Universidad de los Andes
Ingeniería de Sistemas y Computación
ISIS 2203 Infraestructura Computacional

Caso de Estudio – Canales Seguros
Sistema de Gestión Empresarial y Operativa de una Compañía Transportadora
Caso 2 - Canales seguros

Objetivos

- Identificar los requerimientos de seguridad de los canales usados para transmisión de la información en el sistema de gestión empresarial y operativa de una compañía transportadora.
- Construir un prototipo a escala de una herramienta que evalúa la resistencia del algoritmo de integridad que la empresa usa.

Problemática:

Como se indicó en el documento que describe el contexto del caso, las principales tareas del sistema son la recepción de órdenes de recogida, gestión de rutas, rastreo de unidades de distribución y paquetes, y gestión administrativa contable de recursos y de clientes.

En este contexto, surgen diferentes problemas de seguridad para algunas de las transacciones que el sistema soporta, tanto a nivel de transmisión, como en procesamiento y almacenaje de datos. Como consecuencia, es necesario evaluar riesgos y determinar medidas para mitigar los problemas detectados. Su tarea en este caso es actuar como consultor de seguridad y analizar la seguridad de las tareas relacionadas con el rastreo de unidades de distribución. Para ello resuelva las partes A y B que se plantean a continuación.

A. [85%] Implementación del Prototipo.

En esta parte del proyecto nos centraremos únicamente en la evaluación del algoritmo de integridad que la compañía usa. Su tarea consiste en escribir un programa en Java que, a partir del nombre del algoritmo y un código criptográfico de hash, identifique la cadena que se usó para generar dicho código. Para ello su programa debe incluir dos métodos:

- El método generar_codigo. Recibe una cadena de texto y una cadena con el nombre de un algoritmo. Retorna el código criptográfico de hash correspondiente.
- El método identificar_entrada. Recibe un código criptográfico de hash y una cadena con el nombre de un algoritmo. Retorna la cadena que se usó para generar dicho código (null si no encuentra una respuesta).
- Puede usar métodos auxiliares.
- No puede usar las instrucciones break, ni continue. Vamos a contribuir al debate break, continue, goto vs. programación estructurada.
- Para probar sus métodos, desde el main invoque el método generar_código y use el resultado para invocar el método identificar_entrada.
- No use librerías especiales, solo las librerías estándar de java (java.security). Si tiene alguna duda sobre una librería específica consulte con los profesores.

Para simplificar un poco el problema:

- Supondremos que las cadenas de entrada cumplen dos condiciones: tienen una longitud máxima de 7 caracteres y solamente incluyen letras minúsculas (a-z).
- Los algoritmos para generación de código criptográfico de hash que pueden ser usados son: MD5, SHA256, SHA384, SHA512.

Adicionalmente, resuelva las siguientes tareas:

1. Busque información adicional sobre los algoritmos mencionados: (i) cuáles se usan hoy día y en qué contexto y (ii) por qué dejamos de usar aquellos que se consideran obsoletos.
2. Registre los tiempos que toma el método identificar_entrada por cada algoritmo, en el peor caso, para cadenas de longitud 1,2, 3, 4, 5, 6 y 7.
3. A partir de los tiempos registrados estime cuánto tomaría identificar la entrada por cada algoritmo, en el peor caso, para una cadena de longitud 16.

4. Construya una gráfica que muestre los tiempos registrados en los dos puntos anteriores (2 y 3).
5. Identifique la velocidad de su procesador, y estime cuántos ciclos de procesador toma, en promedio, generar y evaluar una secuencia para determinar si corresponde o no a un código criptográfico de hash. Escriba todos sus cálculos.

B. [15%] Análisis y Entendimiento del Problema.

Suponga que la arquitectura del sistema incluye tres servidores en la oficina principal: uno se encarga del manejo y rastreo de unidades de distribución y paquetes, el segundo del manejo de órdenes de recogida, y el último se encarga del manejo administrativo y contable de recursos y clientes. Todas las comunicaciones usan algoritmos de generación de códigos criptográficos de hash para garantizar integridad.

- Los puntos de atención al cliente se comunican por medio de internet con el servidor de manejo de órdenes para registrar pedidos y contratos.
- Para el rastreo de unidades de distribución y paquetes y optimización de rutas, las unidades se comunican cada 60 segundos con el servidor para informar su estado. El servidor recibe la información y la procesa. Por otro lado, el servidor de manejo de unidades de distribución calcula diariamente a la 1 a.m. las rutas del día. En condiciones excepcionales, los conductores pueden cambiar las rutas asignadas, pero deben informar y justificar.
- El servidor de manejo de órdenes se comunica con el de rastreo y rutas: las rutas se calculan con base en los puntos de atención que han recibido paquetes.
- El servidor de manejo administrativo contable no atiende consultas de clientes vía web; solamente responde a consultas iniciadas en la intranet de la compañía.

Suponiendo que el sistema descrito en el párrafo anterior cuenta con un firewall que filtra paquetes a la entrada de la red y antivirus en todas las máquinas de la compañía:

1. Identifique los datos que maneja el sistema de rastreo y que deben ser protegidos.
2. Identifique los requerimientos de seguridad para cada uno de los datos del punto anterior. Explique su respuesta en cada caso y responda la pregunta: si no se garantiza ese requerimiento para ese dato ¿cómo podría afectar a la entidad?
3. Identifique cuatro vulnerabilidades de este sistema, teniendo en cuenta únicamente aspectos técnicos o de procesos (no organizacionales). Identifique vulnerabilidades no solo en lo relacionado con la comunicación sino también con el almacenamiento y procesamiento de los datos. Explique su respuesta en cada caso.

(*) *Sus explicaciones DEBEN corresponder al contexto planteado. NO entregue respuestas genéricas.*

Entrega:

- Cada grupo debe entregar un zip de un proyecto Java con: La implementación del prototipo. En el subdirectorio docs debe haber un archivo que incluya el informe con las respuestas a los puntos A.1 a A.5 y B.1 a B.3. **Al comienzo del informe, deben estar los nombres y carnés de los integrantes del grupo**. Si un integrante no aparece en el documento entregado, el grupo podrá informarlo posteriormente. Sin embargo, habrá una penalización: la calificación asignada será distribuida (dividida de forma equitativa) entre los integrantes del grupo.
- Recuerde incluir en su informe **todas las referencias** que use para resolver este proyecto.
- El trabajo se realiza en grupos de **2** personas. No debe haber consultas entre grupos.
- El grupo responde solidariamente por el contenido de todo el trabajo, y lo elabora conjuntamente (no es trabajo en grupo repartirse puntos o trabajos diferentes). Se puede solicitar una sustentación a cualquier miembro del grupo sobre cualquier parte del trabajo. Dicha sustentación será parte de la calificación de todos los miembros.
- El proyecto debe ser entregado por Sicua+ por uno solo de los integrantes del grupo.
- **La fecha límite de entrega es 9 de noviembre 2020 a las 23:50 p.m.**

Referencias:

- *Cryptography and network security*, W. Stallings, Ed. Prentice Hall, 2003.
- *Computer Networks*. Andrew S. Tanenbaum. Cuarta edición. Prentice Hall 2003, Caps 7, 8.
- *To use or not to use the goto statement*: Programming styles viewed from Hoare Logic. Hidetaka Kondoh, Kokichi Futatsugi. Science of Computer Programming. Volume 60, issue 1. 2006.