Conceptualización de la ciberseguridad

Elena Gabriela Barrantes Sliesarieva

Se realiza una revisión de los conceptos básicos de seguridad. Asimismo, se tocan aspectos de implantación de seguridad y se ofrecen ejemplos de vulnerabilidades y defensas poco tradicionales.

Introducción

Usualmente se acepta que el objetivo de la ciberseguridad o seguridad informática es descubrir y aclarar la naturaleza de las amenazas y proveer metodologías para mitigarlas. Por lo tanto, al hablar de su conceptualizaciòn, es indispensable definir las clases de amenazas, y las vulnerabilidades y ataques asociados a ellas. No hay que perder de vista, sin embargo que el alcance de cada uno de estos conceptos va a variar de acuerdo al contexto y a la aplicación en particular que se esté analizando.

Para iniciar, se define una amenaza como cualquier ocurrencia potencial, maliciosa o no, que pueda tener un efecto indeseable en los recursos de una organización. Una vulnerabilidad está siempre asociada a una amenaza y es básicamente cualquier característica de un sistema que permita (potencialmente) que una amenaza ocurra.

Claramente, al identificar y bloquear vulnerabilidades se logran mitigar las amenazas respectivas. Finalmente, un ataque involucra un ente malicioso que explota alguna vulnerabilidad para ejecutar la amenaza. Se puede ver un ataque como una instanciaciòn de una o varias amenazas.

Un ejemplo clásico de la interoperabilidad entre los tres conceptos presentados es el siguiente: una amenaza a un sistema es el robo de datos, y una posible vulnerabilidad es un sistema débil o inexistente de autenticación. Un ataque ocurre cuando un usuario conocedor de la vulnerabilidad en fortaleza de palabras de paso se matricula en el sistema y copia todos los datos a los que le da acceso la cuenta que rompió.

Para la construcción de la conceptualizaciòn iniciaremos con la clasificación de las clases básicas de amenazas, la idea de que la seguridad es una carrera armamentista con los atacantes, un recuento de las consideraciones básicas para implementar la seguridad, ejemplos de vulnerabilidades y de ataques, el concepto de análisis forense y una breve reflexión sobre la privacidad.

Clases de amenazas

Existen tres tipos básicos de amenazas: revelación de información, denegación de servicio, o repudio y corrupción de la integridad de los recursos (Amoroso, 1994). Otras amenazas que se van a tocar explícitamente, aunque sean instancias de la última clase son el secuestro del control y la suplantación. La relativa importancia de cada uno de ellos va a depender del sistema estudiado. Por ejemplo, en un sistema de telemedicina en tiempo real, una denegación de servicios representa una amenaza mucho más grande que la revelación de información.

La revelación de información se refiere a la amenaza de que un ente que no cuenta con autorización para el acceso a ciertos recursos, logra accederlos de forma indebida. Un ejemplo es el acceso de un ladrón al número de una tarjeta de crédito ajena, pero también al acceso no autorizado de una compañía de datos personales de ciudadanos con los que no posee ninguna relación legal.

La denegación de servicio, o repudio corresponde a la amenaza "inversa": que los entes que sì cuentan con autorización de acceso a los recursos no consigan entrar (esto es, sean repudiados a la entrada). Por ejemplo, la amenaza de que los usuarios no logren navegar en el sitio web de una empresa debido a que el servicio de nombres (DNS) esté atascado por solicitudes mal formadas.

La corrupción de la integridad es intuitivamente la más "agresiva", ya que se trata del acceso directo a los recursos, y como individuos con mayor o menor grado de territorialidad, es la que despierta mayor grado de rechazo. Sin embargo, se debe recordar que las amenazas no viven en el vacío. Si el recurso indebidamente modificado es de poco valor para la organización, quizás una preparación demasiado reactiva ante esa amenaza sea contraproducente.

La amenaza de corrupciòn de integridad comprende muchos aspectos, más allá de la definición de daño, pérdida o inserción de información falsa. En particular se quiere resaltar dos de ellos: el secuestro de control y la supantación de identidad, ambas amenazas muy reales actualmente. Es fácil imaginarse las consecuencias de que un atacante esté controlando su máquina, que puede ser el servidor corporativo o su laptop, y que además esté utilizando sus datos para realizar transacciones.

La carrera armamentista en ciberseguridad

Claramente las vulnerabilidades que permiten la ocurrencia de ataques y los detalles de los mismos dependen enteramente de cada sistema. Sin embargo, es posible identificar tendencias, y una de las más interesantes es lo que se puede denominar una carrera armamentista, muy similar a la que ocurre en la naturaleza a múltiples niveles, por ejemplo con los virus.

Cuando un organismo vivo es atacado por un virus, este eventualmente logra bloquear alguna de las vulnerabilidades que permiten el ataque, por ejemplo modificar un camino químico que le impide al virus reproducirse en el organismo. Sin embargo, rápidamente aparece una mutación del patógeno que evade la defensa y utiliza alguna vulnerabilidad alternativa. Por cuanto los organismos vivientes son sistemas muy complejos, este tipo de interacciones pueden seguir operando para siempre.

En el caso de los sistemas computacionales, la situación es muy similar a la descrita previamente. Son sistemas complejos, en constante evolución: algunas vulnerabilidades se bloquean, pero otras aparecen al modificar el software, y los atacantes se adaptan. Es poco probable que esta tendencia cambie en algún momento.

Es también importante aclarar que el tema de la seguridad ha sido una preocupaciòn de los diseñadores y operadores de sistemas informáticos desde su inicio. Por ejemplo, en 1974 se publica un reporte técnico que describe un proceso de análisis de vulnerabilidades en un sistema Multics, mediante un test de penetración., y muchas de las clases de vulnerabilidades y ataques que proponen, descubren o usan, conceptualmente aún están siendo utilizadas. Este es el caso del ataque que llamaremos por extensión de buffer overflow, que depende de las siguientes vulnerabilidades genéricas: (a) errores u omisiones en el procesamiento de datos de entrada que (b) permiten modificar apuntadores de uno u otro tipo que (c) hacen posible modificar, leer o bloquear el acceso a datos que no estaban dentro del alcance del usuario o programa que realizó originalmente la entrada de datos (Karger, 1974). A pesar de los grandes cambios que se han dado en la computación hasta este momento siguen existiendo ataques reales que, a nivel de concepto siguen estando emparentados con el buffer overflow.

La tendencia es entonces a que se cierra un portillo y aparecen muchos más. Esto se ve reflejado tanto en el creciente tamaño de las conferencias técnicas en seguridad como en el tamaño de las Bases de Datos utilizadas por los antivirus y otros programas de seguridad para filtrar la información que entra a los sistemas.

Algunas consideraciones para implementar la seguridad

Uno de los aspectos más importantes a rescatar es que la seguridad debe estar incorporada desde el diseño, para minimizar el número de vulnerabilidades, y que permita arreglarlas cuando se descubran de una manera más metódica y completa. Otro es que se debe aceptar que no existe ningún sistema completamente seguro y planificar de forma acorde. Finalmente, bajo ninguna circunstancia se debe usar seguridad por oscuridad, dado que los atacantes rápidamente

descubrirán sus vulnerabilidades, pero los defensores no contarán con el beneficio de una comunidad grande organizada trabajando en detectar vulnerabilidades y reportarlas rápidamente, y con apoyo para mejorar el software incrementalmente.

Es importante no perder de vista que la seguridad siempre implica un compromiso con la usabilidad. Este compromiso implica que para implantar una seguridad efectiva, se debe estar dispuesto a negociar con las comunidades involucradas dentro de la organización, dado que existe una tendencia general a subestimar los costos de no implementar medidas de seguridad, lo que redunda en resistencia a pagar los costos de implantación. Para vencer esta resistencia al cambio a todos los niveles se pueden usar varias tácticas, pero -aunque efectivo- es poco recomendable utilizar demostraciones en vivo de ataques, por cuanto se pueden perder o revelar datos reales, o darle demasiada información a entes externos.

Una consideración significativa es que los usuarios tienden a recordar los errores pero olvidarse de los éxitos, así que una solución implementada con poco cuidado puede deshacer meses de cuidados trabajo de convencimiento, por lo que es altamente recomendable siempre realizar la evaluación de riesgos y el análisis costo-beneficio, antes de intentar convencer a la organización.

Ejemplos de vulnerabilidades

En esta sección se ofrecen algunos ejemplos específicos de vulnerabilidades. El primer ejemplo es sobre los canales ocultos. Aún en un ambiente donde toda la información explícita esté protegida (por ejemplo, todos los archivos son inaccesibles desde el exterior y los mensajes viajan cifrados), algo de la información sobre el sistema se fuga. Por ejemplo, un atacante puede contar mensajes, o ver de donde vienen y para donde van, o medir el tiempo entre paquetes. Esta información "filtrada" se denomina "canales ocultos", y existen en múltiples puntos de los sistemas. Se han dado ataques reales exitosos utilizando información tan pública como la que se está presentando. Así que suponer que toda la información está protegida solo porque los datos estén ocultos es claramente peligroso.

Otra fuente de vulnerabilidades son los esquemas de cifrado, que pueden tener problemas de implementación (varios ataques aprovecharon esto) o problemas de fondo, como tamaño de la llave, supuestos de los algoritmos etc. El problema es que típicamente los sistemas de cifrtado son complejos de por sí, y es realmente difícil visualizar estas vulnerabilidades.

Por mucho, la forma más fácil de robo de datos es la ingeniería social. Por ejemplo, de nada sirven múltiples sistemas de seguridad si un empleado que está legítimamente autorizado a usar un sistema se lleva los datos y los vende a un tercero.

Finalmente hay que considerar las potenciales vulnerabilidades de los sistemas sobre los que corren las aplicaciones y sobre ls que se tiene poco control, como errores en el hardware, el sistema operativo o la plataforma de programación. Para considerar estos casos hay que mantenerse al día con los parches respectivos y programar aplicaciones de forma paranoica, sin confiar en nada obtenido del sistema hasta no revisarlo.

Ejemplos de defensas

Existen cada vez más formas de protección de datos, y decidir entre ellas es complejo. Parte de la solución está en establecer defensas en profundidad en lugar de desechar una para instalar otra. Para herramientas cuyo objetivo sea el mismo (por ejemplo, los antivirus), se debe estar monitoreando constantemente las actualizaciones Asimismo, si es posible, se debe establecer diversidad, contando con dos o más productos equivalentes simultáneamente implantados en la red.

Otra manera de aumentar la diversidad, lo que aumenta la resistencia a los ataques es utilizar diferentes tipos de defensa: tanto estáticas como adaptativas. Un ejemplo de sistemas adaptativos son los nuevos sistemas de detección de intrusos. La ventaja es que estos sistemas cuentan con procesos de aprendizaje por lo que no dependen de constantes actualizaciones de la base de datos. El problema es que al haber mucho ruido en la señal (distinción entre propio y ajeno), muchas veces se disparan demasiado

o insuficientemente, y ambos casos son peligrosos. Es por esto que los sistemas adaptativos siempre deben tener algún grado de supervisión y soporte con sistemas estáticos.

Un caso interesante de un sistema estático pero no dependiente de patrones es la introducción de ruido semi-aleatorio para perturbar las máquinas de inferencia de los canales ocultos. Por ejemplo si el atacante está tratando de adivinar la estrategia que se está usando para asignar reservaciones, unas cuantas transacciones fantasmas al azar pueden perturbar lo suficiente al mecanismo del atacante como para que no logre efectuar la deducción.

Análisis forense

El análisis forense es muy útill para determinar de la forma más exacta posible cómo sucedió un ataque para poder encontrar las vulnerabilidades que este aprovechó y cerrarlas, pero al mismo tiempo para evaluar la extensión del daño y tratar de mitigarla.

Privacidad y seguridad

Este es un tema largo e importante, pero al menos debe quedar claro que ninguna conceptualizaciòn de la seguridad es completa sin tocar aspectos de protección de datos de los usuarios finales, y nuestro país tiene grandes lagunas legales y de concientización al respecto. Por ejemplo, el correo electrónico es totalmente “abierto” a menos que se cifre de punto a punto, pero muchos usuarios ignoran esto y lo usan como si fuera totalmente secreto con resultados a veces trágicos.

Todos y todas debemos informarnos, informar a los demás, y mantenernos alertas sobre la tecnología que usamos, la protección de la que disponemos y sobre la visibilidad de nuestros datos en Internet.