Biba: Modelo de Integridad

Cristian Adrián Ontivero
2018-05-13

En 1975 Kenneth. J. Biba publicó en un reporte el primer modelo de integridad [1]. Este reporte fue posteriormente revisado y abierto al público en 1977 [2], aproximadamente un año luego de la última publicación de MITRE del modelo de Bell-La Padula. El modelo de Biba fue también desarrollado dentro de MITRE Corporation, como parte del *Secure General Purpose Computer Project* de la Fuerza Aérea de Estados Unidos. En sus reportes, Biba describió un modelo en el que se usaban controles similares a los de BLP, pero para integridad en vez de confidencialidad, y haciendo una examinación de cómo es posible mantener la validez de información. Para salvaguardar contra la modificación indebida de información permitida en Bell-La Padula, Biba introdujo los conceptos de niveles de integridad y política de integridad. La idea básica de su modelo es que la información de baja integridad no debería fluir a objetos de mayor integridad (pero si vice-versa). El modelo suele resumirse como *"read up, write down"* (lo opuesto a Bell-La Padula).
Mientras BLP se ocupa de proteger contra la diseminación no autorizada de información, Biba se ocupa de identificar y hacer cumplir la correcta modificación de información. Este modelo consta de:

- Un conjunto S de sujetos.
- Un conjunto O de objetos.
- Tres modos de acceso: $\underline{\mathtt{o}}$ (*observe*), $\underline{\mathtt{m}}$ (*modify*), $\underline{\mathtt{i}}$ (*invoke*). Formalmente, estos son relaciones (los dos primeros subconjuntos de $S \times O$, el tercero subconjunto de $S \times S$). Dados sujetos $s, s' \in S$ y un objeto $o \in O$, decimos:
  - $s \mathrel{\underline{\mathtt{o}}} o$ si s tiene la capacidad de observar o.
  - $s \mathrel{\underline{\mathtt{m}}} o$ si s tiene la capacidad de modificar o.
  - $s \mathrel{\underline{\mathtt{i}}} s'$ si s tiene la capacidad de invocar s'.
- Un conjunto de niveles de integridad I (*integrity levels*) con un orden parcial $\leq$.

Tanto sujetos como objetos son primitivas del modelo, y qué son en la práctica dependerá de la implementación. Los sujetos son aquellos elementos del sistema que realizan acceso de información (son "procesadores de información"). Los objetos son aquellos elementos que son accedidos (son "repositorios de información"). Los modos de acceso son abstractos, con observación y modificación siendo análogos a lectura y escritura en BLP. La invocación, por el contrario, no es lo mismo que ejecución. La invocación es un pedido lógico de servicio, de un sujeto a otro. Invocación representa un acceso de control entre distintos sujetos, mientras que ejecución es el acceso de un sujeto a un objeto con el fin de obtener instrucciones. De hecho, para los propósitos del modelo de Biba, ejecución es equivalente a observación (ya que para ejecutar, un sujeto necesita observar las instruciones dentro del objeto).
Los niveles de integridad son elementos de $I = C \times \mathcal{P}(K)$, donde C es el conjunto de clases de integridad (parcialmente ordenadas), y $\mathcal{P}(K)$ es el conjunto partes de K, siendo K el conjunto de compartimientos. Esto es análogo a los niveles de seguridad de Bell-La Padula. En el primer reporte se usan a modo de ejemplo las clases de integridad *Important* (I), *Very Important* (VI), y *Crucial* (C), en orden creciente. Aun así, estas no son particularmente estandar, y las clases usadas en la práctica dependerán del ámbito en que se use el modelo[1].
Dependiendo de qué tan confiable es un individuo, se le asigna un nivel de integridad. Este mismo criterio se usa para asignarle un nivel de seguridad. En contraste, la asignación de un nivel de integridad a un objeto se hace en base a distintos criterios que los usados al asignarle un nivel de seguridad: los niveles de integridad se asignan para prevenir sabotaje de información; los de seguridad para prevenir divulgación de información. Esto lleva a la conclusión que es preferible usar distintos valores para los niveles de integridad y seguridad (es decir, distintas clases y distintas categorías/compartimientos), ya que la semántica (los criterios de asignación) es distinta. El modelo cuenta también con una función $il\colon S \times O \to I$ que define el nivel de integridad de sujetos y objetos.

[1] Poco después de mencionar estas tres clases de integridad, Biba procede (por simplicidad o descuido) a mezclar su terminología, usando las clases de integridad mencionadas como si fueran niveles de integridad. Esto no quita validez a su modelo, ya que usarlas como niveles es isomorfo a usar clases de integridad con un conjunto vacío de compartimientos.

0.1. Políticas Mandatorias de Integridad

En su reporte, Biba describió tres políticas mandatorias de integridad. Todas las políticas comparten las siguientes dos propiedades (dadas como axiomas por Biba):

1. Un sujeto s puede modificar un objeto o sólo si $il(o) \leq il(s)$.

   Esta propiedad a veces se la conoce por el nombre de propiedad-* de integridad.

2. Un sujeto s_1 puede invocar a un sujeto s_2 sólo si $il(s_2) \leq il(s_1)$.

   A veces conocida como propiedad de invocación (*invocation property*).

La propiedad (1) asegura que la modificación directa maliciosa es imposible. Si un sujeto pudiera alterar un objeto de mayor confianza, podría implantarle información de menor integridad (porque el sujeto es menos confiable). Si esto pasara, de cierta manera el objeto se volvería tan confiable como el sujeto, por lo que se lo prohibe. La propiedad (2) previene la modificación indirecta de objetos de mayor integridad por sujetos, a través de otro sujeto de mayor integridad. Con estas dos se maneja el problema de la modificación directa de información.

0.1.1. Política Low-Water Mark

A veces conocida bajo el acrónimo LOMAC (*Low-water Mark Mandatory Access Control*), esta política hace uso de un función[2] inf: $\mathcal{P}(I) \to I$, que devuelve el ínfimo (máxima cota inferior) de los niveles de entrada. Además de las dos propiedades mencionadas, esta política agrega la siguiente:

3.1 Luego de cualquier observación de un objeto o por un sujeto s, el nivel de integridad del sujeto $il'(s)$ inmediatamente luego del acceso, se define como:

$$il'(s) = \inf\{il(s), il(o)\}$$

La propiedad (3.1) previene modificaciones indirectas indebidas. De los tres modelos, este es el único dinámico, en el sentido que el valor del nivel de integridad de un sujeto no es estático, sino que monótono no creciente. La *low-water mark* (marca de bajamar) hace referencia al menor nivel de integridad de un objeto observado por un sujeto; efectivamente, el sujeto se "marca" o "ensucia" con el menor nivel de integridad al que accede. Esta política tiene el problema de que los sujetos tienden a reducir su integridad con el tiempo, y no hay forma de recuperar el nivel original salvo reinicializar el sujeto.

0.1.2. Política Ring

Esta política esta definida por las propiedades (1) y (2) mencionados anteriormente, y no agrega ningún otro. Es por esto que solo aborda el problema de la modificación directa, pero no asegura nada contra la modificación indirecta. El modelo bajo la política ring[3] es estático, ya que los niveles de integridad de sujetos y objetos se mantienen fijos. Es más flexible que low-water mark, a expensas de tener menos garantías de integridad.

0.1.3. Política Strict Integrity

Cuando se habla simplemente del "modelo de Biba" sin especificar, se hace referencia a esta política, siendo que es la principal. La misma consiste en las propiedades (1) y (2), y agrega la siguiente:

3.2 Un sujeto s puede observar un objeto o sólo si $il(s) \leq il(o)$.

   Esta propiedad a veces se la conoce como propiedad simple de integridad o *no write up* (NWU).

[2] Llamada min por Biba, pero evitaremos el nombre por ser este levemente engañoso.
[3] Su nombre origina de la similitud con un mecanismo de protección homónimo en Multics.

Esta política provee capacidades similares a la política low-water mark, pero es más restrictiva: cuando una lectura en low-water mark alteraría el nivel de integridad de un sujeto, en strict integrity se la prohibe. La observación clave de esta política es que integridad y confidencialidad son en cierto sentido conceptos duales: integridad es una restricción sobre quién puede alterar o escribir un objeto, y confidencialidad sobre quién puede observarlo o leerlo. Mientras que la información fluye hacia arriba en Bell-La Padula, en Biba fluye hacia abajo. Un esquema de esto se observa en la Figura 1, donde los ω_i representan niveles de integridad y los λ_i niveles de seguridad. En ambos casos, los niveles son monótonamente no decrecientes.

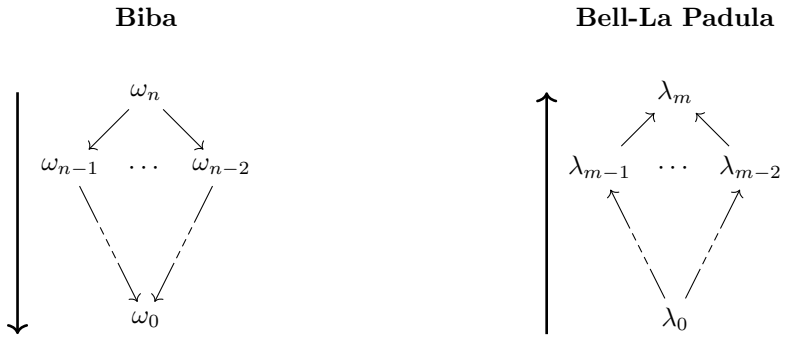

Figura 1: Flujo de información, representado por flechas, en Biba y Bell-La Padula.
Los ω_i representan niveles de integridad, y los λ_i niveles de seguridad.

Definición 1. Un camino de transferencia de información es una secuencia de objetos $\langle o_0, \ldots, o_{n+1} \rangle$ y una secuencia de sujetos correspondiente $\langle s_0, \ldots, s_n \rangle$, tal que

$$\forall i \in \{0, \ldots, n\}, \quad s_i \underline{\mathtt{o}}\, o_i \quad \wedge \quad s_i \underline{\mathtt{m}}\, o_{i+1}$$

El siguiente teorema nos asegura que la política de integridad estricta mantendrá la integridad de los objetos, como definida por la asignación de niveles de integridad.

Teorema 1. Si existe un camino de transferencia de información de un objeto o_0 a un objeto o_{n+1}, entonces hacer cumplir la política estricta de integridad requiere $il(o_{n+1}) \leq il(o_0)$.

Demostración. Supongamos que existe un camino de transferencia de información, entonces por definición existe la secuencia de sujetos y objetos especificada. Por la propiedad-* de integridad, y la propiedad simple de integridad, tenemos:

$$\forall i \in \{0, \ldots, n\} \quad il(o_{i+1}) \leq il(s_i) \leq il(o_i)$$

Esto puede observarse en la Figura 2 (usando $\geq$ en vez de $\leq$ con su significado obvio, para explicitar la secuencia de desigualdades).

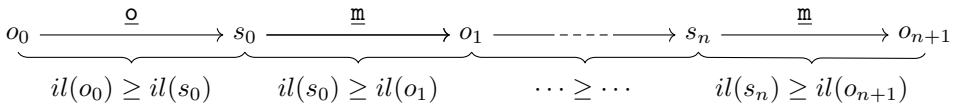

Figura 2: Camino de transferencia de información, con las desigualdades establecidas por las propiedades (1) y (3.2). La observación de o por s se representa mediante $o \xrightarrow{\underline{\mathtt{o}}} s$, y mediante $s \xrightarrow{\underline{\mathtt{m}}} o$ la modificación de o por s.

Como $\leq$ es un orden parcial, es por definición transitivo, entonces:

$$\forall i \in \{0, \ldots, n\} \quad il(o_{i+1}) \leq il(o_i)$$

Por lo tanto, $il(o_{n+1}) \leq il(o_0)$. □

En [3] vemos que la similitud entre el modelo de integridad estricta de Biba, y el modelo Bell-La Padula va más allá de lo mencionado. No es necesario pensar a los niveles de mayor integridad arriba, y los de menor abajo; "arriba" y "abajo" son términos relativos, no absolutos. Podemos decir que los niveles de mayor integridad estan abajo y los de menor arriba, o equivalentemente, que los niveles de mayor seguridad se encuentran abajo, y los de menor arriba en Bell-La Padula. De cualquiera de las dos maneras, coincidiría el sentido del flujo de información en ambos modelos. Con esto vemos que no hay una diferencia fundamental entre la política de integridad estricta de Biba, y el modelo de Bell-La Padula: ambos se ocupan del flujo de información en un retículo de niveles, donde la información solo tiene permitido fluir en un sentido. Como el sentido del flujo es relativo, un sistema que soporta uno de estos modelos puede soportar el otro (necesitando quizás reordenar etiquetas para invertir la relación de dominancia).

Referencias

[1] Kenneth. J. Biba. Integrity Considerations for Secure Computer Systems. Technical Report MTR-3153, MITRE Corp., June 1975.

[2] Kenneth. J. Biba. Integrity Considerations for Secure Computer Systems. Technical Report MTR-3153, MITRE Corp., April 1977.

[3] Ravi S. Sandhu. Lattice-Based Access Control Models. *Computer*, 26(11):9–19, November 1993.