Nicolas Alvarado 201630444

Parte A

1.

MD5: Sigue siendo usado, principalmente para confirmar la integridad de un archivo. Ya no se usa en muchos campos ya que no es muy seguro.

SHA-2 (256, 384, 512): Se siguen usando en varios campos. Se usan en múltiples protocolos como TSL, SSH entre otros, también es usado en los sistemas unix para el hasheo de las contraseñas. Las cripto monedas también usan este algoritmo para funcionar.

2.

MD5:

Longitud 1: 35 ms

Longitud 2: 67 ms

Longitud 3: 325ms

Longitud 4: 2s y 508ms

Longitud 5: 30s y 846ms

Longitud 6: 12min, 21s y 722ms

Longitud 7: 12min, 32s y 99ms

SHA-256

Longitud 1: 4 ms

Longitud 2: 37 ms

Longitud 3: 480ms

Longitud 4: 2s y 513ms

Longitud 5: 33s y 346ms

Longitud 6: 14min, 17s y 6ms

Longitud 7: 13min, 54s y 179ms

SHA-384:

Longitud 1: 46 ms

Longitud 2: 43 ms

Longitud 3: 460ms

Longitud 4: 2s y 591ms

Longitud 5: 45s y 822ms

Longitud 6: 17min, 49s y 250ms

Longitud 7: 18min, 43s y 70ms

SHA-512

Longitud 1: 5 ms

Longitud 2: 109 ms

Longitud 3: 311ms

Longitud 4: 3s y 15ms

Longitud 5: 46s y 440ms

Longitud 6: 18min, 57s y 164ms

Longitud 7: 18min, 18s y 583ms

Nota 1: El orden en que nuestro algoritmo busca las cadenas es el siguiente:

a, aa, aaa, aaaa, aaaaa, aaaaaa, aaaaaaa, aaaaaab, aaaaaac, etc.

Por lo que el tamaño de la entrada no esta relacionado con el tiempo en que se demora. Por esto las entradas que escogimos para las pruebas son:

aaaaaaz (Longitud 1)

aaaaazz (Longitud 2)

etc.

Nota 2: La diferencia entre las cadenas de longitud 6 y lonngitud 7 es mininma. Esto se debe a que usamos threads (uno para cada letra). Esto resulta en que la primara letra no afecta mucho el resultado final en estos casos (Longitud 6 y 7).

Parte B

1.

Datos que debes ser protegidos:

-Toda la información de los clientes.

-Toda la información que intercambian las unidades de distribución con los servidores.

Esto porque esta es la información que viaja por internet, el resto de información viaja dentro de la oficina que esta protegida por un firewall y los computadores dentro de esta tienen antivirus.

2.

Para la información de los clientes y para la información de las unidades de distribución se necesita confidencialidad, integridad, autenticación y no-repudio.

Para los clientes:

Se necesita confidencialidad porque cuando se conectan con el servidor mandan información privada y sensible como su usuario y contraseña. De ser robados estos datos, alguien podría hacer pedidos a nombre de otra persona.

Se necesita integridad para asegurar que el pedido que le llego a la empresa es el pedido que hace el cliente. Si esto no se cumple alguien podría hacer un ataque de MITM y enviar un pedido distinto.

Se necesita autenticación para asegurar que quien hace un pedido es quien dice ser y no otra persona. Si esto no se cumple cualquiera podría hacer pedidos a nombre de otra persona.

Finalmente se necesita no-repudio para que un cliente no pueda negar que hizo un pedido que si hizo. Si esto no se cumple un cliente podría hacer pedidos y después negar que los hizo, lo cual seria una perdida de tiempo y recursos para la empresa.

Para las unidades de distribución:

Se necesita confidencialidad porque estas unidades intercambian información privada con los servidores, como los pedidos que van a entregar y las rutas que van a usar. Si alguien obtiene esta información podría saber que clientes hacen que pedidos lo cual es información privada de cada cliente.

Se necesita integridad para estar seguros de que la información que le manda el servidor a la unidad y viceversa sea correcta. De lo contrario puede llegar la ruta equivocada o la posición de la unidad errada.

Se necesita autenticación para asegurar que quien manda la posición es la unidad y no otra persona. Si esto no se cumple alguien podría mandar que ya se entrego un pedido cuando en realidad no se entrego este.

Finalmente se necesita no-repudio para que una unidad no pueda negar que tenia un pedido que entregar, o negar que entrego un pedido.

3.

La comunicación entre las unidades de distribución y la plataforma de integración no están encriptadas, por lo que cualquiera podría interceptarlas y leerlas sin mucho esfuerzo. Esto es espionaje.

Un tercero podría crear una antena de celular falsa para capturar los paquetes mandados por las unidades y editarlos, esto seria adulteración.

Las unidades de distribución no se autentican con la plataforma de integración eso significa que cualquiera podría replicar un dispositivo como el que llevan las unidades y crear reportes falsos. Esto constituye suplantación.

Finalmente la plataforma de integración no tiene ninguna protección contra un ataque de denegación de servicios, este ataque seria letal ya que dejaría sin funcionar a todo el sistema.