Proyecto TEL-252

“Seguridad en sensores con firmas digitales mediante curvas elípticas”

Integrantes: Ignacio Barrera
ignacio.barrerag@usm.cl

Felipe Marquez
felipe.marquez@sansano.usm.cl

Carlos Arredondo
carlos.arredondoc@usm.cl

Vicente Tejos
vicente.tejos@usm.cl

Profesora: Berioska Contreras
Ayudante: Valentina Espinoza

Grupo: Los elípticos

Índice

Resumen	2
Introducción	2
Método	3
Resultados	3
Análisis	4
Conclusión	4
Retroalimentación a “Los mensajeros elípticos”	5
Trabajos a futuro	5
Referencias	6

Resumen

A través de ECDSA (Elliptic Curve Digital Signature Algorithm) se implementará una forma de asegurar la integridad de los datos enviados por el cliente (sensor de temperatura) hacia el servidor, para este fin simularemos los sensores con scripts en Python que serán enviados a la nube. Estos cumplirán la función de enviar la información a través de la red de redes. Por otro lado, se tendrá un servidor que cumplirá con el rol de almacenar estos datos y simular el centro meteorológico.

Introducción

Bajo la problemática de un centro meteorológico el cual está teniendo comportamientos erráticos en los valores recibidos desde sus sensores, se decide investigar posibles causas de este fenómeno, llegando a la conclusión que el problema no es de los sensores, indicando que el problema es el envío de datos, por lo que se busca un algoritmo el cual asegura la seguridad de los datos enviados. Así también dando la certeza de la integridad de los datos y asegurando su transmisión en la red.

Método

Se implementa un servidor en la nube el cual actuará como el centro meteorológico, recibiendo los datos enviados por los sensores, los cuales tendrán como datos el id, temperatura y certificado, esta arquitectura del servidor es realizada con Fast API y jinja2 para el template que se muestra a través de la página. En la parte del cliente se utiliza request para generar las peticiones Post hacia el servicio meteorológico (simulado).

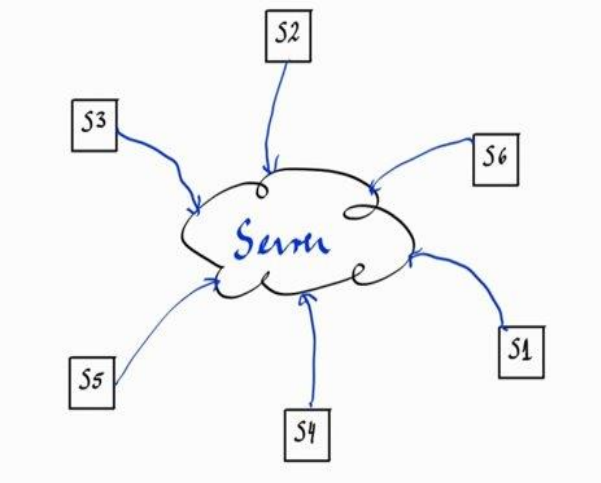

Figura 1. Arquitectura Clientes-Servidor

Se utiliza la biblioteca ECDSA, para la generación de la firma digital, asegurando el no repudio y la integridad de los datos enviados por los sensores, validarlos en el servidor y si estos no son válidos el servidor los rechazara por integridad.

Resultados

Se lograron todos los objetivos propuestos, todo el ambiente es funcional y la firma digital funciona de manera correcta y se rechazan las solicitudes de usuarios no identificados en el sistema que no cumple con la verificación de firma a través de la curva elíptica (ECDSA).

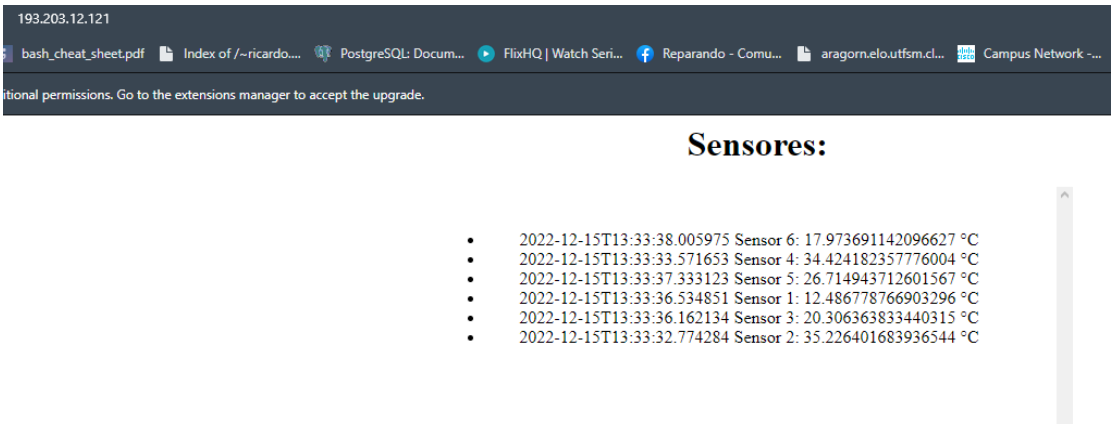

Figura 2. Centro meteorológico que recibe las temperaturas de los sensores

Análisis

En nuestro caso bob sería un sensor y alice sería el servidor

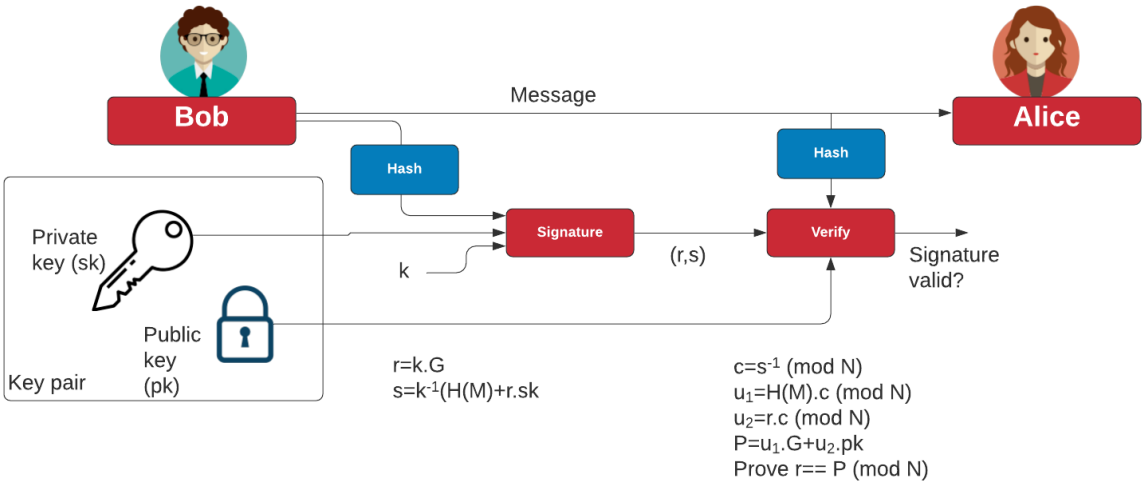

Fig 3. Firma digital con ECDSA

Discusión

Un punto de discusión es que en este proyecto se enfocó en la seguridad y robustez del sistema antes que la eficiencia, esto puede ser visto ya que cada sensor generaba su firma y luego todas estas firmas eran verificadas en el servidor, si se hubiera elegido eficiencia, la implementación hubiera cambiado tal que en el servidor se tuviera una sola firma para todos los sensores la verificarán y así simplificando de cierta manera la arquitectura.

Por otra parte, como puntos de mejora para el futuro, se plantea una reformulación del funcionamiento de los sensores, haciendo que estos envíen sus datos al menos 1 vez al día (como es planteado en el desafío).

Conclusión

En este proyecto, se logró cubrir los requerimientos solicitados tanto por el lado de la infraestructura como a nivel de integridad de los datos. Cumpliendo con el objetivo principal que era proveer una firma digital con curvas elípticas para resguardar la integridad y no repudio de los datos.

Esto aumenta la seguridad de la información, pero dicha situación no implica que se está libre de un ataque de captura de tráfico e intercepción de las llaves privadas y públicas por parte de los sensores y vulneración de los datos. Por eso debemos remontarnos a unas de las primeras clases, donde se sabe que atacante es audaz, es una persona que tiene tiempo y buscará la manera de romper el sistema, pero al realizar la verificación de las firmas digitales con curva elíptica se hace que sea un poco más difícil y que le deberá tomar más tiempo.

Retroalimentación por parte de “Los mensajeros elípticos”

Respecto del proyecto presentado por el grupo “Los Elípticos”, nosotros como grupo (Los mensajeros) encontramos que pudieron lograr de forma satisfactoria el desafío planteado en la actividad, en donde pusieron en práctica los conocimientos adquiridos en el curso. Esto queda claramente evidenciado en el uso de firma digital con curvas elípticas, algo que se trató hacia el final del curso y el poder verlo en práctica ayuda a tener una mejor comprensión.

Del trabajo realizado, encontramos que es importante destacar el contar con un servidor público funcionando en Canadá, ya que ayuda a hacer el proyecto más real aún.

Como algo que se puede sugerir mejorar en una siguiente versión es el hecho de que, además de firmar la información, también se podría cifrar para mantenerla de forma confidencial. También se recomienda probar valores negativos de temperatura para prevenir posibles problemas en una implementación real.

Retroalimentación a “Los mensajeros elípticos”

Creemos como equipo que el grupo mensajeros elípticos, cumplieron con las competencias respectivas del ramo, debido a que utilizaron los contenidos adquiridos en administración de redes de computadores e implementaron 2 entornos virtuales que simulan el servidor como el sensor en este caso. Simulando la problemática planteada y se puede notar que el grueso de su trabajo fue la encriptación de curva elíptica y la operación de esta.

Por otro lado, es cierto que solicitaba realizar desplegaciones a una nube o github, pero notando los conocimientos adquiridos en la actualidad se encuentra razonable su simulación de la problemática y adecuada debido a que tienen el foco en asegurar los datos.

Trabajos a futuro

Implementar firma digital al servidor y que ésta sea verificada por los sensores, así aliviando el tiempo de respuesta para N sensores.

Exponer la llave pública del servidor para que así los sensores envíen su firma digital utilizando solo dos llaves que serían asimétricas y no generando una en cada sensor como se había propuesto en un inicio para con esto lograr un mejor manejo de llaves.

Realizar la encriptación del payload completo que envía el sensor al servidor mediante curvas elípticas.

Referencias

https://ecdsa.readthedocs.io/en/latest/

https://infocenter.nordicsemi.com/index.jsp?topic=%2Fsdk_nrf5_v17.0.2%2Fgroup__nrf__crypto__ecdsa.html

Enlaces de interés

 Video Demo

 Repositorio de GitHub