

Concepto de Operaciones

Sistema de comunicaciones seguras con segmentación virtual de dominios

Alberto Daniel Lange

10 de febrero de 2025

Resumen

Este documento es una descripción basada en el método Arcadia del concepto de operaciones del sistema completo. Es un documento de alto nivel que busca presentar, en función de los conocimientos actuales, no solo una visión general del sistema y su funcionamiento, sino también introducir conceptos generales acerca de comunicaciones seguras.

v1.0

Índice

1. Introducción	2
1.1. Antecedentes	2
1.2. Suposiciones y restricciones	4
1.3. Resumen del sistema propuesto	4
2. Objetivos, metas y justificación del nuevo sistema	5
3. Usuarios y modos de operación	6
3.1. Usuarios	6
3.2. Modos de operación	6

1 Introducción

1.1 Antecedentes

En el ámbito de las comunicaciones, es fundamental contar con un sistema que garantice seguridad proveyendo confiabilidad respecto a la autenticación, confidencialidad e integridad de la información transmitida. Cuando la comunicación se desarrolla sobre un medio considerado inseguro, garantizar las propiedades mencionadas implica abordar desafíos adicionales como mitigar la posibilidad de suplantación de identidad, encriptar la información para asegurar confidencialidad y evitar que el mensaje sufra modificaciones. Se han desarrollado soluciones privativas al problema descrito. Sin embargo, la inexistencia de back-doors y mecanismos de vigilancia es algo que no puede ser verificado por completo en dichas soluciones. Es por esto que en áreas como defensa y servicio diplomático es de interés contar con soluciones completamente auditables que no dependan de licencias de exportación. A su vez, que la funcionalidad y validación formal del equipo no dependa de las funciones criptográficas utilizadas, y que estas puedan ser provistas o implementadas por el usuario final.

La tríada de la CIA (Confidentiality, Integrity, Availability) es un modelo que constituye la base para el desarrollo de sistemas de seguridad. Es utilizada para identificar vulnerabilidades de un sistema y proponer soluciones que cumplan con estos principios.

- **Confidencialidad:** consiste en proteger la información sensible de accesos no autorizados. Los métodos para reforzar este aspecto pueden involucrar la encriptación de la información y la implementación de controles de acceso.
- **Integridad:** refiere a asegurar la consistencia y confiabilidad de la información transmitida y mitigar el riesgo de que los mensajes sufran alteraciones por parte de agentes no autorizados. La implementación de firmas digitales es uno de los métodos empleados para reforzar este principio.
- **Disponibilidad:** cumplir con este aspecto requiere asegurar que la información sea accesible para usuarios autorizados cada vez que sea requerida. Un sistema robusto en este aspecto tiene que ser capaz de soportar ataques de denegación de servicio. Los métodos que refuerzan este aspecto pueden involucrar introducir redundancia a los componentes del sistema.

En el contexto de comunicaciones, un canal inseguro es un medio de transmisión en el que la información se encuentra expuesta a ciertos ataques. La escucha pasiva, la suplantación de identidad y la denegación de servicio son algunos ejemplos de ataques típicos de un canal inseguro. Los primeros dos corresponden al área de confidencialidad en el modelo descrito, y pueden tratarse implementando algún método de encriptación.

La encriptación de las comunicaciones garantiza la confidencialidad de las mismas y es la base de un sistema de comunicaciones seguras. Existen dos enfoques principales para realizar encriptación, el enfoque simétrico y el asimétrico.

- **Encriptación simétrica:** consiste en un método en el cual las partes utilizan una misma clave para la encriptación y desencriptación de la información. Esto trae como problema que cualquier entidad con acceso a dicha clave tiene la capacidad de leer y reescribir la información. Aún así, se trata de un método eficiente y muy utilizado para transmitir grandes volúmenes de datos. Cualquier implementación con este enfoque requiere como complemento de una forma segura de intercambiar la clave utilizada en un contexto de canales inseguros debido a que mantener la confidencialidad de la comunicación depende de que ambas partes resguarden la clave simétrica.
- **Encriptación asimétrica:** bajo este enfoque cada entidad posee un par de claves únicas, denominadas clave pública y clave privada, que guardan relación entre sí. La clave pública es utilizada para encriptar información y la clave privada correspondiente al mismo par es utilizada para desencriptarla. Este método no suele ser utilizado para la transmisión de grandes volúmenes de información debido a que, al ser de mayor complejidad computacional, se vuelve poco eficiente en estos casos. A diferencia del enfoque simétrico, aquí la confidencialidad de lo que transmite una de las partes depende de que la misma mantenga asegurada su clave privada.

El método de Diffie-Hellmann propone combinar ambos enfoques para lograr acordar, empleando el concepto de encriptación asimétrica, una clave simétrica de manera segura que puede ser usada posteriormente para encriptar información. La principal ventaja del método radica en que ambas partes logran generar la misma clave simétrica sin transmitirla por el canal, mitigando un gran problema de seguridad del enfoque simétrico. La figura 1 describe las operaciones matemáticas sobre las cuales funciona el método de Diffie-Hellmann.

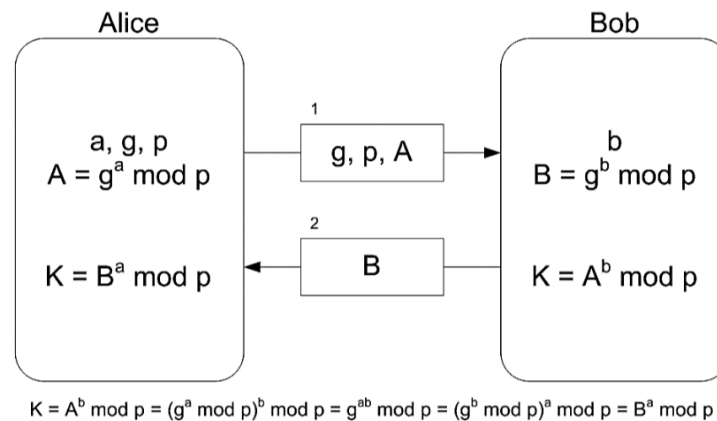


Figura 1: Método de Diffie-Hellmann para el acuerdo de una clave común.

Para los estándares de seguridad actuales, un esquema de establecimiento de comunicaciones requiere mayor complejidad para abordar desafíos como un ataque de tipo man-in-the-middle. Aún así, el método de Diffie-Hellmann es la base de numerosas implementaciones por su simplicidad y el elevado costo computacional que supone calcular la clave K conociendo únicamente las claves públicas A y B .

1.2 Suposiciones y restricciones

Distintas soluciones de encriptación pueden proponerse según la capa del modelo OSI que se analice. La encriptación a nivel de capa física minimiza las penalidades en rendimiento a costa de introducir complejidad al sistema, que se manifiesta en la necesidad de hardware dedicado de extremo a extremo de la red. Esta restricción puede volver inviable la encriptación a nivel de la capa física cuando el sistema de comunicaciones requiere de escalabilidad, principalmente por el costo de despliegue y mantenimiento. La encriptación en capas superiores provee mayor flexibilidad en la implementación del sistema. Si bien esto introduce una mayor latencia a la red, reduciendo el rendimiento de la misma, se pueden lograr valores aceptables de latencia con suficiente optimización. Las soluciones de encriptación en la capa 3 tienen la ventaja de ser independientes de la capa física, reduciendo la complejidad del sistema y permitiendo mayor flexibilidad en la implementación y compatibilidad con infraestructura preexistente. Esto implica que, cualquier sitio que cuente con una conexión a Internet y un dispositivo de encriptación tiene la infraestructura suficiente para acceder a una red segura, denominada red privada virtual.

En sistemas de criptografía, usualmente se utiliza el concepto de dominios rojo/negro para describir las partes del sistema que trabajan con información legible (dominio rojo) y aquellas que contienen información cifrada (dominio negro). La arquitectura de un sistema de comunicación seguro debe tener en cuenta este concepto para una correcta segregación de dominios, mitigando así la posibilidad de filtraciones indeseadas de información. La normativa actual que refiere a la segregación de dominios no contempla la segregación virtual, es decir, contener en un mismo dispositivo ambos dominios y aislarlos empleando herramientas de software. El implementar un sistema de este estilo capaz de cumplir las normas de seguridad existentes es un desafío importante.

1.3 Resumen del sistema propuesto

El sistema de comunicaciones seguras que se propone contempla el diseño de un único dispositivo, denominado encriptador, con la capacidad de formar un túnel VPN entre redes preexistentes, asegurando ciertos estándares de autenticación y confidencialidad sobre las comunicaciones entre dichas redes. El sistema opera a nivel de capa 3 del modelo OSI, y requiere de un mínimo de dos encriptadores para su funcionamiento, aunque también se encuentra prevista la escalabilidad del sistema. El propósito del sistema es brindar confiabilidad respecto a la autenticación, confidencialidad e integridad de la información transmitida entre redes interconectadas, afectando al mínimo el rendimiento de la red.

En el esquema de la figura 2 se describen los denominados dominios rojos, correspondientes a redes donde se trata con información sensible. El complemento de estos se denominan dominios negros, que usualmente se consideran canales inseguros donde la información proveniente de un dominio rojo requiere estar encriptada. El dispositivo encriptador actúa de interfaz entre dominios rojo y negro, motivo por el cual gran parte de la seguridad del sistema recae sobre este. Este dispositivo cuenta con acceso a claves utilizadas para establecer sesiones seguras con otros dispositivos, y al mismo tiempo cuenta con acceso a Internet. Debe poder garantizarse la seguridad en la gestión de estas claves y rechazar accesos no autorizados al dominio rojo.

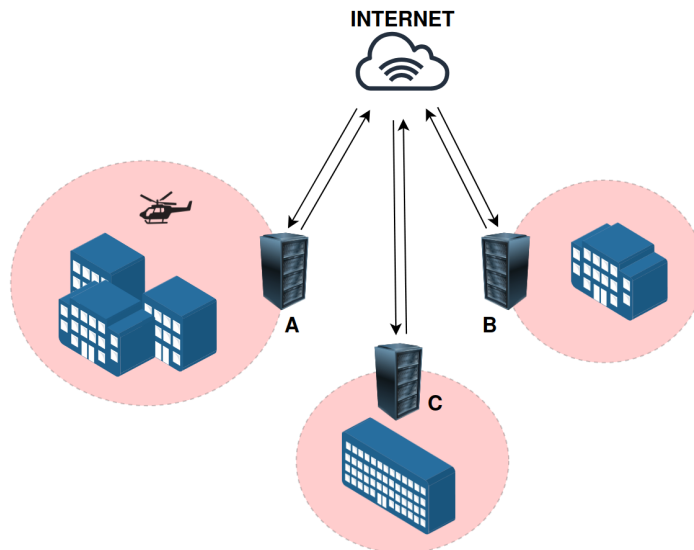


Figura 2: Esquema simplificado del sistema de comunicaciones seguras.

2 Objetivos, metas y justificación del nuevo sistema

Un dispositivo en el cual los dominios rojo y negro no estén correctamente segmentados se encuentra con que la información confidencial respecto al túnel VPN como claves y permisos se hallan expuestos en el caso de una intrusión desde Internet o desde la propia red interna. Esto lleva a la posibilidad de que un agente no autorizado sea capaz de descryptar y modificar información que viaje por el túnel, así como también acceder a dispositivos dentro de una organización.

En el diseño del encriptador, se propone implementar la segmentación virtual de dominios rojo/negro, esto es, representar los dominios como entidades virtuales independientes que ejecutan sobre hardware compartido. Este concepto puede implementarse a través de los denominados hipervisores, software que permite que varios sistemas operativos independientes trabajen juntos, compartiendo los mismos recursos físicos.

La segmentación permite que la entidad negra, la cual está conectada a Internet, realice el control del tráfico y oculte la existencia de la entidad roja para cualquier servicio fuera de la red virtual privada. Por otro lado, la entidad roja es la responsable de encriptar/descryptar las comunicaciones entre organizaciones que se encuentren dentro de la red privada y de gestionar las claves de encriptación y los privilegios de usuarios. Esta segmentación permite un control estricto sobre el tráfico entre ambas entidades, mitigando la posibilidad de transferir información como claves contenidas en la entidad roja hacia la entidad negra.

3 Usuarios y modos de operación

3.1 Usuarios

- **Administrador de red:** responsable de la configuración y mantenimiento del encriptador. Cuenta con acceso a la interfaz de administración del dispositivo y es el encargado de configurar el encriptador para funcionar dentro de la red segura. La configuración del encriptador incluye la definición de las redes que se conectarán a través del túnel VPN, la configuración de las claves de encriptación y la definición de los permisos de los usuarios.
- **Usuario final:** utiliza la red segura para compartir información sensible a otros nodos de la red. No tiene acceso a la configuración del encriptador y su interacción con el sistema se limita a utilizar la red segura como si de su red local se tratase.

3.2 Modos de operación

El diseño prevee que, una vez configurado el dispositivo, la operación del encriptador sea transparente para el usuario final, el cual no necesita interactuar con el dispositivo para utilizar la red segura.

- **Nodo pequeño:** en este modo de operación, el encriptador opera también como router para las comunicaciones seguras y no seguras. Ofreciendo una funcionalidad conocida como *split tunneling*, el encriptador permite que los usuarios finales puedan acceder a la red segura y a Internet simultáneamente.
- **Nodo grande:** en este modo de operación, el encriptador únicamente opera como encriptador de las comunicaciones seguras, y se conecta a un router preexistente para las comunicaciones no seguras.