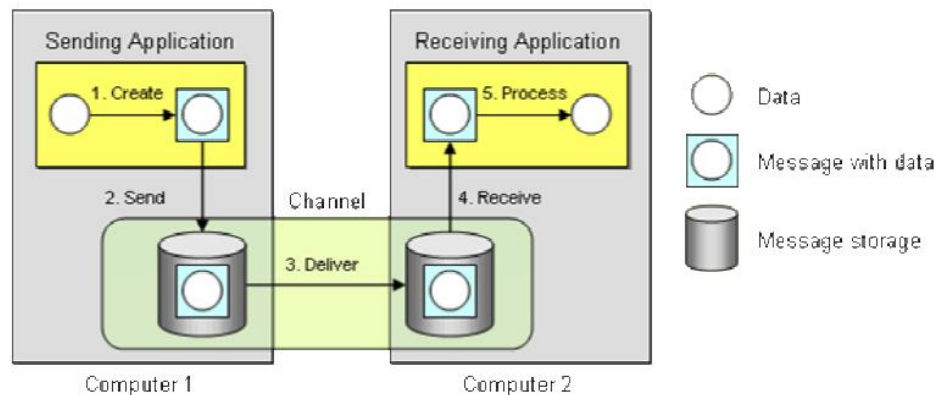
Servicios de localización móvil

Tracker - GSM



Sistema de mensajería

- La mensajería es una tecnología que permite la comunicación de programa a programa, asincrónica y de alta velocidad con entrega confiable.
- Los programas se comunican mediante el envío de paquetes de datos llamados mensajes entre sí.
- Los canales, también conocidos como colas, son rutas lógicas que conectan los programas y transmiten mensajes.
- El *mensaje* en sí es un tipo de estructura de datos.



Sistema de mensajería

- Un *canal* se comporta como una colección o matriz de mensajes, pero uno que se comparte entre varias computadoras y puede ser utilizado simultáneamente por varias aplicaciones.
- Un *emisor* es un programa que envía un mensaje escribiendo el mensaje a un canal.
- Un *receptor* es un programa que recibe un mensaje leyéndolo (y eliminándolo) de un canal.



Sistema de mensajería

- Las capacidades de mensajería generalmente las proporciona un sistema de software separado llamado messaging system or message-oriented middleware (MOM).

Preguntas de evaluación

- Entonces, ¿qué es un sistema de mensajería?.
- ¿Por qué usar un sistema de mensajería?



Principios de seguridad en red

¿Qué es seguridad de la red?

- La seguridad de la red es la protección de la infraestructura de red subyacente contra el acceso no autorizado, el uso indebido o el robo.
- Implica crear una infraestructura segura para que los dispositivos, las aplicaciones, los usuarios y las aplicaciones funcionen de manera segura.
- La implementación de la seguridad de la red logra las siguientes metas:
 - Comprobar la **confidencialidad** de los datos.
 - Mantener la **integridad** de los datos.
 - Mantener la **disponibilidad** de los datos.



Principios de seguridad en red



¿Por qué es necesaria la seguridad de la red?



- Para mantener fuera entes maliciosos que traten de vulnerar el sistema y acceder a información restringida.
- Para asegurarse de que la información y acceso al sistema no se otorguen inadvertidamente a un tercero.



Principios de seguridad en red

¿Qué es un ciberataque?

Es un intento malicioso y deliberado por parte de una persona u organización de atacar el sistema de información de otra persona u organización.

Por lo general, el atacante busca algún tipo de beneficio al interrumpir la red de la víctima.



Video

<https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html?socialshare=anchor-info>



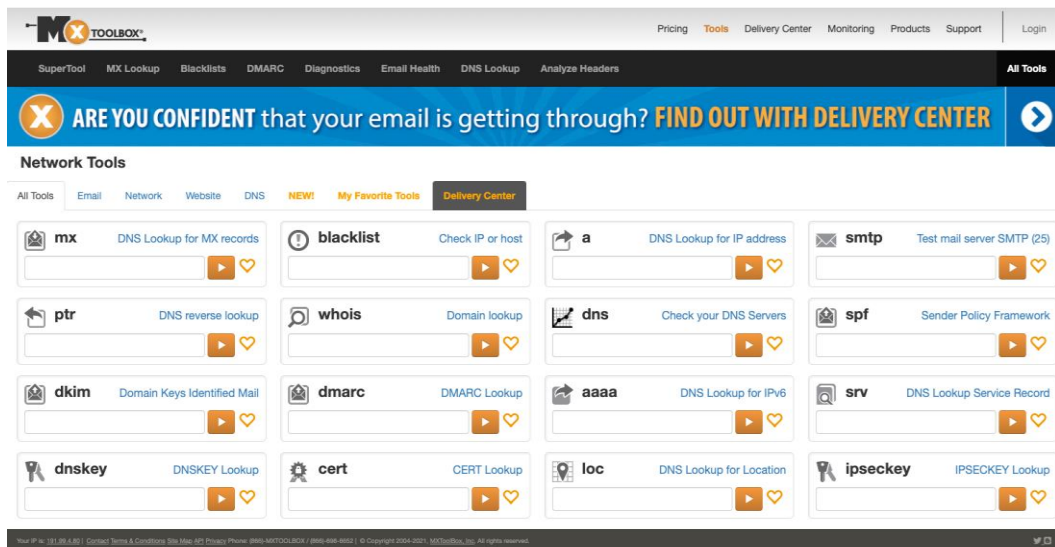
Principios de seguridad en red

La primera fase de un ciberataque es la fase de Reconocimiento.

Existen plataformas web gratuitas que permiten realizar esta primera fase como por ejemplo:

<https://mxtoolbox.com/>

<https://centralops.net/co/>



The screenshot displays the MXToolbox website interface. At the top, there's a navigation bar with links for Pricing, Tools, Delivery Center, Monitoring, Products, Support, and a Login button. Below this is a secondary navigation bar with categories like SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. A prominent blue banner reads "ARE YOU CONFIDENT that your email is getting through? FIND OUT WITH DELIVERY CENTER" with a right-pointing arrow. Underneath, the "Network Tools" section is active, showing a grid of 16 tool cards. Each card includes an icon, a tool name, a brief description, and a search input field with a play button and a heart icon. The tools listed are: mx (DNS Lookup for MX records), blacklist (Check IP or host), a (DNS Lookup for IP address), smtp (Test mail server SMTP (25)), ptr (DNS reverse lookup), whois (Domain lookup), dns (Check your DNS Servers), spf (Sender Policy Framework), dkim (Domain Keys Identified Mail), dmarc (DMARC Lookup), aaaa (DNS Lookup for IPv6), srv (DNS Lookup Service Record), dnskey (DNSKEY Lookup), cert (CERT Lookup), loc (DNS Lookup for Location), and ipseckey (IPSECKEY Lookup). The footer contains small text about IP addresses, contact information, and copyright details.

Principios de seguridad en red

Entre otros comandos usados en la fase de reconocimiento se menciona:

NMAP: Es una herramienta de código abierto para exploración de red y auditoría de seguridad mediante el escaneo de puertos a una dirección IP o un dominio.

```
adita - -bash - 76x18
Last login: Tue Aug 23 16:35:26 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
Adrianas-MacBook-Pro:~ adita$ nmap espol.edu.ec
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 00:22 -05
Nmap scan report for espol.edu.ec (192.188.59.149)
Host is up (0.018s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

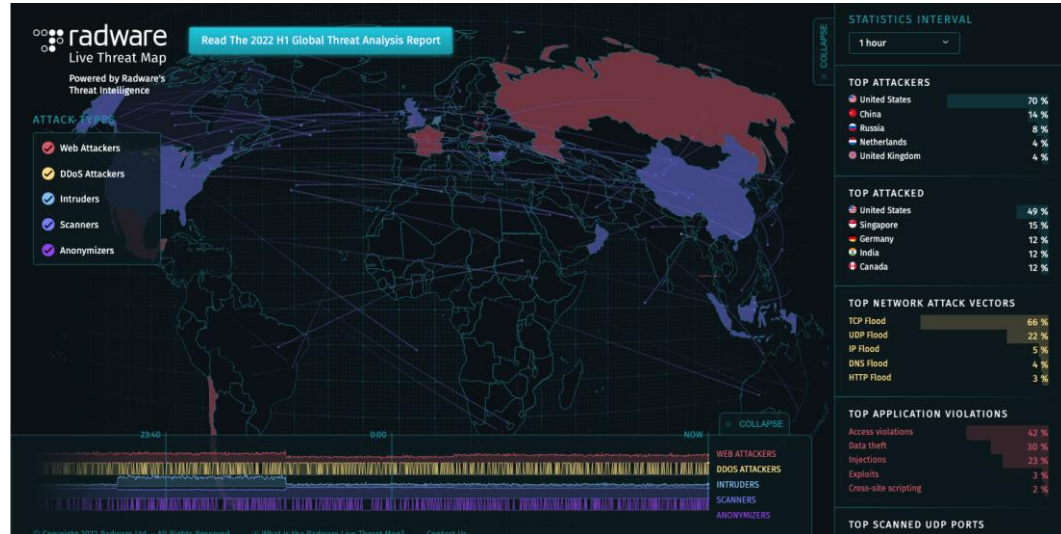
Nmap done: 1 IP address (1 host up) scanned in 42.05 seconds
Adrianas-MacBook-Pro:~ adita$
```



Principios de seguridad en red

Tipos de ciberataques

1. Malware
2. Phishing
3. Man-in-the-middle attack
4. Denial-of-service attack
5. SQL injection
6. Spam



Referencia

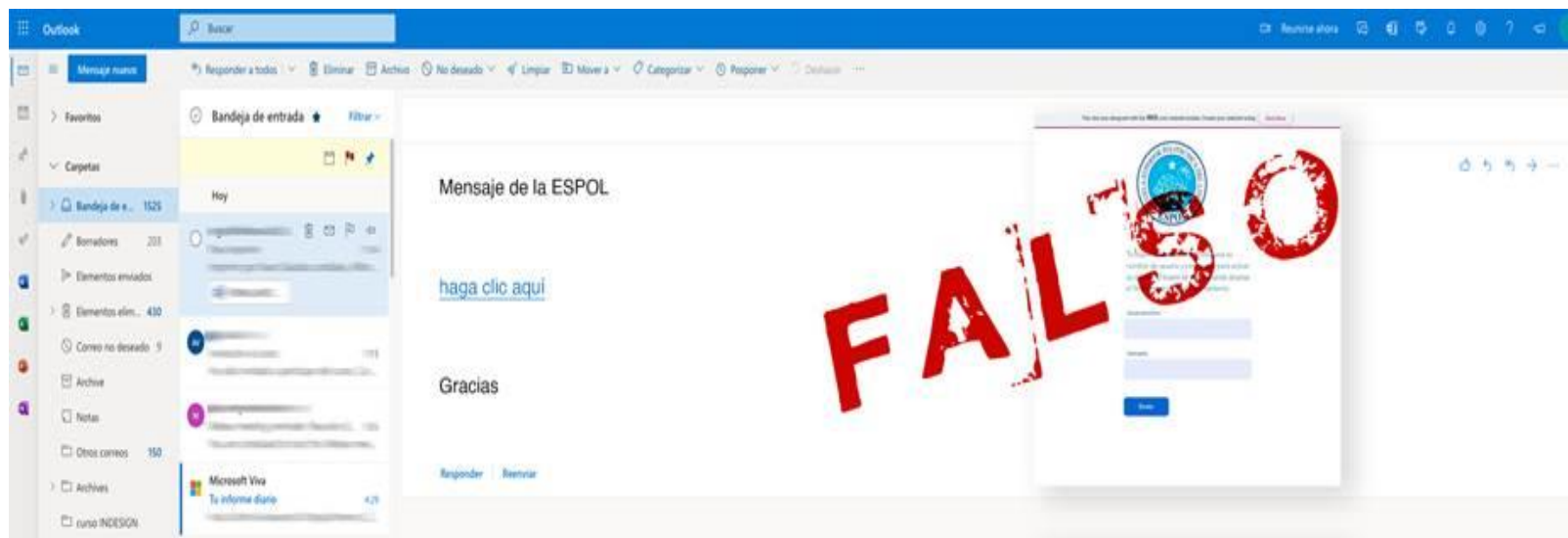
<https://livethreatmap.radware.com/>



Principios de seguridad en red

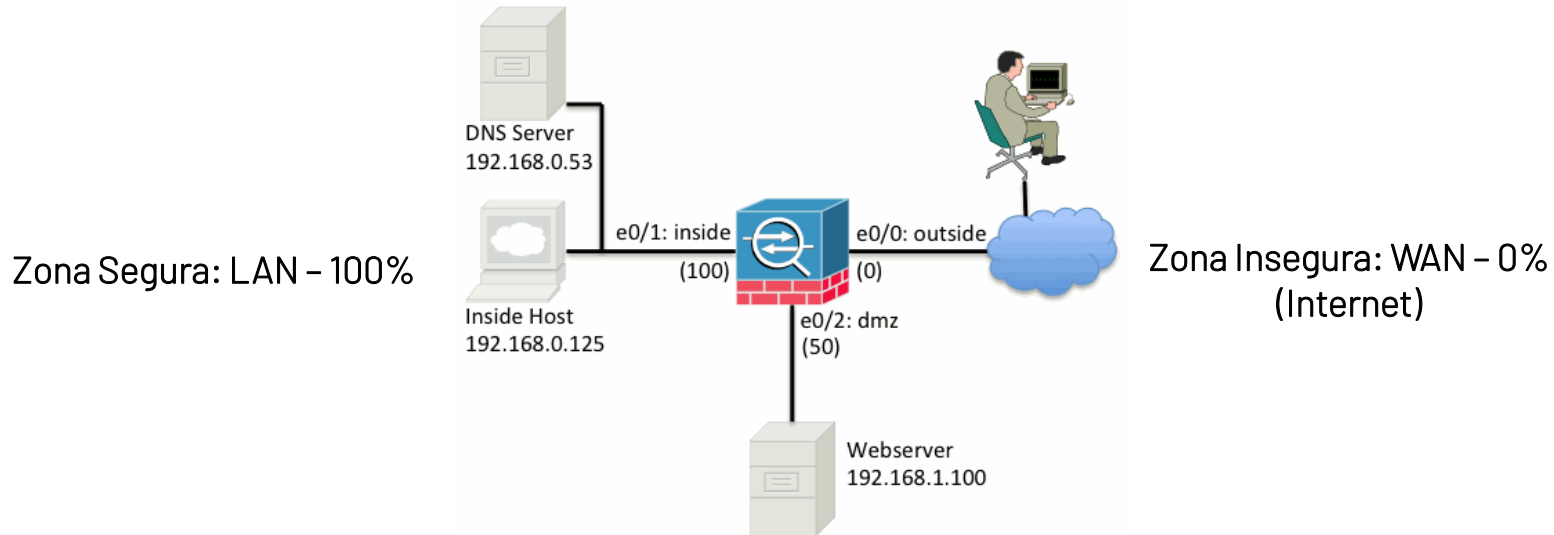
Tipos de ciberataques

Spam



Aseguramiento de sistemas telemáticos

Zonas seguras e inseguras

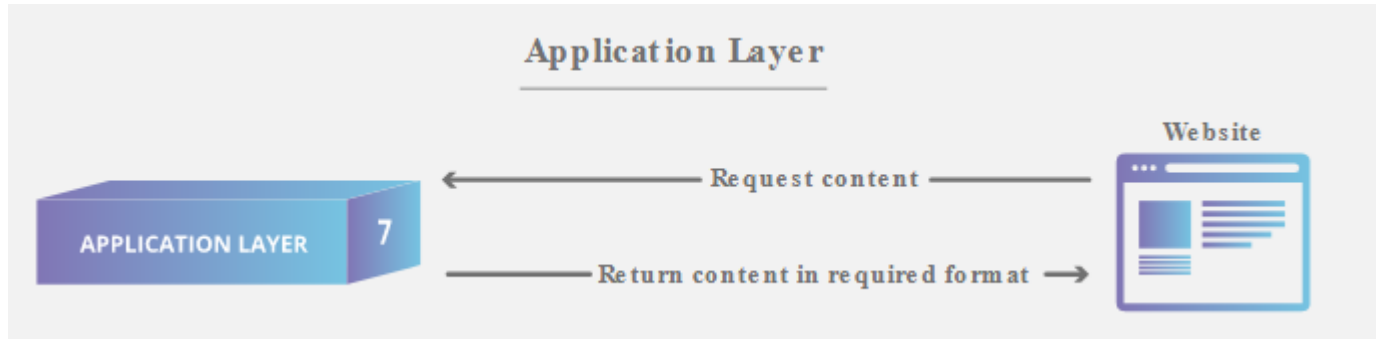


Problemas de Seguridad: Modelo OSI



Los problemas de seguridad en aplicaciones pueden ocurrir desde el hardware, hasta el software o bien los canales de distribución. Es por ello que estos pueden clasificarse según las capas del modelo OSI. Siendo la capa de aplicación la más significativa.

Capa de Aplicación



20

Es la capa más importante para proteger la aplicación. Aunque el resto de capas sean inseguras si controlamos debidamente esta capa podemos generar una aplicación segura.

Los principales problemas de seguridad para una aplicación que no utiliza redes, pueden ser: cifrado de datos para autenticación o autorizaciones. Mientras que para una en red (OSI aplicable) se suman los problemas de comunicación encriptada.

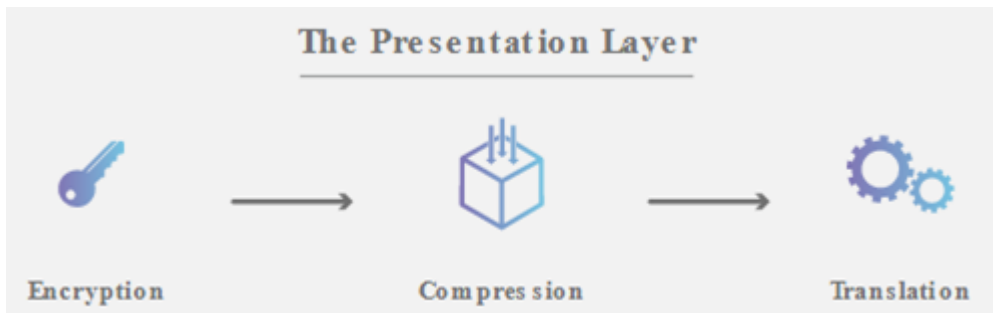


Capas de Presentación y Sesión

SSL (Secured Socket Layer) es la tecnología estándar más popular y con mayor soporte de plataformas. Su propósito es mantener la seguridad de conexiones a internet. Así como también, proteger la información que se transfiere entre dos sistemas, imposibilitando que individuos no autorizados accedan a la data y la lean o alteren.

Se puede entender como los 2 sistemas a un modelo de servidor y un cliente, o a uno de servidor a servidor.

Este protocolo hace uso de algoritmos de cifrado para codificar los datos previo y posterior a su transferencia.



Capas de Transporte y Red



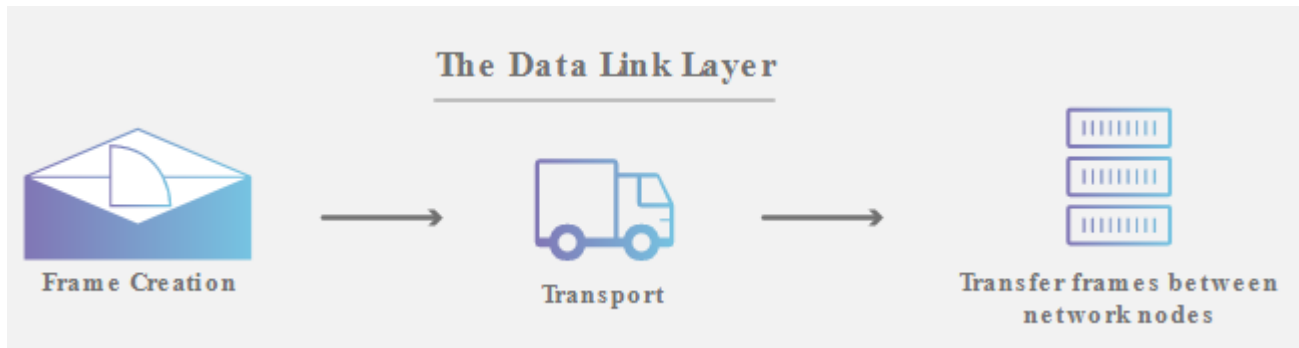
IPSec, acoge respectivamente a los protocolos TCP e IP.

Asegura que los nodos que se comunican no sean maliciosos. Además, proporciona cifrado de bajo nivel y permite hacer un "IP Tunneling".

Se considera importante dentro de la infraestructura porque soporta la aplicación móvil.

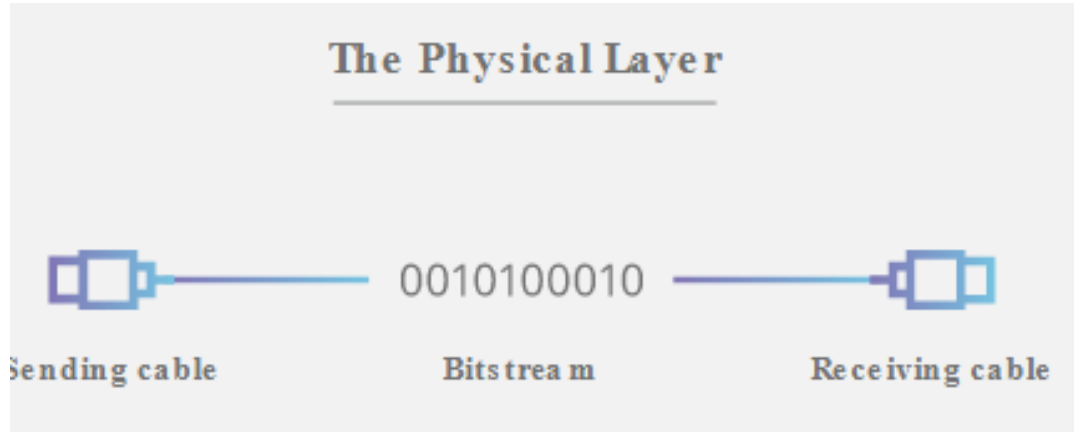


Capa de Enlace de Datos



Alberga las direcciones MAC (Medium Access Control). Violentar esta capa resulta difícil dado que en ella se implementa hardware y es mucho más costoso vulnerar estos sistemas. Sin embargo, no dejan de ser susceptibles a problemas de seguridad. Por lo que, previamente son sometidos a rigurosas pruebas por parte de los proveedores, con la finalidad de garantizar su seguridad.

Capa Física



A diferencia de los sistemas móviles no se encuentran conectados a una red por conexión inalámbrica, sino que son sistemas cableados (fibra óptica, cable coaxial, de par, trenzados), funcionando como canales de comunicación que permiten la transferencia de datos dentro de un medio físico.

La detección de atenuaciones de señal o cambios de fase y otros fenómenos es más sencilla en comparación a una red inalámbrica.

Preocupaciones experimentadas por aplicaciones estacionarias

1. Autenticación segura y autorización de nodos.
2. Comunicaciones seguras entre los nodos autenticados y autorizados de la red a través de una conexión inalámbrica (SSL).
3. Implementación segura de una aplicación.
4. Almacenamiento seguro y recuperación de información.



Preocupaciones experimentadas por aplicaciones estacionarias

5. Asegurar la información recopilada o proporcionada por la infraestructura de la aplicación móvil.
6. Garantizar conversiones de contenido para soportar aplicaciones multimodales.
7. Asegurar la sincronización e intercambio de información entre diferentes canales en un entorno de comunicación multicanal.
8. Defenderse del uso fraudulento del servicio inalámbrico.
9. Resguardar el sistema de ataques de denegación de servicio que pueden interrumpir el servicio los usuarios de la red.



Niveles de amenaza

- Las aplicaciones móviles son un superconjunto de su contraparte estacionaria.
- Problemas de seguridad introducidos por las diversas dimensiones de movilidad y la naturaleza distribuida de las aplicaciones.
- Considerar el estado de seguridad en cada nivel de la aplicación, teniendo en cuenta que serán diferentes. Sin embargo, no debería subestimarse ningún nivel. El punto más crítico del proceso es la recopilación de requisitos.

