

Apuntes Seguridad Informática

Seguridad Física

Perímetro de seguridad

El perímetro de seguridad son las paredes del establecimiento, lo que protege al activo. Son todas las barreras existentes para evitar que el activo sea accedido, contaminado o perjudicado por alguna persona. Dependiendo de la criticidad del activo, es la cantidad de capas de seguridad que se le aplican al activo. Esto se complementa con el control de acceso.

Control de acceso físico

Hay distintos tipos de control de acceso, lectores de rostro, retina, dactilar, etc. Esto se utiliza para validar la identificación de la persona.

Racks

Los rack es donde yo almaceno mi equipamiento. Van a estar configurados según la ubicación del activo. Son como armarios.

Los dispositivos se almacenan por unidades, hay de distintos tamaños. Se almacenan según un orden, así no se pone en riesgo la vida útil de dispositivo además de la disponibilidad del servicio.

Los racks consumen bastante energía, por lo cual se colocan en habitaciones con buena ventilación. Además como generan mucho calor, se necesitan instalaciones especializadas que nos permitan inyectar aire fresco además de poder sacarlo de la habitación.

Estos equipos trabajan en un rango de temperatura para no quemar los equipos ni el servicio brindado.

Los caños amarillos de arriba es por donde viaja la fibra óptica. Los caños de acero de arriba son extractores, sacan el aire caliente de la habitación, se filtra, refrigera y se vuelve a meter a la habitación.

Piso técnico

La instalación de los racks también contempla el piso donde se colocan, esto es para que la corriente y todo el sistema sea colocado de forma segura además de poder permitir una buena refrigeración. El piso técnico es un piso especial el cual yo lo puedo remover fácilmente y por donde viajan los cables de alimentación de los racks, también es por donde se inyecta aire frío a los racks.

Circuitos eléctricos

Debemos de colocar los equipos en habitaciones con una adecuada instalación eléctrica para que la distribución de energía no me cause problemas en la instalación.

Generalmente se ordena por circuitos y se coloca una computadora por circuito, con un margen de crecimiento.

Disyuntor eléctrico y llaves térmicas

Disyuntor eléctrico: Son los que cortan la corriente y hacen que no pasen a través del cuerpo humano. Además protegen la instalación eléctrica del lugar, al ver que puede haber un corto circuito, cortan la corriente, el famoso salto la térmica.

Las llaves térmicas protegen la instalación eléctrica de las sobrecargas. Con una sobrecarga, se pueden quemar los activos. Hay que tener en cuenta también la instalación eléctrica ya que si el cable no soporta cierta capacidad de corriente, también se puede quemar.

Toma a tierra

La toma a tierra protege de al sistema ya que llevan la fuga eléctrica por este cable y hace que no dañe al activo.

También sirven para las descargas atmosféricas, es decir, pararrayos. Estos se encuentran en la parte superiores del edificio y lo que hacen es aumentar la probabilidad de que el rayo caiga ahí y hace que la corriente eléctrica sea conducida a una jabalina el cual esta enterrada para disipar la corriente eléctrica.

Seguridad de equipamiento

Son las contra-medida para poder resguardar nuestro centro de procesamiento de datos, tanto almacenamiento como procesamiento de los datos. Para que esto funcione bien se necesita una buena conexión con los equipos. Para poder garantizar la buena conexión con los equipos, debemos asegurarnos de que la instalación sea coherente y segura, para eso se utiliza un cableado estructurado con distintos niveles de certificación que me permite asegurar la disponibilidad a los equipos, tanto entre equipos como los usuarios al servidor.

En los centros de datos se utilizan tendidos de distintos colores para poder virtualizar los distintos tendidos que hay. Los cables de color azul para transportar cables UTP y cables de color amarillo para transportar fibra óptica.

Garantizar de que los centros de datos tengan una buena conexión no solo se queda en que tenga un buen ancho de banda, sino que también debe de ser seguro y que cumpla con ciertas certificaciones de seguridad para poder garantizar la disponibilidad a los mismos.

Las instalaciones eléctricas también deben de ser seguras. Debemos asegurar que el equipamiento de las instalaciones que va a estar recibiendo energía pertinente mientras procesa datos, reciba dicha energía de forma segura, limpia.

Hablar que sea segura implica que sea:

- Segura para su sobre consumo: En caso de que se produzca un sobre consumo, no se me prenda fuego las instalaciones por algún fallo eléctrico en los

componentes o en los cables, además de que asegurar la seguridad de los operadores de las instalaciones.

- Sea segura para un consumo limpio: La energía eléctrica consumida debe ser limpia, en el sentido de que no hayan alteraciones de voltaje que haga que se reinicie computadoras o se quemen componentes.

Una energía limpia gráficamente es una línea alterna bastante proporcional. Pueden suceder varias situaciones en la transmisión de la corriente:

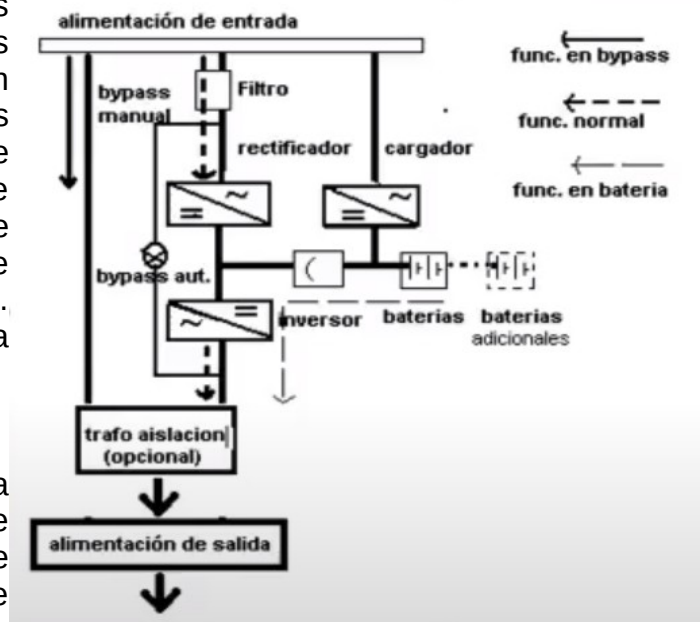
- Ruido Eléctrico: La energía viene con distorsión
- Micro corte: se corta la corriente por micro-segundos. Puede generar la pérdida del estado de la computadora
- Baja de tensión: la tensión que llega al dispositivo no es la mínima para su uso, ejemplo que llegue 190v a algo que necesite 220v.
- Sobretenión: Es un exceso de tensión
- Pico de tensión: Es cuando se recibe de golpe mucha tensión sobre la línea eléctrica provocando fallos en los dispositivos conectados a la corriente eléctrica. Ejemplo cuando cae un rayo a una casa y quema una heladera. En un momento los dispositivos reciben un pico de tensión para el cual no están preparados provocando que se quemen.
- Apagón: Corte de luz imprevisto.



Existen 2 tipos de suministros eléctricos:

- La línea que me da el proveedor de la calle. Si tengo una línea eléctrica propia, le puedo pedir al proveedor que me de 2 líneas eléctricas de 2 centros de distribución distintos
- Proveer energía alternativa limpia y segura. Esto quiere decir que me permite evitar todos los problemas mostrados en el gráfico de la corriente alterna. Para esto se utiliza una unidad proveedora de energía limpia (UPS). Esta compuesta por un

conjunto de baterías de 12v en forma de serie. Esto me sirve para el caso en que el proveedor de energía eléctrica se le haya caído el servicio, pueda proveerle energía desde otro lugar a mi equipamiento, pero para poder asegurar eso, debe ser un sistema ininterrumpido de energía. Su funcionamiento es simple: la corriente eléctrica provista por el proveedor pasa por 2 lados, en uno se filtra todos los ruidos que trae y se la limpia para que vaya directamente al dispositivo conectado a la corriente, por otro lado pasa por las baterías cargándolas en caso de que se corte la corriente. Ambas salidas de corriente desembocan en un inversor de corriente ya que la corriente que utiliza los equipos es alterna y la que viene del proveedor es continua. En caso de que se produzca un corte de corriente, las baterías proveerán de corriente mientras se espera el regreso de la corriente por parte del proveedor. Los equipos nunca se enteraron que hubo un corte de corriente ya que le fue provista por las baterías. Obviamente, su duración depende de la capacidad de las baterías.



Un corte eléctrico es una amenaza, la vulnerabilidad es que el equipamiento necesite de energía para poder funcionar. Si esa amenaza se cumple, mi salvaguarda es la UPS, aunque después de un tiempo se va a quedar sin baterías y volvemos a tener vulnerabilidades. Todo tiene un límite.

Adicional a esto, como contra-medida a la UPS, se puede utilizar grupos electrógenos el cual mejora la autonomía, es decir, garantiza de que haya energía limpia por durante mucho mas tiempo. Aunque depende del combustible del motor del grupo electrógeno. Este trabaja en conjunto con la UPS, cuando se corta la corriente la UPS empieza a trabajar primero ya que el grupo electrógeno tarda mas en conectarse y cambiar la linea(del proveedor a la del grupo electrógeno). Sin UPS, se cortaría la corriente por unos instantes y se podrían quemar equipos o parar el procesamiento de transacciones, etc.

Seguridad del equipamiento

El equipamiento lo alojo en lugares con buena:

- Distribución eléctrica
- Seguridad en el cableado de datos
- Clima controlado
- Extinción de incendio

Clima Controlado

Los equipos cuando superan determinadas temperaturas, por protección, se apagan por lo cual el lugar donde estén ubicados los equipos deben de tener un clima controlado, es decir, el ambiente debe estar libre de polvo, temperatura que ronde entre los 10° y 15°, debe de tener una muy buena contingencia anti incendios, ademas de ser libre de agua o

humedad. Los equipos pueden generar todo ese calor ya que transforman la energía eléctrica, el cual consumen mucho, en calor.

Como contra-medida a la temperatura, lo que se hace es utilizar un sistema de refrigeración que inyecte aire frío por debajo de los equipos y tome el aire caliente que largan por arriba, luego este aire caliente se enfría y se vuelve a hacer el proceso de enfriamiento. Aunque este sistema consume mucha energía, es por ello que los proveedores de datacenter han invertido millones de dólares en otros sistemas como refrigeración por conductos de agua.

Extinción de incendios

Se utilizan sistemas anti incendios el cual detectan de antemano cuando se puede producir un incendio, activando alarmas para indicar que hay potenciales focos de incendios. Esto se produce cuando levantan mucha temperatura los equipos. Como extintores se puede usar agua (aunque puede destruir los equipos) o gases, como el fb 200 que no le hace ningún daño mortal al personal de trabajo, aunque estos gases son muy específicos y tiene un alto precio.

Seguridad y alta disponibilidad en el equipamiento

Cuando se habla de equipamiento de alta disponibilidad se habla de equipamiento que me garanticen disponibilidad y no ponen en riesgos los servicios del servidor. Generalmente son las fuentes de alimentación, conectividad, almacenamiento, etc

El hot swap permite la alta disponibilidad en los discos, me permite cambiar en caliente un disco que se haya roto por otro que este nuevo, esto se puede llevar a cabo ya que generalmente se aplica algún sistema de raid en el almacenamiento haciendo que los datos se escriban en distintos discos físicos, haciendo que si un disco se rompa, yo puedo recuperar la información mediante los datos escritos en un disco backup.

La virtualización

Ya que tener un data-center implica gastar mucho dinero en contra-medidas de disponibilidad, confidencialidad e integridad, la virtualización disminuye los costos de los mismos ya que por un lado no se necesitan todas las contra-medidas de disponibilidad ya que no hay que preocuparse por los equipos y lo que le puede llegar a suceder porque para ello se encarga del proveedor de cloud de la disponibilidad a los equipos virtuales.

Usar cloud trae ciertos beneficios:

- **Disponibilidad:** Al tener varios nodos andando, si se cae uno, otro nodo en caliente puede tomar su lugar.
- **Confidencialidad**
- **Elasticidad:** Me permite flexibilidad en el crecimiento de mi aplicación, a medida que se necesiten mas nodos, yo los puedo agregar en caliente, permitiendo que el servicio crezca sin afectar nada
- **Velocidad de Implementación:** Su velocidad de implementación es mucha mas rápida que la forma tradicional de data-center ya que no necesito instalar ningún hardware o software que me lleve mucho tiempo

- **Ahorro:** Tanto monetariamente como en tiempo. Monetariamente ya que no necesito de comprar toda la infraestructura para poder correr mi servicio, solo pago la demanda de uso de la infraestructura en la nube. Tiempo ya que si algo sucede mal, el tiempo perdido en lanzar maquinas virtuales es mínimo, en cambio si algo sucedía en el data-center, poder arreglarlo me demandaba una mayor cantidad de tiempo

Aunque no todo es perfecto ya que hay que establecer contra-medidas en el acceso controlado a los servicios de las aplicaciones corriendo en las nubes.

En la nube se pueden implementar distintos servicios:

- **SaaS:** Software as a service
- **Paas:** Plataform as a service
- **IaaS:** Infraestructure as a service

Contra-medidas para la cloud

- Perímetro de seguridad
- Control de acceso
- Resguardo de la información
- Encriptacion
- Certificados digitales
- Firmas digitales
- Blockchain
- Token

VPN

Una VPN es un red virtual privada que conecta una o más computadoras de una red privada a través de una red pública como internet, encapsulando un protocolo de red sobre otro generando un túnel bidireccional donde transita la información encriptada. Para ello, los extremos hacen uso de llave publicas y privadas. La clave privada encripta y la clave publica desencripta. Esta ultima es la que yo comparto con el receptor del mensaje así puede desencriptar el mensaje enviado.

Control de acceso

Ética al hacking

Es una persona pagada por la empresa que se dedica a buscar vulnerabilidades en el sistema.

Zona militarizada

Es una red privada en donde los usuario son un ecosistema conocido y controlados, son los usuario que pertenecen a la organización, ademas que cuenta con recursos compartidos, impresoras, servicios, etc. También se la conoce como LAN o red de área privada. Por ejemplo server de aplicaciones, server de correo electrónico corporativo.

Zona desmilitarizada

Es la red publica, es decir, el internet. Es la zona donde tenemos control de acceso pero no sabemos quienes son los usuario que nos están visitando

Métodos de autenticación

Password

Es el primer método de autenticación conocido por todo el mundo, consta de un usuario y contraseña el cual se le puede agregar mas métodos de autenticación para reforzar el control de acceso.

Fortaleza del password

La fortaleza del password esta dada por la cantidad de caracteres utilizados y que tipos de caracteres son utilizados, pueden ser caracteres especiales, minúsculas, mayúsculas y numéricos. Es recomendable no utilizar el nombre del usuario como contraseña. Esto se hace para fortalecer el control de acceso.

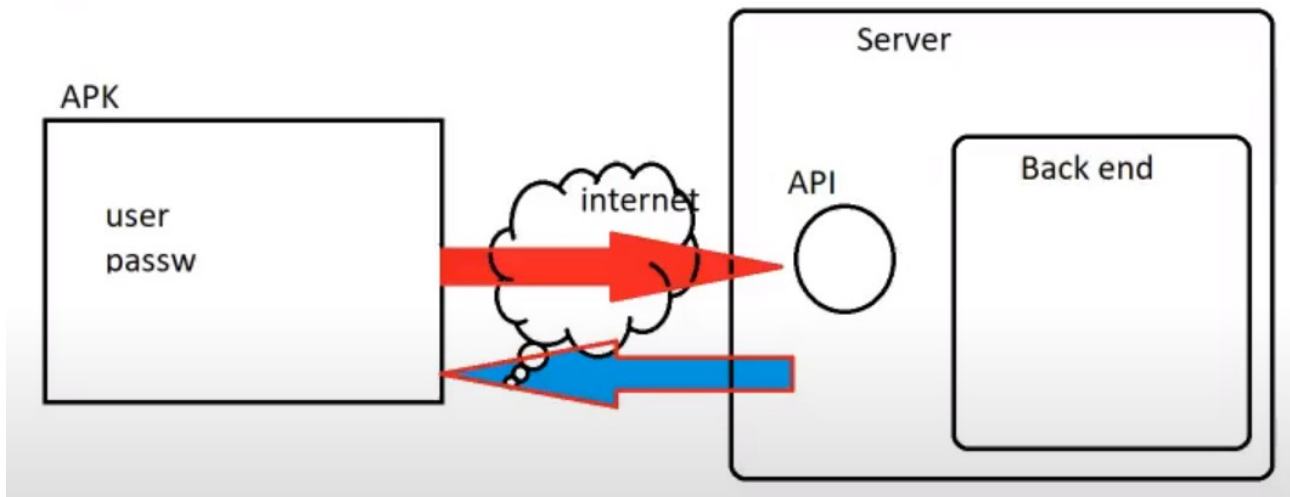
Una vez el usuario ya accede al servicio, las medidas de control de acceso que se toman son preventivas para mantener un control de lo que el usuario hace, es decir, se sigue el comportamiento del usuario

Token

Sirve para el control de acceso, en la autenticación de doble factor, lo que se busca es garantizar la autenticidad de la persona. Generalmente para aplicaciones simples ya con el usuario y la password es suficiente, pero cuando se realizan transacciones mas importantes como bancarias, hace falta de una identificación mas que asegure que quien accede es el usuario propietario de la cuenta. El token es un mensaje o clave que envía, el ente que quiere confirmar tu autenticidad, a un dispositivo o email, etc, el cual sabe que tenes total acceso al mismo. Este token luego es el que se coloca después de colocar el email y la password. Luego de un tiempo el token pierde efectividad para iniciar sesión por lo cual se va a requerir solicitar otro token.

Otra forma de poder controlar el acceso es mediante el uso de herramientas metrificas, de manera que se pueda confirmar la autenticidad del usuario.

También sirve para las **API**. Una API es una interfaz para comunicar aplicaciones. A su vez, estas pueden ser públicas o privadas. En las públicas, cualquier persona puede acceder a ella, en cambio en las privadas, necesitas de una autenticación para acceder a ella. Cuando te autentica por primera vez, el servidor te devuelve un token, este será solicitado si vuelves a ingresar al servidor, si el token no se ha vencido, no te pedirá de nuevo la contraseña al servicio, en cambio sí se venció, deberás autenticarte.



La aplicación funcionaria de la siguiente manera, el apk le manda de forma encriptada el usuario y la contraseña a la API, el cual va a validar la autenticación del mismo en el server, una vez que la validación sea correcta, la API generara el token para el usuario el cual es único para esa persona, ademas de tener un tiempo limite de vida.

Los tokens tienen 3 partes: header, payload y una firma que se genera a través del header y el payload. El payload tiene una verificación de usuario, una fecha de creación del token y una fecha de expiración. Cuando el token expira, se debe de crear uno nuevo para el usuario.

El token generado por la API es mandada a la APK y esta es almacenada luego para mantener la sesión del usuario así no tiene que volver a ingresar el usuario y la contraseña. Luego cualquier acción que haga el cliente contra el server, va a estar acompañada del token para controlar el acceso al server y garantizar la integridad de los datos.

En caso de que quieran atacar a la comunicación, se utiliza un código hash el cual me permite saber después si la comunicación fue intervenida o no



Catpchat

Sirve para asegurarse que la que persona que ingresa no sea un robot.

Control de networking

Dentro de una red privada hay que controlar a donde acceden los usuarios y que acciones realizar en la red. Para ello hay que controlar cuales son las IP de donde provienen los usuarios, para poder identificar la región o lugar donde se encuentra.

Para poder tener un mejor control sobre la red militarizada lo que se utiliza es un firewall. Al momento de lanzar una app, la debería hacer en un server que este en la zona desmilitarizada, así los datos sensibles de la empresa no se ven bajo la amenaza de algún hacker. Aunque los datos de la app deberían estar en una zona militarizada para no sufrir amenazas de hackeo. Esto generalmente se cumple tanto en la cloud como en el mundo físico

Seguridad aplicada en capas

Al sistema se lo considera como una seguridad aplicada en capas ya que esta compuesta por muchos elementos, no solamente software, sino también políticas de privacidad, hardware, buenas practicas, técnicas, etc. Esto me permite generar capas de seguridad e instancias de seguridad que me garantiza cierta disponibilidad frente ataques.

Perímetro de seguridad en la nube

Al momento de lanzar una aplicación a la nube, a usuario que yo desconozco, debo de poder implementar ciertas medidas de seguridad para poder garantizar de que no haya perdida de Integridad, Confidencialidad y Disponibilidad de la información. Basado en eso, se necesita poder identificar las vulnerabilidades y amenazas para poder aplicar las contra-medidas correspondientes.

El perímetro de seguridad en la nube son algunos recursos que nos permiten implementar contra-medidas para poder contrarrestar las amenazas a nuestra información., aplicación, servicio o activo. El activo es el servicio acompañado junto a los datos. Algunos de ellos son:

- Firewall: esto funciona a nivel de red
- WAF (web application firewall): Es un firewall a nivel de aplicación
- Antivirus: Es un perímetro de seguridad a nivel de aplicación
- IDS (Detectores de intrusos): Es un perímetro de seguridad a nivel de aplicación
- Antispam: Es un perímetro de seguridad a nivel de aplicación

En la teoría se dice que no existe perímetro de seguridad en las redes ya que los ataques que se realizan son ataques que tienen que ver directamente con las aplicaciones y no con lo que esta por debajo de la aplicación, teniendo en cuenta la capa OSI, es decir, el enlace, la red, transporte y sesión.

Aun así se aplican distintas contra-medidas para que la red también no se vea amenazada por ningún hacker o usuario

Firewall

Funciona a nivel de red. Es un servidor que funciona como gateway de la red, por el pasa toda la información. que sale y entra a la red privada o militarizada. Recibe la información. del segmento publico, lo descripta, analiza el trafico y luego lo manda al destino que tenia que ir la información.

Un ejemplo de esto es el gateway MSTP(forma parte del protocolo TCP, es el puerto 25) el cual es el gateway utilizado para el servicio de correo electrónico. Recibe todo el trafico MSTP, lo analiza y en caso de no presentar amenazas lo enviá al servicio de correo electrónico.

WAF (web application firewall)

Es un firewall a nivel de aplicación. Son dispositivos que analizan el protocolo de red a nivel aplicación, aunque si la aplicación encripta la información., entonces no lo va a poder analizar. Para evitar esto, hay que ver en que nivel es donde se encripta la información. así no priva al WAF de poder analizar el protocolo de red. Se debería descriptar la información. antes del firewall.

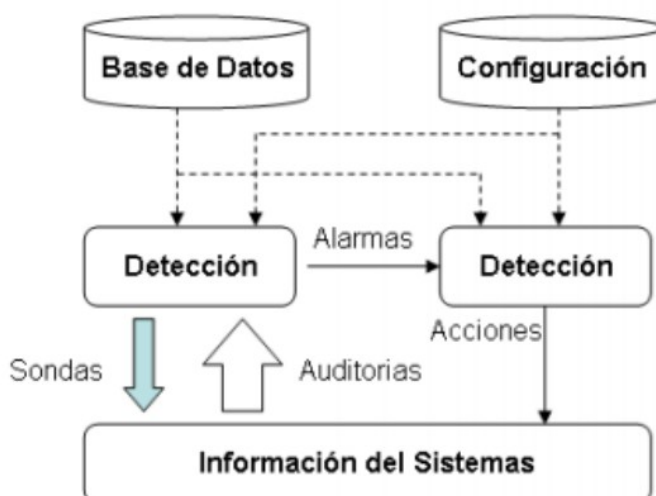
Antivirus

Es un perímetro de seguridad a nivel de aplicación. Tomando el concepto de capas de seguridad, luego de ver que se utiliza un firewall para el acceso de información. a la zona militarizada, por ejemplo el server de correo electrónico., se puede aplicar otra capa mas de seguridad dentro del servidor, en este caso seria dentro del server del correo electrónico., el cual esta capa es el antivirus. Esto me permite generar capas de seguridad e instancias de seguridad que me garantiza cierta disponibilidad frente ataques. Se recomienda no utilizar la misma marca de antivirus en todos los servers para que tengan firmas distintas con la actualización del software

IDS (Detectores de intrusos)

Es un perímetro de seguridad a nivel de aplicación. Es un hardware que se instala dentro de los servicios de red y buscan patrones de conducta dentro de la aplicación, es decir, vigilan el comportamiento de determinados usuarios o trafico de datos que pueden ser dudosos. En muchas situaciones el IDS se refuerza con inteligencia artificial para mejorar la revisión del comportamiento a los usuarios o el trafico de datos.

Es un programa utilizado para analizar la detección de supuestos intrusos en la red o un computador, basado en sensores virtuales, permiten monitorear el tráfico de la red, permitiendo así evitar posibles ataques.



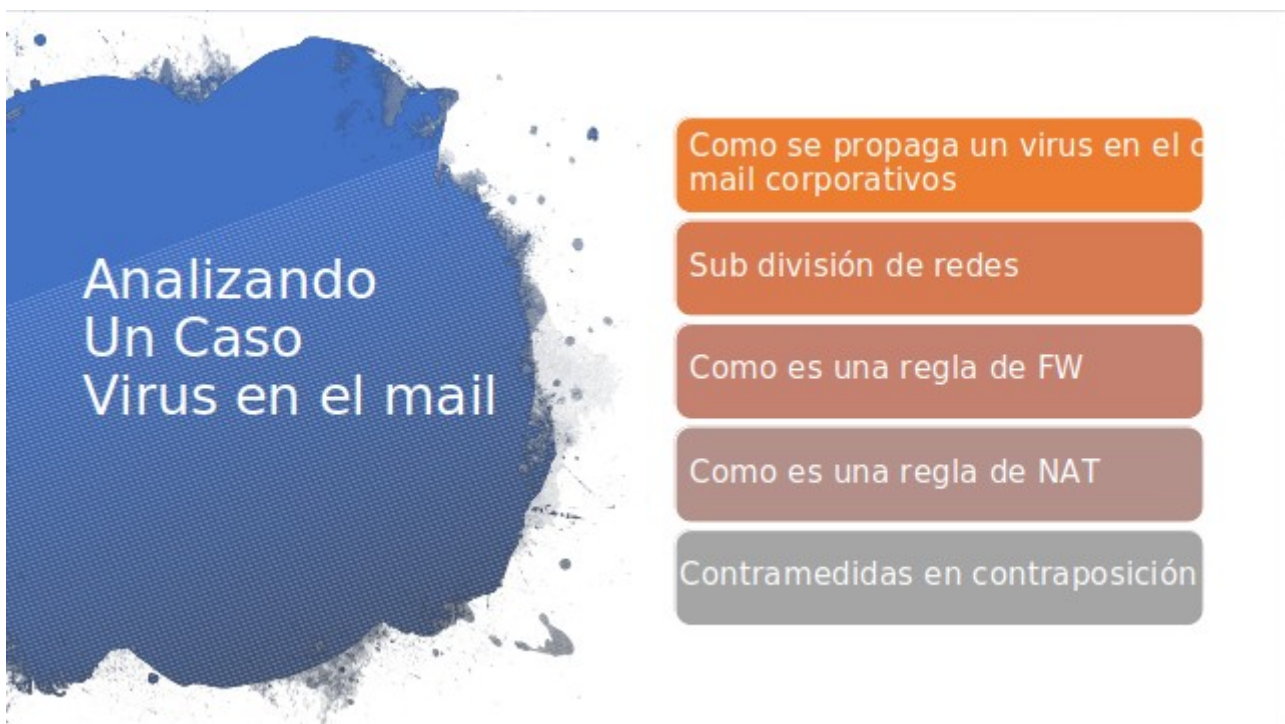
- El IDS, no solo analiza el tráfico de la red, sino su comportamiento y contenido.
- La cual es integrado por lo general a un Firewall. Estos IDS, poseen una base de datos de ataques, con “firmas”.

Tipos de IDS

- HIDS.- IDS basados en Host, estos solo procesan determinadas actividades de los usuarios o computadoras. Ejemplos: Tripwire, SWATCH, LIDS, RealSecure y NetIQ Vigilant.
- NIDS.- IDS basados en Red, realizan sniffing en algún punto de la red, en busca de intrusos. Bien ubicados los NIDS en la red, puede ser una alternativa excelente para la prevención de los intrusos y un bajo impacto en la red al abarcar grandes redes. Ejemplos: SNORT, RealSecure, NFR y el IDS de CISCO.
- DIDS.- Es parte del NIDS, solo que distribuido en varios lugares de la red, con un consolidado en un solo banco de información.
- IDS basados en Log, revisa los archivos de Logs en busca de posibles intrusos, se caracteriza por su precisión y completitud.

Antispam

Es un perímetro de seguridad a nivel de aplicación. Es otra capa de seguridad que se aplica en los servers, por ejemplo de correo electrónico., el cual detecta spam y bloquea luego al usuario que envía esa información. así deja de entrar esa información. al server.



Este es el caso de la propagación de un virus dentro de un correo corporativo, salteando varias barreras de seguridad como el control de acceso y a nivel de aplicación también, además de que el firewall y la regla de nat tampoco lo pudieron impedir.

El virus funcionaba de la siguiente manera:

- Tomaba la maquina del cliente como una maquina anfitriona, transformándola en un servicio de correo electrónico., tomaba los contactos del usuario de su correo electrónico. y le mandaba emails de propagación a toda la cadena de contactos del usuario.
- En pocos minutos la red corporativa se convirtió en un caos
- El virus llego al firewall el cual lo dejo pasar, re transmitiendolo al virus al servidor del correo corporativo.
- El antivirus del servicio del correo electrónico. no estaba actualizado contra esa firma por lo cual no pudo hacer nada y dejo que el servicio de correo electrónico. lo re direccionara al usuario destino.
- El usuario destino abre el email que contenía el virus, el ejecutable embebido que traía el virus se instalo como servicio de correo electrónico. en el computador del usuario, fallando también el perfil del usuario ya que generalmente se le dan perfiles el cual no tienen el poder para poder instalar o eliminar aplicaciones.
- El virus tomo la cadena de contactos del usuario y le empezó a mandar emails a todos, haciendo que, cuando los destinatarios abrieran ese correo, se volvería ejecutar todo el proceso de instalación del virus y propagación del virus

Como contra-medida a esta problemática, se tuvo que desconectar al servidor de correo electrónico. de la red, ya que era este el que recibía y re-transmitía los emails a los usuarios de la red. Si el antivirus hubiera estado actualizado contra esta firma, esto no hubiera sucedido.

Luego de esta experiencia lo que se hizo fue colocar un gateway SMTP en el puerto 25 del firewall que analizaba el protocolo de red y los paquetes que eran mandados al mismo. Si no presentaba ninguna amenaza se mandaba al servidor del correo electrónico. el cual también se le había actualizado el antivirus, el mismo analizaba el paquete que había sido enviado y si no presentaba ninguna amenaza, era re enviado al destino.

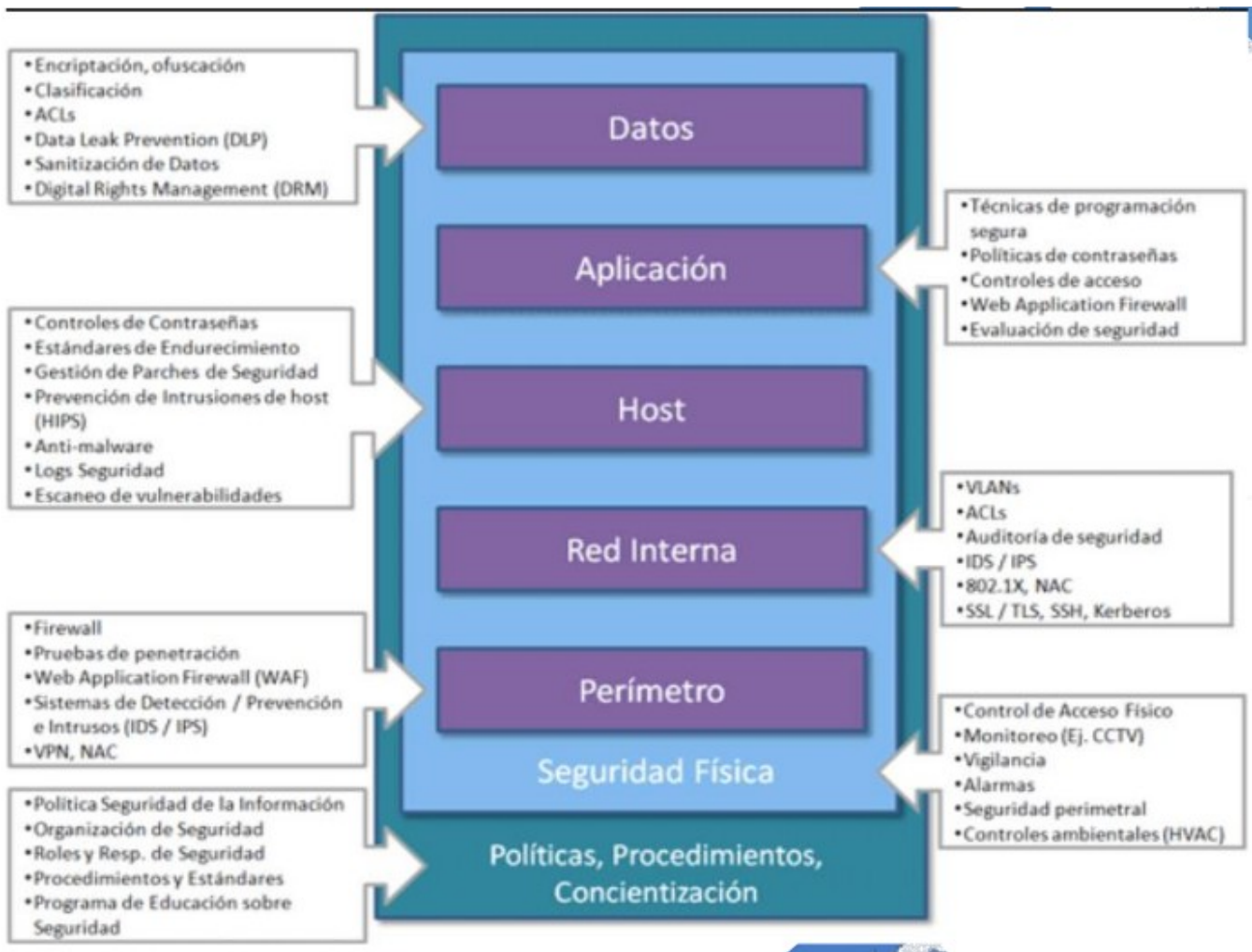
Amenazas a las que nos podemos enfrentar

- Robo de identidad
- Ingeniería social
- Ataques DoS: es un ataque de demanda, lo que se busca es la denegación de servicio ya que el server se encuentra saturado, hacen por lo tanto una perdida de disponibilidad de servicio. Las contra-medidas pueden ser un crecimiento de las instancias de cloud de manera vertical y horizontal.
- Ataques de DNS
- Explotar puertos abiertos
- Virus
- Ransomware: Raptan información. de internet
- Smurf attack: Gran cantidad de solicitudes de eco ICMP a la dirección IP broadcast
- SYN flood: es una forma de [ataque](#) de [denegación de servicio](#) en el que un atacante inicia rápidamente una conexión a un servidor sin finalizar la conexión. El servidor tiene que gastar recursos esperando conexiones a medio abrir, que pueden consumir suficientes recursos para que el sistema no responda al tráfico legítimo. Contra-medida, acortar el tiempo de espera para la conexión.
- Ping flood: consiste en saturar una línea de comunicación con un número excesivo de paquetes ICMP. Esta saturación causará una degradación de los servicios prestados por otros protocolos. El ataque en cuestión utiliza las definiciones de la

longitud máxima de protocolo IP así como la capacidad de fragmentación de los datagramas IP.

- Ping de la muerte: consiste simplemente en crear un [datagrama](#) IP cuyo tamaño total supere el máximo autorizado (65.536 bytes). Cuando un paquete con estas características se envía a un sistema que contiene una pila vulnerable de protocolos TCP/IP, este produce la caída del sistema.
- Escaneos de puertos: ARP Spoofting
 - Ataque de inundación MAC: bombardear el switch con una gran cantidad de solicitudes, cada una de ellas con una dirección MAC falsa, con el objetivo de saturar rápidamente esa tabla. Para eso se limita la cantidad de MAC que puede aprender el puerto, así cuando esta llena la tabla, se descartan aquellas MAC desconocidas. También hay que deshabilitar los puertos que no se usen
 - IP Spoofing: cuyo propósito es transformar la dirección IP correcta de la fuente para que el sistema al que se dirige un paquete no pueda detectar correctamente al remitente. De esta manera el ataque puede ser inadvertido ya que no pueden detectar su IP, además de poder saltar las firmas de seguridad. Contra-medida: Tener una buena configuración de firewall.

Contra-medidas



Configuración de un firewall

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red, entrante y saliente, y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Analizando los protocolos de red y de transporte por donde pasan los paquetes de información. En la configuración nosotros establecemos los puertos TCP/UDP que vamos a habilitar para recibir información. y vamos a establecer las IPs de la red interna a la que pueden ir estos paquetes analizados.

Ademas de establecer un tablero de reglas en donde se define que esta permitido para el envío de paquetes.

Tipos de Firewall

- Firewall proxy: Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red. Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir.
- Firewall de inspección activa: Un firewall de inspección activa, que ahora se considera un firewall “tradicional”, permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Monitorea toda la actividad desde la apertura hasta el cierre de una conexión. Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.
- Firewall de administración unificada de amenazas(UTM): Un dispositivo UTM suele combinar de forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso.
- Firewall de próxima generación (NGFW): Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir lo siguiente:
 - Capacidades de firewall estándar, como la inspección activa
 - Prevención de intrusiones integrada
 - Control y reconocimiento de aplicaciones para ver y bloquear aplicaciones riesgosas
 - Rutas de actualización para incluir futuras fuentes de información
 - Técnicas para afrontar amenazas de seguridad en constante evolución
 - Si bien estas funcionalidades se están convirtiendo cada vez más en el estándar para la mayoría de las empresas, los NGFW pueden hacer más.
- NGFW centrado en amenazas: Estos firewalls incluyen todas las funcionalidades de un NGFW tradicional y también brindan funciones de detección y corrección de amenazas avanzadas. Con un NGFW centrado en las amenazas, puede hacer lo siguiente:
 - Estar al tanto de cuáles son los activos que corren mayor riesgo con reconocimiento del contexto completo

- Reaccionar rápidamente ante los ataques con automatización de seguridad inteligente que establece políticas y fortalece las defensas de forma dinámica
- Detectar mejor la actividad sospechosa o evasiva con correlación de eventos de EndPoints y la red
- Reducir significativamente el tiempo necesario desde la detección hasta la eliminación de la amenaza con seguridad retrospectiva que monitorea continuamente la presencia de actividad y comportamiento sospechosos, incluso después de la inspección inicial
- Facilitar la administración y reducir la complejidad con políticas unificadas que brindan protección en toda la secuencia del ataque
- Firewall de hardware: Este cortafuegos, normalmente, se halla instalado en el router que empleamos para acceder a Internet y, por tanto, sirve para proteger a todos los ordenadores de una red que hagan uso del mismo.
- Firewall de software: Se trata del firewall que viene con el sistema operativo del ordenador y, por tanto, en este caso, tan sólo protege un equipo –y no todos los que integran una red–. Se ocupa de rastrear el tráfico para bloquear aquél que no está autorizado. Un cortafuegos como éste es, por ejemplo, el que se puede instalar desde Windows.
- Firewall de software comercial: Es el que está integrado en las suites de antivirus. Funciona de la misma manera que los anteriores, aunque ofrece mejores niveles de protección y mayores posibilidades de control y configuración.

Reglas de Firewall

Las reglas de Firewall definen qué tipo de tráfico de Internet se permite o bloquea.

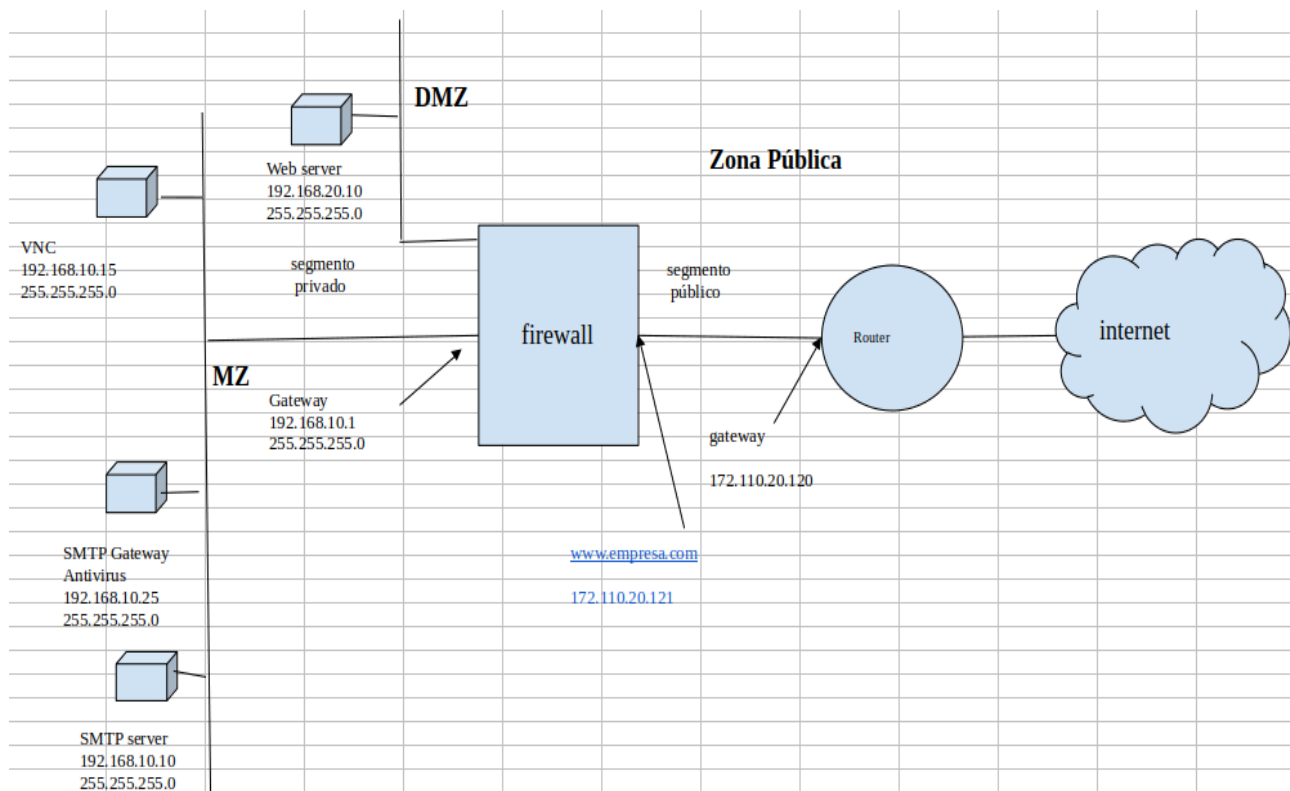
Cada perfil de cortafuegos tiene un conjunto predefinido de reglas de cortafuegos, el cual no puede cambiar. Sólo puede agregar reglas nuevas a algunos de los perfiles. En algunos perfiles no podrá agregar sus propias reglas. También es posible que haya un perfil sin reglas predefinidas que le permita agregar sin restricciones su propio conjunto de reglas. El perfil de cortafuegos seleccionado también afecta la prioridad que reciben sus propias reglas en relación a las reglas predefinidas.

Una regla de cortafuegos se puede aplicar al tráfico procedente de Internet a su equipo (entrante) o desde su equipo a Internet (saliente). Una regla también se puede aplicar a ambas direcciones de forma simultánea.

Una regla de cortafuegos consta de servicios de cortafuegos, que especifican el tipo de tráfico y los puertos que este tipo de tráfico puede utilizar. Por ejemplo, una regla llamada Navegar por Internet tiene un servicio llamado HTTP, que utiliza TCP y el puerto número 80.

Las reglas de cortafuegos también definen si aparecen ventanas emergentes de la alerta de cortafuegos que muestran el tráfico que coincide con las reglas del cortafuegos.

Vamos a tomar como ejemplo esta red y su configuración de firewall.



configuracion de un firewall

estados	interfaces	puertos TCP UDP		IP	
denegar	segmento privado	25	SMTP	192.168.10.1	gateway
permitir	segmento público	80	web	192.168.10.10	server smtp
	segmento DMZ	110	Pop3	192.168.10.15	VNC
	All segmento	21	ftp	192.168.20.10	server web
		5900	VNC	192.168.10.25	smtp Gateway
		1025	SMTP GW	172.11.20.121	
		All ports		All IP	

tablero de configuración de reglas					
IP Origen	segmento Origen	Puerto	segmento destino	IP destino	estado
All IP	segmento público	All ports	All segmento	All IP	denegar
All IP	All segmento	All ports	segmento público	All IP	denegar
All IP	segmento público	80	segmento público	172.11.20.121	permitir
All IP	segmento público	80	segmento DMZ	192.168.20.10	permitir
192.168.20.10	segmento DMZ	80	segmento público	All IP	permitir
All IP	segmento público	1025	segmento privado	192.168.10.25	permitir
192.168.10.10	segmento privado	25	segmento público	All IP	permitir

Configuración de NAT

La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation), es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. La idea es sencilla, hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública.

Regla de nat: Sirve para controlar la navegacion, ya que tenemos una sola IP publica. Son servicios de traslación de servicios. A este le llega el paquete de internet y lo redirecciona a la IP que le corresponde en el destino.

Siguiendo con el ejemplo de la red anterior:

tablero de configuración de NAT					
IP Origen	Puerto Origen	Puerto destino	IP destino	estado	
172.11.20.121	80	80	192.168.20.10	permitir	nat web
172.11.20.121	25	25	192.168.10.10	permitir	nat smtp
172.11.20.121	25	1025	192.168.10.25	permitir	nat smtp GW

Servidor DNS, Verificar que la IP coincidan. Además es donde se publican los dominios o URL. Relaciona el dominio con una dirección IP. La función más importante de los servidores DNS es la traducción (resolución) de los nombres de dominios y nombres de host identificables por los humanos en sus direcciones numéricas del Protocolo de Internet (IP), [192.168.0.1] or 105.125.240.74 correspondientes, el segundo principal espacio de nombres del Internet, que es usado para identificar y localizar a las computadoras y recursos en Internet.

Download de archivos (FTP): FTP es una herramienta muy útil para mover información desde la computadora en la que trabajas al servidor donde se aloja un sitio web. También se usa ocasionalmente para compartir archivos: una persona puede cargar uno en un servidor FTP y luego compartir un enlace con otra persona. Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

SMTP Gateway

El protocolo para transferencia simple de correo (en inglés Simple Mail Transfer Protocol o SMTP) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

Es un servicio de correo electrónico. Lo que hace es analizar firmas a nivel de capa de aplicación, las mismas son comparadas con firmas que se encuentran en la base de datos

de firmas o vulnerabilidades, si se encuentra en el correo electrónico., algún email que contenga una firma comparable con la de la BD, entonces se aisló ya que presenta una amenaza al sistema.

Funcionamiento de SMTP Gateway

Uno de los firewall que se utiliza en las cloud es la comparación de firmas con la BD. En la base de datos de la cloud están las firmas almacenadas, cuando le llega algo de internet para verificar de que no sea malicioso, se compara la firma que tiene con la de la BD, si no coinciden entonces es un ente no malicioso, sino, es malicioso y no deja que el mensaje sea recibido. Este servicio funciona en las últimas 3 capas de la capa OSI. Se compara de un bloque de datos las firmas ya existentes con el nuevo bloque de entrada.

Otra manera de proteger las cloud es con Inteligencia artificial, analizando el comportamiento de los vecinos en la red. Esto se realiza en la capa de aplicación a comparación del análisis de firmas que se produce en la capa de sesión.

Se genera una línea base del comportamiento de los usuarios el cual también tiene una BD donde se almacenarán las distintas líneas de comportamiento. Se analiza el comportamiento de los usuarios y si el comportamiento es muy distinto a la línea base, lo que se hace es a un registro de comportamiento que representan una amenaza. Ahí con Machine Learning lo que se hace es detectar esas amenazas para poder generar firmas. Esto se agrega al bloque de firmas conocidas para próximos bloques de datos de entrada.

Los sistemas de hoy en día utilizan tanto la comparación de firmas como también ML para el análisis de bloque de datos.

Un ejemplo de como funcionaria sería el caso de que un usuario quiera acceder pero coloque 3 veces mal la contraseña, a partir de esto el ML detecta esta actividad y decide realizar una acción de acuerdo a los registros ya detectados en la Base de Datos.

Puerto Gateway SMTP → Meterle un antivirus

Computación de borde: Son todos aquellos dispositivos o aplicaciones que tienen acceso y cercanía con los usuarios que la utilizan, esto es para poder lograr una mayor eficiencia y para enviar una menor cantidad de datos, procesando la información directamente en el borde. A su vez permite analizar los datos de estos dispositivos de bordes. Un dispositivo de borde puede ser un celular.

Esto genera varios desafíos en la seguridad del borde, ya que antes se sentaba en que la seguridad estuviera en los Firewall, pero en este caso el dispositivo o aplicación se encuentra al lado del usuario, haciendo que el firewall sea obsoleto para poder solucionar estos problemas.

Lo primero fue ver la encriptación, con la encriptación yo puedo proteger la integridad, disponibilidad y confidencialidad de los datos que se transfieren durante una transacción. Además se le aplican códigos hash el cual me permiten saber si la información ha sido modificada.

Canal Seguro

Canal que me brinde seguridad a la hora de realizar transacciones, es decir, que no haya pérdida de integridad de los datos cuando se este realizando una transacción. electrónica o se caiga dicha transacción.

Transacción electrónica

Garantizar la identidad tanto del usuario como del extremo que dice ser, ademas que debo asegurar que las transacciones se realicen de manera correcta sin ningún daño en la integridad de los datos

Lo que se debe realizar en una transacción. electrónica es:

1. Autenticación de doble factor
2. Certificaciones digitales: Garantiza que el extremo es quien dice ser. Hay entidades que se encargan de emitir estos certificados como lo es certisur.
3. Firma Digital
4. Blockchain
5. Criptomonedas

Para eso hay que tener en cuenta la integridad, confidencialidad y la disponibilidad

Integridad: Que los datos no se modifiquen y lleguen al destino tal cual salieron del origen. Para esto se utiliza el código Hash. El código hash es un procedimiento que se ejecuta sobre bloques de datos, se saca un código y este código es cual se controla en el otro extremo. En el destino se corre el mismo código hash y si el resultado es el mismo código del origen, entonces no se modificaron los datos. Este algoritmo es distinto a la descriptacion con llaves publicas y privadas

Confidencialidad: Esto se logra mediante la encriptacion, hay 4 métodos. Hay una diferencia en tiempo de procesamiento

1. Encriptacion Asimétrica: El origen tiene una clave de encriptacion y desenscriptacion el cual se aplican sobre un algoritmo que me encripta el dato enviado. Cuando llega al origen, el mismo también tendrá una clave de encriptacion y desenscriptacion el cual se aplican sobre un algoritmo que me desenscripta el dato enviado. Este sistema utiliza una clave publica y otra privada. Para encriptar los datos utilizo la clave publica y privada del origen, ademas de la clave publica del destino. Para desenscriptar los datos del otro lado se utiliza la clave publica y privada del destino, ademas de la clave publica del origen. Una amenaza a esto son las listas de claves publicas falsas que hay en internet. Lo que se hace es encriptar la información. con una clave publica falsa, el cual el hacker tiene la clave privada falsa también, entonce ataca al canal, desenscripta la información. con la clave publica falsa, escribe lo que quiere que vaya en el canal, encripta con las verdaderas claves publica del origen del mensaje, haciendo de cuenta que nada sucedió. Como contra-medida se utiliza certificados digitales. Si una persona que emite un mensaje a un destinatario, usa la llave pública de este último para cifrarlo; una vez cifrado, solo la clave privada del destinatario podrá descifrar el mensaje, ya que es el único que debería conocerla. Por tanto se logra la confidencialidad del

envío del mensaje, es extremadamente difícil que lo descifre alguien salvo el destinatario. Cualquiera, usando la llave pública del destinatario, puede cifrarle mensajes; los que serán descifrados por el destinatario usando su clave privada.

2. Encriptación Simétrica: es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y este lo descifra con la misma clave.
3. Encriptación híbrida: Combina la encriptación simétrica con la asimétrica

Disponibilidad:

Existen cinco necesidades básicas que un sistema debería poder garantizar en una transmisión por Internet:

- Control de acceso: sólo los usuarios autorizados deben poder acceder a las redes de comunicación y a la información contenida en las mismas.
- Confidencialidad: la información transmitida sólo debe poder leerse por aquel o aquellos a quién está dirigida.
- Integridad: la información transmitida debe de ser protegida contra manipulaciones no autorizadas.
- Autenticación: el emisor de la información debe de poder ser identificado.
- No repudio: el emisor debe de ser identificado de tal manera que no pueda negar la autoría de un mensaje o una transacción. Es asegurar que la persona hizo la transacción.

Múltiple factor de autenticación: Algo que se(password) y algo que tengo(Un dispositivo que tengo a mi poder a la cual se le hace llegar un token que se va a utilizar para garantizar tu identidad).

El entorno PKI se basa en tres componentes:

Las claves públicas y privadas de cada usuario

- La base del sistema de certificación PKI son las claves públicas y privadas de cada usuario, que se generan mediante unos algoritmos matemáticos basados en números primos.
- Cada pareja de claves es única.
- Estas claves sirven para cifrar, descifrar, firmar y comprobar la información que se transmite.
- Poseen la propiedad de que "lo que una llave cierra (cifrar) sólo lo puede abrir la otra (descifrar)".

El certificado digital

- El elemento de Software firmado por una CA que determina la identidad del titular del certificado. (contiene registros con el nombre, NIF, etc.).
- Un certificado está asociado a una persona, servidor o empresa.
- Entre otros registros contiene la clave pública del titular del certificado.

Las Autoridades de Certificación. (CA's)

- Son las instituciones encargadas de la emisión, revocación, y administración de los identificadores digitales. Son la tercera parte confiable (TTP) que asegura identidades en Internet.

- Una CA puede a su vez crear Autoridades Certificadoras de Segundo Nivel (CAC's)
- Una CAC proporciona las mismas funciones que una CA, pero en entornos cerrados
- (dentro de una misma empresa o en las relaciones de ésta con terceros).

PKI como solución estándar de seguridad: Utilidades y tipos de certificados

Los Certificados:

- Identifican un usuario, servidor o empresa.
- Permiten el cifrado de las comunicaciones (con las claves).
- Permiten la firma un documento electrónico.

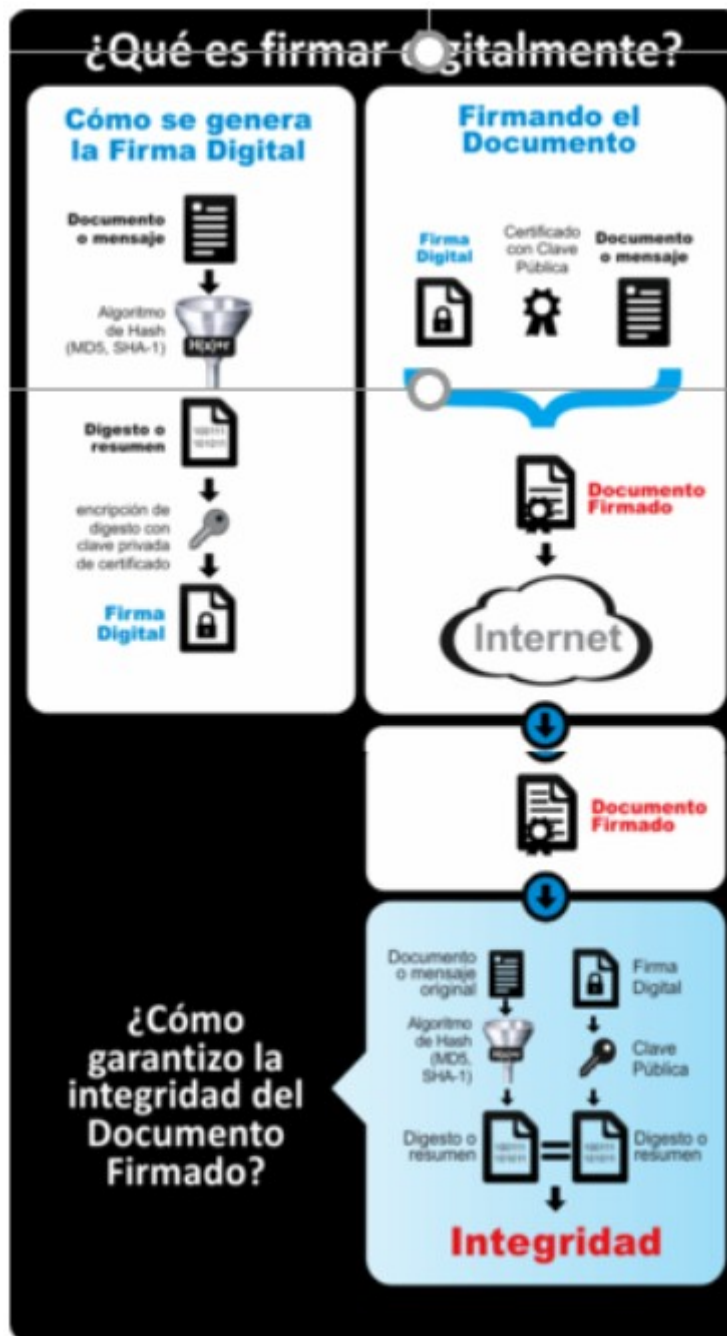
Existen varios tipos de certificados según el protocolo de comunicaciones y la aplicación que se esté utilizando:

- Certificado personal: documento de identificación de un usuario de Internet para navegar, comprar, enviar y recibir correo, firmar documentos electrónicos, etc. de forma segura.
- Certificado de servidor: permite asegurar toda comunicación entre un navegador y un servidor web.
- Certificado para VPNs: permite la comunicación segura, entre las empresas y sus empleados, clientes y proveedores, mediante la creación de redes privadas virtuales en el entorno abierto de internet.
- Certificado Servidor WAP: permite asegurar toda comunicación entre un terminal móvil y un servidor WAP.
- Certificado para firmar código: permite a una empresa firmar su software y distribuirlo de forma segura.

Mecanismo de firma electrónica

La firma electrónica tiene las siguientes etapas:

1. Cuando el emisor crea un documento electrónico también crea, gracias a una aplicación de firma digital, un resumen con sus parámetros clave.
2. Este resumen lo cifra con su clave privada y lo adjunta al documento.
3. Cuando le llega al receptor, éste genera, con la misma aplicación de firma, otro resumen y con la clave pública del emisor descifra el resumen recibido.
4. Si ambos resúmenes son idénticos significa que el documento no ha sido alterado.



Certificados digitales → Es un documento

Un certificado digital o certificado electrónico es un fichero informático firmado electrónicamente por un prestador de servicios de certificación, considerado por otras entidades como una autoridad para este tipo de contenido, que vincula unos datos de verificación de firma a un firmante, de forma que únicamente puede firmar este firmante, y confirma su identidad. Tiene una estructura de datos que contiene información sobre la entidad. El certificado digital permite la firma electrónica de documentos. El receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado y el autor de la firma electrónica no podrá negar la autoría de esta firma.

Un Certificado Digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja.

El titular del certificado debe mantener bajo su poder la clave privada, ya que si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red. En este caso el titular debe revocar el certificado lo antes posible, igual que se anula una tarjeta de crédito sustraída.

La clave pública forma parte de lo que se denomina Certificado Digital en sí, que es un documento digital que contiene la clave pública junto con los datos del titular, todo ello firmado electrónicamente por una Autoridad de Certificación, que es una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos del titular.

Garantiza que el extremo es quien dice ser, además de que garantiza de que un sitio sea seguro. Por ejemplo: TLS o SSL. Estos certificados contienen la clave pública así quien quiera mandarle información, con la clave pública del destino puede encriptar la información. Existen también certificados digitales falsos el cual no son reconocidos por los browsers. Para ser precavidos hay que instruir a las personas para que miren las url y se fijen que se meten a la indicada y no a una falsa. También sirve para el no repudio.

Hay distintas entidades de certificaciones digitales, por ejemplo certisur. Encripto con la llave privada y el certificado trae la llave pública para desencriptar.

Farming: Obligar a que te metas en una url trucha para estafarte.

Phishing: Te piden datos para estafarte

Firma electrónica o digital

Es un comprobante, hecho mediante un algoritmo matemático que lo que genera es un no repudio. Valida además que la persona que se presenta es quien dice ser. Permite firmar documentos y validar dichos documentos. Se usa generalmente en transacciones.

Permite al receptor:

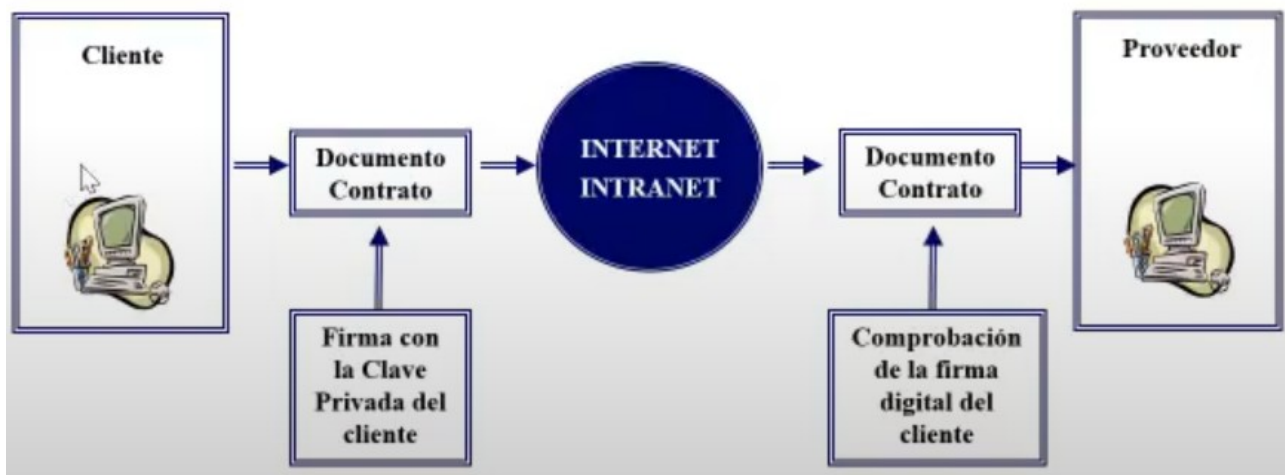
Identificar al firmante de manera inequívoca,

Garantizar la integridad del documento firmado. Es decir, asegurar que el documento es original y no ha sufrido ningún tipo de manipulación o alteración desde su firma.

Con un certificado digital, puedes realizar firmas digitales a través de internet. Sin embargo, no necesitas contar con un certificado digital emitido por una Autoridad de Certificación para poder firmar un documento electrónicamente de forma segura y legal.

Veremos un ejemplo para entenderlo mejor.

En un entorno de comercio electrónico, en que dos entidades quieran llevar a cabo un acuerdo mediante un contrato, pueden utilizar la firma electrónica como mecanismo para autenticar sus identidades.



El sistema funciona de la siguiente manera, el documento/contrato es firmado por el cliente, en esta instancia el cliente firma con la clave privada de él. Se encripta la información y el cliente agrega la clave pública de él, el cual luego cuando llegue al proveedor lo que va a hacer es comprobar esa clave pública y si en verdad funciona para descifrar la información.

Para que esto no sufra de alguna vulnerabilidad, la firma que lleva la clave pública es comprobado con un certificador de firmas para autenticar que la firma es verdadera y no es alguna falsa que hay en internet.

Seguridad en email

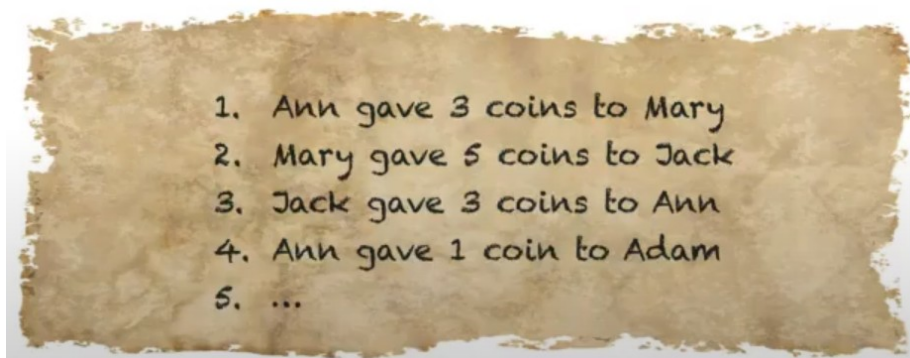
- Cuando se envía un e-mail el programa de correo del emisor lo cifra con la clave pública
- del receptor (que es pública bien porque está en algún registro de la Autoridad de Certificación o bien porque el receptor se la ha enviado en un e-mail anterior).
- Cómo lo que se cifra con esa clave pública del receptor, sólo se puede descifrarse con su clave privada, la comunicación es absolutamente segura (CONFIDENCIALIDAD).
- Además el emisor puede firmar el mensaje y de esa forma asegurar su identidad. (AUTENTICACIÓN).

Blockchain

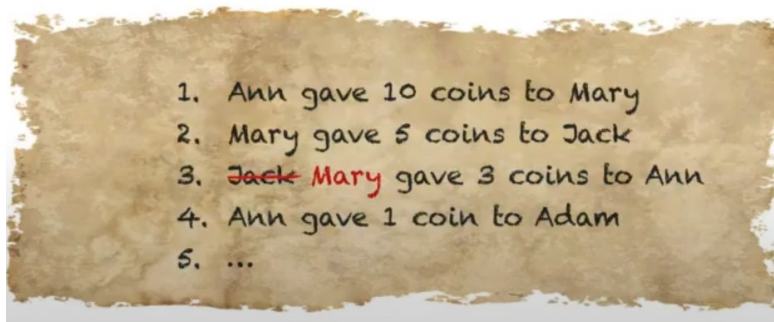
¿Como funciona?

Vamos a ver un ejemplo de 6 amigos que se pasan dinero de forma electrónica, en donde todas las transacciones se registraba los montos que se pasaban.

Deben seguir un flujo de fondos, por lo que una persona llamada BOB decidió llevar una lista con todas las transacciones



Uno de los amigos(Jack) decide modificar a su favor una transacción. Cambiando la identidad de una de las personas, perdiéndose la integridad de la transacción. y de toda la secuencia



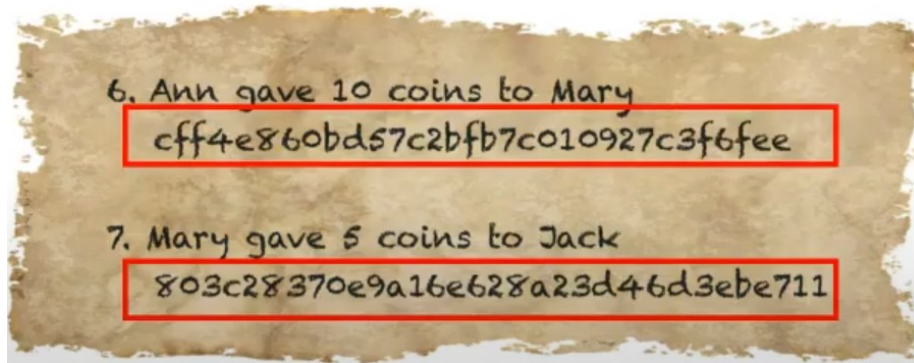
Lo necesario en esta situación es garantizar la integridad de la información, el cual se torna muy difícil cuando se realizan muchas transacciones a la vez y hay que revisarlas a todas por igual. Para ello lo que se hace es correr un código HASH el cual es un código que se implementa para garantizar la integridad de los datos. Lo que hace este código es recibir parámetros de entrada (datos) el cual son procesados por el código devolviéndonos una secuencia única de string, es decir, es una función criptográfica que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija, independientemente de la longitud de los caracteres del bloque de datos. Esta nueva secuencia de string se agrega a la transacción. Esta secuencia siempre tiene el mismo largo pero tienen un orden en particular en consecuencia a los datos de entrada. Por eso es que si se modifica por lo menos un bit, una letra o el largo del string que devolvió como resultado, uno puede saber que la integridad de los datos fue afectada.

Se aplica de la siguiente manera, al comienzo de la transacción. se corre el código HASH sobre los datos de la transacción., generandome este string único. Cuando llega al destino, el mismo corre el código HASH sobre los datos que le han enviado, si las 2 secuencias de string son iguales, entonces la integridad de los datos no fue afectada y esta bien la transacción., pero si no coinciden las secuencia de string del código HASH, entonces fue afectada la integridad de los datos.

Siguiendo con el ejemplo BOB noto que alguien había modificado su listado de transacciones y decidió implementar medidas de seguridad para que esto no sucediera de nuevo. Implemento una contra-medida que garantiza la integridad del listado de transacciones y pensó en una función hash.

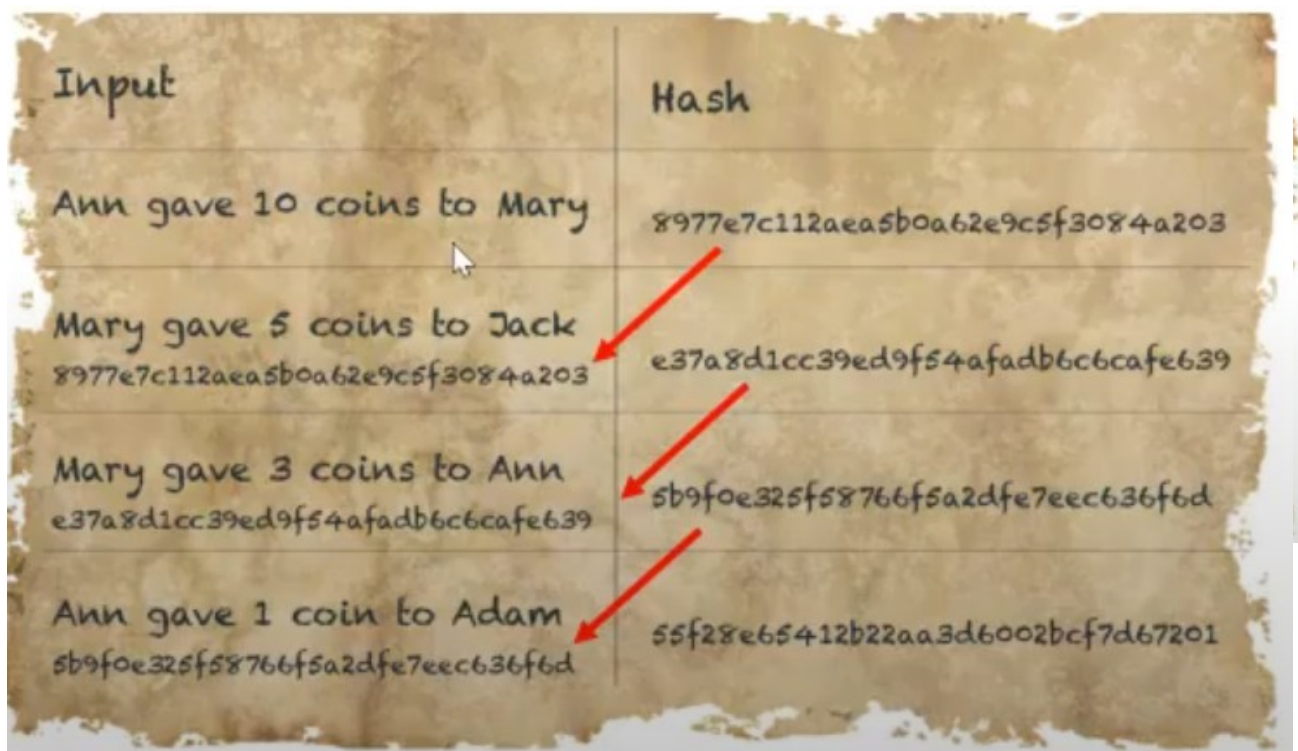
Input	Output (Hash)
Cat	93g56gtf229hbno00r45sktrpbs59so9r3t7saer
A white cat is outside	js03bbstgo94r6s1z8mg05fgt3sba9tob32bsap7
A white cat is inside	bbr19007go2tsi52bsi50o21nmiseas45on23mjn
A whiet cat is inside	339n5sbk249nb9530gjd104h92jg02jg9sm93hpz
A white cat is insid	4bbj390osoh9djm395bksh94gf03sg034dfjh31x

Implemento una función HASH después de cada registro de transacción.



6. Ann gave 10 coins to Mary	cff4e860bd57c2bfb7c010927c3f6fee
7. Mary gave 5 coins to Jack	803c28370e9a16e628a23d46d3ebe711

Jack con el interés de beneficiarse, nuevamente altera una transacción. a su favor y genero un nuevo código hash. Esto lo hace ya que al modificar la transacción. la función hash que se aplica sobre el bloque de datos me devuelve una nueva secuencia de strings el cual agrega a la transacción., cumpliendo con el requisito de que la secuencia de string lleve el código hash aunque este sea falso, aun sigue corrompiendo la integridad de la transacción.



Input	Hash
Ann gave 10 coins to Mary	8977e7c112aea5b0a62e9c5f3084a203
Mary gave 5 coins to Jack 8977e7c112aea5b0a62e9c5f3084a203	e37a8d1cc39ed9f54afadb6c6cafe639
Mary gave 3 coins to Ann e37a8d1cc39ed9f54afadb6c6cafe639	5b9foe325f58766f5a2dfe7eec636f6d
Ann gave 1 coin to Adam 5b9foe325f58766f5a2dfe7eec636f6d	55f28e65412b22aa3d6002bcf7d67201

BOB nuevamente detecto que alguien había alterado el registro y con la intención de garantizar confianza sobre la moneda que se había gestado, implemento nuevas contra-medidas. Agrego un código hash después de cada registro. Este se genera a partir del registro de transacción. mas el ultimo código hash generado.

De esta manera se mejora la integridad de los datos ya que si se quiere modificar un código hash, ya que alteraste alguna transacción., se debe modificar el nuevo código hash que me da como resulta la transaccion(Lado derecho del cuadro) como también se debe modificar el registro de transacciones para atrás, haciendo de esta manera que coincida al final el código hash(lado derecho del cuadro) aplicado a la transacción.(lado izquierdo) mas el resultado del código hash de la transacción. anterior. Esto mejora la integridad de los datos aunque para vulnerabilizarla llevara de mucho tiempo ya que hay que modificar todo el registro de transacciones para no dejar huellas de las alteraciones realizadas.

Jack muy interesado en seguir intentando de hacerse de mas dinero, se propuso tomarse el trabajo de modificar todos los hash. Como respuesta Bob decidió agregar un numero después de cada registro(NONCE).

El Nonce debe elegirse de modo que el hash generado termine en 2 o mas ceros. Mientras mayor es la cantidad de ceros al final de la secuencia, mayo es la seguridad de los datos ya que hay que hacer una mayor cantidad de cuentas para poder llegar al resultado de la secuencia del hash.

Ahora, para falsificar registros, Jack tendría que pasar horas y horas eligiendo Nonce para cada linea. Mas importante aun, no solo las personas, sino que las computadoras no pueden descifrar el Nonce rápidamente.

Input	Hash
Ann gave 10 coins to Mary <u>451</u>	219711e62645a21f2742ada2c6f2a900
Mary gave 5 coins to Jack <u>13</u> 219711e62645a21f2742ada2c6f2a900	1cc4c07fa0757848b439e2361ce87d00
Mary gave 3 coins to Ann <u>467</u> 1cc4c07fa0757848b439e2361ce87d00	e43a132f4b67c65ba6914824a39b3900
Ann gave 1 coin to Adam <u>56</u> e43a132f4b67c65ba6914824a39b3900	99012fe16897c19465941d5350afa900

Bob con intención de dar un limite a la cantidad de transacciones decidió limitar las transacciones definiendo una longitud del bloque. En este caso la longitud del bloque seria de 5000 transacciones y a eso llamo bloque de transacciones, estando relacionado el bloque con la cantidad de transacciones que soporta este bloque.

Ademas para dar mayo seguridad(disponibilidad, integridad y confidencialidad) implemento otra contra-medida. Implemento copias del bloque en 5000 computadoras del mundo. A cada computadora se le llama nodo. Cuando se completan las 5000 transacciones se genera un nuevo bloque.

Para que una transacción. entre en un bloque esta debe ser validada por el 51% de los nodos. Acá se genera la famosa minería de datos, donde se están realizando muchas transacciones el cual deben de ser aprobadas por una cantidad mínima de nodos. Es muy importante el orden en que entra la transacción. al bloque. Una secuencia de bloques se les llama **BLOCKCHAIN**. Es una estructura de datos cuya información se agrupa en conjuntos (bloques) a los que se les añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal. Si una transacción. se vio modificada entonces no va a ser aprobada por el 51% de los nodos y no va a formar parte del bloque de transacciones.

De acá surgen 2 conceptos nuevos: Billetera y firma digital

Las firmas digitales garantizan la identidad digital de las personas.

Las billeteras son una clave publica. Cuando yo quiero realizar una transacción., le comparto mi llave publica para que encripte los datos de la transacción. y la única manera de desencriptar esa información es con la llave privada que tiene el dueño de esa transacción.

El código hash también se utiliza para antivirus. Se toma un rastro del virus y se genera un hash del virus que se guarda en la base de datos de firmas de virus. Lo que se hace después es comparar los códigos hash del virus y si coinciden entonces es una amenaza, sino coinciden entonces no es un virus, hasta cierto punto. Así yo no comparo toda la firma, sino solamente el código hash de la firma. El firmware WAP también hacen uso de esto.

También se usa para la autenticación. Los usuarios en una BD se almacenan encriptados así no corre riesgo esta información que es tan critica. Luego cuando se crea una nueva contraseña, se corre alguna función hash sobre el usuario y la password para generar el código hash que se va a aguardar en la base de datos. Con esto yo protejo el control de acceso y la integridad de ese bloque de información que se esta guardando. Aunque una vulnerabilidad de esto es si realizan un proceso inverso de hash para obtener los datos del usuario, es decir, si se conoce el algoritmo de hash que se usa para hacer el código hash, también lo podrían usar de forma inversa para obtener los datos del usuario.

Otro sector que se utiliza es para las comunicaciones, generalmente cuando encriptamos. Lo que se quiere proteger es la disponibilidad y la integridad de la comunicación, es decir, se corre una función hash antes de encriptar la info y después de encriptarla, se compara los resultados y si dan los mismos resultados entonces no hubo ningún problema en la comunicación, pero en el caso de que no coincidan los códigos hash, la integridad de los datos se vera afectada ademas de la disponibilidad ya que los datos que tengo no me sirven para poder realzar una conexión exitosa.

Otras funcionalidades que tiene son el sha1, sha2 y MD5.

Normativas internacionales

Están hechas por organismos internacionales de organización con el fin de que las empresas lo incorporen para poder generar una especie de compatibilidad entre organizaciones. Por ejemplo que una empresa debe prestarle servicios de transacciones comerciales a otra empresa por lo cual la empresa proveedora de este servicio va a tener que asegurar que cumple con las normativas PCI para garantizar la integridad de las transacciones. Esta norma se enfoca en todo el proceso de la transacción., autenticación del usuario, encriptación y desencriptación de datos, etc.

Estas normativas son recomendaciones de las ISO 17799 y 27001 que nos ayudan a poder organizar e implementar nuestras aplicaciones o organización.

SOC es otra normativa el cual esta enfocada al procesamiento y análisis de sistemas. Otra normativa mas es la SLA el cual trata de la disponibilidad de los servicios.

Hay que tener en cuenta estas normativas ya que a la hora de largar nuestra aplicación, la disponibilidad de la misma no debe verse afectada por el cumplimiento de las normas.

Lo interesante de esto es que si yo uso instancias de proveedores de cloud que ya cumplan con estas normativas, yo me debo de despreocupar por tratar de que mi aplicación lo cumpla ya que con el solo hecho de usar estas instancias que si cumplen con las normas, mi aplicación también va a cumplirlas.

Aunque también hay que tener en cuenta los costos que esto implica ya que usar instancias por ejemplo de Amazon, el precio de la instancia depende de la usabilidad que este tenga. En la cloud se puede crecer de 2 maneras, verticalmente, al mismo nodo le agrego mas procesadores, mas almacenamiento y mas RAM, aunque este crecimiento tiene un limite, se puede crecer hasta lo máximo que soporte el nodo. El otro crecimiento es el horizontal en donde yo agrego mas nodos a mi aplicación. Para hacer uso de estos nodos, se agrega un balanceador de carga que se encarga de hacer una distribución de todos los requerimientos que van a la nube a los distintos servidores. El balanceador de carga se puede configurar de tal manera que si se supera el máximo de usuarios en el nodo, me largue una nueva instancia para que estos nuevos usuarios puedan acceder a la aplicación.

¿Que significa tener un certificado de seguridad ISO 27001?

Significa que tengo un sistema de seguridad gestionado, de decir, esta regido por un análisis de riesgo que es base sobre el cual se va a implementar un sistema de seguridad, y a partir de aquí, se implementa una gestión de riesgo que esta asociado a las vulnerabilidades que surgieron del análisis, las amenazas asociadas a esas vulnerabilidades y a las contra-medidas implementadas para reducir esas vulnerabilidades. Este certificado debe ser emitido por alguna empresa de autenticación. o certificación.

Este certificado puede ser un requerimiento de una matriz de requerimiento que utilizan las empresas y le exigen a quienes le ofrezcan algún servicio con el fin de asegurarse que hay un lineamiento de las políticas de seguridad que ellos aplican en la empresa y que el proveedor de servicios cumpla con ellos para poder trabajar con la empresa.