INTERCAMBIO DE INFORMACIÓN TÁCTICA ENTRE SISTEMAS DE MANDO Y CONTROL DESPLEGADOS EN REDES CON DISTINTO NIVEL DE CLASIFICACIÓN DE SEGURIDAD

Autor: Álvaro Diego Martín
Director/es: Miguel Rodelgo Lacruz

I. INTRODUCCIÓN Y CONTEXTO

En las operaciones militares es fundamental el intercambio de información debido a la naturaleza conjunto combinadas de éstas. Esto es, en las operaciones en las que nos vemos envueltos, formamos parte de un contingente que lo conforman distintas naciones aliadas, así como distintos tipos de ejércitos (Tierra, Armada y Aire). Por tanto, cada tipo de ejército necesita un tipo de información para ejercer su mando y control y entre ellos compartirla entre los distintos países del contingente.

Esta información de mando y control es crítica, ya que de ella depende la conciencia situacional de los ejércitos y no puede caer en manos de las fuerzas enemigas, por lo que hay que tomar las medidas de seguridad adecuadas. Además, debido al entorno multinacional en el que se envuelven, tal vez no toda la información quiera ser compartida, siguiendo el principio de *need-to-know* (necesidad de conocer).

Dentro de este contexto, es necesario intercambiar información entre los distintos sistemas de mando y control o con el sistema de mando y control propio de cada nación situado en distintos dominios de seguridad, esto es, que los sistemas estén acreditados para el manejo de información de distinto nivel de seguridad, por lo que no pueden compartir toda la información.

La información puede estar clasificada dependiendo de lo crítica que sea. Para manejar dicho tipo de información clasificada hay que hacerlo siguiendo unas medidas de seguridad, tanto nacionales como a nivel de la misión. Por tanto, para enviar y recibir información con distinto nivel de seguridad hay que hacerlo siguiendo unas medidas de seguridad, entre otras, emplear pasarelas de seguridad que no permitan conexiones punto a punto entre las distintas redes y sólo permita intercambiar el tráfico deseado y permitido.

Además, para que ocurra correctamente este intercambio de información se tienen que emplear una serie de estándares bien conocidos por las naciones y que sus sistemas de información de mando y control los implementen correctamente. Dentro de estos aspectos se debe considerar tanto el marcado de seguridad en un entorno digital, así como la información táctica que se envía, que debe ser interpretable para todos los sistemas con los que interoperen. Esto es, se debe emplear un modelo de datos que modele las necesidades comunes de las naciones, un tipo de protocolo de intercambio de datos común y, en caso de que se le añadan metadatos (como el marcado de seguridad digital) debe ser bien conocido y añadirse a la información táctica siguiendo unos estándares.

II. DESARROLLO Y RESULTADOS

El desarrollo del trabajo consiste fundamentalmente en estudiar la base de datos de la aplicación TALOS, basada en un modelo de datos de OTAN para que pueda almacenar la información necesaria a la hora de intercambiar información indicando la clasificación de seguridad que debe tener esta, además de parámetros adicionales que nos indican los estándares que hay para tal efecto.

Aunque el modelo de datos contiene las clases necesarias para almacenar esta información, hay relaciones que hay que añadir, para que además de las unidades, instalaciones, materiales… tengan clasificación de seguridad la propia operación, líneas de acción de la propia operación, o las fases en las que se compone cada línea de acción. Hay que tener que la última versión del modelo de datos es de 2012 y la evolución de éste ya contiene estas relaciones necesarias.

Además, hay que identificar qué formato deben tener los mensajes para que se pueda intercambiar información con marcado de seguridad de manera que sea comprensible por todos los sistemas de información de mando y control de la alianza. Para ello hay dos estándares en los que se definen: el marcado de seguridad para archivos digitales, de manera que se cumpla la política de seguridad de la OTAN para tal efecto; cómo unir los metadatos que contienen el marcado de seguridad con los datos de información.

Hay que tener en cuenta que para intercambiar información entre distintos dominios de seguridad hay que emplear pasarelas o diodos, que rompen el protocolo TCP/IP. Esto es, no permiten conexiones entre los dos extremos, sino que la propia pasarela debe realizar esta acción.

Además, de acuerdo a las directivas de seguridad que hay, cuando se envía información desde el dominio de mayor seguridad al de menor, esta información debe estar firmada digitalmente para que autentifique al emisor y asegure la integridad de los datos.

El principal problema es que, a la hora del intercambio de información, además de estas cuestiones de marcado de información, los datos tácticos que se envían deben estar basados en estándares. Actualmente los estándares internacionales más ampliamente utilizados para el intercambio de este tipo de información están en proceso de actualización. Por tanto, estas modificaciones sólo servirían para intercambiar información empleando la misma aplicación.

III. CONCLUSIONES

Actualmente dentro del entorno de los sistemas de mando y control se está empezando a implementar las modificaciones necesarias para permitir actuar estos sistemas en distintos dominios de seguridad.

Dentro de los sistemas de mando y control existe el acuerdo de emplear un modelo de datos común para los distintos SIC2. Esto permite intercambiar información entre las

distintas naciones de forma que todos tengan la capacidad de almacenar y generar mensajes con la misma información. Además, en caso de necesidades adicionales pueden extender dicha base de datos.

Los estándares de interoperabilidad internacionales están en desarrollo para incluir el marcado de seguridad necesario, así como el etiquetado necesario para incluir estos metadatos. Esto provoca que cualquier implementación que se haga en este sentido se debe hacer a nivel del SIC2 o empleando estándares nacionales.

Para intercambiar mensajes de mando y control entre dominios de distinta seguridad es necesaria una pasarela que rompa el protocolo TCP/IP, esto es, que no permita abrir ningún socket directamente entre las redes separadas por la pasarela. Además de poder filtrar el tráfico al igual que lo hace un Firewall. Las adaptaciones de estas pasarelas pasan por poder verificar inequívocamente el formato de los mensajes que le llegan de los SIC2.

El futuro de estos sistemas de información de mando y control pasa porque lleguen las actualizaciones de dichos estándares para que las pasarelas de seguridad puedan adaptarse a estos mensajes sin necesidad de estar modificándolas continuamente. Pruebas en este ámbito se están haciendo en ejercicios internacionales con los prototipos de los estándares mencionados.