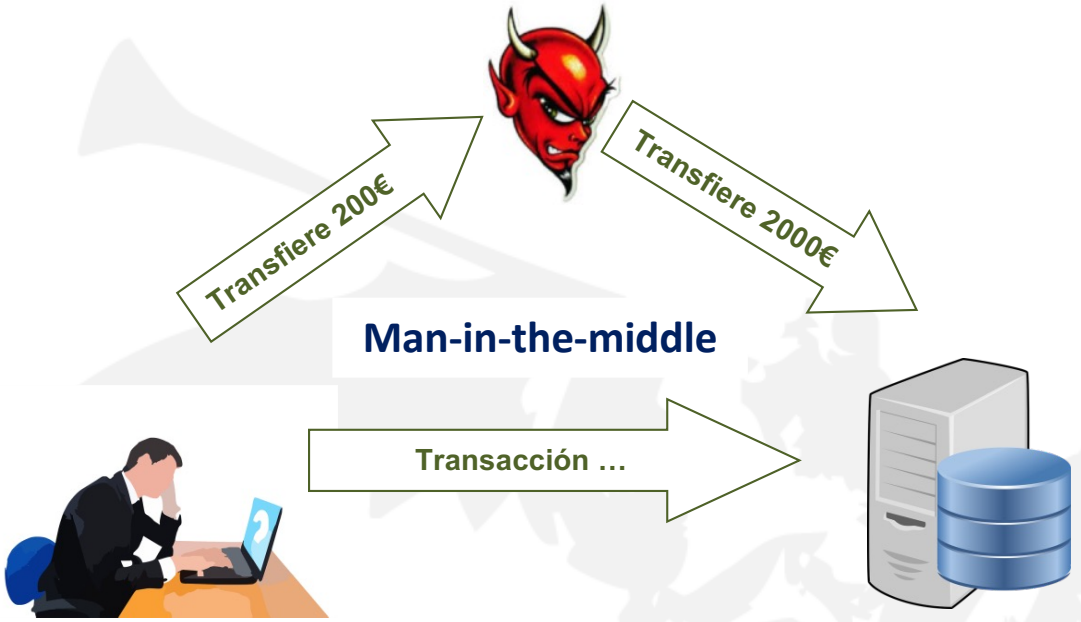
UNIVERSIDAD D SEVILLA

PAI – 2. VERIFICADORES DE INTEGRIDAD EN LA TRANSMISIÓN PUNTO-PUNTO PARA ENTIDAD FINANCIERA

Ángel Jesús Varela Vaca
Grupo de Investigación **IDEA Research Group**,
Universidad de Sevilla

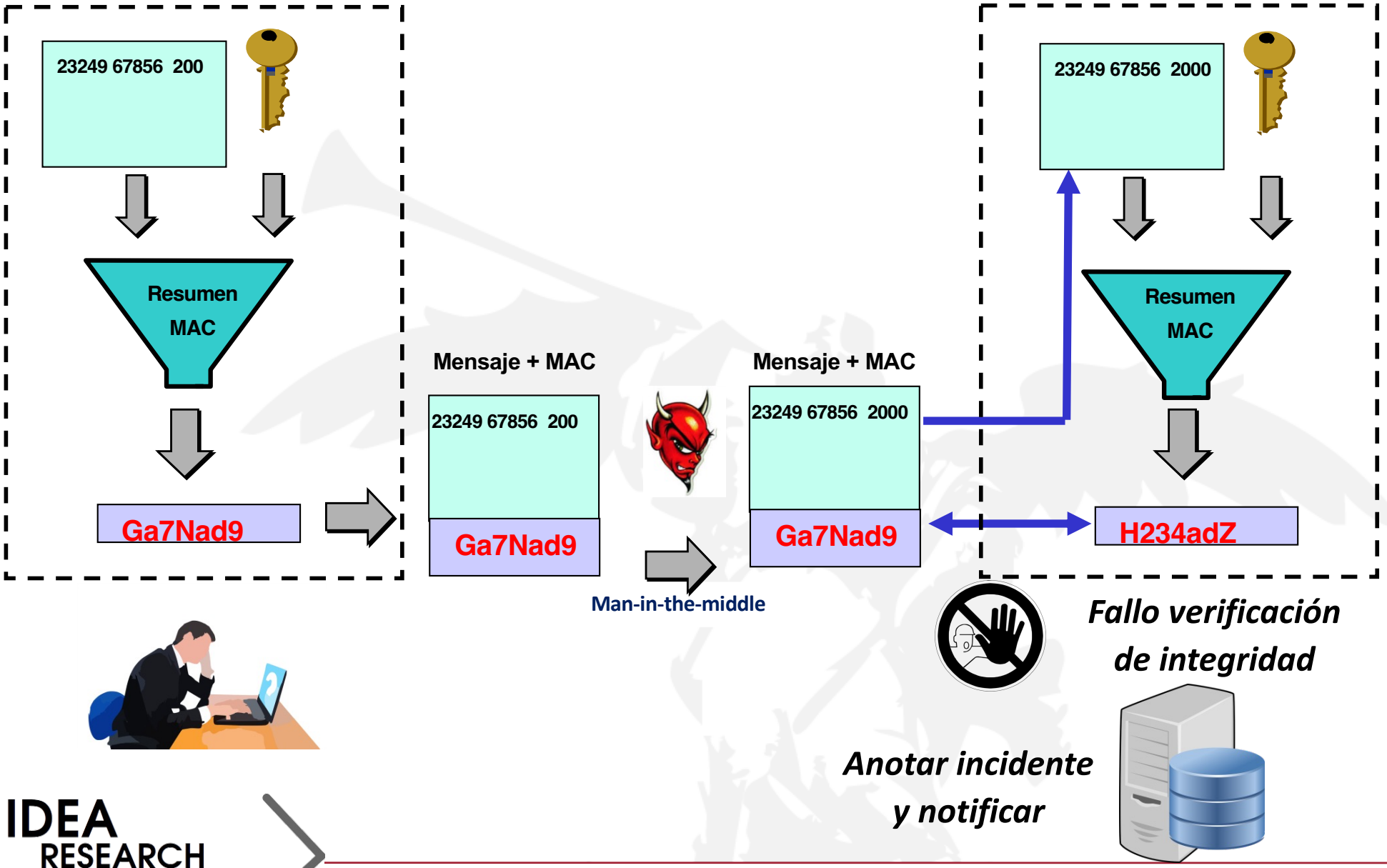
Integridad en la Transmisión Punto-Punto



Integridad de la información transmitida

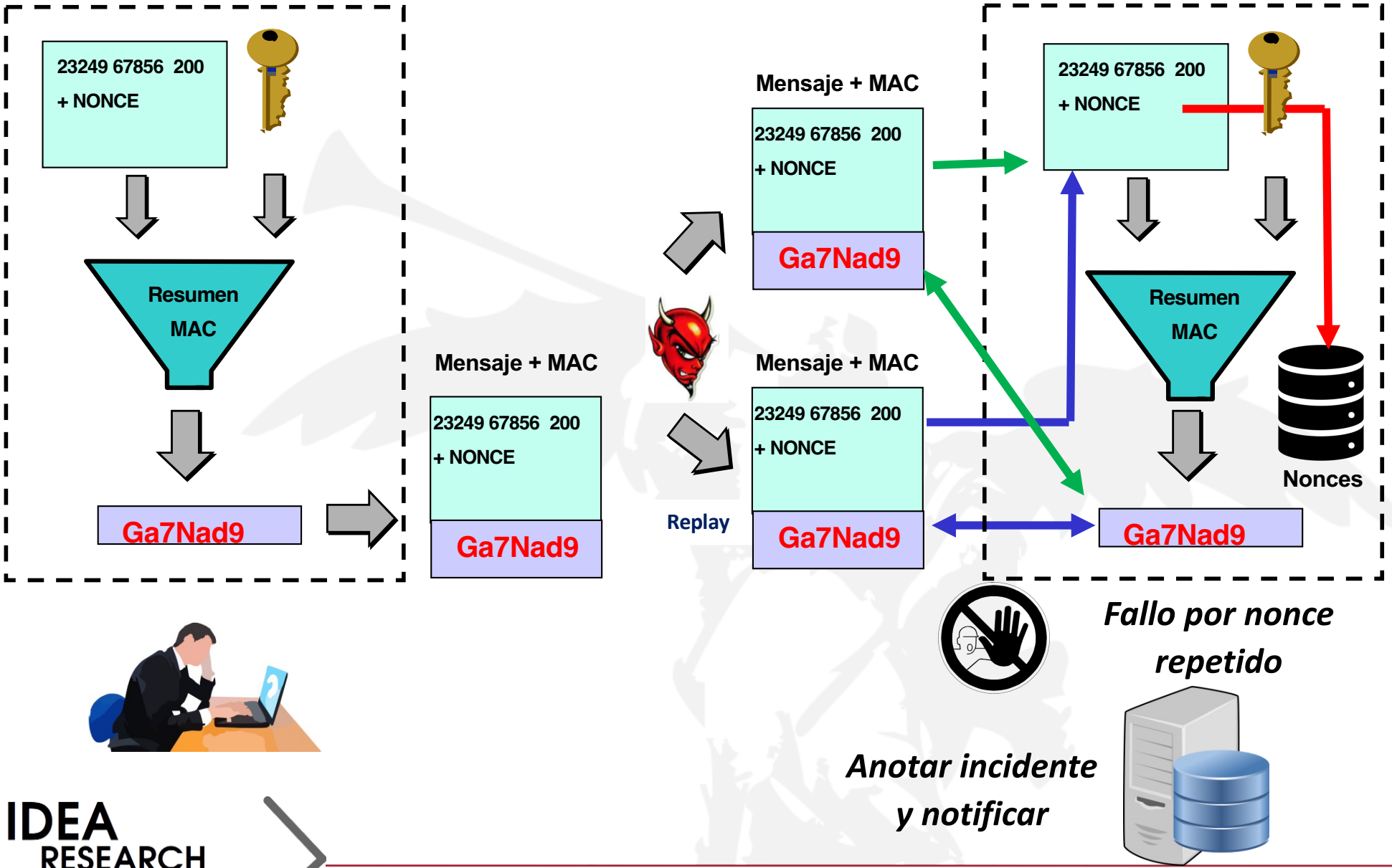
Verificar la integridad de datos en la transmisión por redes públicas y evitar los diferentes tipos de posibles ataques

Integridad en la Transmisión Punto-Punto



#IDEA RESEARCH GROUP beta v1.0

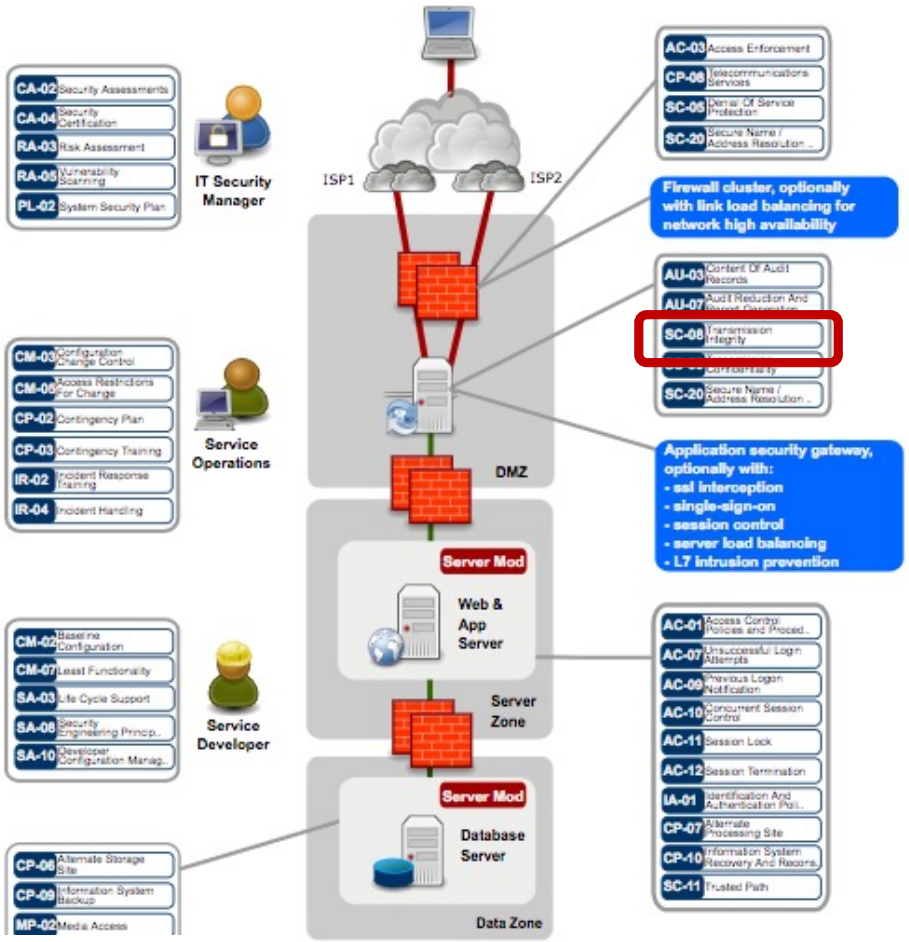
Integridad en la Transmisión Punto-Punto



#IDEA RESEARCH GROUP beta v1.0

SP-008: Public Web Server Pattern

Diagram:



"Control: The information system protects the integrity of transmitted information."

#IDEA RESEARCH GROUP beta v1.0

Se propone a los Security Teams de INSEGUS alcanzar los objetivos siguientes:

1. ***Desarrollar/Seleccionar*** el verificador de integridad para los mensajes de transferencia bancaria que se transmiten a través de las redes públicas evitando los ataques de **man-in-the-middle** y de **replay** (tanto en el servidor como en el cliente).

2. **Desplegar** un verificador de integridad en los sistemas **cliente/servidor** para llevar a cabo la realización de la verificación de forma práctica de los mensajes transmitidos entre un servidor y un cliente**.**

- Para llevar a cabo estos objetivos se debe tener en cuenta que:
  - **Input** del sistema: El mensaje (Cuenta Origen, Cuenta Destino, Cantidad) a verificar la integridad en su transmisión, nombre del algoritmo que se usará para verificar la integridad, clave utilizada por el cliente y el servidor.
  - **Output** del sistema: Indicación en el cliente y servidor si se ha conservado la integridad o no se ha conservado. La salida podría ser presentada en una ventana al emisor del mensaje y en el servidor dejar constancia en un fichero de logs de los mensajes que no han llegado de forma íntegra.

- El **KPI** será la ratio de mensajes que se envían de forma íntegra/número total de mensajes enviados entre los usuarios y la entidad financiera

- Se debe detallar el **procedimiento** que ha llevado a cabo para que el cliente y servidor tengan la **misma clave** para hacer la comprobación de la integridad y discuta la eficiencia de dicho procedimiento

Documento (30%)

- Tamaño del informe.
- Calidad del informe aportado y justificaciones.
- Calidad de pruebas presentadas y resultados.

Código/Configuración aportada (70%)

- Cumplimiento de requisitos establecidos.
- Calidad del código entregado.
- Complejidad de la automatización.
- Recolección de métricas y reportes.
- Pruebas entregadas.