**UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA**

**UNAN-León**

****

**FACULTAD DE CIENCIAS Y TECNOLOGÍA**

**DEPARTAMENTO DE COMPUTACIÓN**

**INGENIERÍA EN TELEMÁTICA**

**COMPONENTE:** Seguridad de Redes

**DOCENTE:** Santiago Molina

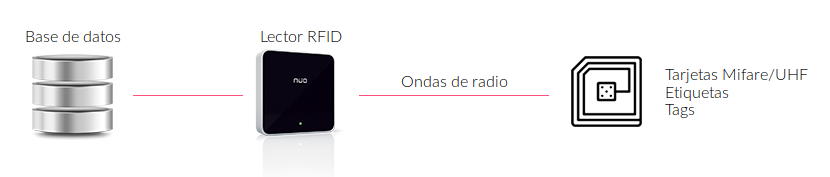
**TEMA:** Investigación.

**FECHA:** 25/06/19

**INTEGRANTE:** Jonathan Eduardo Ochoa Velasquez 15-01898-0

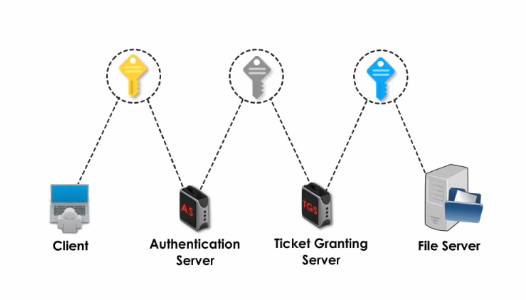
¡A la libertad por la Universidad!

**¿Qué es y como funciona RFID? ¿Cuáles son sus aplicaciones?**

R= RFID (Radio Frequency Identification) es una tecnología que permite identificar mediante radiofrecuencia un objeto, persona, etc. Su arquitectura se basa en un lector RFID, una tarjeta o etiqueta y una base de datos. El lector realiza peticiones por radiofrecuencia a la etiqueta, esta responde con su identificador (que es único), el lector busca ese identificador en la base de datos (el identificador fue almacenado previamente en la base de datos y asociado a un objeto o persona), permitiendo así identificar el objeto o persona en tiempo real.

Las aplicaciones las podemos encontrar principalmente en los supermercados, poniendoles etiquetas a todos los productos para una fácil identificación, para el control de inventarios, movimiento de mercancías, control de vehículos, etc.

**¿Cuál es la arquitectura y funcionamiento de Kerberos?**

****

R= Kerberos es un sistema de autenticación de usuarios. Se basa en una arquitectura cliente servidor, la cual añade una 3ra entidad (Kerberos) que proporciona 2 servicios: el de autenticación (AS, Authentication Service) y el de tickets (TGS, Ticket Granting Service). Kerberos se base es criptografía simétrica, y este tiene las claves privadas de los clientes y de los servidores, los 2 servicios de Kerberos comparten una clave privada. Si un cliente quiere comunicarse con un servidor, primero debe de autenticarse, para realizar la autenticación realiza lo siguiente:

* El cliente envía una solicitud de autenticación cifrado con su clave privada al AS.
* El servicio AS recibe la petición y la descifra con la clave privada del cliente, de esta manera se asegura que el cliente es quien dice ser.
* El AS le envía al cliente un boleto cifrado con la clave compartida por los servidores Kerberos.
* El cliente le envía este boleto al TGS y le indica que quiere establecer una conexión con un servidor, el TGS así se asegura que el cliente es quien dice ser.
* El TGS le envía un token al cliente cifrado con la clave privada del servidor al que el cliente se desea conectar y una clave privada para que el cliente use con el servidor que se desea conectar, esta clave privada es enviada en el token y en otro mensaje cifrado con la clave del cliente.
* El cliente le envía ese token al servidor, el servidor descifra el token con su clave privada, asegurándose que el cliente es quien dice ser, y ya se pueden intercambiar información de forma segura por un periodo de tiempo limitado, que está indicado en el token.

**¿Cómo funciona la autenticación single sign-one?**

R= La autenticación con mensajes se basa en una relación de confianza entre sitios web, el funcionamiento es el siguiente:

* El sitio web primero verifica si ya ha sido autenticado por SSO, de ser así le da acceso al sitio.
* Si no lo has hecho, te envía a SSO para iniciar sesión.
* Te registras.
* SSO pasa los datos de autenticación al sitio web que ingresaste antes de ser redirigido a SSO y te regresa a este sitio.
* Al ingresar a un sitio nuevo (que tiene relación de confianza con SSO), este verifica si ya te has autenticado en SSO y como ya lo has hecho te da acceso al sitio sin necesidad de ingresar tus datos.

**¿Qué es y como funciona el mecanismo de autenticación One Time Password?**

R= OTP (One Time Password) es un mecanismo el cual consiste en la generación automática de contraseñas que solo podrán ser usadas una vez, esto ayuda enormemente a evitar ataques de fuerza bruta y la suplantación de identidades. OTP genera contraseñas automáticamente (valida por un corto periodo de tiempo) para un determinado usuario y esa contraseña es enviada al móvil del usuario vía sms, algunos de los algoritmos usados para la generación automática de contraseñas generan las contraseñas nuevas a partir de las contraseñas anteriores.