

ANÁLISIS DE SEÑALES MÚLTIPLES PARA LA IDENTIFICACIÓN DE ÁMBITO AFECTADO

ANTECEDENTES

Los servicios en línea están bajo riesgo casi constante de terceros malintencionados que buscan comprometer los dispositivos dentro de los servicios en línea para subvertir su funcionalidad o comprometer los datos sensibles almacenados en dichos servicios. Los dispositivos comprometidos pueden presentar datos exfiltrados en un dispositivo exterior, o pueden ser ordenados para realizar diversas acciones por el tercero malintencionado, tal como, por ejemplo, como parte de una botnet (conjunto o red de robots informáticos). La identificación de huéspedes individuales que han sido comprometidos en el servicio en línea puede ser un recurso y una operación que consuma tiempo, lo que puede dejar al tercero malintencionado en el control de uno o más dispositivos durante un largo período de tiempo, a pesar de las contramedidas desplegadas en el servicio en línea. Los sistemas Información Actual de Seguridad y Administración de Eventos (SIEM, por sus siglas en inglés) pueden perder algunos dispositivos comprometidos o identificar erróneamente dispositivos seguros como comprometidos, lo que aumenta la cantidad de tiempo que el tercero malintencionado permanece en control y aumenta los recursos de procesamiento necesarios para volver a asegurar el servicio en línea.

BREVE DESCRIPCIÓN DE LA INVENCION

Esta Breve Descripción se proporciona para introducir una selección de conceptos en una forma simplificada que se describen a continuación en la sección de Descripción Detallada. Esta Breve Descripción no pretende identificar todas las características clave o esenciales de la materia objeto reclamada, ni está concebida como una ayuda para determinar el alcance de la materia objeto reclamada.

En la presente se proporcionan sistemas, métodos y dispositivos de almacenamiento legible por computadora que modaliza instrucciones ejecutables de procesador para detectar máquinas huésped comprometidas. Se reciben señales de seguridad por un analizador de anormalidad de señal para determinar un nivel de anormalidad para una acción dada en el servicio en línea que se está asegurando. En un gran servicio en línea, se espera que grupos de dispositivos se comporten igual cuando funcionan correctamente y, por lo tanto, los comportamientos que no son comunes son tratados con mayor sospecha. Los resultados de detección clasificados son agregados de acuerdo con diversas poblaciones de dispositivos o sub-comportamientos y las puntuaciones de anormalidad se pasan a un analizador de señales múltiples, que recoge los resultados de detección a través de ventanas enrollables de tiempo y los divide en diversos ámbitos basados en el dispositivo para análisis para determinar si debe generarse una alerta de que un determinado dispositivo está comprometido.

Mediante el uso de un análisis de ventana de ámbitos, la presente descripción aborda el problema centrado en computadora para detectar amenazas persistentes avanzadas, de movimiento

lento, así como ataques de rápido movimiento, concentrados en un servicio en línea con una fiabilidad mejorada. La seguridad de los datos alojados por computadora se mejora de esta manera, los recursos de procesamiento del servicio en línea son más eficientemente asignados a procesos legítimos, en contraposición a los procesos ejecutados en nombre de terceros malintencionados, además de una asignación más efectiva de la atención de usuarios analistas a presuntas infracciones.

Se implementan ejemplos como un proceso de computadora, un sistema de cómputo o como un artículo de fabricación tal como un dispositivo, producto de programa de computadora o medio legible por computadora. De acuerdo con un aspecto, el programa producto de computadora es un medio de almacenamiento por computadora legible por un sistema de computadora y que codifica un programa de computadora que comprende las instrucciones para ejecutar un proceso de computadora.

Los detalles de uno o más aspectos se presentan a continuación en los dibujos acompañantes y la descripción. Otras características y ventajas serán evidentes después de leer la siguiente descripción detallada y un examen de los dibujos asociados. Se entiende que la siguiente descripción detallada es sólo explicativa y no es restrictiva de las reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los dibujos anexos, que se incorporan y forman parte de esta descripción, ilustran varios aspectos. En los dibujos:

La Figura 1 ilustra un ejemplo de entorno en donde la presente descripción puede ser practicada;

La Figura 2 muestra los detalles del calificador de anomalía de firma;

La Figura 3 es un diagrama de bloques de las ventanas y eventos de ámbito para análisis de señales múltiples;

La Figura 4 ilustra detalles del detector de señales múltiples;

La Figura 5 es un diagrama de flujo que muestra etapas generales involucradas en un método ilustrativo para detectar ámbitos huésped comprometidos en un servicio en línea;

La Figura 6 es un diagrama de flujo que muestra etapas generales involucradas en un método ilustrativo para la puntuación de resultados de detección en función a anomalías;

La Figura 7 es un diagrama de flujo que muestra etapas generales involucradas en un método ilustrativo para la detección de señales múltiples de ámbitos comprometidos;

La Figura 8 es un diagrama de bloques que ilustran componentes físicos ilustrativos de un dispositivo de cómputo; y

Las Figuras 9A y 9B son diagramas de bloques de un dispositivo de cómputo móvil.

DESCRIPCIÓN DETALLADA

La siguiente descripción detallada se refiere a los dibujos anexos. Siempre que sea posible, los mismos números de referencia se utilizan en los dibujos y la siguiente descripción se refiere a elementos

iguales o similares. Aunque se pueden describir ejemplos, son posibles modificaciones, adaptaciones y otras implementaciones. Por ejemplo, se pueden hacer sustituciones, adiciones o modificaciones a los elementos ilustrados en los dibujos y los métodos descritos en este documento pueden ser modificados al substituir, reordenar o agregar etapas a los métodos descritos. En consecuencia, la siguiente descripción detallada no es limitante, sino que más bien, el alcance adecuado es definido por las reivindicaciones anexas. Los ejemplos pueden tomar la forma de una implementación de *hardware* o una implementación totalmente de *software* o una implementación que combina aspectos de *software* y *hardware*. La siguiente descripción detallada, por tanto, no debe tomarse en un sentido limitante.

La Figura 1 ilustra un ejemplo de un entorno 100 en donde la presente descripción puede ser practicada. Como se ilustra, un servicio en línea 110 comunica firmas de evento a un detector de eventos 120, que utiliza varios conjuntos de lógica de detección para proporcionar resultados de detección que indican los comportamientos que ocurren en el servicio en línea 110 a un calificador de anomalía de firma 130. El calificador de anomalía de firma 130 determina cuán común o infrecuente un determinado comportamiento es para el servicio en línea 110 y almacena los recuentos y el resultado de detección en una memoria caché de agregados de señal 140 y una memoria caché de resultados de detección 150, respectivamente.

Un detector de señales múltiples 160 acepta las puntuaciones de anomalías y resultados de detección del calificador de anomalía de firma 130 y la memoria caché de resultados de detección 150 (nuevos y observados anteriormente, respectivamente) de forma predictiva para determinar si el comportamiento observado es indicativo de actividad maliciosa o benigna en el servicio en línea 110. Las determinaciones de predicción son almacenadas en una memoria caché de resultados de señales múltiples 170 y pueden ser transmitidas a un generador de alertas 180 cuando indican un comportamiento malicioso. Un analista o usuario administrativo transmite alertas del generador de alertas 180 y puede acceder a los resultados guardados en memoria caché en la memoria caché de resultados de detección 150 y la memoria caché de resultados de señales múltiples 170 para una revisión adicional.

En varios aspectos, el calificador de anomalía de firma 130 y el detector de señales múltiples 160 se conocen colectivamente como el detector de anomalías 190. El detector de anomalías 190 puede estar alojado dentro del servicio en línea 110 como un dispositivo dedicado o conjunto distribuido de dispositivos en él, o puede ser un dispositivo externo o un conjunto de dispositivos. Además, el detector de eventos 120 puede ser parte del servicio en línea 110, del detector de anomalías 190, un servicio de tercera parte y combinaciones de los mismos. Análogamente, las memorias cachés utilizadas por el detector de anomalías pueden ser parte del detector de anomalías 190, el servicio en línea 110 o dispositivos de almacenamiento externos.

El servicio en línea 110, el detector de eventos 120, las memorias caché, el generador de alertas 180 y el detector de anomalías 190 son ilustrativos de una multitud de sistemas computacionales, incluyendo, sin limitación, sistemas de computadoras de escritorio, sistemas de cómputo alámbricos e inalámbricos, sistemas de cómputo móviles (por ejemplo, teléfonos móviles, netbooks, tableta o computadoras tipo pizarra, computadoras portátiles y computadoras laptop), dispositivos de mano,

sistemas de multiprocesador, electrónica de consumidor basada en microprocesador o de consumidor programable, minicomputadoras, impresoras y computadoras centrales. El hardware de estos sistemas de cómputo se discute con mayor detalle en relación con las Figuras 8, 9A y 9B.

Mientras el servicio en línea 110, el detector de eventos 120, memorias cachés, el generador de alertas 180 y el detector de anomalías 190 se muestran de forma remota desde otra para propósitos ilustrativos, cabe señalar que varias configuraciones de uno o más de estos dispositivos alojados localmente a otro dispositivo ilustrado son posibles, y cada dispositivo ilustrado puede representar varias instancias de ese dispositivo. Varios servidores e intermediarios familiares a aquellos expertos en la materia pueden estar entre los sistemas de componentes ilustrados en la Figura 1 para enrutar las comunicaciones entre dichos sistemas, que no son se ilustran para no distraer la atención de los aspectos novedosos de la presente descripción.

El servicio en línea 110 representa un conjunto de dispositivos de cómputo en red, tal como un centro de datos de nube, que ofrece servicios de "nube" a diversos usuarios, incluyendo, pero no limitado a: Infraestructura como un Servicio (IaaS, por sus siglas en inglés), en donde el usuario proporciona el sistema operativo y el *software* que se ejecuta en los dispositivos del servicio en línea 110; una Plataforma como un Servicio (PaaS, por sus siglas en inglés), en donde el usuario proporciona el *software* y el servicio en línea 110 proporciona el sistema operativo y los dispositivos; o *Software* como un Servicio (SaaS, por sus siglas en inglés), en donde el servicio en línea 110 proporciona el sistema operativo y el *software* para ejecutar en los dispositivos de los usuarios.

Varios eventos de auditoría son generados en los dispositivos dentro del servicio en línea 110 y son manejados por varios detectores de eventos 120 que ejecutan la lógica de detección dentro de una Información de Seguridad y Administración de Eventos (SIEM), así como sistemas de detección externa proporcionando resultados de la auditoría externa de otros sistemas y servicios. Los varios eventos de auditoría incluyen, pero no están limitados a: trazas de comunicación de red, registros de error, registros de eventos, comandos del sistema y similares.

En cuanto al servicio en línea 110, los comportamientos asociados con los usuarios o programas no autorizados (por ejemplo, virus) se clasifican como maliciosos, mientras que los comportamientos asociados con usuarios o programas autorizados se clasifican como benignos. Para clasificar estos comportamientos, los resultados de detección se pasan desde el detector de eventos al detector de anomalías 190, que almacena sus resultados en la memoria caché de agregados de señal 140, la memoria caché de resultados de detección 150 y memoria caché de resultados de señales múltiples 170.

El detector de anomalías 190 utiliza diversos enfoques de aprendizaje de máquina para desarrollar modelos que permitan evaluar las múltiples señales a lo largo de un período de tiempo para determinar si un determinado comportamiento es malicioso o benigno. La operación del calificador de anomalía de firma 130 y el detector de señales múltiples 160 del detector de anomalías se discute con mayor detalle en cuanto a las Figuras 2 y 4.

En respuesta a la determinación de que un determinado comportamiento es malicioso, el detector de anomalías 190 pasa su determinación a un generador de alertas 180. El generador de alertas 180

puede transmitir y presentar las alertas al usuario analista en una variedad de formatos, incluyendo, pero no limitado a: un mensaje de aplicación (por ejemplo, dentro de una aplicación SIEM), correo electrónico (a una cuenta de correo electrónico), un mensaje de texto o multimedia (a una celda o voz a través de una cuenta de Protocolo de Internet (VOID) cuenta), una página (a un número de localizador), etc. Se proporcionan alertas en tiempo casi real (por ejemplo, representando tiempo de procesamiento y de transmisión) al evento que resultó en la clasificación de los comportamientos como maliciosos, pero también pueden ser almacenados para su posterior consulta y revisión.

La Figura 2 ilustra los detalles del calificador de anomalía de firma 130. El calificador de anomalía de firma 130 acepta resultados de detección sin procesar de diversos detectores de eventos 120 da salida a recuentos de anomalía agregados a la memoria caché de agregados de señal 140, que se utilizan para actualizar cómo el calificador de anomalía de firma 130 produce resultados de detección calificados al detector de señales múltiples 160. El calificador de anomalía de firma 130 distingue si un determinado comportamiento es nuevo o ha sido visto antes y en qué medida se ha visto antes.

Los resultados de detección sin procesar son recibidos por un reconocedor de identificador 210, que determina un identificador para utilizar en conjunción con los resultados de detección. Los distintos valores de campo del resultado de detección sin procesar se combinan para formar el identificador, que puede incluir uno o más de los siguientes: un papel para el dispositivo desde el cual el comportamiento se observó, un usuario del dispositivo desde el cual el comportamiento se observó, una clase de comportamiento, un solicitante de comportamiento (usuario o proceso), un objeto de comportamiento (usuario o proceso), una marca de tiempo, u otros campos presentes en la señal de evento. Por ejemplo, un comportamiento del usuario *A* que otorgar al usuario *B* permiso administrativo a un dispositivo de tipo *C* en un tiempo *D* puede resultar en un identificador de *ABCD*. En varios aspectos, los identificadores son producidos en función de los valores de campo, pero no incluyen los valores de texto simple de esos campos. Por ejemplo, un algoritmo/función de hashing o codificación críptica se aplica a los valores de campo a la hora de formar el identificador.

El agregador de población 220 busca los recuentos históricos para el identificador particular de la memoria caché de agregados de señal 140 y, por consiguiente, actualiza las cuentas. Los recuentos históricos están agrupados según un recuento de la población para el número total de detecciones previamente observadas del tipo de comportamiento determinado y según un recuento de subpoblación del número total de detecciones previamente observadas compartiendo un determinado identificador.

El calificador de resultado de detección 230 añade al menos una puntuación de anomalía a los resultados de detección con base en los recuentos históricos para el comportamiento observado. La puntuación de anomalía se basa en la proporción entre el recuento de subpoblación y el recuento de población para el comportamiento dado, de manera que la subpoblación se convierte en una parte mayor de la población, la anomalía del comportamiento se reduce. Por ejemplo, la puntuación de anomalía puede utilizar el formato mostrado en la **Fórmula 1**, en donde *x*, *y*, y *z* son variados en diferentes aspectos que afectan a los valores proporcionados para la puntuación de anomalía. Como puede apreciarse, la **Fórmula 1** es dada como un ejemplo no limitante de cómo asignar una puntuación a una

anomalía.

Fórmula 1: Puntuación = $x - ((y \cdot \text{subpoblación}) \div (z \cdot \text{población}))$

Las puntuaciones pueden ser calculadas de acuerdo con los diferentes recuentos de ámbitos de población que utilizan recuentos sin procesar de todos los eventos que coincidan con un determinado comportamiento o recuentos de ámbito para los distintos dispositivos (huéspedes) en el servicio en línea 110 exhibiendo el comportamiento dado o el usuario que solicita el comportamiento observado. Para ilustrar, considerar la posibilidad de eventos E_1 y E_2 ocurridos en los dispositivos D_1 y D_2 de la línea 110 en servicio en donde E_1 se ha observado tres veces (dos veces en D_1 y una vez en D_2) y E_2 se ha observado una vez en D_2 . El recuento de población sin procesar en el ejemplo ilustrado es cuatro, ya que E_1 ocurrió en el servicio en línea 110 tres veces y E_2 una vez, y los recuentos de subpoblación son tres y uno para E_1 y E_2 , respectivamente. El uso de la **Fórmula 1** con un valor de uno para cada uno de x , y , y z , produce una puntuación de anomalías para E_1 de $0.25 [1 - (1 \cdot 3) \div (1 \cdot 4)]$ y una puntuación de anomalía para E_2 de $0.75 [1 - (1 \cdot 1) \div (1 \cdot 4)]$.

Una puntuación de anomalías de ámbito ilustrativa, sin embargo, puede producir resultados diferentes a partir de recuentos sin procesar dependiendo de los ámbitos seleccionados para la población. Al usar un ámbito de recuento de dispositivo, el recuento de población de dispositivo de ámbito sería de dos en la ilustración actual, ya que hay dos dispositivos distintos (D_1 y D_2) en el servicio en línea 110 en el ejemplo ilustrado. Como E_1 ha sido visto en ambos dispositivos, su recuento de subpoblación es dos, mientras que E_2 sólo se ha visto en D_2 , por lo que su recuento de subpoblación es uno. El uso de un ámbito de distintos dispositivos y la **Fórmula 1** con un valor de uno para cada uno de x , y , y z , produce una puntuación de anomalía para E_1 de cero $[1 - (1 \cdot 2) \div (1 \cdot 2)]$ y una puntuación de anomalía para E_2 de $0.5 [1 - (1 \cdot 1) \div (1 \cdot 2)]$.

Para evitar que nuevos eventos o eventos de baja población proporcionen puntuaciones espurias de anomalía, se usa un umbral de filtro en algunos aspectos para excluir los eventos de muy baja frecuencia de examen (al menos temporalmente). En un ejemplo, los eventos recientes son "antirrebotados" de manera que la primera observación de un comportamiento no será calificada hasta que otras instancias de ese comportamiento dado sean observadas. En un segundo ejemplo, un umbral de población se ajusta de manera que una probabilidad de cero se asigna si la población de eventos es demasiado pequeña para proporcionar resultados fiables (por ejemplo, durante el inicio del detector de anomalía 190). En un tercer ejemplo, un umbral de subpoblación se ajusta de manera que (dependiendo de las opciones del sistema) una puntuación máxima o mínima de anomalía se asigna si una subpoblación de comportamientos es demasiado pequeña para proporcionar resultados fiables en la estimación de una probabilidad de que el comportamiento pueda ser visto (por ejemplo, para una subpoblación recién asignada a observar).

En varios aspectos, los comportamientos observados se establecen de acuerdo con una ventana de tiempo de enrollamiento, de modo que los eventos considerados parte de una población o subpoblación (y sus recuentos asociados) se basan en cuándo se produjeron. Por ejemplo, solamente los comportamientos que se han observado en los últimos días d pueden ser parte de la ventana de tiempo

de enrollamiento y, por lo tanto, los recuentos de población y subpoblación para determinar una puntuación de anomalía pueden basarse en comportamientos recientes en lugar de todos los comportamientos observados para el servicio en línea 110. Una ventana enrollable para puntuaciones de anomalía de señal proporciona una línea de base para cómo aparecen las operaciones "normales" en el servicio en línea 110 (por ejemplo, cuáles son los patrones de uso del mes pasado).

Además, observando los comportamientos durante un período de tiempo, un ataque de movimiento lento en el servicio en línea 110 puede observarse que de otra manera podría perderse. Una ventana de señales múltiples enrollable garantiza que comportamientos de baja población o de movimiento lento, tales como las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés), son observados al recolectar todos los eventos que se producen en un determinado dispositivo en el servicio en línea 110 para determinar si existe un patrón malicioso para comportamientos.

La Figura 3 es un diagrama de bloques 300 de eventos de ventana y de ámbito para análisis de señales múltiples. Como se ilustra, varios bloques de evento 310 (individualmente, 310a-n) representando los comportamientos observados y sus identificadores asociados, puntuaciones, vectores de características, marcas de tiempo, etc., se muestran en un primer estado de organización 301 y un segundo estado de organización 302. Un arreglador de ámbito 320 está configurado para formar ventana y ámbito de los bloques de evento 310 desde el primer estado de organización 301 al segundo estado de organización 302, que incluye varios bloques de ámbito 330 (individualmente, 330a-n) que son alimentados al detector de señales múltiples 160 para su análisis. El detector de señales múltiples 160 se alimenta de los eventos asociados en cada ámbito para determinar si el ámbito está asociado con actividades maliciosas (por ejemplo, un dispositivo comprometido, una cuenta de usuario que tiene acceso a archivos restringidos, una cuenta de usuario que envía grandes cantidades de datos a un destino sospechoso, un proceso de actúa erráticamente, etc.).

El primer estado de organización 301 puede ser utilizado por una memoria caché de resultados de detección 150 u otro dispositivo de almacenamiento o una secuencia de eventos desde el calificador de anomalía de firma 130. Los eventos individuales pueden incluir aquellos que caen dentro de ventanas de tiempo previas (por ejemplo, aquellas con marcas de tiempo en los últimos días *d*), tales como bloques de evento 310a-h en el ejemplo ilustrado, y aquellos que, dentro de una ventana de tiempo actual (por ejemplo, los últimos *m* minutos), tales como los bloques de evento 310 g-n en el ejemplo ilustrado. Los eventos que están fuera de la ventana actual de tiempo incluyen aquellos eventos que han sido almacenados durante más tiempo que las ventanas de análisis que no están incluidas en el segundo estado de la organización 302 para análisis posterior.

Un analista u otro usuario administrativo establece cuánto tiempo la ventana de análisis está y qué propiedades se van a utilizar como ámbitos para el segundo estado de la organización 302. Por ejemplo, un identificador de dispositivo, tipo de dispositivo o usuario que solicita puede ser utilizado para separar los distintos bloques de evento 310 en diferentes bloques de ámbito 330 para su análisis. Los varios bloques de evento 310 que están designados para su posterior análisis (aquellos dentro de la ventana de análisis de enrollamiento) se organizan en bloques de ámbito 330 en función de la

característica de ámbito designado por el arreglador de ámbito 320.

Por ejemplo, cuando un ámbito se define para diferentes dispositivos, un primer bloque de ámbito 330a puede corresponder a un primer dispositivo en el servicio en línea 110, e incluye bloques de eventos 310 que están asociados con el primer dispositivo y han sido designados para su posterior análisis (bloques de eventos 310a, 310d y 310e). Asimismo, el segundo bloque de ámbito 330b y enésimo bloque de ámbito 330n corresponderían a un segundo y enésimo dispositivo, respectivamente, desde el servicio en línea 110 e incluyen los bloques de eventos 310 que están asociados con el segundo o el enésimo dispositivo y han sido designados para su posterior análisis (bloques de eventos 310b, 310i, 310G y 310h; y bloques de eventos 310c, 310f y 310n).

De los bloques de eventos 310 ilustrados, el bloque de eventos 310j no está asignado a ninguno de los ilustra el alcance de 330 bloques. En varios aspectos, un bloque de eventos 310 puede permanecer sin asignar a un boque de ámbito 330 cuando cae fuera de la ventana de análisis de enrollamiento, cuando el bloque de eventos 310 carece de datos a través de los cuales los eventos son asignados a diferentes ámbitos (por ejemplo, el identificador de dispositivo no está incluido en el bloque de eventos 310j), o el ámbito está configurado para excluir el tipo de resultado de detección del bloque de eventos dado 310 (por ejemplo, se define que el ámbito incluye sólo algunos comportamientos potenciales).

La Figura 4 ilustra detalles del detector de señales múltiples 160. El detector de señales múltiples 160 recibe, en una base de ámbito por ámbito (por ejemplo, resultados de detección calificados en una base por dispositivo, por usuario o por proceso), grupos de ámbito de uno o más resultados de detección calificados. Un extractor de característica 410 recibe la colección de resultados de detección calificados para el ámbito que ser y está configurado para extraer varias características de los resultados de detección calificados para producir un vector de característica para usarse por un modelo predictivo 420 para determinar si un determinado ámbito está produciendo un comportamiento malicioso.

El extractor de característica 410 está configurado para identificar las características de los resultados de detección calificados, tales como, por ejemplo: el puerto utilizado, la dirección IP a la que se conecta, identidad/tipo del dispositivo, identidad de usuario, identidad de proceso, medidas adoptadas, marca de tiempo, puntuación de anomalía, etc. Las características se convierten en valores numéricos (es decir, las características) para usarse como un vector de características para el modelo predictivo 420. El modelo predictivo 420 es un algoritmo entrenado según una técnica de aprendizaje de máquina para un vector determinado de característica para proporcionar una puntuación de confianza de si el ámbito del que se extrajo el vector de característica está exhibiendo comportamientos maliciosos.

El modelo predictivo 420 puede ser reentrenado continuamente, de acuerdo con una amplia variedad de técnicas de aprendizaje de máquina. Un experto en la materia estará familiarizado con diversas técnicas de aprendizaje de máquina que pueden ser empleadas en combinación con la presente descripción, las cuales incluyen una sesión de aprendizaje supervisado, semi-supervisado y no supervisado. En varios aspectos, una pluralidad de modelos predictivos 420 puede estar disponible a partir de la cual el detector de señales múltiples 160 (o un analista o usuario administrativo) puede

seleccionar uno o más para analizar un ámbito determinado basándose en su precisión conforme a un conjunto de datos de evaluación, áreas bajo las curvas de precisión y retiro, u otras métricas y para la comparación con otros modelos predictivos 420.

Las puntuaciones de confianza producidas por el modelo predictivo 420 se almacenan en la memoria caché de resultados de señales múltiples 170, para revisión por un analista o usuario administrativo y/o para fines de entrenamiento de modelo. Además, se utiliza lógica de alerta para determinar si una alerta relacionada con un resultado de detección debería ser transmitida a un analista o usuario administrativo. Cuando la puntuación de confianza producida por el modelo predictivo 420 satisface un umbral de confianza que el vector de característica para el ámbito determinado indica que el ámbito está exhibiendo un comportamiento malicioso, un generador de alertas 180 comunicará la determinación y los detalles necesarios para generar una alerta detallando el comportamiento malicioso.

La Figura 5 es un diagrama de flujo que muestra etapas generales involucradas en un método ilustrativo 500 para detectar ámbitos huésped comprometidos en un servicio en línea 110. El método 500 comienza con la OPERACIÓN 510, en donde se reciben resultados de detección de eventos. Los resultados de detección se reciben según la lógica de detección identificando varios comportamientos en el servicio en línea 110 e incluyen información proporcionada en una o más señales o archivos incluyendo, pero no limitado a: trazas de comunicación de red, registros de error, registros de eventos, comandos del sistema y similares.

El método 500 pasa a la OPERACIÓN 520, en donde los resultados de detección se puntúan de acuerdo con cómo los comportamientos anómalos que ellos representan están dentro de una ventana de tiempo enrollable. En varios aspectos, los comportamientos desde fuera de la ventana de tiempo enrollable se incluyen en la puntuación de anomalía del evento de detección para incluir comportamientos históricos o hipotéticos (denominados colectivamente como comportamientos históricos) que son designados por un analista u otro usuario administrativo para posteriores análisis.

En la OPERACIÓN 530, los resultados de detección puntuados son organizados por diversos ámbitos. Los ámbitos incluyen divisiones de los resultados de detección en función de una o más características elegidas por un analista o cualquier otro usuario administrativo para dividir el servicio en línea 110 en partes de componente para analizar si las actividades maliciosas pueden aislarse a una parte dada. Los ámbitos ilustrativos incluyen, pero no están limitados a: dispositivos/huéspedes individuales dentro del servicio en línea 110, cuentas de usuario y procesos/aplicaciones. Los eventos que no caen dentro de un ámbito determinado y los ámbitos que no tienen un número de eventos que supere una cantidad umbral, pueden ser excluidos de una ronda actual de análisis.

Pasando a la OPERACIÓN 540, la lógica de detección de señales múltiples se aplica a los resultados de detección en puntuación y en ámbito para determinar un nivel de confianza de si un determinado alcance ha sido comprometido. Varios modelos de aprendizaje de máquina capacitados (que pueden ser continuamente reentrenados y actualizados con base en las señales de detección de entrada) se utilizan de forma predictiva para determinar si un determinado dispositivo (o usuario o proceso) se está comportando maliciosamente con base en los resultados de detección puntuados

presentados en el ámbito. Varias características de los resultados de detección proporcionados en el alcance se convierten en características (representaciones numéricas de las varias características) y se introducen en un modelo predictivo 420 para producir una puntuación de confianza en cuanto a si el comportamiento es malicioso.

En la DECISIÓN 550, la puntuación de confianza se compara con un umbral de confianza en cuanto a si alertar a un analista u otro usuario administrativo de comportamiento malicioso. En respuesta a la puntuación de confianza satisfaciendo el umbral de confianza, se determina que el analista u otro usuario administrativo va a ser alertado y el método 500 pasa a la OPERACIÓN 560. De lo contrario, en respuesta a la puntuación de confianza que no cumpla el umbral de confianza, el método 500 puede terminar, pero podría repetir la OPERACIÓN 510, en respuesta a la recepción de un resultado de detección subsecuente.

En la OPERACIÓN 560 se genera una alerta y se transmite. En varios aspectos, la alerta identifica el comportamiento y el resultado de detección que desencadenó la alerta, así como el ámbito que se analizó para activar la alerta. Por ejemplo, una alerta puede indicar que en el tiempo t , el usuario A otorgó al usuario B permisos administrativos (comportamiento) sobre el dispositivo C (ámbito). Una alerta puede ser generada y transmitida de acuerdo con una pluralidad de formatos, incluyendo, pero no limitado a: un mensaje de aplicación (por ejemplo, dentro de una aplicación SIEM), correo electrónico (a una cuenta de correo electrónico), un mensaje de texto o multimedia (a una celda o cuenta de voz sobre protocolo de Internet (VOIP)), una página (a un número de localizador), etc. El método 500 podrá entonces terminar, pero podría repetir la OPERACIÓN 510, en respuesta a la recepción de un resultado de detección subsecuente.

La Figura 6 es un diagrama de flujo que muestra etapas generales involucradas en un método 600 ilustrativo de resultados de detección de puntuación basados en anomalías. El método 600 es un ejemplo de sub-pasos de la OPERACIÓN 520 de la Figura 5. El método 600 comienza con la OPERACIÓN 610, en donde se calcula un identificador para el resultado de detección. En varios aspectos, diferentes valores de campo del resultado de detección (por ejemplo, el nombre del dispositivo fuente, la dirección IP de destino, el usuario, el tipo de acción, efectos de acción, marca de tiempo) se utilizan para crear el identificador. El identificador puede usar los valores de campo en sí (con o sin los nombres de campo) o un valor derivado de uno o más valores de campo, tal como un hash criptográfico de los valores de campo, como un identificador para el comportamiento observado.

En la OPERACIÓN 620, los recuentos de agregado para el identificador se recuperan de la memoria caché de agregados de señal 140. Los recuentos de agregado para la población de comportamientos observados y subpoblaciones particulares para el comportamiento dado se pueden recuperar en función de una ventana de tiempo enrollable, de tal manera que los recuentos se basan en comportamientos que ocurrieron dentro de un período determinado de tiempo desde la hora actual (por ejemplo, en los últimos d días). En algunos aspectos, los comportamientos históricos observados definidos por un usuario analista son incluidos en los recuentos de la población, independientemente de si éstos fueron observados en la ventana de tiempo enrollable.

El método 600 procede a la OPERACIÓN 630, en donde los recuentos de agregado se actualizan en la memoria caché de agregados de señal 140. En varios aspectos, los recuentos para varias poblaciones y subpoblaciones (por ejemplo, los comportamientos para el dispositivo *A*, usuario *B*, proceso *C* y combinaciones de los mismos) se incrementan en respuesta a la observación de un comportamiento determinado o conjunto de comportamientos. Estos incrementos afectan el recuento agregado siempre que el comportamiento que dio lugar a incrementar la cuenta en particular esté designado como parte de la ventana de análisis enrollable; los comportamientos envejecerán y el recuento se reducirá en consecuencia a menos que el comportamiento sea designado para usarse como un comportamiento histórico.

En la OPERACIÓN 640 se calcula una puntuación de anomalía para el resultado de detección. En diversos aspectos, un analista o usuario administrativo puede seleccionar una o más fórmulas (tales como la **Fórmula 1**, dada anteriormente). En varios aspectos, un recuento sin procesar de todos los hechos observados en el servicio en línea 110 dentro de una determinada ventana de análisis se proporciona como un recuento de población, mientras que en otros aspectos un recuento de ámbito de los eventos observados en el servicio en línea 110 que se ajusten a un ámbito definido por el analista del servicio en línea 110 se proporcionan como un recuento de población. Además, los recuentos de subpoblación para el número de observaciones anteriores del comportamiento compartiendo el identificador calculado en la OPERACIÓN 610 se proporcionan con relación a la población sin procesar y las poblaciones de ámbito (si se define).

Las puntuaciones de anomalía proporcionan una representación de la medida en la que un determinado comportamiento ha sido observado anteriormente. En los aspectos en donde un recuento de población (sin procesar o en ámbito) cae por debajo de un umbral de población, un valor predeterminado para la puntuación de anomalía (por ejemplo, 100% anómala, 0% anómala) puede ser asignado en función de las preferencias del analista. De forma similar, cuando un recuento de subpoblación cae por debajo de un umbral de subpoblación, un valor predeterminado para la puntuación de anomalía (por ejemplo, 100% anómala, 0% anómala) puede ser asignado o el comportamiento puede ser "antirrebotado" para esperar y permitir que la subpoblación potencialmente crezca antes de asignar una puntuación de población.

Una o más de estas puntuaciones de anomalías, los recuentos de población y los recuentos de subpoblación se conservan como nuevos atributos de los resultados de detección sobre los que se basan y son transmitidos al detector de señales múltiples 160 en la OPERACIÓN 650. El método 600 puede concluir después de la OPERACIÓN 650 y se puede repetir de la OPERACIÓN 610 en respuesta a la recepción de un resultado de detección subsecuente.

La Figura 7 es un diagrama de flujo que muestra etapas generales involucradas en un método 700 ilustrativo para la detección de señales múltiples de ámbitos comprometidos. El método 700 es un ejemplo de sub-pasos de la OPERACIÓN 540 de la Figura 5. El método 700 comienza con la OPERACIÓN 710, en donde se seleccionan uno o más modelos predictivos 420. Los modelos predictivos 420 son seleccionados en base a una serie de razones, incluyendo, pero no limitado a: conjuntos de

características disponibles para el análisis; una exactitud o precisión predictiva en comparación con otros modelos; un comportamiento deseado para analizar; recursos de procesamiento disponibles; si se despliega un modelo para producción, entrenamiento o evaluación; etc. Uno o más modelos predictivos 420 puede ser seleccionado para un determinado ámbito que es analizado que corresponde a varios comportamientos que un analista u otro usuario administrativo desea buscar dentro del servicio en línea 110.

En la OPERACIÓN 720, se extraen las características de los resultados de detección calificados que corresponden al conjunto de características de los modelos predictivos seleccionados 420. Cada modelo predictivo 420 está entrenado para reconocer distintos comportamientos en el servicio en línea en función de las características de los resultados de detección y puede estar asociado con un vector determinado de característica que representa una o más características en un formato numérico (por ejemplo, en forma de una matriz de números). Ya que las características pueden incluir valores numéricos (por ejemplo, las puntuaciones de anomalías, los recuentos de población), valores de texto (por ejemplo, nombres de usuario, nombres de acción, nombres de proceso), y valores pseudo-numéricos (por ejemplo, una dirección IP, una marca de tiempo), las características son calificadas para su conversión en características en la OPERACIÓN 730. Un experto en la materia estará familiarizado con varias operaciones a través de las cuales se convierten valores no numéricos en valores numéricos para usarse como características. En varios aspectos, se aplica una operación de compresión o de formateo (por ejemplo, una función de presión sigmoidea) a las conversiones numéricas (y originalmente numéricas) de las características para dar formato al valor de característica para el consumo por el modelo predictivo 420.

Pasando a la OPERACIÓN 740, el modelo predictivo seleccionado 420 se pasa al vector de característica para generar una puntuación de confianza en cuanto a si el comportamiento(s) de los resultados de detección son maliciosos o benignos. El modelo predictivo 420 es un algoritmo que acepta uno o más vectores de característica (y, en algunos aspectos, las salidas de otros modelos predictivos 420) como entradas para producir una puntuación de confianza como una salida. La puntuación de confianza es una predicción que indica un nivel de certeza en cuanto a si un comportamiento representado por las entradas puede ser clasificado como malicioso o benigno. En varios aspectos, el modelo predictivo 420 se desarrollará a lo largo de muchas épocas de un proceso de aprendizaje continuo de máquina para predecir si un determinado comportamiento debería ser tratado como malicioso o benigno, y puede adaptar sus predicciones en función a la retroalimentación recibida del analista u otros usuarios administrativos y otros modelos a medida que el tiempo avanza a lo largo de sucesivas fases de aprendizaje.

Una vez que se genera una puntuación de confianza, ésta se almacena para la transmisión o uso posterior en la OPERACIÓN 750. Por ejemplo, la puntuación de confianza puede almacenarse en una memoria caché de resultados de señales múltiples 170 para su uso en un conjunto de entrenamiento para mejorar iterativamente los modelos predictivos 420 en una siguiente fase de aprendizaje de un proceso de aprendizaje de máquina. En otro ejemplo, la puntuación de confianza se almacena para su

transmisión a un generador de alertas 180, en donde se podrá determinar si desea generar una alerta para el comportamiento observado en función de la puntuación de confianza y lógica de alerta. El método 700 después puede concluir y se puede repetir la OPERACIÓN 710 en respuesta a la recepción de otro ámbito de resultados de detección para analizar.

Mientras que las implementaciones han sido descritas en el contexto general de módulos de programa que se ejecutan en conjunción con un programa de aplicación que se ejecuta en un sistema operativo en una computadora, los expertos en la materia reconocerán que pueden también implementarse aspectos en combinación con otros módulos de programa. Generalmente, los módulos de programa incluyen rutinas, programas, componentes, estructuras de datos y otros tipos de estructuras que realizan determinadas tareas o implementan tipos de datos abstractos particulares.

Los aspectos y funcionalidades aquí descritas pueden operar a través de una multitud de sistemas computacionales, incluyendo, sin limitación, sistemas de computadoras de escritorio, sistemas de cómputo alámbricos e inalámbricos, sistemas de cómputo móviles (por ejemplo, teléfonos móviles, netbooks, computadoras de tipo tableta o pizarra, notebook y computadoras laptop), dispositivos de mano, sistemas de multiprocesador, electrónica de consumidor programable o basada en microprocesador, minicomputadoras y computadoras centrales.

Además, de acuerdo con un aspecto, los aspectos y funciones aquí descritas operan sobre sistemas distribuidos (por ejemplo, sistemas de cómputo basados en nube), en donde la funcionalidad de la aplicación, la memoria, el almacenamiento y recuperación de datos y diversas funciones de procesamiento son operados remotamente desde el uno al otro a través de una red de computación distribuida, tal como la Internet o una intranet. De acuerdo con un aspecto, se muestran interfaces de usuario e información de diversos tipos mediante presentaciones de dispositivos de cómputo a bordo o a través de unidades de visualización remotas asociadas con uno o más dispositivos de cómputo. Por ejemplo, las interfaces de usuario e información de diversos tipos se muestran e interactúan con una superficie de pared sobre la cual las interfaces de usuario y la información de distintos tipos se proyectan. La interacción con la multitud de sistemas de cómputo con los que se practican las implementaciones incluyen entrada de pulsaciones de teclas, entrada de pantalla táctil, entrada de voz u otro audio, entrada de gestos en donde un dispositivo de cómputo asociado está equipado con funcionalidad de detección (por ejemplo, cámara) para capturar e interpretar los gestos del usuario para controlar la funcionalidad del dispositivo de cómputo, y similares.

Las Figuras 8, 9A y 9B y las descripciones asociadas proporcionan una discusión de una amplia variedad de entornos operativos en los que se practican los ejemplos. Sin embargo, los dispositivos y sistemas ilustrados y discutidos con respecto a las Figuras 8, 9A y 9B son para propósitos de ejemplo e ilustración y no se limitan a un gran número de configuraciones de dispositivos de cómputo que se utilizan para practicar los aspectos descritos en el presente documento.

La Figura 8 es un diagrama de bloques que ilustran los componentes físicos (es decir, *hardware*) de un dispositivo de computación 800 con el cual los ejemplos de la presente descripción pueden ser practicados. En una configuración básica, el dispositivo de cómputo 800 incluye al menos una unidad de

procesamiento 802 y una memoria de sistema 804. De acuerdo con un aspecto, dependiendo de la configuración y el tipo de dispositivo de cómputo, la memoria de sistema 804 incluye, pero no está limitado a, almacenamiento volátil (por ejemplo, memoria de acceso aleatorio), almacenamiento no volátil (por ejemplo, memoria de sólo lectura), memoria flash, o cualquier combinación de tales memorias. Según un aspecto, la memoria de sistema 804 incluye un sistema operativo 805 y uno o más módulos de programa 806 adecuados para ejecutar aplicaciones de *software* 850. De acuerdo con un aspecto, la memoria de sistema 804 incluye detector de anomalías 190. El sistema operativo 805, por ejemplo, es adecuado para controlar la operación del dispositivo de cómputo 800. Además, los aspectos son practicados en conjunción con una biblioteca gráfica, otros sistemas operativos o cualquier otro programa de aplicación y se limitan a una aplicación o sistema particular. Esta configuración básica se ilustra en la Figura 8 mediante los componentes dentro de una línea discontinua 808. De acuerdo con un aspecto, el dispositivo de cómputo 800 tiene características o funcionalidad adicionales. Por ejemplo, según un aspecto, el dispositivo de cómputo 800 incluye dispositivos de almacenamiento de datos adicionales (removible y/o no removible) como, por ejemplo, discos magnéticos, discos ópticos o cinta. Tal almacenamiento adicional se ilustra en la Figura 8 mediante un dispositivo de almacenamiento removible de 809 y un dispositivo de almacenamiento no removible 810.

Como se ha señalado anteriormente, de acuerdo con un aspecto, un número de módulos de programas y archivos de datos se almacenan en la memoria de sistema 804. Durante la ejecución de la unidad de procesamiento 802, los módulos de programa 806 (por ejemplo, detector de anomalías 190) realizan procesos, incluyendo, pero no limitado a, una o más de las etapas de los métodos 500, 600 y 700 ilustrados en las Figuras 5, 6 y 7. Según un aspecto, se utilizan otros módulos de programa de acuerdo con ejemplos e incluyen aplicaciones tales como correo electrónico y aplicaciones de contactos, aplicaciones de procesamiento de textos, aplicaciones de hojas de cálculo, aplicaciones de bases de datos, aplicaciones de presentación de diapositivas, programas de aplicación asistidos por dibujo o computadora, etc.

De acuerdo con un aspecto, el dispositivo de cómputo 800 tiene uno o más dispositivos de entrada 812 tal como un teclado, un ratón, un lápiz óptico, un dispositivo de entrada de sonido, un dispositivo de entrada táctil, etc. El dispositivo(s) de salida 814 tal como una pantalla, altavoces, una impresora, etc. también está incluido de acuerdo con un aspecto. Los dispositivos antes mencionados son ejemplos y se pueden utilizar otros. De acuerdo con un aspecto, el dispositivo de cómputo 800 incluye una o más conexiones de comunicación 816 que permiten la comunicación con otros dispositivos de cómputo 818. Ejemplos de conexiones de comunicación adecuadas 816 incluyen, pero no están limitados a, transmisor de radio frecuencia (RF), receptor y/o circuitería de transceptor; conductor común en serie universal (USB), puertos paralelos y/o en serie.

El término medio legible por computadora, tal como se utiliza aquí, incluye medios de almacenamiento. Los medios de almacenamiento de computadora incluyen medios volátiles y no volátiles, removibles y no removibles implementados en cualquier método o tecnología para el almacenamiento de información, tales como instrucciones legibles por computadora, estructuras de datos

o módulos de programa. La memoria de sistema 804, el dispositivo de almacenamiento removible 809 y el dispositivo de almacenamiento no removible 810 son todos ejemplos de medios de almacenamiento de computadora (es decir, almacenamiento en memoria). De acuerdo con un aspecto, los medios de almacenamiento por computadora incluyen RAM, ROM, memoria de sólo lectura programable y eléctricamente borrrable (EEPROM), memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro tipo de almacenamiento óptico, casetes magnéticos, cintas magnéticas, almacenamiento en discos magnéticos u otros dispositivos de almacenamiento magnético, o cualquier otro artículo de fabricación que se pueda utilizar para almacenar información y que puede ser accedido por el dispositivo de cómputo 800. Según un aspecto, cualquiera de dichos medios de almacenamiento por computadora forma parte del dispositivo de cómputo 800. Los medios de almacenamiento por computadora no incluyen una onda portadora u otra señal de datos propagada.

De acuerdo con un aspecto, los medios de comunicación se modalizan por instrucciones legibles por computadora, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, tal como una onda portadora u otro mecanismo de transporte e incluyen cualesquiera medios de entrega de información. De acuerdo con un aspecto, el término "señal de datos modulada" describe una señal que tiene una o más características fijadas o cambiadas de tal manera como que codifica la información en la señal. A modo de ejemplo, y sin limitación, los medios de comunicación incluyen medios alámbricos tal como una red alámbrica o conexión de cable directa y medios inalámbricos tales como medios acústicos, de radiofrecuencia (RF), infrarrojos y otros medios inalámbricos.

Las Figuras 9A y 9B muestran un dispositivo de cómputo móvil 900, por ejemplo, un teléfono móvil, un teléfono inteligente, una computadora personal tipo tableta, una computadora portátil y similares, con el cual los aspectos pueden ser practicados. Con referencia a la Figura 9A, se ilustra un ejemplo de un dispositivo de cómputo móvil 900 para implementar los aspectos. En una configuración básica, el dispositivo de cómputo móvil 900 es una computadora portátil que tiene tanto elementos de entrada como elementos de salida. El dispositivo de cómputo móvil 900 normalmente incluye una pantalla 905 y uno o más botones de entrada 910 que permiten al usuario introducir información en el dispositivo de cómputo móvil 900. Según un aspecto, la pantalla 905 del dispositivo de cómputo móvil 900 funciona como un dispositivo de entrada (por ejemplo, una pantalla táctil). Si se incluye, un elemento de entrada lateral opcional 915 permite más entrada de usuario. De acuerdo con un aspecto, el elemento de entrada lateral 915 es un conmutador giratorio, un botón, o cualquier otro tipo de elemento de entrada manual. En ejemplos alternativos, el dispositivo de cómputo móvil 900 incorpora más o menos elementos de entrada. Por ejemplo, la pantalla 905 puede no ser una pantalla táctil, en algunos ejemplos. En ejemplos alternativos, el dispositivo de cómputo móvil 900 es un sistema de teléfono portátil, como un teléfono celular. De acuerdo con un aspecto, el dispositivo de cómputo móvil 900 incluye un teclado opcional 935. De acuerdo con un aspecto, el teclado opcional 935 es un teclado físico. Según otro aspecto, el teclado opcional 935 es un teclado "suave" generado en la pantalla táctil. En varios aspectos, los elementos de salida incluyen la pantalla 905 para mostrar una interfaz gráfica de usuario (GUI), un indicador visual 920 (por ejemplo, un diodo emisor de luz) y/o un transductor de audio 925 (por ejemplo, un altavoz). En

algunos ejemplos, el dispositivo de cómputo móvil 900 incorpora un transductor de vibraciones para proporcionar al usuario una retroalimentación táctil. En otro ejemplo, el dispositivo de cómputo móvil 900 incorpora puertos de entrada y/o salida, tales como una entrada de audio (por ejemplo, un micrófono), una salida de audio (por ejemplo, una toma de auriculares) y una salida de vídeo (por ejemplo, un puerto HDMI) para enviar señales a o recibir señales desde un dispositivo externo. En otro ejemplo, el dispositivo de cómputo móvil 900 incorpora un puerto de dispositivo periférico 940, tal como una entrada de audio (por ejemplo, un micrófono), una salida de audio (por ejemplo, una toma de auriculares) y una salida de vídeo (por ejemplo, un puerto HDMI) para enviar señales a o recibir señales desde un dispositivo externo.

La Figura 9B es un diagrama de bloques que ilustran la arquitectura de un ejemplo de un dispositivo de cómputo móvil. Es decir, el dispositivo de cómputo móvil 900 incorpora un sistema (es decir, una arquitectura) 902 para implementar algunos ejemplos. En un ejemplo, el sistema 902 se implementa como un "teléfono inteligente" capaz de ejecutar una o más aplicaciones (por ejemplo, navegador, correo electrónico, calendarios, administradores de contactos, clientes de mensajería, juegos, y clientes/jugadores multimedia). En algunos ejemplos, el sistema 902 está integrado como un dispositivo de cómputo, como un asistente digital personal integrado (PDA) y un teléfono inalámbrico.

Según un aspecto, uno o más programas de aplicación 950 están cargados en la memoria 962 y se ejecutan en o en asociación con el sistema operativo 964. Ejemplos de los programas de aplicación incluyen programas de marcador de teléfono, programas de correo electrónico, programas de administración de información personal (PIM), programas de procesamiento de texto, programas de hojas de cálculo, programas de exploradores de Internet, programas de mensajería, y así sucesivamente. Según un aspecto, el detector de anomalías 190 está cargado en la memoria 962. El sistema 902 también incluye un área de almacenamiento no volátil 968 dentro de la memoria 962. El área de almacenamiento no volátil 968 se utiliza para almacenar información persistente que no debe perderse si el sistema 902 está apagado. Los programas de aplicación 950 pueden utilizar y almacenar la información en el área de almacenamiento no volátil 968, tal como correo electrónico u otros mensajes usados por una aplicación de correo electrónico, y similares. Una aplicación de sincronización (no mostrada) también reside en el sistema 902 y está programada para interactuar con una aplicación de sincronización correspondiente residente en una computadora huésped para mantener la información almacenada en el área de almacenamiento no volátil 968 sincronizada con la correspondiente información almacenada en la computadora huésped. Como se debe apreciar, otras aplicaciones pueden ser cargadas en la memoria 962 y se ejecutan en el dispositivo de cómputo móvil 900.

De acuerdo con un aspecto, el sistema 902 tiene un suministro de energía 970, el cual está implementado como una o más baterías. Según un aspecto, el suministro de energía 970 incluye, además, un suministro de energía externa, tal como un adaptador de CA o una base de acoplamiento energizada que suplementa o recarga las baterías.

De acuerdo con un aspecto, el sistema 902 incluye una radio 972 que realiza la función de transmitir y recibir comunicaciones de radio frecuencia. La radio 972 facilita la conectividad inalámbrica

entre el sistema 902 y el "mundo exterior", a través de una portadora de comunicaciones o proveedor de servicio. Las transmisiones a y de la radio 972 se llevan a cabo bajo el control del sistema operativo 964. En otras palabras, las comunicaciones recibidas por la radio 972 pueden ser difundidas a los programas de aplicación 950 a través del sistema operativo 964, y viceversa.

De acuerdo con un aspecto, el indicador visual 920 se utiliza para proporcionar notificaciones visuales y/o una interfaz de audio 974 se utiliza para producir notificaciones audibles a través del transductor de audio 925. En el ejemplo ilustrado, el indicador visual 920 es un diodo emisor de luz (LED) y el transductor de audio 925 es un altavoz. Estos dispositivos pueden ser directamente acoplados al suministro de energía 970, de modo que cuando se activan, permanecen en una duración determinada por el mecanismo de notificación, aunque el procesador 960 y otros componentes podrían cerrar para conservar la energía de la batería. El LED puede ser programado para permanecer indefinidamente hasta que el usuario tome medidas para indicar el estado de encendido del dispositivo. La interfaz de audio 974 se utiliza para proporcionar señales audibles a y recibir señales acústicas del usuario. Por ejemplo, además de estar acoplada al transductor de audio 925, la interfaz de audio 974 también puede acoplarse a un micrófono para recibir entrada audible, tal como para facilitar una conversación telefónica. De acuerdo con un aspecto, el sistema 902 incluye además una interfaz de vídeo 976 que permite una operación de una cámara 930 para grabar imágenes fijas, flujo de video y similares.

De acuerdo con un aspecto, un dispositivo de cómputo móvil 900 que implementa el sistema 902 tiene características adicionales o funcionalidad. Por ejemplo, el dispositivo de cómputo móvil 900 incluye dispositivos de almacenamiento de datos adicionales (removibles y/o no removibles) tal como, por ejemplo, discos magnéticos, discos ópticos o cinta. Tal almacenamiento adicional se ilustra en la Figura 9B por el área de almacenamiento no volátil 968.

Según un aspecto, los datos/información generada o capturada por el dispositivo de cómputo móvil 900 y almacenada a través del sistema 902 se almacenan localmente en el dispositivo de cómputo móvil 900, tal como se ha descrito anteriormente. De acuerdo con otro aspecto, los datos son almacenados en cualquier número de medios de almacenamiento que son accesibles por el dispositivo a través de la radio 972 o a través de una conexión por cable entre el dispositivo de cómputo móvil 900 y un dispositivo de cómputo independiente asociado con el dispositivo de cómputo móvil 900, por ejemplo, una computadora de servidor en una red de computación distribuida, tal como Internet. Se debe apreciar que dichos datos/información son accesibles a través del dispositivo de cómputo móvil 900, a través de la radio 972 o a través de una red de computación distribuida. Asimismo, de acuerdo con un aspecto, tales datos/información se transfieren fácilmente entre dispositivos de cómputo para el almacenamiento y la utilización de acuerdo con medios conocidos de transferencia y almacenamiento de datos/información, incluyendo correo electrónico y sistemas colaborativos de compartición de datos/información.

Por ejemplo, las implementaciones se describen anteriormente con referencia a los diagramas de bloques y/o ilustraciones operacionales de métodos, sistemas y productos de programa de computadora de acuerdo con los aspectos. Las funciones/actos señalados en los bloques pueden ocurrir fuera del orden tal como se muestra en cualquier diagrama de flujo. Por ejemplo, dos bloques mostrados en

sucesión pueden de hecho ser ejecutados sustancialmente de manera concurrente o los bloques pueden a veces ser ejecutados en el orden inverso, dependiendo de la funcionalidad/actos involucrados.

La descripción e ilustración de uno o más ejemplos proporcionados en esta solicitud no pretenden limitar o restringir el alcance tal como se reclama en modo alguno. Los aspectos, ejemplos y detalles proporcionados en esta solicitud son considerados suficientes para transmitir la posesión y permitir a otros hacer y usar el mejor modo. Las implementaciones no deben interpretarse como limitantes a cualquier aspecto, por ejemplo, o detalle proporcionado en esta solicitud. Independientemente de si se muestra y describe en combinación o por separado, las distintas características (tanto estructurales como metodológicas) están destinados a ser selectivamente incluidas u omitidas para producir un ejemplo con un determinado conjunto de características. Habiendo sido proporcionados con la descripción e ilustración de la presente solicitud, un experto en la materia puede imaginar variaciones, modificaciones y ejemplos alternativos cayendo dentro del espíritu de los aspectos más amplios del concepto inventivo general modalizado en esta solicitud que no se aparten del alcance más amplio.