Lineamientos de Seguridad IoT para el Ecosistema de Servicios de IoT

Lineamientos de Seguridad IoT para el Ecosistema de Servicios de IoT

Versión 2.0

26 de Octubre 2017

Este es un documento de referencia permanente no vinculante

Clasificación de Seguridad: No-confidencial

El acceso y distribución de este documento está restringido a las personas permitidas por la clasificación de seguridad. Este documento es confidencial para la Asociación y está sujeto a la protección de derechos de autor. Este documento se utilizará únicamente para los fines para los que ha sido suministrado y la información contenida en él no debe divulgarse ni ponerse a disposición en ninguna otra forma posible, en su totalidad o en parte, a personas distintas a las permitidas bajo la clasificación de seguridad sin la aprobación previa por escrito de la Asociación.

Aviso Legal

La Asociación GSM ("Asociación") no acepta ninguna responsabilidad por la representación, garantía o compromiso (expreso o implícito) con respecto al contenido de este documento, así como por la exactitud o integridad o actualidad de la información. La información contenida en este documento puede estar sujeta a cambios sin previo aviso.

Aviso Antimonopolio

La información aquí contenida está en total conformidad con la política de cumplimiento antimonopolio de la Asociación GSM.

Tabla de Contenidos

1 Introducción

1.1 Introducción al Conjunto de Documentos sobre la Seguridad en IoT de la GSMA

Este documento es una parte de un conjunto de documentos sobre lineamientos de seguridad IoT de la GSMA que están destinados a ayudar a la naciente industria del "Internet de las cosas" (IoT) a establecer una comprensión común alrededor de los problemas de seguridad del IoT. El conjunto de documentos de lineamientos no vinculantes promueve una metodología para el desarrollo de servicios de IoT seguros que permite aplicar las mejores prácticas con respecto a la seguridad durante todo el ciclo de vida del servicio. Los documentos proporcionan recomendaciones sobre cómo reducir las amenazas comunes de seguridad y debilidades dentro de los servicios de IoT.

A continuación se muestra la estructura del conjunto de documentos de lineamientostos de seguridad IoT de la GSMA. Se recomienda que el documento 'CLP.11 Descripción General de los lineamientos de Seguridad IoT de la GSMA' [1] se lea primero como base para entender los conceptos básicos antes de leer los otros documentos de apoyo.

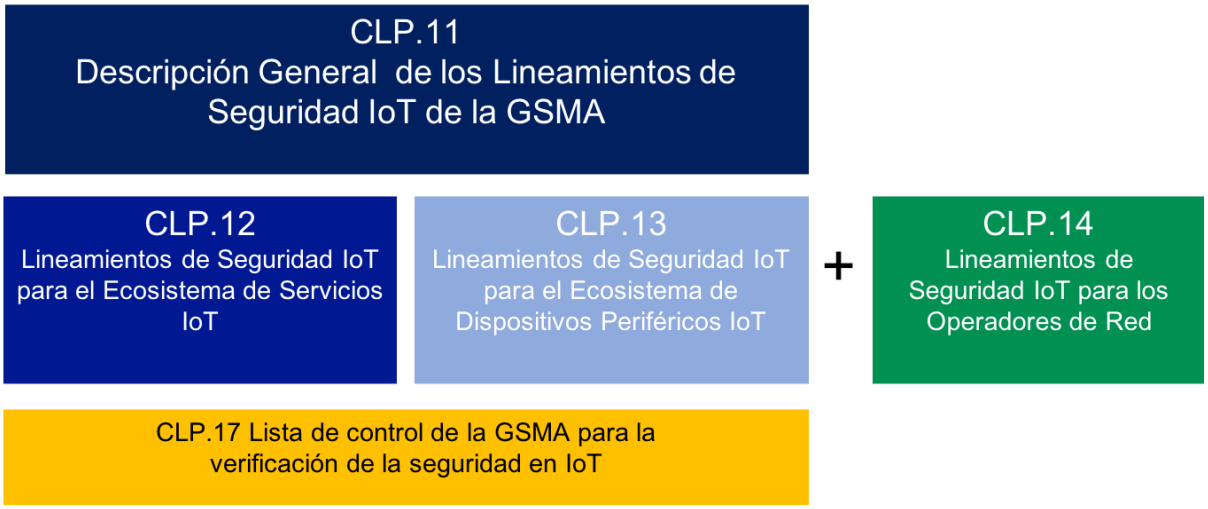

Figura 1 - Estructura del Conjunto de Documentos

Se aconseja a los operadores de red, proveedores de servicios IoT y otros socios en la cadena de valor de IoT, leer el documento GSP CLP.14 "Lineamientos de seguridad del IoT para operadores de red" [13] que proporciona lineamientos de seguridad de alto nivel a operadores de red que pretenden proporcionar servicios a proveedores de servicios IoT, para garantizar la seguridad del sistema y la privacidad de los datos.

1.1.1 Lista de control de la GSMA para la verificación de la seguridad en IoT

Una lista de control y verificación de seguridad IoT se puede encontrar en el documento CLP.17 [16]. Este documento permite a los proveedores de productos, servicios y componentes de IoT comprobar que sus productos son conformes a los lineamientos de seguridad IoT de la GSMA.

Al rellenar la lista de verificación arriba mencionada permitirá a cualquier entidad o empresa demostrar las medidas de seguridad que han tomado para proteger sus productos, servicios y componentes de los riesgos de Cyber-seguridad.

Se pueden obtener constancias de verificación enviando a la GSMA una declaración rellena con los puntos de la lista. Por favor vea el siguiente link en el portal de la GSMA para más información:

https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

1.2 Objetivo del Documento

Esta guía se utilizará para evaluar todos los componentes en un producto de IoT o servicio desde la perspectiva del ecosistema de servicios. El Ecosistema de Servicios incluye todos los componentes que conforman el núcleo de la infraestructura de IoT. Componentes en este ecosistema son, por ejemplo, servicios, servidores, conjuntos de bases de datos, elementos de la red y otras tecnologías que se utilizan para manejar los componentes internos de cualquier producto o servicio.

El ámbito de este documento se limita a dar recomendaciones para el diseño e implementación de servicios de IoT y de elementos de red.

Este documento no está concebido para la creación de especificaciones o estándares de IoT nuevos, pero hará referencias a soluciones ya existentes, así como a estándares y mejores prácticas de la industria.

Este documento no pretende acelerar la obsolescencia de servicios IoT ya existentes. La compatibilidad con los servicios IoT ya existentes de los operadores de red debe mantenerse cuando estos se consideren adecuadamente seguros.

Se hace notar que el cumplimiento de las normas a nivel nacional y de las regulaciones en un territorio concreto, son de obligado cumplimiento y pueden en cualquier momento anular cualquier pauta que se pueda encontrar en este documento.

1.3 Audiencia a la que se Dirige el Documento

A quien se dirige este documento:

- Proveedores de servicios de IoT: empresas u organizaciones que buscan desarrollar productos y servicios conectados nuevos e innovadores. Algunos de los muchos campos en los que operan los proveedores de servicios IoT incluyen hogares inteligentes, ciudades inteligentes, automoción, transporte, salud, servicios públicos y productos electrónicos de consumo.
- Fabricantes de dispositivos IoT: desde los desarrolladores de HW IoT a proveedores de servicios IoT para hacer posibles los servicios IoT.
- Desarrolladores de IoT que crean servicios de IoT para los proveedores de servicios de IoT.
- Operadores de red que brindan servicios a proveedores de servicios de IoT o que son a su vez proveedores directos de servicios IoT.

1.4 Definiciones

Término	Descripción
Lista de Control de Accesos	Lista de permisos referentes a un objeto con capacidad de
Nombre del punto de acceso	Identificador de un punto de conexión de red al que se conecta un dispositivo periférico. Están asociados a diferentes tipos de servicio, y en muchos casos son configurados por el operador de red.
Atacante o “hacker”	Un pirata informático, un agente inteligente (atacante), un atacante, un estafador u otra amenaza maliciosa para un servicio de IoT. Esta amenaza podría provenir de un solo delincuente, del crimen organizado, por terrorismo, de gobiernos hostiles y sus agencias, por espionaje industrial, de grupos de piratería, de activistas políticos, de hackers 'aficionados', investigadores, así como infracciones de seguridad y privacidad no intencionadas.
La “nube”	Una red de servidores remotos en Internet que aloja, almacena, administra y procesa aplicaciones y sus datos.
Contenedor	Tecnología que hace posible correr múltiples sistemas aislados, o contenedores, en un servidor central.
UICC embebido (eUICC)	Es un UICC que soporta la provisión remota de subscripciones de red o servicio que a su vez autentica, como se ha especificado en la GSMA.
Cliente final	Es el consumidor del servicio IoT proporcionado por el proveedor de servicios IoT. Se puede dar el caso de que el cliente final y el proveedor de servicios IoT sean el mismo actor, como por ejemplo una compañía suministradora de servicios públicos.
Ecosistema de Dispositivos Periféricos	Cualquier ecosistema de dispositivos sencillos, dispositivos complejos y pasarelas que conectan el mundo físico al mundo digital de formas novedosas. Ver CLP.11 [1] para más información.
Secreto hacia delante	Es una propiedad de los protocolos de comunicación segura: un protocolo de comunicación seguro se dice que tiene “secreto hacia delante” si el compromiso de claves a largo plazo no compromete las claves de sesión pasadas.
Internet de las Cosas	La Internet de las Cosas (IoT) describe la coordinación entre múltiples máquinas, dispositivos y aparatos conectados a Internet a través de múltiples redes. Estos dispositivos incluyen objetos cotidianos tales como tabletas y electrónica de consumo y otros dispositivos o máquinas tales como vehículos, monitores y sensores equipados con capacidades de comunicación que les permitan enviar y recibir datos.
Dispositivo Periférico IoT	Es un término genérico utilizado para dispositivos complejos periféricos o pasarelas de IoT.
Servicio IoT	Cualquier programa de computadora que utiliza datos desde dispositivos de IoT para prestar el servicio.
Ecosistema de servicios IoT	El conjunto de servicios, plataformas, protocolos y otras tecnologías necesarias para proporcionar capacidades y recopilar datos de Dispositivos Periféricos implementados a “pie de campo””. Ver la sección 3.1 para más información.
Proveedor de un Servicio IoT	Las empresas u organizaciones que buscan desarrollar nuevos productos y servicios conectados innovadores.
Operador de Red	El operador y propietario de la red de comunicaciones que conecta un dispositivo periférico de IoT a un ecosistema de servicios IoT.

Término	Descripción
Raíz de Confianza organizacional	Un conjunto de políticas criptográficas y procedimientos que dictan cómo las identidades, las aplicaciones y comunicaciones pueden y deben asegurarse mediante cifrado.
Grupo de Seguridad	Actúa como un cortafuegos virtual que controla el tráfico para uno o más instancias de servidores virtuales.
Base de Computación Confiable	Una Base de Computación Confiable (TCB) es un conglomerado de algoritmos, políticas y secretos dentro de un producto o servicio. El TCB actúa como un módulo que permite que el producto o servicio mida su propia fiabilidad, mida la autenticidad de los pares de la red, verifique la integridad de los mensajes enviados y recibidos a/o desde el producto o servicio, y más. El TCB funciona como la plataforma de seguridad principal sobre la cual se pueden construir productos y servicios seguros. Los componentes de una TCB cambiarán según el contexto (una TCB hardware para Dispositivos Periféricos o una TCB software para servicios en la nube), pero los objetivos, servicios, procedimientos y políticas abstractas deberían ser muy similares.
UICC	Elemento seguro entendido como plataforma especificada en ETSI TS 102 221 que puede soportar múltiples aplicaciones de autenticación estandarizadas para una red o servicio dentro de distintos dominios de seguridad. Puede ser integrada y encapsulada en varios formatos especificados en ETSI TS 102 671.
Red Privada Virtual	Partición lógica, segura y separada de una red para permitir el uso dedicado por un determinado conjunto de servicios de cliente. Llamado así porque la VPN es privada con respecto al resto de la red y, por lo tanto, actúa como una red virtualizada por derecho propio.

1.5 Abreviaciones

Término	Descripción
3GPP	Asociación de proyectos de 3ra generación (“3rd Generation Project Partnership”)
ACL	Lista de Control de Accesos (“Access Control List”)
API	Interfaz del programa de Aplicación (“Application Program Interface”)
APN	Nombre del punto de Acceso (“Access Point Name”)
CERTS	Equipos de Respuesta a Emergencias Informáticas (“Computer Emergency Response Teams”)
CLP	Programa de la Vida Conectada (“GSMA’s Connected Living Programme”)
DDoS	Denegación de Servicio Distribuido (“Distributed Denial of Service”)
GSMA	Asociación GSM (“GSM Association”)
HSM	Módulo de Seguridad Hardware (“Hardware Security Module”)
IoT	Internet de las cosas (“Internet of Things”)
IP	Protocolo Internet (“Internet Protocol”)
SQL	Lenguaje de Consulta Estructurada (“Structured Query Language”)
TCB	Base de Computación Confiable (“Trusted Computing Base”)
VM	Máquina Virtual (“Virtual Machine”)
VPN	Red Privada Virtual (“Virtual Private Network”)

Término	Descripción
WAF	Cortafuegos de Aplicación Web ("Web Application Firewall")

1.6 Referencias

Ref	Número de Documento	Título
[1]	CLP.11	IoT Security Guidelines Overview Document
[2]	CLP.12	IoT Security Guidelines for IoT Service Ecosystem
[3]	CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem
[4]	CLP.14	IoT Security Guidelines for Network Operators
[5]	n/a	OWASP Secure Application Design Project https://www.owasp.org
[6]	n/a	TCG Trusted Platform Module http://www.trustedcomputinggroup.org
[7]	n/a	TCG Guidance for Securing IoT http://www.trustedcomputinggroup.org
[8]	n/a	OAuth 2.0 http://oauth.net/2/
[9]		OpenID Foundation http://openid.net/foundation/
[10]	n/a	GSMA Mobile Connect https://mobileconnect.io/
[11]	GPC_SPE_034	GlobalPlatform Card Specification www.globalplatform.org/specificationscard.asp
[12]	GPD_SPE_010	GlobalPlatform TEE Internal Core API Specification www.globalplatform.org/specificationsdevice.asp
[13]	CLP.17	GSMA IoT Security Assessment Checklist https://www.gsma.com/iot/iot-security-assessment/
[14]	n/a	ETSI TC SmartM2M specifications www.etsi.org
[15]	n/a	oneM2M Specifications www.onem2m.org
[16]	3GPP TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) www.3gpp.org

2 El Modelo de Servicio

Los productos y servicios modernos de IoT requieren de un Ecosistema de Servicios para proporcionar significado, funcionalidad y valor a los Dispositivos Periféricos, socios y usuarios. Dependiendo de la complejidad de las aplicaciones disponibles a través de la oferta de IoT, la infraestructura puede ser amplia y estar compuesta de muchos tipos

diferentes de servicios y puntos de acceso al servicio. Alternativamente, la infraestructura puede ser muy rudimentaria para aplicaciones más sencillas.

Independientemente del formato, el Ecosistema de Servicios actúa como el nexo de funcionalidad y comunicación para cada vertiente característica de la tecnología de IoT en general. Todos los otros ecosistemas dependen del ecosistema de servicios para la autenticación jerárquica, la conectividad con los usuarios, la disponibilidad, la administración y otras tareas críticas para el funcionamiento cotidiano de IoT. Para llevar a cabo estas tareas, el Ecosistema de Servicios está compuesto por una cantidad variable de capas necesarias para cumplir los objetivos de la infraestructura. Las agrupaciones de bases de datos, los servidores de aplicaciones, los servidores proxy de aplicaciones y otro tipo de elementos de infraestructura son un ejemplo de una capa que se encontraría en muchas implementaciones tipo. Como se deja entrever en el siguiente diagrama, los Ecosistemas de Red y de Dispositivos Periféricos dependen de la funcionalidad del “core” del Ecosistema de Servicios.

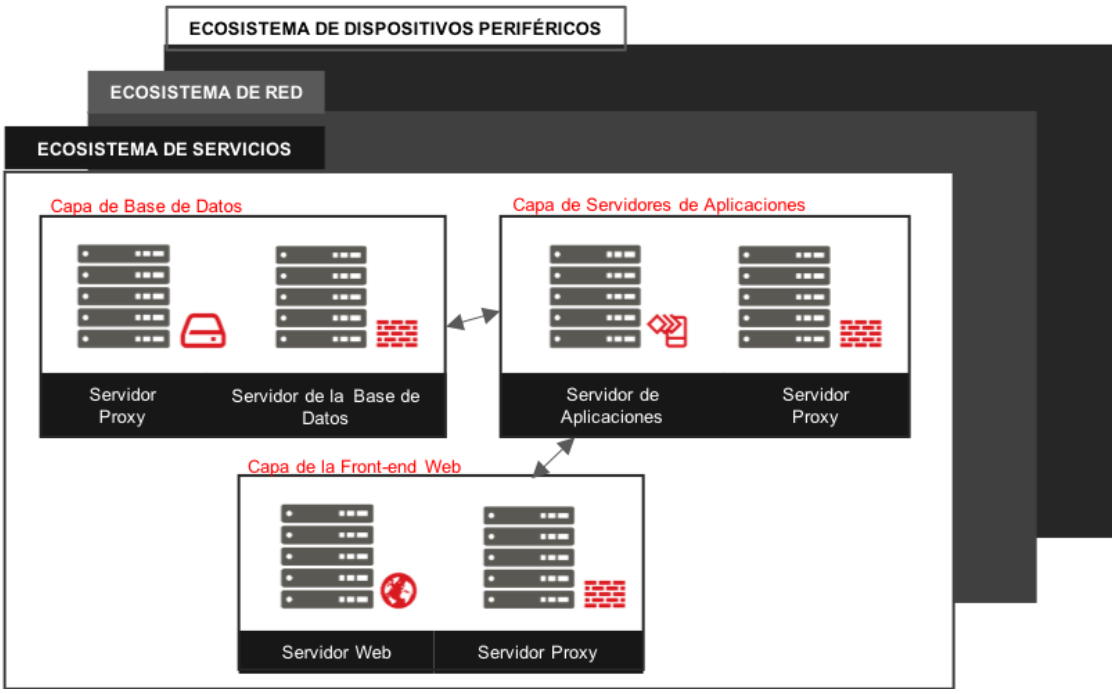

Figura 2 - Dependencias que se Articulan en el Ecosistema de Servicios

Algunos ejemplos de Ecosistemas de servicios modernos incluyen, entre otros:

- Soluciones basadas en infraestructuras en la nube
- Implementaciones de aplicaciones basadas en contenedores
- Entornos tradicionales de centros de datos en servidores
- Agrupación de bases de datos
- Agrupación de servicios para entornos de aplicaciones web

Si bien cada uno de estos entornos ejemplo pueden parecer muy diferentes en su diseño, topología e implementación, se basan en los mismos principios con respecto el tránsito de datos e información hacia y desde una aplicación.

Todos los sistemas informáticos modernos requieren un punto de entrada, conocido como punto de acceso al servicio, hacia la infraestructura de una aplicación. Los subsistemas internos que crean contenido y contexto para esa aplicación deben ser capaces de procesar datos desde redes y entornos seguros y confiables. Los datos deben almacenarse en algún lugar, luego enviarse a la capa de servicio que responde o envía comandos autorizados a varios componentes dentro del mismo ecosistema u otros ecosistemas con sus redes asociadas.

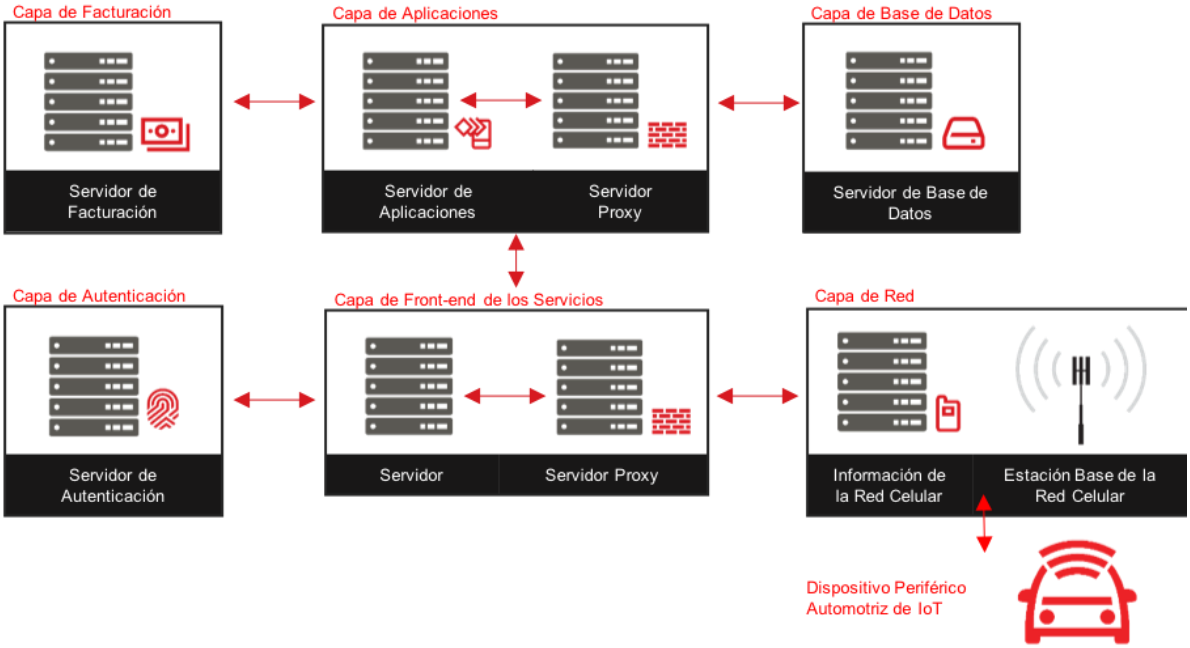

Figura 3 – Una Muestra de un Ecosistema de Servicios

Independientemente de qué tecnologías, modernas o tradicionales, se utilicen para implementar este marco estándar, la información se procesará, servirá y autenticará utilizando protocolos y tecnologías comprobadas por la industria. Si bien las topologías y abstracciones para entornos de procesamiento han cambiado sutilmente para ajustarse a los requisitos modernos de velocidad, potencia de cómputo y almacenamiento, las tecnologías utilizadas para implementar estas mejoras tecnológicas son, en esencia, las mismas. Por ejemplo, cada capa generalmente contiene un proxy o un sistema de cortafuegos que administra la conectividad hacia y desde un conjunto de servidores de un tipo específico. Los servicios de facturación residirán en una capa de facturación. Los servidores de aplicaciones residen en una capa específica para las aplicaciones. Los servicios de base de datos se deben administrar dentro de una capa de base de datos. Todos estos sistemas funcionan en conjunto en función de las reglas de transmisión de datos que se programan y utilizan en los servidores proxy.

Como resultado, el modelo de seguridad para el Ecosistema de Servicios se puede dividir fácilmente en un conjunto de componentes. Estos componentes se describirán en este documento.

3 El Modelo de Seguridad

La seguridad en entornos de servicios para Dispositivos Periféricos se puede diseñar utilizando elementos comunes de infraestructura, estrategias y políticas, independientemente de la topología o las innovaciones utilizadas para crear una arquitectura de aplicaciones. Cada detalle del Ecosistema de Servicios se puede dividir en componentes. Estos componentes deben asegurarse individualmente, utilizando siempre metodologías similares.

Por ejemplo, considere los componentes comunes en la creación de un servicio simple que sea capaz de enviar consultas y respuestas desde y hacia dispositivos periféricos, socios y usuarios. Este modelo debe contener, pero no se limita a, las siguientes capas:

- Una capa de servicios web
- Una capa de servidor de aplicaciones
- Una capa de base de datos
- Una capa de autenticación
- Una capa de red
- Varias capas de aplicaciones de terceros, incluyendo por ej. una capa de facturación

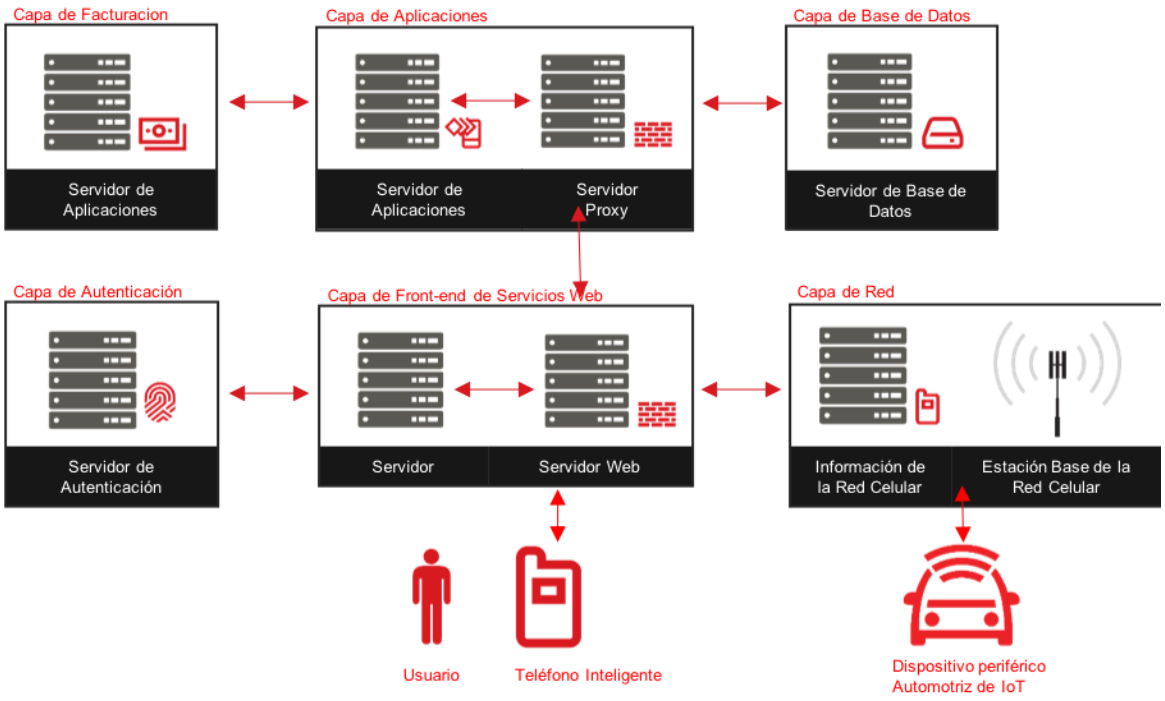

Figura 4 – Un Ejemplo de un Ecosistema de Servicios con Capas Separadas en la Arquitectura.

Incluso si solo hay un servidor en cada capa, es más eficiente desde el punto de vista arquitectónico separar cada concepto lógico en su propia capa. Esto también ayuda a aislar una capa de una tecnología de otras capas en caso de un compromiso o riesgo, o si el sistema necesita ampliarse para atender más transacciones.

Si se piensa en un tipo de sistema desde la perspectiva de un tipo de capa, puede ser más fácilmente asegurado, escalado según la demanda, apagado o en proceso de desconexión o retirada del mercado. El único requisito es una API que sea lo suficientemente versátil como para ser mejorada o ajustada durante toda la vida útil de la capa en cuestión. La definición de esta API está fuera del alcance de este documento. Sin embargo, las recomendaciones con respecto a los atributos de seguridad de alto nivel de la API que la organización elija o defina se analizarán aquí.

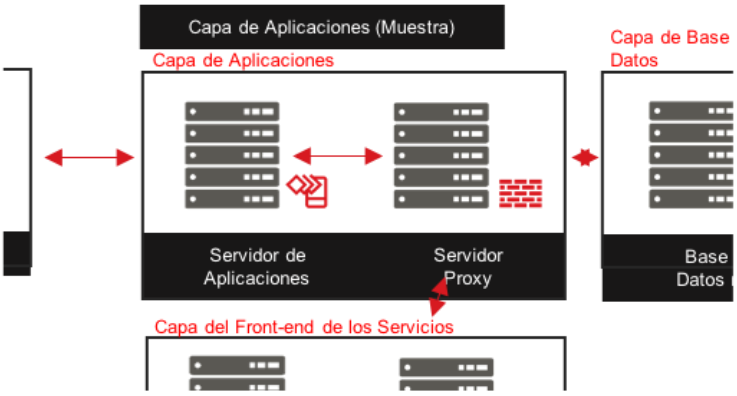

Figura 5 – Una Capa de Aplicaciones Protegida por Tecnologías de Cortafuegos

En el ejemplo anterior, se proporciona una descripción de capa un poco más completa. La única mejora que se necesita para representar la capa es un servidor proxy. Este servidor proxy es solo un descriptor que representa la tecnología de seguridad real que se empleará dentro de la capa. Independientemente de si el control real es un cortafuegos hardware, cortafuegos software, grupos de seguridad, listas de control de acceso (ACL) u otra tecnología, habrá un componente que asegura el control de flujos de datos de entrada y salida en nombre de la capa.

Al elegir o definir una API, la empresa debe considerar las especificaciones existentes que pueden resolver las inquietudes del equipo de ingeniería. La organización debe considerar en particular las siguientes especificaciones:

- ETSI SmartM2M TS 102 690, ETSI SmartM2M TS 102 921 [14]
- oneM2M TS-0001, oneM2M TS-0003 [15]
- 3GPP TS 33.220 [16]

Para los componentes de acceso público, como la capa de “front-end” del servicio, la única mejora que necesita el modelo es un componente de seguridad adicional para:

- Protección contra un ataque Distribuido de Denegación de Servicio (DDoS)
- Balanceo de Carga
- Redundancia
- Capacidad opcional de cortafuego de aplicaciones web (WAF)

Las tecnologías mencionadas anteriormente deben implementarse para que cualquier servicio funcione correctamente y para garantizar que el servicio que protegen esté

disponible incluso en entornos con recursos limitados. La definición de estos componentes está fuera del alcance de este documento, pero se puede encontrar información más detallada refiriéndose a las siguientes entidades:

- La alianza de seguridad en la nube
- Estándares NIST de computación en la nube
- FedRAMP
- Lineamientos de gestión de red de Cisco

Otros atributos necesarios para que una capa funcione de forma segura es la definición del servidor. Esto se define mediante controles administrativos, de aplicación y del sistema operativo internos a la plataforma elegida por el equipo de ingeniería.

Si bien no es exhaustiva, una lista de cuestiones fundamentales relativas al entorno de la plataforma se detalla a continuación:

- Iniciar sesión en un servicio de registro centralizado
- Autenticación y autorización administrativa
- Imposición de la seguridad en las comunicaciones
- Copia de seguridad, restauración y duplicado de datos
- Separación de tareas de aplicación
- Sistema de Supervisión e Integridad

3.1 Ataques a la Infraestructura de Red

Los adversarios que intenten comprometer al Dispositivo Periférico del servicio desde la perspectiva de red supondrán que hay debilidades en la forma en que las entidades se comunican y vulnerabilidades en los servicios expuestos a través de los puntos de acceso al servicio. Estos ataques suponen que una posición privilegiada en la red equivale a una posición de poder sobre el canal de comunicaciones.

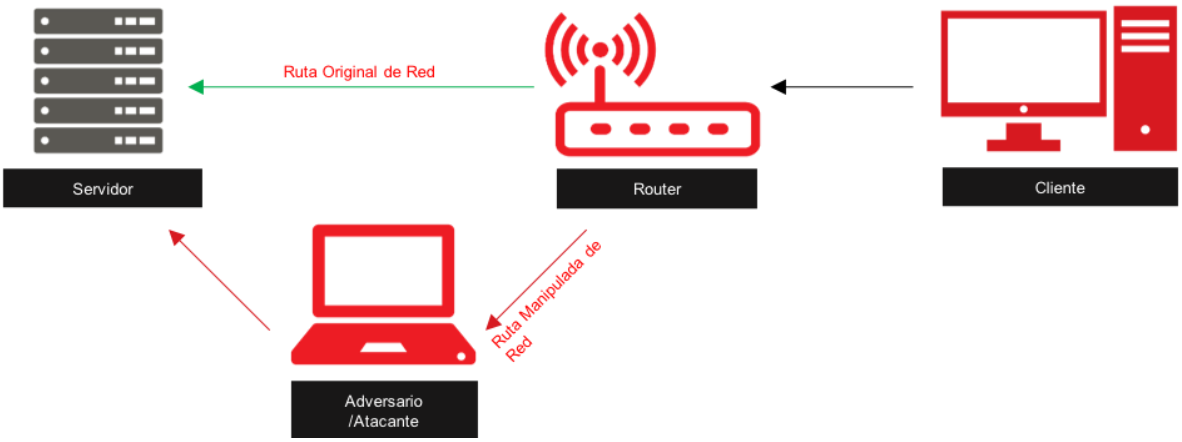

Figura 6 – Un Ejemplo de un Ataque Tipo "Man In The Middle"

La forma más común de ataque en este modelo es el ataque “Man-In-The-Middle” (MITM). Este ataque supone que no hay autenticación de pares, autenticación de pares unilateral o

autenticación mutua interrumpida en el canal de comunicaciones. El objetivo de un adversario es suplantar un lado de la conversación para forzar al otro socio en la comunicación a realizar acciones en su nombre. Este ataque puede evitarse forzando la autenticación mutua, que requiere una Raíz de Confianza Organizativa bien definida, una Base de Computación Confiable (TCB) y un modelo de comunicaciones.

Otros ataques son, por ejemplo, ataques contra el secreto hacia delante, análisis de comunicaciones cifradas y ataques de canal lateral. Estos deben ser evitados usando protocolos, algoritmos y estándares de criptografía adecuados.

Estos ataques son difíciles y requieren acceso a la infraestructura de red, ya sea internamente en una organización, desde la infraestructura central de Internet entre una organización y sus socios o el Ecosistema de Dispositivos Periféricos, o en la infraestructura cercana a los Dispositivos Periféricos. El ataque más simple y común es tratar de manipular la infraestructura de red del Dispositivo Periférico, como una red Wifi, Ethernet o celular, para obtener una posición de privilegio entre el Servicio y su par.

Los ataques contra la infraestructura de un único Dispositivo Periférico están restringidos a ese dispositivo, o al grupo de dispositivos disponibles en esa ubicación física. Los ataques contra la infraestructura central de Internet normalmente involucran el secuestro del protocolo de puerta de enlace de frontera (“Border Gateway Protocol”, BGP), el ataque a un router central o el abuso de la infraestructura del servicio de nombres de dominio (“Domain Name Service”, DNS). Estos ataques proporcionarían una posición de privilegio más independiente de un objetivo en particular, lo que permitiría potencialmente que el atacante tenga acceso a muchos sistemas a la vez. Los ataques contra la infraestructura de red interna requieren acceso físico a esta, lo que implica un ataque interno o una posición de privilegio existente dentro del entorno de una empresa, lo que puede implicar un compromiso del sistema más profundo.

Independientemente del tipo de ataque que se utilice, este modelo es fácil de evitar mediante la autenticación mutua, el secreto hacia adelante y los protocolos y algoritmos criptográficos apropiados. Si se hace esto, se anulará prácticamente la capacidad de un atacante para comprometer esta infraestructura, o se disparará el costo del ataque de tal forma que sería casi imposible para cualquier tipo de atacante.

3.2 Ataques a las Infraestructuras de la Nube o de Contenedores

Estos ataques suponen una posición de privilegio en el entorno de la infraestructura de la nube o del contenedor. Por ejemplo, si un adversario puede poner en peligro una red de servicios en la nube, puede tener acceso a equipos centrales que ejecutan sistemas de máquina virtual (MV) invitados. Esto permitiría al adversario inspeccionar y modificar los sistemas MV en ejecución. El adversario puede tener objetivos específicos en mente, o puede haber tenido suerte y haber comprometido a un proveedor de servicios en la nube solo para acceder a muchos tipos diferentes de sistemas con datos valiosos.

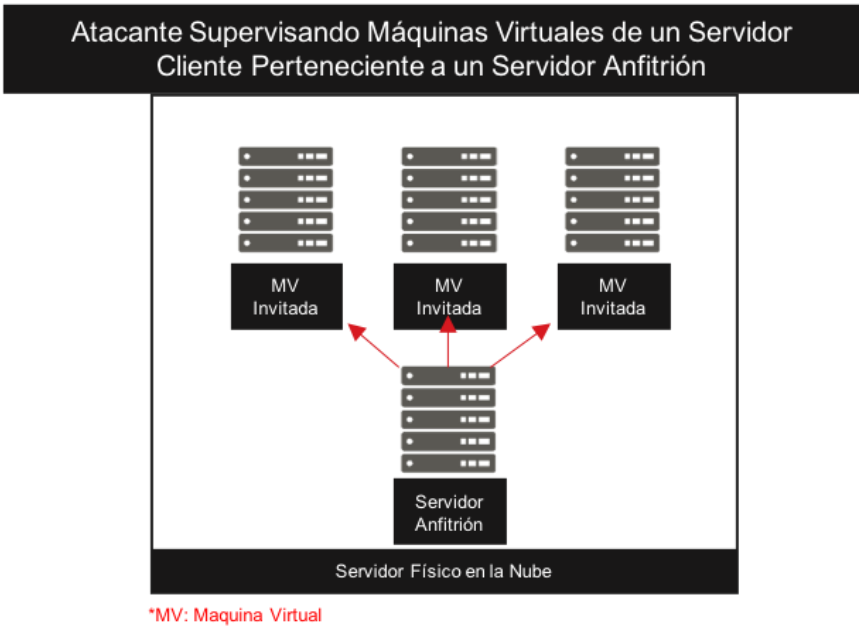

Figura 7 – Ejemplo de un Ataque Utilizando un Modelo de Máquina Virtual

Otro ataque a la infraestructura de la nube o de contenedores supone que el adversario tiene control sobre una MV en el mismo servidor físico que la MV objetivo. El adversario puede usar varias metodologías para comprometer otras máquinas virtuales en un servidor físico. Ellos podrían:

- Usar una vulnerabilidad en la infraestructura de la MV para que, a partir de un cliente, puedan entrar en un sistema servidor
- Usar un ataque de canal lateral para inferir claves secretas de otra máquina virtual invitada
- Consumir recursos excesivos en el servidor físico para forzar a una MV objetivo a migrar a un servidor físico sobre el que el atacante tenga más control

Independientemente del modelo de ataque utilizado, una empresa tendría muy poco que hacer contra este riesgo. En cambio, el proveedor de servicios en la nube debe implementar las medidas adecuadas para reducir la probabilidad de que un atacante pueda afectar la infraestructura de la nube o del contenedor.

Una forma de reducir este riesgo es implementar una arquitectura para los contenedores que limite cada contenedor a un usuario específico y a una identidad criptográfica única. Si bien esta es una actividad que requiere un gran uso de recursos y puede incurrir en costos adicionales, evitará la capacidad de un atacante a alterar la infraestructura de la MV, para obtener acceso a múltiples usuarios o múltiples servicios a la vez.

Si bien una posición de privilegio en un entorno en la nube o en un contenedor es una amenaza crítica para las aplicaciones que se ejecutan en máquinas virtuales huéspedes, se necesita una gran habilidad, tiempo y recursos para obtener acceso a este nivel. Una vez que se adquiere el acceso, el adversario debe mantenerlo el tiempo suficiente para identificar qué sistema contiene la MV que sea relevante para sus intereses. Además, deben poder supervisar o alterar esa MV sin ser detectados por el subsistema de incidentes

del proveedor de servicios en la nube. Esto puede plantear un desafío significativo y debería disminuir la probabilidad de un compromiso.

Sin embargo, es notable que este tipo de compromiso es en gran parte indetectable por la máquina virtual huésped o por una aplicación que se esté ejecutando por encima. Por lo tanto, se pueden recopilar métricas que revelan anomalías en el comportamiento de una MV o contenedor en particular, pero puede ser extremadamente difícil identificar si se produjo o no un compromiso. Esto se debe a que cualquier atacante con suficientes privilegios en la capa del servidor principal de la infraestructura de la máquina virtual podría manipular al huésped para que le sea difícil detectar la manipulación.

Los ataques de “huésped a huésped” son excepcionalmente difíciles de detectar, incluso por el proveedor de servicios en la nube. Sin embargo, es importante señalar que estos ataques son en gran parte de naturaleza teórica. Si bien los ataques de canal lateral son posibles, si son prácticos o no, es tema de debate, ya que estos ataques requieren un nivel de coherencia en la plataforma de ejecución subyacente que no está garantizado en un entorno en el mundo real. Además, los ataques jerárquicos de los huéspedes a los servidores en una MV, contenedor o entorno de hipervisor son difíciles de encontrar e incluso más difíciles de explotar. Esto hace que sea mucho menos probable que por una vulnerabilidad concreta, se pueda obtener información de una manera fraudulenta de una cantidad masiva de invitados o se logre atacar un objetivo específico.

Por lo tanto, si bien esta es una posición de privilegio importante para los atacantes, la probabilidad de que un ataque tenga éxito es baja ya que la dificultad, el costo y la oportunidad hacen que la explotación sea sencillamente impracticable.

3.3 Ataques en las Capas de Aplicación y Servicio

Si bien las discusiones sobre la arquitectura de ejecución de aplicaciones están fuera del alcance de este documento, es importante tener en cuenta que esta capa es la que presenta mayor riesgo frente a un ataque. Si el ecosistema de servicios se ha configurado correctamente, como se recomienda en esta guía, los atacantes dejarán de atacar a la infraestructura de red y se centrarán en la aplicación.

La aplicación presenta el mayor nivel de complejidad en cualquier producto o servicio, y siempre conlleva la posibilidad mayor de que un adversario obtenga réditos a través de múltiples tipos de tecnologías de ataque diferentes. Por lo tanto, si bien el objetivo de este documento es alejar el foco de un ataque de la infraestructura de red, está llevando el foco principalmente al único lugar donde el éxito es mucho más probable.

Para disminuir la probabilidad de ataque, revise la literatura abundante al respecto muy bien documentada sobre seguridad de aplicaciones (por ejemplo, el Proyecto de Diseño de Aplicación Segura OWASP [5]), para implementar la arquitectura de ejecución de la aplicación de la forma más segura posible.

3.4 Privacidad

Si bien los sistemas asociados a una solución de IoT están diseñados para consumir datos / métricas u otros componentes centrados en el usuario para proporcionar un valor agregado al sistema en general, nunca existe una garantía en cuanto al nivel de seguridad implementado en estos. En lugar de simplemente pasar información a un tercero, es

necesario evaluar qué tipo de datos se deben entregar, cuál debe ser el rendimiento tangible y cómo se debe proteger esa información.

La responsabilidad legal puede verse disminuida a través de contratos y cláusulas sobre seguros concretos, sin embargo, la pérdida de clientes puede ocurrir debido a un error de un tercero. En lugar de arriesgarse a perder negocio, una empresa debería evaluar a los equipos de ingeniería de terceros para determinar qué nivel de seguridad aplican a su infraestructura, aplicaciones y APIs. Si el nivel de seguridad no es suficiente, se recomienda buscar socios alternativos.

3.5 Objetos Maliciosos

Los sistemas de terceros están diseñados para mostrar información o ficheros multimedia a los consumidores. Una forma obvia de lograr esto es a través de la publicidad. Varios tipos de archivos son complejos en su estructura, y es difícil que el software los analice correctamente. Las redes publicitarias son un canal interesante para la distribución de malware. Las redes de distribución de contenido (CDN) también representan canales potenciales para la distribución de malware. Cualquier sistema que transmita tipos complejos de información multimedia, o paquetes de código (ya sea para navegadores Web o ejecutables) con el fin de proporcionar información dinámica, puede transmitir malware.

Por lo tanto, es muy importante que la empresa evalúe los diferentes tipos de ofertas tecnológicas que se transmitirán a través de un canal en particular. La empresa debe decidir que se permite entregar a los clientes y que no por ser demasiado “pesado” o complejo. Por ejemplo, una empresa de publicidad puede querer transmitir código Java a través de un servicio a sistemas cliente con una aplicación proxy a los socios del proveedor de servicios IoT. La empresa deberá decidir si los sistemas cliente que se ejecutan en ciertos entornos son más susceptibles a los ataques a través de la tecnología Java. Si se determina que esto es cierto, es posible que la empresa no permita el uso de Java, pero permita otro tipo de tecnologías, como el lenguaje HTML.

Dado que el malware se presenta de muchas formas, desde tipos de archivos polimórficos hasta archivos de tipo Adobe Flash, Java y formatos multimedia, no existe una única manera uniforme de garantizar la seguridad del usuario final. Una solución simple sería que el equipo de ingeniería aplique una política de seguridad que dicte qué tecnologías se pueden utilizar en sus canales y cómo se verán afectados sus usuarios. Se pueden implementar subsistemas de supervisión, así como entornos aislados (sandbox), para garantizar que cualquier objeto procesado en un sistema cliente esté menos sujeto a ataques.

3.6 Autenticación y Autorización

Los socios a menudo ofrecen servicios que solo son específicos para un subconjunto de usuarios. Esto puede incluir servicios de pago a los que un usuario puede suscribirse opcionalmente. Esto también puede representar una forma en que un usuario puede autenticarse en el sistema, usando credenciales compartidas con una tecnología diferente y bien conocida, como las API de autenticación ofrecidas por los proveedores de servicios en la web, como las redes sociales y entidades de administración M2M o IoT existentes.

Si bien estas son excelentes formas de compartir tecnología entre plataformas, los ingenieros deben asegurarse de que la tecnología no consuma inadvertidamente

credenciales que puedan utilizarse para abusar de permisos que no se otorgan expresamente a un servicio de terceros. Por ejemplo, ciertas API de la plataforma permiten restringir los permisos a una clase que el usuario acepte o rechace. Esto permite al usuario ajustar la experiencia de uso a una que sea adecuada para sus necesidades de privacidad concretas. Si la plataforma no puede ofrecer permisos de seguridad detallados, debe indicar a qué tecnologías desea acceder.

Es necesario que el equipo de ingeniería solicite a sus socios que el servicio que ofrezcan permita configurar permisos de manera detallada para garantizar que, al revocar el servicio en cuestión, no se permita inadvertidamente una ventana temporal de exposición de los datos de ese usuario que continúe incluso después de que se revoque la suscripción.

3.7 Falsos Positivos y Falsos Negativos

Si bien los servicios de supervisión y registro son formas excepcionales de mejorar una infraestructura de seguridad existente, se deben evaluar cuidadosamente para detectar falsos positivos y falsos negativos. Debido a que estos sistemas solo interpretan datos que se originan en varios ecosistemas dentro de un producto o servicio de IoT, y estos sistemas no son desarrollados por el equipo de ingeniería interno, solo pueden ofrecer una visión superficial de un evento. Sin embargo, es posible que no puedan distinguir con precisión si se está produciendo un evento sospechoso.

Como resultado, es importante involucrar a los equipos de TI (Tecnologías de la Información) e ingeniería para determinar si un evento sospechoso es, de hecho, atribuible a un comportamiento malicioso. Esto ayudará a evitar la posibilidad de que el equipo de supervisión desautorice el acceso de un usuario legítimo al sistema. Si este proceso es automático y el proceso es incorrecto, muchos usuarios podrían no poder acceder a su servicio totalmente legítimo debido a un falso positivo que puede atribuirse a una anomalía en la aplicación o infraestructura del cliente. Cuando se produce un evento crítico que es cuestionable, los equipos de TI e ingeniería deben echar un vistazo a los datos para evaluar si efectivamente hay un ataque.

Además, los ingenieros deben tener cuidado de modelar la información recibida a través de canales analógicos. Los falsos positivos y falsos negativos, especialmente en ecosistemas donde los datos deben procesarse a tasas de transmisión excepcionalmente altas, pueden tener consecuencias negativas si la aplicación no evalúa adecuadamente qué camino seguir de manera segura en caso de que los datos adquiridos no sean completamente fiables. Es notable que, con el tiempo, la tecnología y la experiencia suficientes, todos los datos analógicos se pueden suplantar con un sistema digital.

4 Preguntas Frecuentes sobre Seguridad

En este documento, la seguridad de un servicio se instrumenta con recomendaciones unidas a prioridades diferentes. Pero, sería más útil evaluar las recomendaciones desde un punto de partida práctico. Los ingenieros generalmente comienzan a elaborar una lista de recomendaciones basadas en objetivos técnicos o con un sesgo empresarial, olvidándose de la seguridad en primera instancia. Esta sección describe los objetivos comunes unidos a la seguridad desde una perspectiva de Dispositivos Periféricos y qué recomendaciones son relevantes para lograr esos objetivos.

4.1 ¿Cómo Combatimos la Clonación?

Diferenciar entre dispositivos válidos fabricados por el proveedor de servicios IoT y dispositivos que son reproducciones o "estafas" (clones) es una reto importante. Ningún proveedor de servicios de IoT desea proporcionar servicios para Dispositivos Periféricos no autorizados, ya que los proveedores de servicios tienen que pagar por el tiempo de CPU, el ancho de banda, el almacenamiento en disco y otros recursos. La empresa debe pagar independientemente de si el dispositivo fue o no fabricado por el proveedor de servicios IoT.

Además, la organización debe ser capaz de discernir si su arquitectura de Dispositivos Periféricos está siendo atacada. Esto permite que la organización reaccione ante un dispositivo que ha sido clonado en múltiples instancias del mismo dispositivo. Esto podría hacerlo un fabricante sin escrúpulos o un hacker que intenta hacerse pasar por un usuario en particular.

Revise las siguientes recomendaciones para obtener ayuda sobre el uso del Servicio para

- Definir una raíz de confianza organizativa
- Usar los servicios de autenticación de red
- Forzar la autenticación a través del Ecosistema de Servicios
- Definir la autenticación y la autorización a nivel de aplicación

4.2 ¿Cómo se Autentican los Usuarios a Través del Dispositivo Periférico?

Uno de los conceptos más importantes en IoT es la separación de la autenticación del Dispositivo Periférico, de la autenticación de usuario. Un Dispositivo Periférico puede ser autenticado con su Base de Computación Confiable (TCB), pero la forma en que se autentica el usuario es un proceso aparte que depende de la TCB del Dispositivo Periférico para la seguridad de las comunicaciones. Lo más importante de esta abstracción es evaluar qué tan fiable es el canal de comunicaciones para la autenticación del usuario.

Por ejemplo, si la fiabilidad de un Dispositivo Periférico es baja porque no tiene TCB, o se usa una implementación de TCB de Dispositivo Periférico no muy robusta, no se puede confiar en el mecanismo de autenticación de usuario que se basa en el software/firmware del Dispositivo Periférico. Esto significa que cualquier usuario que se autentique a través de un Dispositivo Periférico no puede considerarse efectivamente autenticado.

Desde una perspectiva diferente, una TCB de Dispositivo Periférico bien estructurada puede autenticar pobremente al usuario final si el esquema de autenticación se puede evitar o deducir fácilmente. Por lo tanto, el Ecosistema de Servicios debe confiar en la fiabilidad del Dispositivo Periférico, así como en la implementación del mecanismo de autenticación para garantizar que el Ecosistema del Servicios pueda garantizar que el usuario correcto está conectado al sistema.

Considere las siguientes recomendaciones que le ayudarán en hacer frente a estos retos:

- Implementar una Base de Computación Confiable del servicio
- Definir una raíz de confianza organizativa
- Definir un modelo de autorización clara
- Usar los servicios de autenticación de red

- Mejorar la autenticación a través del Ecosistema de Servicios
- Aplicar una política de contraseña robusta
- Definir la autenticación y la autorización a nivel de aplicación

4.3 ¿Cómo Puede Identificar el Servicio un Comportamiento Anómalo en un Dispositivo Periférico?

Uno de los aspectos más complejos de la administración de Dispositivos Periféricos en una red distribuida de IoT, es determinar si un Dispositivo Periférico se comporta de manera anormal o no. Esto no solo es importante desde una perspectiva de seguridad, sino desde una perspectiva de fiabilidad. A menudo, el comportamiento anómalo puede indicar que existe un problema con el firmware o el hardware, y puede ser una señal de que la empresa debe prepararse para corregir un problema inesperado. Sin embargo, si el comportamiento se produce en una parte de la red que no puede ser analizada por el proveedor de servicios de IoT, estas métricas se perderán, dejando a la organización con una ventaja mucho menor.

La solución a este problema requiere tener la capacidad de inspeccionar el comportamiento en el Dispositivo Periférico, la capa de red y el Ecosistema de Servicios. Sin embargo, si la infraestructura, los servicios y las asociaciones correctas no se crean para recopilar estos datos concretos, la empresa no tendrá la información necesaria para tomar una determinación sobre la existencia de un problema o si este en concreto está relacionado con la seguridad o la fiabilidad.

En este punto hay que evaluar las siguientes recomendaciones desde la perspectiva del Ecosistema de Servicios:

- Definir una infraestructura de seguridad para sistemas expuestos a una Internet abierta
- Definir un enfoque de registro y supervisión de sistemas
- Definir un modelo de comunicaciones
- Usar los servicios de autenticación de red
- Implementar una verificación de entrada
- Implementar un filtrado de salida
- Usar servicios de supervisión mejorados para los socios
- Usar un APN privado para la conectividad inalámbrica
- Definir un modelo de evaluación para falsos negativos o positivos

4.4 ¿Cómo puede el Servicio Restringir los Privilegios de un Dispositivo Periférico que se Esté Comportando de Manera Anormal?

Una vez que se identifica que un Dispositivo Periférico se comporta de manera anormal, el servicio debe tomar decisiones sobre qué recursos deben limitarse o restringirse. Esta cuestión es relevante para cada capa de la infraestructura del servicio.

Por ejemplo, un Dispositivo Periférico habilitado con tecnología celular que se conecta y desconecta constantemente de la red celular en un bucle frenético se debe inhabilitar por la fuerza, hasta que se resuelva este comportamiento anómalo. Otro ejemplo útil es un

Dispositivo Periférico comprometido que un adversario está usando para tratar de atacar servicios del back-end. En este escenario, los servicios de back-end deberían bloquear por completo al Dispositivo Periférico en cuestión.

La forma de manejar cada escenario depende del proveedor de servicios de IoT, y depende de sus objetivos comerciales y de cómo se deben manejar los incidentes que se detectan. Para ayudar a desarrollar los lineamientos de seguridad al respecto, considere las siguientes recomendaciones:

- Definir una raíz de confianza organizativa
- Definir una infraestructura de seguridad para sistemas expuestos al Internet público
- Definir un modelo de respuesta a incidentes
- Definir un modelo de recuperación
- Definir un modelo de retirada gradual del servicio (apagado)
- Definir un modelo de comunicaciones
- Definir una política de incumplimiento para los datos que sean expuestos
- Aumentar la autenticación a través del Ecosistema de Servicios
- Use un APN privado para la conectividad inalámbrica
- Definir un modelo de evaluación de falsos negativos o positivos

4.5 ¿Cómo Puedo Determinar si un Servidor o un Servicio ha Sido "Hackeado"?

Si bien las anomalías en Dispositivos Periféricos son más complejas y raras, requieren de una gran cantidad de análisis de comportamiento para descubrir la mayoría de los ataques, en el Ecosistema de Servicios esto es más fácil de detectar. Los servicios y servidores se implementan dentro de un entorno estrechamente controlado por el proveedor de servicios de IoT o por sus socios que administran la infraestructura de la nube o del servidor. Por lo tanto, la organización y sus socios pueden usar sistemas de supervisión y diagnóstico fácilmente disponibles para identificar y evitar problemas potenciales.

Revise las siguientes recomendaciones como apoyo:

- Definir un modelo de administración
- Definir un enfoque de registro y supervisión de sistemas
- Definir un modelo de respuesta a incidentes
- Implementar una verificación en la entrada de datos
- Implementar filtrado de salida

4.6 ¿Que Puedo Hacer Cuando un Servidor ha Sido "Hackeado"?

Cuando se ha verificado que un servidor ha sido comprometido, el equipo de administración debe resolver el problema lo más rápido y eficientemente posible. La complejidad de hacerlo a menudo surge al determinar qué recursos, información y cuentas se han puesto en peligro. En algunos entornos con una arquitectura muy poco elaborada, los efectos de un compromiso no son a menudo cuantificables. Por lo tanto, la organización debe implementar en paralelo un plan para resolver la vulnerabilidad de seguridad y un plan para asegurar activos actualmente desplegados que estén en peligro. Una vez que se ha asegurado el ecosistema y la vulnerabilidad, la empresa puede ejecutar un plan para reconstruir la tecnología afectada.

Revise las siguientes recomendaciones para obtener más información:

- Definir un modelo de respuesta a incidentes
- Definir un modelo de recuperación
- Definir un modelo de retirada gradual y desconexión de un servicio o dispositivo
- Definir un conjunto de clasificaciones de seguridad
- Definir clasificaciones para conjuntos de tipos de datos

4.7 ¿Cómo Deben Interactuar los Administradores con los Servidores y Servicios?

Desarrollar un modelo administrativo que no ponga en peligro el ecosistema del servicio es una parte importante de la arquitectura de un servicio de IoT. Hay varias capas de administración, y cada capa debe ser considerada por los equipos de ingeniería y de seguridad. Por ejemplo, los administradores que gestionan el servidor (independientemente de si se utiliza una arquitectura virtual, de microservicios o de kernel único) deben poder interactuar con servidores en tiempo real a través de un canal de comunicaciones fiable y seguro. Los administradores que gestionan la aplicación web a menudo interactúan con la aplicación a través de la misma capa de comunicación web, pero a través de una aplicación especializada incorporada en el código.

Independientemente de la necesidad administrativa, la interfaz debe tener acceso restringido para limitar la capacidad de los adversarios de interactuar o comprometer una tecnología en concreto. Considere los siguientes recursos:

- Definir una infraestructura de seguridad para sistemas expuestos al Internet público
- Definir un modelo de administración
- Definir un modelo de autorización claro
- Definir un modelo de comunicaciones
- Use un APN privado para la conectividad inalámbrica

4.8 ¿Cómo Puede la Arquitectura de los Servicios Limitar el Impacto de un Compromiso?

Un atributo fascinante de una red IoT es su capacidad única de conectar servicios a usuarios específicos. En los servicios web, cada usuario debe tener la capacidad de interactuar con el servicio desde cualquier tipo de dispositivo o, potencialmente, desde cualquier lugar del mundo. Esto no es verdad para la tecnología de IoT. La tecnología de IoT generalmente requiere un dispositivo periférico específico para interactuar con los servicios de IoT. Debido a esta diferencia, los arquitectos del ecosistema del servidor pueden aprovechar la relación uno-a-uno entre los dispositivos periféricos y los usuarios para restringir el acceso de un dispositivo periférico a los datos de back-end.

Considere el escenario en el que un dispositivo periférico está transmitiendo las mediciones de un sensor a un servicio de back-end. En una arquitectura de microservicio, el Ecosistema de Servicios puede implementar un microservicio o un kernel específico para gestionar a un usuario en particular. Usando esta arquitectura, el ingeniero puede garantizar que el

microservicio se suministre solo con los recursos y las capacidades de acceso requeridas para entregar datos y servicios específicos para el usuario individualmente.

Esto significa que si un servicio se ve comprometido y el Dispositivo Periférico es el único elemento tecnológico que puede comunicarse con ese servicio específico, no hay ningún beneficio adicional en comprometer ese servicio, ya que el acceso obtenido por el ataque se limitará a los recursos que ya estarían de todas formas disponibles. En esencia, no se obtendría una ganancia adicional con el ataque.

Revise las siguientes recomendaciones como ayuda:

- Implementar una Base de Computación Confiable para el servicio
- Definir un método arranque (“Bootstrap”)
- Definir una infraestructura de seguridad para sistemas expuestos al Internet público
- Definir un modelo de almacenamiento persistente
- Definir un modelo de administración
- Definir un modelo de retirada gradual y desconexión de un servicio o dispositivo
- Definir un modelo claro de autorización
- Utilizar Servidores donde sea posible
- Definir un entorno de ejecución de aplicaciones
- Compromisos de máquina virtual (MV)

4.9 ¿Cómo Puede una Arquitectura de un Servicio Reducir la Pérdida de Datos durante un Compromiso?

Otra característica interesante de la arquitectura IoT es el reducir la pérdida de datos al máximo. Esto es similar a cómo los servicios se pueden aislar con respecto a un usuario específico. Los datos también se pueden aislar para un usuario específico una vez que el usuario ha sido autenticado. Sin embargo, el almacenamiento de datos no se puede implementar fácilmente para cada usuario debido al costo que representa en la infraestructura de almacenamiento y en una base de datos.

En su lugar, se deben suministrar tokens únicos a servicios que luego actúen en nombre de un usuario específico dentro de la infraestructura de almacenamiento. De esta forma, un atacante con acceso al entorno de almacenamiento de datos puede conectarse al servicio, pero no debería poder interactuar, recuperar o alterar datos de usuario que no sean propios del usuario que se ha visto comprometido.

Desde la perspectiva de la capa de red, también es un requisito reducir el tráfico de datos del ecosistema del servidor hacia Internet. Los controles de salida obligan a un adversario a utilizar fraudulentamente la propiedad intelectual o los datos de los clientes a través de canales específicos. Esto puede aumentar la dificultad en mover grandes cantidades de datos o forzar su paso a través de capas de comunicación concretas que pueden detectar y cortar la comunicación durante ataques.

Para obtener más información, considere las siguientes recomendaciones:

- Definir un método de arranque (“Bootstrap”)
- Definir una infraestructura de seguridad para sistemas expuestos al Internet público

- Definir un modelo de almacenamiento persistente
- Definir un conjunto de clasificaciones de seguridad
- Definir clasificaciones para conjuntos de tipos de datos
- Utilizar servidores donde sea posible
- Definir un entorno de ejecución de aplicaciones
- Reglas en los cortafuegos de apertura por defecto o apertura por error

4.10 ¿Cómo Puede la Arquitectura del Servicio Limitar la Conectividad a Usuarios No-Autorizados?

Un beneficio de aprovechar las arquitecturas comunes de IoT, es restringir la posibilidad de que los usuarios de Internet no autorizados se conecten directamente a los servicios de back-end. La mayoría de las aplicaciones web no tienen esta posibilidad y deben estar disponibles para uso público. Sin embargo, en IoT, dado que el Dispositivo Periférico es la entidad que debe conectarse a un servicio en particular, se puede usar una red privada virtual (VPN) para restringir quién tiene acceso a los servicios de back-end. Esto se puede implementar a través de protocolos estándar de Internet, o se puede implementar utilizando servicios móviles, como un APN privado. Revise las siguientes recomendaciones para obtener más información:

- Definir una infraestructura de seguridad para sistemas expuestos al Internet público
- Use un APN privado para conectividad inalámbrica

4.11 ¿Cómo Reducir la Probabilidad de una Operación Remota?

La operación remota de aplicaciones y servicios web es una preocupación constante de los administradores de la infraestructura. Asegurar que los adversarios no tengan una ruta a la red interna, o simplemente a recursos valiosos, es una batalla diaria. La única forma de reducir la posibilidad de que los adversarios pongan en peligro el ecosistema de los servicios es reducir los objetivos potenciales en un conjunto manejable de servicios que se pueda mantener rápida y fácilmente. La segunda mejora más importante en la arquitectura es el diseño de la arquitectura subyacente: la arquitectura de ejecución, la configuración del sistema operativo, la cadena de herramientas de implementación, la seguridad del lenguaje de programación y otras opciones que definen qué tan segura puede ejecutarse una aplicación. Estas opciones pueden marcar la diferencia entre un bloqueo de la aplicación y un compromiso de la infraestructura.

Para obtener más información sobre cómo reducir la posibilidad de operar remotamente aplicaciones, consulte:

- Definir una infraestructura de seguridad para sistemas expuestos al Internet público
- Definir un modelo de actualización
- Implementar la verificación de entrada de datos
- Implementar filtrado de salida
- Reglas de cortafuegos de apertura por defecto o apertura por error
- Definir un entorno de ejecución de aplicaciones
- “Rowhammer” y ataques similares

- Compromisos de máquina virtual

4.12 ¿Cómo Puede el Servicio Gestionar la Privacidad del Usuario?

A medida que los proveedores de servicios de IoT aumentan, invariablemente crearán relaciones con empresas que utilizarán los datos de los usuarios de maneras innovadoras. Sin embargo, estos datos tienen un “costo” sobre la privacidad del consumidor. Los consumidores deben tener derecho a determinar qué datos se comparten con los socios de un servicio y cómo se usarán. Además, se debería exigir a los socios que usen los datos de formas específicas. Los modelos de autorización pueden ayudar a resolver el problema, pero esto implica la necesidad de una discusión mucho más amplia sobre la privacidad, las repercusiones legales, los seguros comerciales y demás.

Para comenzar la discusión dentro de su empresa, revise las siguientes recomendaciones:

- Definir un conjunto de clasificaciones de seguridad
- Definir clasificaciones para conjuntos de tipos de datos
- Definir un modelo de autorización clara
- Definir una política de incumplimiento para los datos expuestos
- Evaluar el modelo de privacidad de las comunicaciones
- Definir una política de distribución de datos a terceros
- Crear un filtro de datos con respecto a terceros
- Crear una API para que los usuarios controlen los atributos de privacidad

4.13 ¿Cómo Puede el Servicio Mejorar su Disponibilidad?

Los ataques de denegación de servicio (DoS) o de denegación distribuida de servicio (DDoS) son tan comunes en el Internet moderno que todas las empresas deberían estar preparadas para enfrentarse a un ataque de esta clase, y deberían poder mantenerse activos incluso durante ataques prolongados. La razón por la cual estos ataques se han vuelto tan comunes es que necesitan de muy pocos conocimientos para ejecutarse y las herramientas para implementar dichos ataques están disponibles en internet. De hecho, hay servicios en internet donde un “ente malicioso” puede pagar a un atacante para implementar un ataque DDoS contra un objetivo en particular.

Como resultado, se han construido modelos completamente nuevos para la disponibilidad de servicios para combatir esta amenaza. Considere las siguientes recomendaciones al construir el Ecosistema de Servicios:

- Definir una infraestructura de seguridad para sistemas expuestos al Internet público
- Definir un enfoque de registro y supervisión de sistemas
- Definir un modelo de respuesta a incidentes
- Definir un modelo de recuperación
- Definir un modelo de comunicaciones
- Reglas de cortafuegos abiertas por defecto o abiertas por error

5 Recomendaciones Críticas

Al desarrollar un Dispositivo Periférico seguro, siempre se deben implementar las siguientes recomendaciones. Estas ayudan a implementar una arquitectura segura para un Dispositivo Periférico. Sin estas recomendaciones, el Dispositivo Periférico tendrá un perfil de seguridad incompleto que un adversario podría atacar.

5.1 Implemente una Base de Computación Confiable para el Servicio

Una Base de Computación Confiable (TCB) es un conjunto de hardware, software, protocolos y políticas. Una TCB debe ser la base de cualquier plataforma informática determinada, y debe definir el entorno en el que una aplicación puede ejecutarse de manera fiable, segura y con alta calidad.

Se puede construir y desplegar una TCB para cualquier clase de sistema, como equipos móviles (teléfonos inteligentes), terminales IoT e incluso servidores que funcionan en un Ecosistema de Servicios. Las TCB están compuestas siempre de tecnologías similares. Sin embargo, dependiendo de la clase de sistema, esas tecnologías pueden adoptar características muy diferentes. Por ejemplo, el arranque de una TCB en un servidor en la nube será muy diferente a su arranque en un Dispositivo Periférico.

Crear una TCB en un ecosistema de servicio significa definir la forma en que se desplegará una imagen de una aplicación. Una imagen en este contexto representa los datos binarios en bruto que comprende un ejecutable de aplicación, sus archivos de configuración y sus metadatos. Todo esto unido se conoce comúnmente como imagen de la aplicación o simplemente imagen. En la mayoría de los ecosistemas de servicios modernos, los sistemas se replicarán, encenderán o adaptarán según demanda para que escalen reactivamente con los cambios en el entorno informático. Esto significa que una TCB debe definir una forma de permitir que los sistemas escalen de manera efectiva mientras se mantiene un modelo de seguridad persistente.

Para hacer esto correctamente, el equipo debe:

- Estandarizar la plataforma informática:
  - Elija un conjunto de modelos de servidores físicos
  - Seleccione un conjunto de plataformas en la nube o imágenes de máquinas virtuales (MV)
- Definir el conjunto de aplicaciones, bibliotecas y archivos de configuración que se ejecutarán en la plataforma informática:
  - Definir un entorno contenedor, si corresponde
- Generar una imagen de aplicación, compuesta por el conjunto de elementos citados más arriba
- Firme criptográficamente un archivo de la imagen usando la clave de firma de la TCB de una capa concreta
- Almacenar de forma segura el archivo y la firma

La realización de este conjunto de tareas dará como resultado una imagen aprobada de la aplicación que se puede implementar en una capa específica. Cada capa tendrá un hardware diferente y un modelo de aplicación que funcione mejor para esa capa específica.

Por ejemplo, el hardware de una base de datos tiene necesidades de almacenamiento y rendimiento muy diferentes a las de una capa de aplicación. Una capa de almacenamiento tendrá requisitos para el hardware de almacenamiento similares a un a capa de base de datos, pero tendrá diferentes requisitos de rendimiento. Después de estandarizar la definición de cada capa, el resultado es una imagen que se puede implementar y verificar en cada plataforma hardware.

La dificultad para implementar una TCB proviene de:

- Configurar una raíz de confianza organizativa para administrar la firma criptográfica de imágenes
- Configurar un procedimiento para firmar cada imagen
- Configurar un procedimiento para verificar cada imagen
- Configurar un procedimiento para desplegar imágenes de forma automática, pero con verificación de imagen

Considere utilizar material bibliográfico de las siguientes organizaciones para ayudar con esta recomendación:

- Especificación de la tarjeta GlobalPlatform [11]
- Especificación TPM de Trusted Computing Group [6]
- Especificación de la API de núcleo interno TEE de GlobalPlatform [12]

5.1.1 Riesgo

Sin una Base de Computación Confiable bien definida, las plataformas informáticas no pueden verificar que se esté ejecutando en todo momento bajo una configuración aprobada por el equipo de ingeniería. Esto es importante ya que el subsistema de aplicación debe poder determinar si ha sido comprometido por un adversario. Se puede usar una TCB para corregir este riesgo, así como proporcionar una capa de seguridad para todas las comunicaciones de red.

5.2 Defina una Raiz de Confianza Organizativa

Una Raíz de Confianza Organizativa es un certificado o sistema basado en clave pública para autenticar entidades de una plataforma informática en una organización/empresa. Cada plataforma informática en un Ecosistema de Servicios debe autenticarse criptográficamente durante las comunicaciones de red. Esto disminuye la capacidad de un intruso, o alguien desde una posición privilegiada de la red, de suplantar o abusar de la confianza de un sistema con privilegios.

Para construir una Raíz de Confianza Organizativa, simplemente realice las siguientes acciones:

- Cree o adquiera, por ejemplo, un Módulo de seguridad de hardware (HSM) para almacenar el secreto de la raíz de la organización
- Genere un secreto de raíz y / o certificado
- Asegúrese de que la parte privada del secreto se almacena de forma segura
- Genere un conjunto de una o más claves de firma para ser usadas como clave de firma de la TCB de un nivel determinado
- Firme la parte pública de la clave de firma con la raíz de la organización

- Asegúrese de que estas claves no se utilicen sin la autenticación y autorización de los gestores empresariales y de ingeniería

Cada vez que se defina un nuevo sistema de capas, su clave o certificado criptográfico único ahora se puede firmar con la clave de firma. Si otro sistema se conecta a este nuevo sistema, puede validar la identidad del sistema al verificar la cadena de confianza definida por la raíz de la organización.

Validará criptográficamente que los mensajes fueron firmados por la clave pública que representa el sistema. Luego, verificará la firma que la clave de firma generó a partir de la clave pública única de ese sistema. Luego, el cliente debe verificar que la clave de firma sea efectivamente la clave de firma autenticada por la raíz de la organización.

Porque cada conjunto de certificados o secretos está restringido a cada vez menos personas en la organización, y las políticas y procedimientos definidos deben restringir quién puede usar esos secretos y cuándo, cada nivel de confianza debe aumentar a medida que el cliente desciende a través de la cadena raíz.

Se debe definir un servicio que presente capacidades de autenticación a pares autorizados dentro del Ecosistema de servicios. Por ejemplo, la autenticación que utiliza el certificado o la cadena secreta no se puede usar por sí misma para garantizar la seguridad. Se debe poner a disposición un servicio que verifique si los certificados han sido revocados o si son actualmente válidos. Es posible que sea necesario utilizar otro servicio para autenticar las identidades de servidores o servicios con una vida útil corta, según los requisitos de la infraestructura subyacente.

Durante la definición de la raíz de confianza, considere que:

- Cada secreto debe protegerse contra posibles abusos
- El uso interno de cada secreto debe ser rastreado y supervisado de forma verificable
- Cada individuo aprobado para utilizar un secreto debe usar autenticación multifactor al acceder al/los secreto(s)

Puede ser complicado:

- Definir un conjunto de políticas y procedimientos que impongan un uso coherente y seguro
- Crear un proceso para la retirada o revocación de un certificado
- Identificar si una clave ha sido descifrada
- Elegir el conjunto correcto de algoritmos criptográficos

Para leer más sobre el concepto de Raiz de Confianza, considere las siguientes fuentes de información:

- Trusted Computing Group
  - TPM Specification [6]
  - TCG Guidance for Securing IoT [7]
  - ISO 11889
- Especificaciones de PKI
  - RFC 2510
  - RFC 3647

5.2.1 Riesgo

El riesgo de no usar una raíz de confianza organizativa es que cualquier compromiso de una sola clave puede resultar en un compromiso para todo el ecosistema. Al separar la organización jerárquicamente y desplegar claves separadas para cada nivel jerárquico, las claves se pueden reciclar a intervalos regulares y de acuerdo con la prioridad de la aplicación o suborganización, a la cual pertenezca la clave.

5.3 Defina un Método de Arranque

Para que una aplicación se ejecute correctamente, debe cargarse y ejecutarse de manera consistente en una plataforma confiable, de alta calidad y segura. La TCB define cómo formular esta plataforma, pero el modelo de Arranque define cómo se ejecutará la aplicación sobre la plataforma.

Para definir un modelo de arranque de manera efectiva, se debe considerar lo siguiente:

- Defina una API que permita a la aplicación identificarse criptográficamente con sus extremos
  - Considere la posibilidad de utilizar una API existente definida por un líder reconocido en la industria
- Defina cómo la aplicación autenticará Dispositivos Periféricos, servicios cliente y Socios
- Defina cómo debe ser la configuración de la aplicación
- Fuerce que cada aplicación diferente tenga una identidad única, especialmente las aplicaciones que se ejecutan en capas diferentes

Si bien puede parecer intuitivo que una aplicación se debe identificar criptográficamente a sus pares, y puede no necesitar una API para hacerlo, el proceso en producción podría no parecer intuitivo. Esto se debe a que en el modelo de arranque, uno debe considerar cómo se suministra la identidad criptográfica para la aplicación. ¿Cómo adquiere la aplicación su identidad? ¿La identidad se adquiere de forma segura? ¿Cuál es el proceso para revocar secretos que la identidad usará en caso de que los secretos se actualicen o modifiquen?

En tiempo de ejecución, las aplicaciones requieren ciertos recursos para ejecutarse de manera efectiva. La aplicación debe poder comunicarse y realizar una autenticación mutua con todos los servicios externos, Dispositivos Periféricos y socios que participan en este proceso.

La configuración de una aplicación a menudo determina qué tan segura es durante su producción. Se debe forzar una configuración determinada y presentarla como de solo lectura a una aplicación. La aplicación, o alguien que abuse de la infraestructura de la aplicación, no debería ser capaz de simplemente alterar la configuración de una aplicación.

Use la Raíz de Confianza Organizativa para definir modelos de confianza para cada capa desplegada en el ecosistema en general. Esto permitirá que cada aplicación por separado tenga una identidad criptográfica única. Esto proporcionará a los pares la capacidad de diferenciar entre un servicio de base de datos y un servicio de aplicación, por ejemplo.

5.3.1 Riesgo

Sin un modelo de arranque bien definido, el sistema no tendrá forma de verificar cada capa que requiere para operar. En esencia, no existe una capa de confianza en cada capa de la plataforma tecnológica. Esta falta de capas de confianza introduce complejidad que puede dar lugar a lagunas que adversarios pueden aprovechar.

5.4 Defina una infrastructura de Seguridad para Sistemas Expuestos al Internet Púbico

Para servicios de acceso público, se requieren de varias piezas tecnológicas de seguridad y fiabilidad para mantener la disponibilidad, confidencialidad e integridad del servicio:

- Una infraestructura resistente a DDoS
- Una infraestructura de equilibrio de carga
- Sistemas de redundancia
- Cortafuegos de aplicaciones web (opcional)
- Cortafuegos tradicionales

Estas tecnologías adicionales deben colocarse por encima de la capa de aplicación para garantizar que atacantes públicos no puedan manipularlas. Si bien el modelo de seguridad de las comunicaciones remediará o mitigará el potencial de un tercero anónimo para acceder al sistema, estas tecnologías disminuirán la capacidad del adversario para desconectar el sistema y no esté disponible para sus usuarios.

La seguridad del “front-end” debe aplicarse a todos los protocolos utilizados en los servicios. Por ejemplo, si el servicio está disponible en IPv4 e IPv6, se deben aplicar las mismas restricciones de seguridad para el acceso al servicio en ambos protocolos. Si se puede acceder a un servicio a través de TCP y de “Stream Control Transmission Protocol” (SCTP), las restricciones de seguridad también deberían aplicarse a ambos protocolos. Los puertos que no ofrecen servicios públicos relativos al producto o servicio de IoT no deberían ser accesibles.

Asegúrese de que se gestionen los filtros de entrada y salida, siempre que sea posible. Si bien el filtrado de entrada detiene una variedad de ataques, cualquier ataque contra un servicio de acceso público puede resultar en un compromiso del Ecosistema de Servicios. El filtrado de salida es imperativo, en este punto, para garantizar que un atacante no utilice un componente comprometido del Ecosistema de Servicios para moverse “lateralmente” dentro del ecosistema. Además, el filtrado de salida complica la capacidad de los atacantes para filtrar datos críticos del Ecosistema a Servidores controlados por el adversario, dejando más tiempo para que los administradores identifiquen y aíslen al atacante.

Varias organizaciones ofrecen estos servicios en un modelo de API simple que se puede integrar en una tecnología determinada. Esto permite que esta tecnología se use fácilmente. No se requiere mucho esfuerzo de ingeniería más allá de registrar y configurar la aplicación dentro del sistema del proveedor de servicios. Consulte con su proveedor de servicios para determinar la mejor forma de implementar las tecnologías de seguridad que tenga para su entorno en concreto.

Considere utilizar recomendaciones y tecnologías de las siguientes organizaciones para cumplir con las recomendaciones arriba mencionadas:

- Mejores Prácticas de Amazon para la resiliencia en DDoS:
  - https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf
- Mejores prácticas de mitigación de DDoS de Arbor Networks:
  - https://www.arbornetworks.com/images/documents/Arbor%20Insights/AI_DDoSMitigation_EN2013.pdf
- Guía de la defensa en contra de DDoS de Cisco:
  - http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

5.4.1 Riesgo

Una infraestructura segura para servicios y aplicaciones públicas es imprescindible debido a la naturaleza volátil de Internet. Los ataques DDoS aleatorios ocurren a menudo, y sin ninguna razón aparente. Los servicios que implementan ataques DDoS se pueden comprar en el "mercado clandestino" por unos cuantos cientos de dolares. Por lo que los principales responsables de dichos ataques no tienen porque ser sólo los competidores del negocio o de los socios de este último. Se pueden producir ataques aleatorios solo para ver si es posible alterar o parar un sistema. Es mejor estar preparado contra tales ataques para garantizar que los servicios críticos de IoT no sean desactivados inesperadamente. La disponibilidad es una propiedad crítica de un producto o servicio de IoT.

5.5 Defina un Modelo de Almacenamiento Persistente

Los entornos de aplicaciones en la informática moderna a menudo son efímeros, como los sistemas basados en contenedores o entornos en la nube. Como resultado, el almacenamiento asignado a estos sistemas no es lo suficientemente grande, ni está diseñado para estar disponible por un largo espacio de tiempo, ni para que la aplicación use tecnologías de almacenamiento persistente. Además, estos sistemas se pueden definir como entidades bajo demanda y pueden no tener apariencia de un servicio centralizado. En otras palabras, no hay forma de que los otros sistemas definan qué sistema tiene suficiente almacenamiento para un uso persistente.

Esta es la razón por la cual los sistemas centrales de almacenamiento son muy importantes, y por qué deben ser cuidadosamente asegurados. Como los sistemas de almacenamiento deben ser accesibles para cualquier sistema temporal dado en este tipo de entorno, cualquier servidor o servicio temporal (o capa determinada del sistema) que se vea comprometido tendrá acceso a una entidad de almacenamiento persistente utilizada por muchos otros servidores o servicios. Esta es a menudo una manera efectiva de que los atacantes puedan comprometer lateralmente (o potencialmente, verticalmente) cualquier red.

Para restringir esto, cada servidor o servicio debe tener acceso a un almacenamiento persistente, pero debe almacenar información sobre la aplicación que representa y, lo que es más importante aún, información del Dispositivo Periférico, socio o usuario único que la aplicación esté representando en cualquier momento. Esto último es el punto más relevante, ya que imponer el acceso al almacenamiento persistente en nombre de una entidad con identidad determinada, limita el acceso temporal a los datos del servidor o servicio.

En otras palabras, un adversario que ha comprometido un “sistema de vida corta” solo puede afectar los datos almacenados en nombre de la identidad vinculada a ese mismo sistema de vida corta. Si ese sistema solo tiene acceso a los datos de una sola identidad, el adversario no puede usar el compromiso de este sistema para migrar lateralmente a otras cuentas. Están restringidos al acceso a la información para esa identidad individual. Esto limita significativamente la capacidad del adversario para aprovechar una vulnerabilidad y comprometer de manera importante el resto del sistema.

5.5.1 Riesgo

Si no se define un modelo de almacenamiento persistente seguro, no habrá una arquitectura que imponga atributos exclusivos por usuario que estén separados de manera segura de otros activos. El resultado puede ser que cualquier compromiso de un token que otorgue a un adversario acceso a un dispositivo de almacenamiento puede provocar el compromiso de muchos y variados datos de usuario. Sin embargo, un modelo de almacenamiento persistente puede aislar el compromiso de un solo usuario o una sola tecnología de almacenamiento con datos encriptados. En cualquier caso, el alcance del compromiso se reduce significativamente, lo que otorga a la organización más tiempo para reaccionar y combatir la amenaza tanto para los usuarios como para el negocio.

5.6 Defina un Modelo de Gestión

Todos los sitemas deben de tener un acceso Administrativo para solucionar problemas y diagnosticar averías o problemas en las aplicaciones. Esto puede ser un desafío en entornos donde los servicios o servidores son efímeros, si un modelo administrativo no está bien diseñado.

Para lograr esto, identifique cómo el equipo administrativo se comunicará con cada sistema en cada capa. Debe haber “fronteras” entre los sistemas para la autenticación, como VPNs que separan sistemas diferentes entre sí. Asegúrese de que el equipo administrativo deba autenticarse en cada capa.

Además, identifique cómo el administrador interactuará con el sistema. ¿Se puede tomar una “instantánea” del sistema, similar a una MV? ¿Se usa un terminal? ¿Se utiliza una “Shell” segura remota (SSH) para interactuar con el sistema? ¿Existen APIs para supervisar y analizar las métricas del sistema, como el uso de la CPU, el uso del disco y el uso de la red? ¿Se pueden usar estas para solucionar problemas o identificar anomalías?

Independientemente del modelo, hay ciertas cosas que deben definirse:

- Cómo los administradores se autenticarán en el entorno
- Cómo se puede atribuir la autenticación de los administradores a las identidades físicas:
    - Uso de autenticación de dos factores (2FA)
- Cómo se pueden generar “instantáneas” de los sistemas
- Cómo se pueden hacer los cambios y se deben rastrear

5.6.1 Riesgo

Los entornos sin una ruta bien estructurada para el acceso administrativo suelen terminar utilizando medios ad-hoc para acceder a los sistemas en producción. Esto a menudo conduce a que puertos administrativos estén abiertos públicamente, o a que servicios de diagnóstico, no estén restringidos y por ende que terceras partes los utilicen. Un modelo administrativo claro reduce las vías potenciales que los atacantes pueden tomar para obtener acceso privilegiado a recursos críticos del IoT.

5.7 Defina un Método para el Registro y Supervisión de Sistemas

Cada sistema debe ser supervisado para permitir que los administradores y las Tecnologías de la Información (TI) ayuden a detectar y diagnosticar anomalías. La monitorización debe realizarse en múltiples capas. Por ejemplo, la supervisión de red a nivel de infraestructura ayuda a diagnosticar ataques sobre aplicaciones o DDoS contra componentes de red. La supervisión por capas identifica si se han comprometido aplicaciones específicas o partes de la infraestructura. Mientras que la supervisión a nivel del sistema define si las aplicaciones individuales o las plataformas de aplicaciones están siendo atacadas o comprometidas.

Obviamente, esto requiere múltiples capas de supervisión y consolida la información en un recurso que se puede transmitir a un equipo de supervisión global. Hay varias aplicaciones comerciales que proporcionan esta tecnología y convierten las métricas en sistemas visuales que profesionales de TI e ingenieros pueden utilizar.

Las anomalías que indican un comportamiento inusual que puede conducir a la detección de un ataque pueden incluir, pero no están limitadas a:

- Aumento del tráfico de red
- Aumento del tráfico de red en una cierta dirección (especialmente salida)
- Flujo de tráfico de red en un recurso que no debería tener dicho comportamiento
- Uso anormal de la CPU
- Utilización de la GPU en sistemas sin interfaz gráfica (tienen una GPU como parte de la CPU)
- Uso de almacenamiento en disco o red
- Cambios anormales en la utilización del tiempo útil de sistema en un servidor particular

Si bien sistemas de supervisión para detectar anomalías están disponibles comercialmente, el contexto de utilización puede ser específico para la aplicación o la infraestructura utilizada por la empresa. Consulte con el negocio que proporciona el sistema de supervisión para determinar cómo capturar e interpretar las métricas de una manera que sea más efectiva para la implementación específica.

Las capas por separado pueden tener anomalías diferentes que indican un ataque o compromiso. Evalúe cuáles son esos indicadores para cada capa.

Considere utilizar material bibliográfico de las siguientes organizaciones para ayudar con esta recomendación:

- Documentación de Supervisión EC2 de Amazon

    - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html
- Supervisión de Google Cloud
    - https://cloud.google.com/monitoring/
- Supervisión de Microsoft Azure
    - https://azure.microsoft.com/en-us/documentation/articles/best-practices-monitoring/
- Tutoriales de supervisión de DigitalOcean (General)
    - https://www.digitalocean.com/community/tags/monitoring?type=tutorials

5.7.1 Riesgo

La tecnología de supervisión de sistemas es una propiedad clave del modelo de seguridad de IoT. Sin supervisión, no hay manera de determinar si se ha encontrado una vulnerabilidad en los componentes críticos del servicio. La supervisión permite a los administradores diagnosticar rápidamente puntos problemáticos en el servicio y la infraestructura, y puede ayudar a diferenciar entre incidentes de seguridad y errores de software.

5.8 Defina un Modelo de Respuesta a Incidentes

No es suficiente detectar un posible compromiso o un ataque en curso. La organización debe ser capaz de reaccionar y combatir el ataque. Si un sistema se ve comprometido, “limpiarlo” o apagarlo no es suficiente. La organización debe, en cambio, ser capaz de diagnosticar el origen del compromiso, aplicar un parche al sistema y desplegar el parche en toda la infraestructura existente.

Esto puede ser difícil si se utiliza un entorno basado en contenedores donde las aplicaciones clonadas se ejecutan en una configuración vulnerable. El sistema de aplicaciones debe ser capaz de detectar un evento de "reinicio" o "actualización", donde la conexión a una aplicación se transfiere de manera elocuente a otro sistema en la nube, o el usuario se desconecta por la fuerza, para permitir que se realice una actualización.

Sin importar cuál sea el modelo de ejecución, sin embargo, el equipo de ingeniería debe ser capaz de capturar métricas de una manera que permita el análisis “forense”. Estas políticas y procedimientos deben ser inamovibles y aprobados por el equipo legal (y posiblemente el equipo de seguros) para validar si la información se representa de una manera adecuada para los oficiales encargados de hacer cumplir la ley (LEO). El cumplimiento ayudará a garantizar que el negocio no solo cumpla con las leyes locales y federales, sino que también proporcione muestras de un compromiso que pueda utilizarse en los tribunales.

Una vez que las muestras son capturadas, cada aspecto del sistema general debe ser evaluado para registros, métricas y otros datos que puedan corroborar el evento en cuestión. Todos estos datos deben capturarse y almacenarse en un sistema seguro para su revisión legal.

Considere utilizar material bibliográfico de las siguientes organizaciones como ayuda para esta recomendación:

- Recomendaciones del CERT para crear un CSIRT
  - http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm

5.8.1 Riesgo

Las organizaciones que carecen de un modelo de respuesta a incidentes necesitarán mucho más tiempo para organizar sus recursos, identificar sistemas comprometidos, poner en cuarentena esos sistemas y revisar los sistemas para obtener información. Esto también ralentiza significativamente los esfuerzos que se deben realizar para parchar y restaurar un sistema determinado. Esta falta de preparación otorga a los adversarios una gran oportunidad para aprovechar un compromiso al moverse lateral o verticalmente dentro de un entorno determinado. Esto puede provocar un compromiso significativamente mayor debido al aumento del tiempo de respuesta. Las organizaciones deben estar preparadas para responder a un incidente casi de inmediato para reducir el tiempo que un adversario tiene para controlar elementos críticos del servicio.

5.9 Defina un Modelo de Recuperación

Independientemente de si un usuario o aplicación se ve afectado debido a un compromiso de seguridad o un problema en el hardware, debe producirse un proceso de recuperación. Se debe implementar un procedimiento para recuperar la información y la capacidad dentro de la capa de las aplicaciones. El procedimiento debe adaptarse al contexto de cada aplicación y capa.

Por ejemplo, si una aplicación ha alamcenado información de un Dispositivo Periférico con respecto al resultado de una acción en particular, y hay un error de almacenamiento que impide que la aplicación guarde el resultado de esos datos en un almacenamiento persistente, la aplicación puede:

- Intentar almacenar de nuevo los datos hasta que tenga éxito (puede ser interminable)
- Intentar el almacenamiento durante un número limitado de intentos hasta alcanzar ciertos umbrales de éxito o error
- Fallar inmediatamente, pudiendo perder las métricas
- Pedir nuevamente al Dispositivo Periférico la misma información (puede que nunca esté disponible)

Se debe elegir el método que sea más adecuado para la aplicación y el requisito empresarial. Esto, nuevamente, dependerá del contexto de la aplicación, y puede no ser fácil de modelar fuera de un entorno determinado.

Involucre tanto al equipo de ingeniería como a los directivos de la empresa para determinar cómo debería recuperarse una aplicación con un comportamiento erróneo o comprometida, especialmente en el contexto de la actividad de un usuario.

Para sistemas que han sido comprobadamente comprometidos por un adversario, debe existir un modelo para validar que la aplicación o el sistema ha sido suficientemente parcheado antes de la recuperación. Sin este conjunto de políticas y procedimientos definidos, un sistema vulnerable simplemente puede ser desplegado nuevamente en el Ecosistema de Servicios, facilitando compromisos adicionales.

5.9.1 Riesgo

Los modelos de recuperación garantizan que la información, las aplicaciones y las configuraciones se restablezcan correctamente. Sin un modelo de restauración, el equipo puede redistribuir involuntariamente subsistemas vulnerables a servidores o a elementos de la infraestructura. Además, los datos viciados que podrían haber sido manipulados por un adversario en una base de datos o en un entorno de almacenamiento podrían replicarse en múltiples sistemas, propagando malware involuntariamente o simplemente datos modificados. Los procesos de recuperación reducen la capacidad de los adversarios para abusar de las debilidades en la recuperación de un incidente, lo que se suma a un evento que ya es costoso.

5.10 Defina un Modelo de Retirada Gradual

Cada sistema implementado por una empresa y cada capa utilizada tiene una vida útil. Incluso si la organización implementa el mismo producto o servicio durante décadas, las tecnologías utilizadas para impulsar ese producto o servicio cambiarán. Por lo tanto, no solo debe haber un plan para diseñar e implementar el producto o servicio, debe haber un plan para retirar del mercado ese producto o servicio.

Este proceso ayuda a garantizar que todas las tecnologías sean revocadas y desmanteladas de tal manera que un adversario no pueda asumir la identidad de una tecnología determinada, o utilizar sus facilidades y características. Por ejemplo, un caso simple es un dominio atribuido a un producto en particular después de la adquisición de una empresa por parte de una empresa matriz. Si se cambia el nombre del producto y el dominio se migra al dominio de la empresa matriz, un adversario puede tomar posesión del dominio original del producto que en principio ya no existe. Si el adversario puede emitir certificados criptográficos para el dominio obsoleto y aún interactuar con la tecnología implementada bajo ese dominio, habrá una brecha significativa en la seguridad causada por la falta de procedimientos en la retirada de ese producto o servicio del mercado.

Cada tecnología utilizada en la arquitectura, implementación y administración de un determinado producto o servicio debe, entonces, ser catalogada y evaluada desde el punto de vista de su usabilidad. Una vez que esa tecnología ya no pueda ser utilizada, puede retirarse del mercado según el modelo estudiado previamente. Esto permite a los ingenieros y a los directivos empresariales migrar la tecnología a un conjunto más adecuado de productos novedosos sin lagunas de seguridad en las plataformas subyacentes. También garantiza que un producto que ya no se ofrecerá a los socios y usuarios terminará su ciclo de vida sin posibilitar su puesta en peligro por parte de los adversarios una vez que el negocio se cierre.

5.10.1 Riesgo

La falta de un proceso de retirada gradual del mercado puede ocasionar que tanto competidores como adversarios pongan en peligro los Dispositivos Periféricos, así como los servicios. Esto es posible legalmente porque si una organización libera el acceso a ciertos objetos, como nombres de dominio, números de teléfono y otros servicios renovables, un adversario o competidor tiene el derecho de adquirir esos objetos, aunque esto parezca no ser ético. Esto puede poner a disposición de atacantes sin escrúpulos o con intenciones dehonestas, dispositivos o servicios.

5.11 Defina un Conjunto de Clasificaciones de Seguridad

Para gestionar adecuadamente las interacciones con las empresas asociadas a un servicio de IoT de manera efectiva, se deben definir clasificaciones de seguridad. Esto establecerá "el tono" no solo para la política interna de la organización en materia de seguridad de datos, sino que ayudará a definir el nivel de seguridad que las empresas asociadas aplican a los datos transmitidos, sus propios datos y los datos de los clientes.

Si bien este proceso debe ser investigado y adaptado a la empresa, la mayoría de las políticas de clasificación de seguridad de datos deberían comenzar con las siguientes clases:

- Público: cualquier entidad que tenga acceso
- Clasificado: el usuario debe autorizar la publicación
- Secreto: datos específicos del usuario
- Secreto máximo: datos específicos de la organización, que nunca se publicarán

Después de definir las clases básicas, la empresa debe evaluar cómo se debe atribuir cada clase de seguridad a una clase de datos. En otras palabras, evalúe cómo debe usarse la clasificación en la práctica, no solo en la teoría. Determine qué políticas y procedimientos se deben implementar desde una perspectiva comercial y de ingeniería.

Esto permitirá a la empresa no solo definir políticas tecnológicas, sino promulgar políticas comerciales que respalden los requisitos técnicos. Esto facilita que el equipo de ingeniería transmita estos requisitos a los socios y a las organizaciones internas que buscarían contrarestar la política, ya sea intencionalmente o no.

Una vez que las clasificaciones de seguridad han sido estandarizadas, es importante evaluar cómo el modelo de clasificación de seguridad puede verse afectado por los requisitos de privacidad de la empresa y sus usuarios. La empresa debe tomarse el tiempo necesario para aplicar un modelo de privacidad a las clasificaciones de seguridad, dar sentido a los datos de los usuarios y ayudar a proteger su privacidad en caso de que un socio desee acceder a recursos específicos que podrían poner a los usuarios y sus datos personales en riesgo de ser expuestos. Al contextualizar la privacidad dentro de las clasificaciones de seguridad, los socios necesitarán buscar la aprobación de los directivos empresariales y los usuarios, cuando los socios quieran acceder a ciertos tipos de datos centrados en la privacidad. Los usuarios deben tener la opción de proteger sus datos y su privacidad y deben poder limitar la exposición de sus datos a terceros.

5.11.1 Riesgo

La clasificación de los modelos de seguridad es imprescindible para diseñar soluciones que utilicen la seguridad de manera efectiva. Para proteger la información, esta debe ser cualificada de modo que los controles apropiados puedan formularse en base a las políticas y procedimientos correspondientes. Sin estos modelos, los ingenieros tienden a implementar la seguridad de manera abusiva, o no lo hacen en absoluto, dependiendo de su percepción de los riesgos involucrados. Todo el equipo, incluidos los ingenieros y los directivos de la empresa, debe identificar qué significan los datos para la empresa y cómo se deben asegurar dentro de un rango de rentabilidad apropiado.

5.12 Defina Clasificaciones para Conjuntos de Tipos de Datos

Después de definir las clasificaciones de seguridad, la empresa debe definir los tipos de datos que utilizará el producto o servicio general de IoT. Esto le permitirá definir claramente qué tipos de información se adquieren, generan y difunden a sus pares en el sistema IoT, y cómo la organización debe tratar este tipo de datos. Estos datos proporcionarán un contexto y un valor a los componentes generales utilizados en todo el entorno de IoT.

Si bien este documento no intentará presentar un modelo que cubra todas las variaciones posibles en los tipos de los datos, a continuación, se listan unos cuantos tipos:

- Acciones
- Imágenes
- Documentos editables
- Información de identificación personal
- Información protegida de salud

Una información puede atribuirse a uno o más tipos de datos. Pero, a los datos en sí se les debería atribuir solo una clase de seguridad. Si bien el tipo identifica lo que representan los datos y cómo deben procesarse, la clase de seguridad representará cómo, dónde y cuándo se puede usar la información, y con quién se puede compartir.

Definir los distintos tipos de datos y atribuirles clasificaciones es un proceso muy elaborado. Al hacerlo, establece un estándar en la empresa para el negocio y permite que el equipo de ingeniería ejecute controles técnicos sobre los datos y sus clasificaciones. Esto ayuda enormemente a los equipos de ingeniería y de gestión del negocio a negociar cuando sea necesario con posibles socios, cómo se pueden compartir y procesar los datos.

5.12.1 Riesgo

Al igual que con las clasificaciones de seguridad, los controles no se pueden implementar en torno a los datos sin cuantificar qué datos son, y qué relación tienen esos datos con la empresa. Estas clases definen cómo se debe usar la información dentro del sistema y qué protecciones se deben aplicar a los datos para mantener una postura de seguridad adecuada. Sin estas clases, los ingenieros tienden a aplicar medidas de seguridad demasiado estrictas o demasiado débiles. El equipo de ingeniería y los gestores empresariales deben acordar que medidas de seguridad deben aplicarse, para equilibrar los controles con la importancia que los datos tienen para el negocio.

6 Recomendaciones de Alta Prioridad

Las recomendaciones de alta prioridad representan el conjunto de recomendaciones que deben implementarse, pero solo si la arquitectura de Dispositivo Periférico lo requiere. Por ejemplo, no todas las arquitecturas de Dispositivos Periféricos requieren una carcasa o empaquetamiento de producto a prueba de manipulaciones. Estas recomendaciones deben evaluarse para determinar si el caso comercial las considera un requisito.

6.1 Defina un Modelo Claro de Autorización

Si bien el modelo de privacidad se relaciona con la forma en que se ofrece la información del usuario a los socios, el modelo de autorización define cómo la empresa o los socios actuarán en nombre de un usuario. Esto, por ejemplo, sería útil para un sistema de

domótica en el que las métricas de un socio podrían optimizar el uso de la calefacción o el aire acondicionado en una casa determinada. El modelo de autorización le otorgaría al socio la capacidad de cambiar los parámetros de la calefacción o aire acondicionado para la casa de ese usuario cuando el socio midiera ciertos valores en los sensores.

Para lograr esto, tenga una GUI (Interfaz Gráfica) que describa las capacidades de autorización detalladas y cómo se distribuirán a los socios. Permita que el usuario otorgue acceso o revoque el acceso a ciertas capacidades cuando sea necesario. Asegúrese de que las capacidades revocadas actúen de inmediato, para disminuir el potencial de abuso o ataques.

El sistema debe supervisarse en gran medida para garantizar que los socios no tomen medidas que no están autorizados a tomar. El control granular del modelo de autorización debería permitir a los usuarios configurar cuándo los socios tienen acceso a ciertas capacidades y con qué frecuencia. Atributos de este tipo, permitirán al usuario ejercer el control sobre su sistema evitando que un socio abuse o comprometa (piratee) su producto.

6.1.1 Riesgo

Sin un Modelo de Autorización, los terceros no tendrán al acceso restringido a los datos con las capacidades de un usuario. Esto puede permitir que un tercero malintencionado o “hacker” pueda acceder sin limites a la tecnología en cuestión o a los datos de un usuario. Al crear un modelo de autorización, el acceso está restringido según los atributos que un usuario programa y autoriza. Esto permite al usuario tener un mayor control sobre qué capacidades y datos están disponibles para terceros, y reduce el riesgo del proveedor de servicios IoT al reducir el potencial de un compromiso generalizado.

6.2 Gestione una Arquitectura Criptográfica

Toda la tecnología implementada en un entorno IoT debe usar capacidades criptográficas, independientemente de si la tecnología utilizada es un Dispositivo Periférico “ligero” o un servicio robusto en la nube. Para implementar correctamente la seguridad en un producto o servicio de IoT, la criptografía utilizada debe estar bien estructurada, gestionada y ajustada para cumplir con las especificaciones cambiantes a lo largo del tiempo.

El equipo de ingeniería debe identificar si:

- Sus algoritmos criptográficos han quedado obsoletos
- Están usando claves criptográficas con longitudes de bits adecuadas
- Los algoritmos “hash” están sujetos a ataques de colisión
- Se usa un generador de números aleatorios robusto
- Los mensajes están suficientemente protegidos con datos aleatorios
- Los protocolos criptográficos, como TLS, están actualizados con las mejores prácticas
- Se utilizan conceptos centrados en la privacidad, como el secreto hacia adelante
- Las contraseñas de texto simple o los números de pin se transmiten a través de las redes
- Se utilizó un algoritmo criptográfico personalizado

Cada uno de estos puntos, y algunos más no considerados aquí, son importantes para mantener una arquitectura criptográfica de alta calidad dentro del producto o servicio de IoT.

El éxito en la implementación de una solución criptográfica está estrechamente ligado a la capacidad del equipo de ingeniería de aprovechar las soluciones de criptografía más flexibles para implementar parches en tecnologías que usan soluciones menos flexibles.

Por ejemplo, recientemente se descubrió que el algoritmo RC4 tiene importantes fallos de seguridad. Si un parche se puede distribuir de forma segura a los clientes configurados para usar el algoritmo RC4, reemplazando RC4 con el algoritmo AES-256, entonces RC4- el algoritmo empleado- no es en sí un motivo de preocupación. Si la autenticación mutua se realiza utilizando una tecnología más resistente, como el intercambio de claves Ephemeral Diffie Hellman y claves asimétricas, o un token de seguridad UICC, el parche puede verificarse sin utilizar el algoritmo criptográfico vulnerable.

Las contraseñas y los pines utilizados por un usuario o Dispositivo Periférico nunca se deben transmitir a través de la red en formato de texto simple, incluso si el canal de comunicaciones está protegido mediante cifrado. En su lugar, se debe usar el hash criptográfico de la contraseña o pin, para garantizar que cualquier configuración incorrecta en el túnel criptográfico no exponga la contraseña. La contraseña y al menos un token único cada vez deben generar el hash. Si bien es común que este token se tome de la sesión de red, es más seguro tomar el valor de un código continuo almacenado tanto en el Dispositivo Periférico como en la infraestructura del servicio. De esta forma, un atacante con una posición de privilegio en la red no puede distruibuir el hash con valores beneficiosos, lo que puede resultar en un ataque de firma forzada.

Algoritmos criptográficos personalizados (algoritmos diseñados específicamente) nunca deben usarse. Utilice siempre algoritmos recomendados desarrollados por criptógrafos y recomendados por organizaciones de supervisión especializadas en seguridad criptográfica. Siempre evite el uso de algoritmos mal diseñados, algoritmos obsoletos o comprimidos, de conversión de binario a texto u otros algoritmos comúnmente confundidos con algoritmos criptográficos, como LZO, base64, ROT13 y XOR.

Revise las siguientes guías y referencias para obtener más información sobre este tema:

- ISO 18033-1: 2015 - Algoritmos de encriptación
- ISO 18033-2: 2015 - Cifrados asimétricos
- ISO 18033-3: 2015 - Cifras de bloque
- www.owasp.org/index.php/Guide_to_Cryptography
- csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
- csrc.nist.gov/groups/ST/toolkit/key_management.html

6.2.1 Riesgo

La implementación adecuada de una solución con una arquitectura criptográfica asegura que los algoritmos, protocolos y secretos utilizados estén dentro de las recomendaciones que se mencionan en este capítulo. Además, las recomendaciones cambian con el tiempo. Sin una arquitectura criptográfica, será más difícil identificar todas las tecnologías que han quedado obsoletas, lo que crea una oportunidad para aprovechar las lagunas en la seguridad.

6.3 Defina un Modelo de Comunicaciones

Cada sistema en el Ecosistema de Servicios debe ser capaz de implementar autenticación mutua. Ningún usuario público anónimo debería tener acceso a ninguna plataforma informática dentro de este ecosistema. Cada Dispositivo Periférico, Socio o Usuario se comunicará con el Ecosistema de Servicios a través de tecnologías que requieren autenticación mutua. Dado que los servicios que conforman la interfaz de usuario suelen implementarse y administrarse en un entorno separado, la interfaz de acceso público debe estar resguardada en ese espacio. El Ecosistema de Servicios, sin embargo, comprende el conjunto de todos los sistemas utilizados para desplegar servicios hacia todos los recursos autenticados.

Esto incluye los Dispositivos Periféricos que aún no han sido aprovisionados por el sistema, ya que el proceso de fabricación y personalización del hardware debe configurar el hardware lo suficientemente bien como para que pueda autenticarse como un recurso implementado por la empresa.

Por lo tanto, el modelo de comunicación debe proporcionar:

- Autenticacion mutua
- Confidencialidad
- Integridad

Para lograr esto de manera efectiva, el modelo de comunicaciones también debe proporcionar:

- Una raíz de confianza centralizada o, como alternativa, una raíz de confianza descentralizada
- Aprovisionamiento de identidad y un método de revocación
- Secreto perfecto hacia adelante (PFS)

Se debe usar una raíz de confianza para garantizar que cada entidad en el modelo de comunicaciones esté autorizada por la misma organización que el par. Esto ayuda a garantizar que todas las entidades hayan sido aprovisionadas y autorizadas por una organización central. La tecnología utilizada para asegurar esta raíz de confianza puede ser centralizada (similar a los certificados TLS) o descentralizada (similar a los modelos IoT basados en la cadena de bloques de Bitcoin, como por ejemplo, el proyecto ADEPT de IBM / Samsung, Tilepay y otros). De todos modos, una empresa central debe ser la propietaria del modelo y proteger el sistema de aprovisionamiento.

El aprovisionamiento y la revocación deben ser parte del modelo de comunicaciones, para ayudar a garantizar que cualquier secreto o identidad comprometida se pueda eliminar del sistema con un mínimo esfuerzo. Tecnologías como el protocolo de seguridad de certificados en línea (OCSP) ayudan con este proceso.

El protocolo de comunicaciones debe emplear una tecnología que mitigue el potencial de comprometer las comunicaciones pasadas. Esto se hace mediante la creación de claves criptográficas asimétricas efímeras que se utilizan para intercambiar un secreto de comunicaciones. Si un certificado se ve comprometido, el secreto efímero no lo será. Esto garantiza que el almacenamiento de mensajes cifrados durante un período de tiempo

prolongado no provocará que un adversario los descifre si el certificado de secreto privado se ve comprometido o expuesto.

El desafío de la seguridad de las comunicaciones radica en la implementación y la longevidad de la tecnología. Los algoritmos de encriptación pueden seleccionarse con un alto grado de confianza por parte de entidades autorizadas, lo que disminuye el potencial de error.

Deben usarse implementaciones de bibliotecas y algoritmos diseñados o aprobados por entidades de ingeniería de seguridad contrastadas. No se deben usar implementaciones personalizadas de algoritmos. Esto disminuye no solo el trabajo del equipo de ingeniería, sino también la posibilidad de que un algoritmo sea criptográficamente debilitado por un sistema mal diseñado o implementado incorrectamente.

Considere utilizar el material bibliográfico de las siguientes organizaciones para implementar las recomendaciones mencionadas:

- Guía de procedimientos de autenticación mutua de CafeSoft Apache:
  - http://www.cafesoft.com/products/cams/ps/docs32/admin/ConfiguringApache2ForSSLTLSMutualAuthentication.html

6.3.1 Riesgo

La seguridad de las comunicaciones es la piedra angular de IoT. Sin la seguridad de las comunicaciones, no hay garantía de que los dispositivos integrados se estén comunicando con los servicios de back-end correctos. Esto es imprescindible para servicios críticos que gestionan, configuran y envían comandos a dispositivos tales como unidades telemáticas, dispositivos médicos y sistemas de control industrial. Sin la seguridad de las comunicaciones, no hay garantías de que los comandos se envíen al Dispositivo Periférico correcto. Haga cumplir la seguridad de las comunicaciones para garantizar que los mensajes se transmiten hacia el interlocutor deseado.

6.4 Use Servicios de Autenticación de la Red de Comunicaciones

Al tener operadores de red como socios, los usuarios pueden autenticarse utilizando tokens específicos del operador de red. Si bien estos tokens, presentes en la UICC del operador de red, autentican a un usuario en la capa de red, no necesariamente autentican al usuario en la capa de la aplicación. El uso de las siguientes tecnologías puede facilitar la autenticación de red:

- Arquitectura genérica de arranque (3GPP TS 33.220)
- M2M SM (ETSI TS 102 921)

Evalúe si tendría significado utilizar una tecnología de autenticación en la capa de aplicación. Si el token se puede usar como un almacén de seguridad, determine si el dispositivo se puede usar como una capa de autenticación para que el Dispositivo Periférico físico construya un TCB usando el token.

Si bien muchos operadores de red utilizan la autenticación facilitada por la red de comunicaciones, otorgar acceso a esta API para autenticar usuarios o Dispositivos Periféricos es una tecnología bastante novedosa. Evalúe si el operador de red con el que

está trabajando tiene experiencia contrastada en este tema de seguridad. Si es así, considere usar esta tecnología como algo más que un token de autenticación de capa de red, ya que puede utilizar más fácilmente una sola tecnología para el almacenamiento de tokens de seguridad, en lugar de usar muchas tecnologías diferentes.

6.4.1 Riesgo

Cuando los servicios de autenticación de red incorporan anclas de confianza como el UICC, no utilizar estos servicios para asegurar la capa de aplicación limitará la capacidad de la aplicación para autenticar de manera fiable a los usuarios y aumentará el gasto en la plataforma de Dispositivos Periféricos subyacente. Esto aumenta el costo de implementación y también disminuye la información disponible por parte del operador de red.

6.5 Provisione Servidores cuando Sea Posible

El aprovisionamiento de servidores implica definir, configurar, personalizar y desplegar un servidor en un entorno de producción. El proceso de aprovisionamiento, desde la perspectiva del servicio, garantiza que un servidor esté reforzado desde el punto de vista de seguridad y listo para su implementación en un entorno que puede ser potencialmente hostil.

Independientemente de si el servidor se implementa en una infraestructura en la nube, en un proveedor de almacenamiento dedicado o en el espacio de rack específico de una empresa, un servidor será vulnerable tanto a amenazas internas como externas. El servidor debe reforzarse contra ataques externos antes de que se despligue en la infraestructura del servicio.

Para lograr esto, identifique los servicios que deberían ser accesibles globalmente en el entorno donde van a desplegarse. Defina si el entorno en el que funcionará el servidor será público o privado, y lo que eso significa en el contexto de la seguridad del servidor. Determine si cada servicio que se ejecuta en el servidor debe ser accesible para el público en general, o si solo los clientes autenticados deben conectarse al servicio.

Evalúe el ciclo de vida del sistema operativo que se ejecutará en el servidor. Determine cómo administrar adecuadamente las actualizaciones de software para garantizar que los parches de seguridad se implementarán rápidamente y se asignarán a los servidores que trabajan en producción. Evalúe un modelo de recuperación en caso de que las actualizaciones fallen o provoquen problemas inesperados con los servicios en producción, ya que algunas actualizaciones de bibliotecas o aplicaciones pueden provocar efectos secundarios no deseados.

Finalmente, evalúe el modelo de retirada del mercado del servidor aprovisionado para determinar la forma más segura de eliminar activos del sistema. Esto incluye los registros del sistema que pueden ser necesarios para evaluar el servicio defectuoso o el comportamiento del cliente.

Esta recomendación implica que la organización debe implementar un proceso de gestión de parches para identificar servicios vulnerables, implementar parches y supervisar el éxito de la implementación de dichos parches.

Por favor revise el siguiente material bibliográfico sobre gestión de parches:

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

6.5.1 Riesgo

El aprovisionamiento de servidores es una parte imprescindible de la seguridad general de un entorno de IoT. Sin él, el control de la organización sobre la arquitectura del servidor se verá sustancialmente debilitado. Esto puede generar lagunas en la seguridad debido a la falta de una especificación correcta de la arquitectura. Sin una especificación clara, la organización no puede revisar si las tecnologías implementadas siguen las mejores prácticas actualizadas. Además, la mejora de estas tecnologías requerirá la investigación de cada sistema desplegado para evaluar los cambios puntuales entre los activos desplegados. Esto es ineficiente y una gran preocupación en caso de que se deba implementar una actualización de seguridad crítica. Si no hay consistencia, ni una arquitectura para definir los servicios, no habrá forma de rastrear fácilmente qué sistemas requieren atención inmediata sin tener que verificarlos manualmente uno a uno.

6.6 Defina un Modelo de Actualización

La actualización de un entorno de ejecución, imagen de aplicación o TCB es un proceso muy complejo. Considere el siguiente modelo de ejemplo que simplifica el proceso general:

- Para cada capa de la plataforma de ejecución, defina un recurso de red como una URL única para la nueva imagen de la aplicación
- Genere una clave de firma para cada capa específica
- Genere una imagen para todas y cada una de las nuevas versiones autorizadas de cada capa
- Incluir metadatos que describan la imagen de la capa internamente(versión, marca de tiempo, identidad, etc.)
- Firme la imagen de la capa con la clave de firma
- Haga que la imagen, la firma y la clave pública estén disponibles, posiblemente a través de un recurso de red único, o mediante un servicio de actualización

Cuando se implementa un nuevo sistema, debe:

- Para cada capa:
  - Recuperar la(s) versión(es) a desplegar
  - Verificar criptográficamente la imagen
  - Desplegar la imagen de la capa en el sistema

No se deben almacenar secretos privados en ninguna capa de aplicación. En cambio, los secretos se deben aprovisionar dinámicamente a medida que se implementa cada sistema para personalizarlo. Estas identidades deberían revocarse a medida que el sistema se retira del servicio, sin importar la duración de la vida útil de ese sistema.

Esta recomendación implica que se debe usar un proceso de administración de parches para mantener los servicios y las tecnologías dentro de la infraestructura.

Por favor revise la siguiente documentación para más información:

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

6.6.1 Riesgo

Sin un modelo de actualización bien definido, los servicios y las aplicaciones pueden verse comprometidos a través del abuso del procedimiento de actualización. Los adversarios pueden insertar aplicaciones personalizadas en el proceso de actualización e implementar su propio software en los sistemas de la nube y otros servidores. Si la infraestructura de las comunicaciones no es segura, esto se puede realizar fácilmente simplemente manipulando servicios estándar de red como el servicio de nombres de dominio (DNS). Los ataques más avanzados contra el enrutamiento, como los ataques del “Border Gateway Protocol” (BGP), se han implementado muchas veces anteriormente para comprometer servicios no-seguros.

6.7 Defina una Política para las Brechas de Seguridad en los Datos Espuestos

Definir políticas y procedimientos para la clasificación de datos no es suficiente. También debe haber un modelo para detectar si un socio ha expuesto los datos. La organización debe tener un plan establecido para evaluar si un socio estuvo involucrado en prácticas comerciales que infringen los controles tecnológicos o las políticas establecidas para proteger los datos y la privacidad del usuario.

Para lograr esto, el equipo de ingeniería debe definir las tecnologías de supervisión y registro que se aplican a las clasificaciones de seguridad y no simplemente a los datos del usuario. Esto permitirá que una guía para la auditoría sobre los datos se aplique no solo a la información, sino a la clasificación de esa información. Esto ayudará a la organización a defenderse en caso de que la información del usuario quede expuesta. La organización podrá mostrar que sus clasificaciones de seguridad y los controles técnicos implementados para administrar esas clases administran, almacenan y difunden los datos de acuerdo con la política establecida.

Es beneficioso que la organización utilice la tecnología de supervisión y registro para probar cuándo un socio ha incumplido las normas de las clasificaciones de seguridad. La gestión comercial de la empresa debería, en ese momento, decidir si el socio debe o no estar sujeto a multas, al término de su relación contractual u otras consecuencias.

6.7.1 Riesgo

Sin una política de incumplimiento, existen pocos resguardos legales para proteger a la organización de la responsabilidad sobre los datos que han sido expuestos por un tercero. Si la empresa es la causante de que los datos hayan sido expuestos, el tercero puede haber perdido los datos, pero la empresa es responsable de los datos que entrega a sus socios originalmente.

Las políticas de incumplimiento aseguran que los socios deben mantener un nivel de seguridad adecuado para los datos que se les proporcionan. Cualquier incumplimiento de esa seguridad ayuda a eliminar la responsabilidad del proveedor de servicios IoT siempre que el proveedor de servicios IoT cumpla con sus propios requisitos de seguridad. Luego, le corresponde al socio adherirse a esa política.

Estas políticas deben ser revisadas por los equipos legales y de seguros para garantizar que los modelos, de hecho, reduzcan la responsabilidad de la organización mediante la adhesión a políticas y procedimientos de seguridad rigurosos. Algunas empresas, debido a la naturaleza de los productos o servicios que ofrecen, pueden no estar exentas debido a las regulaciones, estatutos legales u otras cuestiones.

6.8 Fuerce la Autenticación a través del Ecosistema de Servicios

Una interfaz de usuario nunca debe autenticar a un usuario directamente. El sistema siempre debe poder autenticar al usuario utilizando un servicio de autenticación centralizado. La única excepción a esta regla es cuando una aplicación que se ejecuta en un dispositivo móvil está protegida por un código local de acceso. Este código de acceso se puede usar para acceder a la aplicación local. Sin embargo, el acceso a servicios y recursos remotos debe verificarse mediante un token de autenticación separado.

Aunque, para la usabilidad, el equipo de ingeniería puede optar por unir estos dos esquemas de autenticación en uno solo si al usuario se le proporciona suficiente información que describa los riesgos de utilizar este método de autenticación. Tal método permitiría que la contraseña de la aplicación local de un usuario autenticado descifre una base de datos local que contenga un token de autenticación que funcione para el servicio remoto. Este modelo de autenticación por etapas puede ser suficiente para la mayoría de los usuarios.

De todos modos, el servicio de autenticación central primero debe autenticar al usuario en la aplicación local y luego aplicar las políticas y los procedimientos que determinan cómo se puede usar ese token de autenticación y durante qué período de tiempo. Las métricas también se deben recopilar para determinar si el usuario ha migrado a una plataforma informática alternativa, pero está utilizando el mismo token. O bien, si el usuario se ha movido a otra ubicación hace poco, pero está usando el mismo token. Según el tipo y la velocidad de la migración del usuario, estas medidas pueden indicar un posible compromiso del token. En ese momento, el token debería invalidarse, y el usuario debería verse obligado a volver a iniciar la sesión, posiblemente mediante el uso de autenticación multi-factorial, cuando corresponda.

6.8.1 Riesgo

Debido a los posibles abusos en los sistemas de Dispositivos Periféricos, independientemente de qué tan segura sea la arquitectura, la autenticación de un usuario sin la confirmación de un sistema central es siempre poco fiable. Esto presupone que el usuario no ha actualizado sus credenciales, o puede almacenar sus credenciales parcialmente en varios tipos de dispositivos. Esto es ineficiente y puede abrir un espacio donde un dispositivo comprometido está usando una versión anterior de las credenciales del usuario.

6.9 Implemente la Verificación de Datos de Entrada

Todos los datos adquiridos por un Dispositivo Periférico, usuario o supuesto usuario deben analizarse para detectar anomalías. La ruta de ataque más fácil para un hacker siempre se encuentra en los servicios que se utilizan en la interfaz de usuario y que se componen de aplicaciones web. Esto se debe a que esta tecnología debe generar información de forma dinámica, en función de las variaciones de la localización, en las codificaciones y otros

parámetros que cambian de usuario a usuario. Los usuarios expertos pueden manipular ciertos atributos en la codificación de los datos para causar efectos colaterales inesperados que se puedan utilizar en diferentes capas de los subsistemas de procesamiento.

Por ejemplo, un ataque muy interesante consiste en la codificación de un byte nulo en mensajes procesados como cadenas por lenguajes de alto nivel. Algunos lenguajes de alto nivel aceptan bytes nulos como parte de una cadena binaria, en lugar de interpretarlo como un delimitador. Cuando esta cadena binaria se pasa a las bibliotecas de nivel inferior, el byte nulo incorporado se interpreta como un delimitador de cadena, truncando la cadena y así significando algo completamente diferente de lo que la aplicación interpretó en la cadena original. En el pasado, esta ha sido una manera inteligente de acceder a los recursos del sistema de archivos que de otro modo no estarían disponibles para un usuario en particular.

Si bien hay un número infinito de variaciones en que se pueden construir entradas de datos maliciosas, los ingenieros no necesitan realizar pruebas para todos los casos posibles. En cambio, el proceso que se puede utilizar es bastante simple:

- Identificar cómo se usarán los datos internamente
- Aplicar una política sobre qué tipos de codificaciones y caracteres se adhieren al modelo de uso interno
- Diseña una API que analice los datos de acuerdo con esta política
- Levante una excepción cuando se hayan identificado datos que rompan el modelo
- Registre el evento internamente en cada sesión con metadatos para ayudar a detectar un comportamiento anómalo

Todos los datos almacenados dentro del sistema primero deben procesarse y compilarse con un modelo estático. Una técnica efectiva para esto es simplemente codificar todos los datos con el algoritmo base64, y luego almacenarlo en una base de datos. Esto asegura que los datos de ninguna manera pueden manipular la base de datos.

6.9.1 Riesgo

Los sistemas que no emplean la verificación de entrada están sujetos a una serie de ataques posibles, incluidos los problemas a los que se hace referencia en el Top Ten de OWASP, como “SQL Injection” (SQLi), e incluso ataques de ejecución remota de código. Debido a que el rango de posibles abusos es tan amplio, el riesgo no se puede cuantificar completamente aquí. La verificación de entrada es una característica crítica de cualquier aplicación segura, ya sea un servicio en la nube o una aplicación que se ejecuta en un Dispositivo Periférico.

6.10 Implemente Filtrado de Salida de Datos

El filtrado de salida es el complemento para la verificación de entrada. Este proceso no solo protege la capa de presentación de la manipulación maliciosa, sino que también impide que el sistema entregue información privilegeada a un usuario cualquiera.

En el primer caso, todos los datos que debe representar la capa de presentación deben evaluarse antes de abandonar la capa de servicio. Esto asegurará que los datos codificados en la capa de presentación, por ejemplo, en mensajes JSON o JavaScript codificado, no contengan un formato que pueda romper o invalidar la presentación de los datos. Esto significa que los caracteres almacenados en el sistema que, si se representan, podrían

romper el modelo de presentación deben filtrarse o codificarse de tal forma que no alteren la presentación de forma inesperada.

Una metodología para solucionar este problema es filtrar los caracteres restringidos, aplicar una codificación en todos los caracteres para que la presentación de estos caracteres no altere la Interfaz Gráfica de Usuario (los caracteres no son interpretados por un motor de renderizado como códigos de control), o simplemente no mostrando el mensaje. Si bien cualquiera de estos métodos funciona, algunos son más apropiados en ciertas aplicaciones. Al analizar el caso de un foro de mensajes, sería igual de perjudicial que un adversario pudiera colocar “scripts” que otros usuarios puedan copiar y ejecutar sin saber lo que están haciendo. Por lo tanto, en lugar de simplemente renderizar la información de una manera que no inyecte código HTML u otros scripts en la capa de presentación, la información debe eliminarse para que otros usuarios no se vean afectados.

En el caso de que los datos no se deban presentar al usuario, esto no se relaciona con los datos almacenados y procesados por un adversario. Por el contrario, este problema se relaciona con la representación de datos que no son aptos para el consumo público y deben reservarse para administradores e ingenieros. Por ejemplo, si se genera un error interno en la información de procesamiento, ese error no se debe notificar, utilizando los datos completos de depuración, en la interfaz de usuario. Esto puede permitir al usuario en cuestión, identificar e instrumentar un error a los efectos de explotar las debilidades en la aplicación. Esta información debe registrarse internamente, y se debe generar un error genérico hacia el usuario que no proporciona el contexto suficiente para que este pueda utilizar la información de manera maliciosa. Incluso si el usuario puede reproducir el error, el usuario no debería poder evaluar un diferencial en el resultado de la aplicación que indique mejoras en la metodología de ataque utilizada.

6.10.1 Riesgo

La validación de datos de salida es una función crítica para la seguridad de IoT. Los sistemas que no realizan la validación de datos de salida pueden poner en peligro los datos del usuario críticos, los datos relacionados con su privacidad, los datos de diagnóstico de sistema, los mensajes de error detallados y más. Estos mensajes se pueden usar para exponer información del usuario o se pueden usar para lograr un ataque contra un servicio en red.

6.11 Fuerce una Política de Contraseña Segura

Es imperativo que todos los sistemas de autenticación utilicen contraseñas seguras cuando se requieren contraseñas para la autenticación del usuario. La complejidad de la contraseña ha sido una batalla constante en los grupos de investigadores de seguridad de la información, de los ingenieros y de los gestores empresariales. Los gestores empresariales a menudo quieren que los usuarios puedan recordar sus contraseñas fácilmente. Los ingenieros necesitan reducir la complejidad de las interfaces, especialmente para los diseñadores de la capa de presentación. Los investigadores en seguridad de la información a menudo sobreestiman la habilidad de un atacante y exageran al imponer contraseñas complejas determinadas para ciertos sistemas.

La respuesta mas adecuada, sin embargo, se encuentra en un punto intermedio entre todas las opciones arriba mencionadas. Las contraseñas deben ser forzosamente largas, pero no

deben ser complejas. Mientras que las contraseñas de ocho caracteres solían ser la norma y algunos sistemas incluso permiten 6 caracteres incluso hoy en día, la longitud de la contraseña debe determinarse a partir del estándar de mejores prácticas que se considere en un momento dado, pero probablemente excederá incluso los 8 caracteres. Al imponer una longitud de contraseña más larga, se reduce el requisito de complejidad. En lugar de imponer extrañas combinaciones de caracteres, el usuario puede simplemente recordar una frase. Debido a que pueden elegir utilizar espacios en blanco, mayúsculas, números y signos de puntuación, la complejidad se dispara automáticamente para cualquier atacante que aplique fuerza bruta.

No olvidemos que, por lo general, hay cuatro formas en que un atacante comprometerá una contraseña:

- Al robar la base de datos de contraseñas y descifrar las contraseñas individuales
- Al utilizar “fuerza bruta” para entrar en el servicio de autenticación de aplicaciones
- Al instalar malware
- Mediante el uso de contraseñas guardadas “en piedra” o predeterminadas

Forzar contraseñas largas ayuda a disminuir el riesgo en el primer caso. Pero la seguridad en la capa del Ecosistema de Servicios es mucho más beneficiosa. En primer lugar, el atacante no debería poder recuperar la base de datos de contraseñas, lo que nos lleva al segundo punto.

Las aplicaciónes de “fuerza bruta” para generar contraseñas son entonces la forma más efectiva en que un atacante puede abusar de las contraseñas. Esta posibilidad se ve significativamente disminuida por un servicio de autenticación diseñado correctamente. Si se ha introducido una contraseña incorrecta en un momento determinado, el sistema debería comenzar automáticamente a aumentar el tiempo requerido para introducir una nueva contraseña. Luego, se debe definir un umbral que limite el número total de intentos. Si el atacante alcanza este umbral, la cuenta se debe bloquear, y se debe usar la autenticación de dos factores u otro modelo para que el usuario pueda desbloquear y verificar su cuenta. Este tipo de seguridad reduce sustancialmente el beneficio que se pueda obtener de un ataque hecho a través de la red de comunicaciones, lo que nos lleva al último punto.

El malware en los sistemas cliente es algo que debe abordarse directamente por la plataforma informática o por el usuario instalando software a modo de un “antídoto” apropiado. Normalmente, esto no es algo que se pueda solucionar a nivel de aplicación. Dado que hay poco o nada que la aplicación pueda hacer para combatir este riesgo, más allá de implementar una autenticación multi-factor, el ingeniero de aplicaciones habrá reducido satisfactoriamente la posibilidad de amenazas de los ataques a las contraseñas dentro del sistema de autenticación, si este es el único método posible para el adversario.

Sin embargo, se debe tener en cuenta que los beneficios por implementar esta recomendación no son tan importantes. Esto se debe a que no importa qué tecnologías se utilicen para reducir el potencial de atacar la autenticación con contraseña, las contraseñas son, básicamente, un recurso intangible. No son tokens físicos que un solo individuo pueda capturar. Más bien, es un objeto abstracto que se puede copiar cauntas veces se pueda a través de los sistemas informáticos y a través de la observación visual. Por lo tanto, son una fuente de autenticación no muy fiable que, de ninguna manera, identifica inequivocamente a

un usuario en particular. Por lo tanto, las contraseñas, en sí mismas, son una debilidad, y cualquier tecnología que use contraseñas está sujeta a los riesgos que estas implican intrínsecamente.

Las contraseñas nunca se deben codificar físicamente dentro del sistema. Para Dispositivos Periféricos, se deben generar claves criptográficas únicas. Consulte el documento de Dispositivos Periféricos para obtener más información sobre el aprovisionamiento de Dispositivos Periféricos. El usuario debe definir la contraseña cuando se registra en la interfaz de usuario al utilizar los servicios. La contraseña, en ese momento, debe cumplir con estrictos requisitos de seguridad. Nunca permita que un usuario utilice una contraseña predeterminada, débil o mal diseñada.

Asegúrese de que el usuario siempre tenga la posibilidad de cambiar su contraseña en cualquier momento. Haga cumplir los requisitos de una autenticación sólida y de seguridad dentro de las comunicaciones, posibilitando que el usuario pueda cambiar su contraseña. Siempre que sea posible, habilite la autenticación de dos factores (2FA) para verificar la identidad del usuario antes de permitir un cambio de contraseña. Siempre obligue al usuario a volver a ingresar su contraseña original cuando envíe una nueva contraseña al sistema. Esto garantiza que otro usuario no haya usurpado una aplicación web abierta aprovechando un portátil desbloqueado o una ficha robada de una sesión abierta dentro de una aplicación web.

6.11.1 Riesgo

Los sistemas que no aplican controles adecuados sobre las contraseñas corren el riesgo de que los adversarios adivinen fácilmente las contraseñas de los usuarios del sistema.

6.12 Defina Políticas de Autorización y de Autenticación para la Capa de Aplicación

Si bien la raíz organizativa de confianza y sus servicios definirán las tecnologías de autenticación que aseguran la capa de comunicación de la red, las tecnologías de usuario, administración y autorización de los socios se deben configurar por separado. Si bien los canales de comunicación de estas entidades están asegurados con la Raíz de Confianza Organizativa, sus acciones e identidades deben autenticarse usando un sistema separado.

En general, la autenticación en la capa de aplicación será proporcionada por el mismo servicio. Sin embargo, la información se recopilará a partir de un recurso separado. Por ejemplo, es mejor colocar los datos de autenticación administrativa y de usuario en bases de datos separadas. Esto garantiza que si hay una forma de manipular la base de datos a través de la capa de aplicación (por ejemplo, utilizando una inyección SQL), los atacantes solo pueden moverse lateralmente a través de la base de datos del usuario. Es posible que no se muevan verticalmente, elevando sus privilegios a administrador, sin comprometer la base de datos. Esta es una mejora significativa en la seguridad de la organización.

Si es posible, defina sistemas de almacenamiento separados para:

- Identidades de Dispositivos Periféricos
- Usuarios
- Credenciales de administrador
- Socios

Esto creará una separación lógica de tareas para las aplicaciones y la infraestructura, pero dentro de la misma API de autenticación administrada por el servicio de la Raíz de Confianza Organizativa.

Considere utilizar material bibliográfico de las siguientes organizaciones para cumplir con estas recomendaciones:

- OAuth 2.0 [8]
- OpenID Foundation [9]
- GSMA Mobile Connect [10]

6.12.1 Riesgo

Sin una metodología para aplicar la autenticación y la autorización de la capa de aplicación, no hay forma de que el sistema confirme que las acciones supuestamente de un usuario estén realmente autorizadas para ese usuario en concreto. La implementación de esta recomendación garantiza que cada acción pueda rastrearse con respecto a un usuario autenticado y a la autorización pertinente. Estas métricas pueden almacenarse y revisarse posteriormente en caso de que se sospeche de un compromiso. Sin estos pasos, no habrá garantías que minimicen el riesgo de abuso.

6.13 Reglas de Apertura por Defecto y Apertura Fallida para el Cortafuegos y Refuerzo de la Seguridad del Sistema

En algunos entornos de infraestructura de servicios, los mecanismos de protección de entrada y salida no están configurados por defecto. Esto significa que los ingenieros deben emplear cortafuegos o reglas de tráfico de red. Estas reglas deben establecerse en la infraestructura antes de implementar cualquier servicio público.

Sin embargo, hay ocasiones en que estas tecnologías no son suficientes para proteger la infraestructura de los servicios. A veces, los cortafuegos y otros sistemas de protección de tráfico de red fallan. Cuando estos sistemas fallan, normalmente dejan pasar los datos. La razón para que esto ocurra cuando hay un fallo, es que el tráfico de datos global aún debe poder fluir, ya que el tráfico de otros entornos informáticos se enrutará a través de la infraestructura junto con el tráfico del proveedor de servicios de IoT. Por lo tanto, el tráfico no puede detenerse repentinamente. Como resultado, el sistema a menudo deja el tráfico fluir para permitir que el mayor número de servicios posible sigan funcionando.

El equipo de ingeniería debe emplear políticas de aseguramiento del sistema operativo para garantizar que los efectos de fallos en la infraestructura no causen un fallo grave de seguridad. Esto resulta, simplemente en que se puedan hacer más conexiones hacia la infraestructura de servicios existente.

Por ejemplo, los servicios ocultos no deberían protegerse poniéndolos detrás de tecnologías como los cortafuegos. En cambio, las Redes Privadas Virtuales (VPN) u otras protecciones de alta seguridad se pueden usar para proteger los servicios de los posibles adversarios.

Tenga en cuenta que los cortafuegos software conllevan un riesgo adicional, un atacante hábil puede manipularlos en su beneficio. Si se utiliza un cortafuegos software, cualquier infraestructura de servidor que esté mal protegida puede manipularse. En otras palabras, si un servicio público que se ejecuta en un servidor tiene privilegios innecesarios (como

privilegios de super-usuario) y se ve comprometido, es probable que el atacante sea capaz de deshabilitar el cortafuegos software. Por lo tanto, el equipo de ingeniería debe evaluar si un cortafuego software es demasiado peligroso para la arquitectura elegida.

6.13.1 Riesgo

Sin emplear estrategias para compensar los errores en los sistemas de seguridad de tráfico de red, el entorno estará sujeto a ataques innecesarios que podrían evitarse fácilmente con las estrategias estándar de aseguramiento del servicio.

6.14 Evalúe el Modelo de Privacidad de las Comunicaciones

La privacidad de las comunicaciones es un tema ligeramente diferente a la privacidad de la aplicación (descrita anteriormente) o a la seguridad de la información de las comunicaciones. Si bien la privacidad se evalúa en gran medida a partir de la capacidad de terceros para leer o interceptar datos de manera efectiva, la confidencialidad y la integridad no representan todos los conceptos dentro de la privacidad de las comunicaciones.

Otros problemas que influyen en la privacidad de las comunicaciones incluyen:

- Singularidad criptográfica de cada mensaje
- Patrones de transmisión
- Metadatos de texto simple
- Direcciones de hardware o números de serie atribuibles

Si bien cada mensaje debe ser confidencial y verificable desde el punto de vista de su integridad, también debe ser criptográficamente único. Si se envían ciertos mensajes en respuesta a eventos que un atacante puede predecir, este puede reproducir cualquier respuesta que no sea criptográficamente única. Cada mensaje debe ser exclusivo para no permitir que el atacante capture y reproduzca mensajes que sean utilizados en su beneficio.

Los patrones en la transmisión pueden permitir que un adversario identifique a un usuario en particular, o deducir el comportamiento con una determinada acción atribuible. Por ejemplo, la tecnología que emite un mensaje en una red inalámbrica cuando un usuario entra a una determinada zona física, podría ser atacada mediante “sniffers” que podrían capturar las huellas dactilares. Si bien puede no ser evidente, esto podría ser causa de responsabilidad legal si un atacante puede identificar quién está en un sitio concreto y dónde se encuentra físicamente en un momento determinado. Se deben evaluar los patrones de red para determinar si existe una forma sencilla en que los adversarios puedan convertir los patrones de transmisión en datos que se puedan procesar y comprender.

Los servicios de inteligencia han usado los metadatos desde hace tiempo para evaluar el contexto alrededor de los sistemas de mensajería sin requerir de una orden judicial u otro método legal para acceder a los datos encriptados. A menudo, los metadatos representan información suficiente para que una organización deduzca infomación suficiente para ser utilizada en un proceso judicial. Sin embargo, ahora los aficionados, las organizaciones delictivas y los usuarios curiosos pueden usar metadatos para rastrear los datos y para otros fines potencialmente nefastos. Como resultado, es más importante que nunca disminuir la cantidad de metadatos disponibles hacia terceros. Donde sea posible, limite la cantidad de metadatos a solo la información necesaria para que el otro extremo en las comunicaciones evalúe si el mensaje está destinado para él.

Utilizando este mismo razonamiento, la dirección física del hardware del módulo de comunicaciones, y cualquier número de serie único, debe ser protegido o aleatorizado, si es posible. Por ejemplo, Apple cambió el modelo de iOS para probar los puntos de acceso Wifi. En lugar de utilizar una dirección de hardware estático, cambiaron su tecnología para usar una dirección de hardware aleatorizada, lo que disminuye el potencial de que alguien rastree la ubicación de un usuario basándose en escaneos activos de la red Wifi. La tecnología IoT debería funcionar de manera similar, pero tendrá un conjunto más grande de tecnologías de comunicación afectadas por este problema. Algunas tecnologías no podrán generar aleatoriamente direcciones de hardware, como las tecnologías celulares. Pero otras, como 802.15.4, Wifi y Bluetooth, pueden ser capaces de esto dependiendo de la funcionalidad del firmware.

6.14.1 Riesgo

Aunque no hace falta decir que la seguridad de las comunicaciones es vital, a veces no queda demasiado claro. La seguridad de las comunicaciones no solo garantiza que un adversario no pueda leer los datos. También asegura:

- Que un Dispositivo Periférico no pueda suplantarse
- Que un servicio crítico no pueda suplantarse
- Que no se puedan descifrar mensajes interceptados
- Que los cambios en el software o en las configuraciones de seguridad se puedan realizar de forma segura

Sin la seguridad de las comunicaciones, no hay garantías en cuanto a la calidad, fiabilidad o privacidad de un producto o servicio de IoT.

7 Recomendaciones de Prioridad Media

El conjunto de recomendaciones de prioridad media abarca el conjunto de recomendaciones que son relevantes según las opciones tecnológicas de diseño que se escojan para los Dispositivos Periféricos. Por ejemplo, hacer cumplir las mejoras de seguridad a nivel del sistema operativo solo es válido si hay un sistema operativo ejecutándose en el Dispositivo Periférico. Si el Dispositivo Periférico está compuesto por un kernel monolítico o un sistema operativo en tiempo real integrado (RTOS) con una única aplicación integrada, es posible que la recomendación no sea de aplicación. Cuando las recomendaciones se puedan aplicar al diseño que se haya escogido para el Dispositivo Periférico, deben implementarse.

7.1 Defina un Entorno de Ejecución de Aplicaciones

Se deben hacer las siguientes puntualizaciones sobre los entornos de ejecución de aplicaciones:

- El lenguaje de programación utilizado puede tener una relación directa con la seguridad:
    - Los lenguajes como PHP y Ruby pueden tener problemas de seguridad
    - Los lenguajes como GoLang y Erlang pueden disminuir los riesgos
- Las bibliotecas externas (de terceros) deben ser monitorizadas, administradas y auditadas desde el punto de vista de seguridad:

    - Algunas bibliotecas pueden estar obsoletas por falta de mantenimiento
    - Algunas bibliotecas nunca han sido auditadas con respecto a su seguridad contra ataques externos
    - Algunas bibliotecas requieren de referencias externas desactualizadas que tienen problemas de seguridad conocidos
- Siempre ejecute una aplicación como un usuario sin privilegios específicos:
    - Si la aplicación necesita de un recurso que tiene privilegios determinados, use un contenedor para aprovisionar este recurso antes de descartar dichos privilegios y ejecutar la aplicación sin barreras
- Use un modelo bien definido de TCB y de arranque (“Bootstrap”):
    - Las aplicaciones que tienen entornos bien definidos son más fiables y más seguras

Considere utilizar referencias bibliográficas de las siguientes organizaciones para obtener ayuda en la implementación de esta recomendación:

- OWASP [5]

7.1.1 Riesgo

Las aplicaciones que se implementan con una arquitectura segura pueden estar sujetas a compromisos que no se pueden rastrear fácilmente hasta una fuente específica. Las herramientas y técnicas para poner en peligro los servicios y las aplicaciones han avanzado en la última década. Algunas tecnologías de código abierto, como “Metasploit”, permiten el desarrollo y la integración de vulnerabilidades personalizadas en una plataforma de ataque que puede proporcionar tecnologías para aumentar la “invisibilidad” de un ataque.

Un entorno de ejecución de aplicaciones seguro puede contrarestar este riesgo, garantizando la forma en que se ejecutan las aplicaciones, en que interactúan entre sí y los tipos de tecnologías que se utilizan durante el tiempo de ejecución. Estos atributos no solo pueden disminuir la probabilidad de que ocurra un compromiso, sino que también pueden agregar la trazabilidad y las capacidades de registro crítico para rastrear y diagnosticar la vulnerabilidad encontrada por un atacante.

7.2 Utilice Servicios de Supervisión Optimizados para los Socios

Si el socio es un operador de red celular, identifique si este puede ofrecer servicios de supervisión. Algunos operadores de red son capaces de analizar el comportamiento de los Dispositivos Periféricos que se comunican a través de su red. Los operadores con este tipo de capacidades de red tienen experiencia para evaluar qué parámetros indican un comportamiento anómalo y que indique un ataque.

Esto permitirá que el negocio de IoT identifique más rápidamente si un usuario en particular o Dispositivo Periférico es una amenaza o ha sido comprometido por un adversario. Como resultado, las empresas pueden reaccionar de manera más efectiva para prevenir ataques contra otras áreas de la infraestructura de la empresa.

La complejidad de este servicio surge de la capacidad del operador de red para proporcionar estas facilidades en un tiempo razonable. Si el operador de red solo puede

proporcionar el servicio una vez que el adversario ha atacado el negocio de IoT, entonces los sistemas de supervisión y registro instalados en la infraestructura del negocio de IoT deben de poder detectar el comportamiento anómalo. Sin embargo, si el operador de red puede notificar al negocio sobre el comportamiento fraudulento en la capa de red y puede identificar qué usuario concreto ha estado emitiendo tráfico de red anómalo, la empresa puede limitar la exposición del ecosistema de IoT no permitiendo dicho tráfico de datos proveniente del usuario en concreto.

7.2.1 Riesgo

Existen ciertas tecnologías en las que se basará el proveedor de servicios IoT que no podrá supervisar. Una de esas tecnologías es la red de comunicaciones que conecta un Dispositivo Periférico con el servicio y al ecosistema de red. Sin servicios de supervisión, el proveedor de servicios de IoT no tendrá una visión clara de los eventos que ocurren dentro de la red. Por lo tanto, si se detecta en una capa de aplicación que un ente A, está intentando comprometer un servicio, la organización no podrá identificar que el Dispositivo Periférico B es realmente la unidad que se ha conectado a la red de comunicaciones. Esta brecha en la información es crítica, ya que la organización puede atribuir el ataque al ente A y no al Dispositivo Periférico comprometido B.

7.3 Use un APN Privada para la Conexión Celular

Un APN (Application Point Name) es un componente de las comunicaciones celulares que conecta la red inalámbrica a Internet. Este punto actúa, esencialmente, como una red privada virtual (VPN) entre el Dispositivo Periférico con tecnología celular y la infraestructura de servicio con la que debe interactuar. Un APN privado (a veces llamado APN seguro) es una versión de un APN que se ha visto reforzado desde el punto de vista de seguridad implementando los siguientes controles:

- Acceso limitado y restringido a clientes autenticados
- Uso de un Cortafuegos
- La comunicación entre Dispositivos Periféricos se desactiva por la fuerza
- Servicios de supervisión para la detección de anomalías
- Servicios opcionales de seguridad o supervisión

Al restringir el acceso al APN, una empresa puede garantizar que solo los Dispositivos Periféricos autenticados puedan conectarse a la infraestructura del servicio disponible a través del APN. Esto disminuye la posibilidad de que los clientes inalámbricos deshonestos o aleatorios se conecten al APN y accedan a los servicios restringidos. Además, permite a la organización identificar qué clientes específicos se comportan de forma anómala, lo que le permite relacionar el comportamiento negativo con un componente específico del hardware o un usuario específico.

El cortafuegos garantiza que las entidades unidas al APN tanto del lado del cliente (Ecosistema de Dispositivos Periféricos) como del lado del servicio (Ecosistema de Servicios) no puedan comunicarse utilizando canales no autorizados. Esto también restringe la capacidad de un Dispositivo Periférico para abusar del APN utilizándolo como una puerta para abrir los accesos desde y hacia Internet, y acota el tráfico hacia un conjunto específico de servicios aprobados.

Las restricciones de las comunicaciones en los Dispositivo Periférico aseguran que los dispositivos deshonestos no puedan atacar a otros utilizando el APN como una red WAN. En cambio, todas las comunicaciones deben pivotar alrededor de los servicios aprobados por la organización. Si lo desea, la organización puede prohibir por completo la comunicación punto a punto.

Los servicios de supervisión refuerzan las mejoras de seguridad que implementará la empresa al supervisar la infraestructura de los servicios o de la nube existentes. Al combinar los servicios de supervisión existentes con las tecnologías de supervisión de red y APN que ofrece el operador de red, la empresa puede rastrear más fácilmente el origen de un comportamiento anómalo. Esto permite a la empresa inspeccionar más a fondo los incidentes que ocurran contra su Dispositivo Periférico o infraestructura de servicio. Por ejemplo, si la capa de aplicación indica que el usuario A puede estar comprometido, pero el equipo del usuario B está haciendo la conexión autenticada a la APN, la organización podrá usar los servicios de supervisión de APN para identificar que el usuario B ha comprometido potencialmente al usuario A, o que un adversario ha comprometido tanto al usuario A como al usuario B.

Los operadores de red tienen servicios adicionales que pueden agragarse a los servicios descritos anteriormente. Estos servicios ayudarán a incluir en listas negras a los hackers o entes malintencionados, supervisar a usuarios específicos o grupos de usuarios, y pueden redirigir ciertos tipos de tráfico cuando detectan anomalías. Otras opciones pueden estar disponibles. Involucre al operador de red para determinar qué servicios son adecuados para su empresa.

Si bien la utilización de todos estos servicios en conjunto puede parecer complicado, trabajar con el operador de red simplificará el proceso y la integración de estas mejoras tecnológicas en la infraestructura existente de la empresa. La complejidad provendrá de la utilización efectiva de los datos, y requiere un equipo de ingeniería que sea capaz de procesar y administrar los datos de manera razonable. Algunos servicios pueden incurrir en un costo adicional. Determine qué modelo de precios y servicios funcionarán mejor para su empresa y negocio.

7.3.1 Riesgo

Sin un APN privado, un dispositivo Periférico puede conectarse a casi cualquier servicio o tecnología, lo que incluye realizar conexiones directas a otros Dispositivos configurados en el APN o a servicios arbitrarios en Internet. Dado que esto permitiría que un Dispositivo Periférico comprometido interactúe con casi cualquier servicio en Internet y podría convertir al Dipositivo Periférico en un “blanco” para que actue y sea configurado como un proxy para atacar redes o servicios más seguros, esta recomendación debería aplicarse para restringir la capacidad de los Dipositivos Periféricos para conectarse de manera arbitraria y no autorizada a cualquier puntio en la red. Es mucho más valioso para la empresa y para la seguridad de todo el ecosistema de IoT, que los Dispositivos Periféricos se vean siempre obligados a conectarse solo a servicios aprobados previamente.

7.4 Defina Políticas de Distribución de Datos para Terceros

Después de que se hayan definido las clasificaciones de seguridad y se haya atribuido a los tipos de datos una clasificación válida, y se haya definido una política de incumplimiento, se

debe crear una política de distribución de datos. Una política de distribución de datos describe cómo se debe procesar la información a través de controles técnicos y aplicaciones de servicio a las que se ha otorgado permiso para acceder a los datos. El modelo de permisos forma parte de la política de distribución de datos y se combina con la capacidad del usuario para crear permisos detallados para el acceso a los datos.

Si bien una política de distribución de datos puede ser muy descriptiva, existen varios elementos clave que ayudarán a definir una política adecuada:

- ¿Qué nivel de autenticación mutua se requiere para manejar esta información?
- ¿Qué confidencialidad e integridad de los datos se requiere?
- ¿Qué capacidad tiene la empresa para conservar y retener los datos?
- ¿Qué capacidad tiene el socio para conservar y retener los datos?
- ¿Si se permite la conservación de los datos, ¿Por cuanto tiempo se pueden conservar los datos?
- ¿Qué nivel de seguridad de almacenamiento debe aplicarse a los datos?
- ¿Qué clasificación de seguridad de acceso debe aplicarse a los datos?

7.4.1 Riesgo

Las políticas de distribución de datos imponen requisitos de seguridad a los socios que pueden no cumplir de la misma manera internamente que el proveedor de servicios IoT. Dado que el proveedor de servicios de IoT no puede controlar la seguridad que un socio ha implementado en sus servicios internos y en la red, el proveedor de servicios de IoT solo puede hacer cumplir que los datos aportados a un socio se manejan de manera segura. Sin esta definición, el socio puede aplicar configuraciones inseguras que pueden exponer los datos del usuario a adversarios mientras los datos están aún bajo el control del proveedor de servicios IoT. Al aplicar estrictos controles de seguridad para el canal de comunicaciones, el proveedor de servicios IoT demuestra que está haciendo todo lo posible para garantizar la seguridad hasta que los datos estén fuera de su control y reponsabilidad.

7.5 Construya un Filtro para los Datos de Terceros

Si se permite que un socio genere dinamicamente datos, como la publicidad, se requiere un cierto nivel de presunción con respecto a la calidad y seguridad de los datos. En lugar de hacer suposiciones y manipular los datos en la capa de presentación, el equipo de ingeniería debe tomar medidas para garantizar que los datos distribuidos o recibidos de un Socio desde una aplicación perteneciente al servicio estén bien estructurados y no contengan contenido potencialmente malicioso.

Para hacer esto, el equipo de ingeniería debe considerar el siguiente modelo:

- ¿Los datos se ajustan al formato descrito por el socio para el modelo de datos?
- ¿Los datos están bien estructurados?
- ¿Los datos representan un objeto polimórfico que el cliente podría malinterpretar?
- ¿Los datos afectarán la forma en que el cliente procesa los datos en la capa de presentación?
- ¿Los datos afectarán la forma en que el cliente interpreta el funcionamiento de la capa de presentación?

- ¿Los datos provocan o solicitan al usuario que realice una acción que debilitaría la seguridad?
- ¿Los datos burlan la seguridad o son capaces de suplantar un componente (campo de entrada de contraseña) de la Interfaz Gráfica de Usuario (GUI) del cliente?

Rechace cualquier estructura en los datos que no se ajuste a un modelo aprobado. Notifique inmediatamente a la administración sobre la detección de dichos datos e incluya tantas métricas como sea posible con respecto al origen y formato de los datos. Registre una muestra, si es posible, en una base de datos segura.

7.6 Riesgo

Los datos generados dinámicamente por parte de terceros podrían contener malware, contenido inapropiado u otros datos no deseados, ya sea intencionalmente o no. Sin un filtro de entrada configurado para la definición del servicio de un tercero, la organización puede arriesgarse a permitir accidentalmente que el malware u otro contenido malicioso llegue al usuario final. Esto puede resultar en compromisos del sistema, o simplemente pérdida de clientes, debido a los efectos secundarios que podrían causar dichos datos.

8 Recomendaciones de Baja Prioridad

Las recomendaciones de baja prioridad abarcan el conjunto de recomendaciones que se aplican a riesgos que son extremadamente costosos de combatir, o es poco probable que afecten al diseño del Dispositivo Periférico. Si bien estas recomendaciones son valiosas y la información detallada en las recomendaciones es importante, las estrategias de mitigación o remedio discutidas pueden estar fuera del alcance con respecto al negocio. Evalúe cada recomendación y determine si los riesgos descritos son relevantes o importantes para la empresa y sus clientes. Si los clientes requieren que se aborden estos riesgos, aplique las recomendaciones.

8.1 Ataques “Rowhammer” y Similares

Algunas implementaciones de la tecnología RAM moderna, como la memoria de acceso aleatorio dinámico (DRAM) y la memoria estática de acceso aleatorio (SRAM) son vulnerables a errores que se pueden provocar de manera demostrable con ciertas secuencias de acceso a la memoria. Hacer un uso abusivo de este tipo de defecto puede ocasionar la alteración de un bit específico, o bits, en áreas de memoria determinadas. El aprovechar este agujero de seguridad en la memoria puede alterar bits que representan tipos de privilegios programados por software.

En otras palabras, si se explota correctamente, un adversario puede elevar sus privilegios de un usuario a otro mediante la manipulación de un defecto del hardware en las implementaciones modernas de DRAM o SRAM. Se han encontrado muchas implementaciones modernas de DRAM y SRAM potencialmente explotables a través de esta vulnerabilidad. Sin embargo, requiere la capacidad de ejecutar código en el sistema local para crear las secuencias de acceso a la memoria capaces de desencadenar este error.

Y, sin embargo, es posible desencadenar este tipo de comportamiento de forma remota a través de lenguajes en tiempo de ejecución, como GoLang, Python, Erlang, etc... Sin embargo, la precisión de este tipo de ataques aún no se ha documentado, y es altamente improbable que funcione de manera efectiva como un ataque exitoso.

Este ataque debe resolverse a nivel de hardware. Sin embargo, los ingenieros pueden reducir el riesgo de abuso al impedir que los clientes ejecuten el código, incluso a través de una máquina virtual o en tiempo de ejecución, en un servicio determinado. Al restringir esta capacidad, los ingenieros podrán evitar que los adversarios creen las secuencias de acceso a la memoria que se requieren para este ataque.

8.1.1 Riesgo

Sin suficientes protecciones contra este tipo de ataque, los atacantes pueden modificar remotamente ciertos privilegios o ejecutar código arbitrario en un servidor determinado. Sin embargo, se debe tener en cuenta que un ataque exitoso requiere un conocimiento extremadamente profundo del hardware, del sistema operativo, del vector de ataque y otros factores que hacen que este ataque sea improbable y poco frecuente.

8.2 Compromisos en las Máquinas Virtuales

La infraestructura moderna de servicios a menudo utiliza máquinas virtuales para implementar servicios bajo demanda. Si bien este modelo ha demostrado ser

extremadamente conveniente y fácil de implementar, el problema con esta metodología es la seguridad de la infraestructura en general. Si bien el equipo de ingeniería puede implementar una arquitectura adecuada y bien pensada, la organización que administra y despliega la infraestructura virtual puede no ser tan eficiente desde el punto de vista de seguridad.

Una de las principales preocupaciones de la implementación en entornos de servidores virtuales es la posibilidad de que los servidores principales (anfitriones) se vean comprometidos o que los servidores cliente (invitados virtuales) intercepten los datos de otros huéspedes que se ejecutan en la misma infraestructura.

Si bien estos ataques son motivos de preocupación válidos que el proveedor de servicios de IoT debe evaluar, a menudo requieren una gran cantidad de habilidades y tiempo para perfeccionarse. Por lo tanto, existe la posibilidad de que se produzca un ataque, pero es probable que sea un evento relativamente raro. Sin embargo, si la infraestructura del servicio no está bien protegida, es posible que los adversarios puedan comprometer el acceso administrativo a las máquinas virtuales. Este tipo de violación puede no requerir una gran cantidad de “know-how” para tener éxito.

Una forma de combatir este problema es con el aprovisionamiento seguro del servidor. Este proceso asegurará que cada servidor esté codificado con un conjunto único de claves criptográficas. Si se sigue esta filosofía, cualquier compromiso a un solo servidor puede limitarse a ese único servidor.

8.2.1 Riesgo

El riesgo de no luchar contra a este tipo de ataques puede dejar la infraestructura del servicio vulnerable a muchos tipos de ataques. La suplantación del servidor utilizando claves accesibles desde la infraestructura del servicio, la extracción y captura de datos, el compromiso de la privacidad y la suplantación del usuario pueden ser posibles.

8.3 Implemente una API para Usuarios que Pueda Controlar los Atributos de la Privacidad de la Información

Todos los usuarios deben poder controlar qué información ofrecen a terceros a través de las APIs de los servicios. La información debe clasificarse por tipos de datos y se le debe de atribuir clasificaciones de seguridad. Los usuarios deberían poder recuperar los tipos de datos y clasificaciones de seguridad que se usan en el modelado de su cuenta. El usuario debe poder aplicar restricciones al acceso a los tipos de datos, para permitir otorgar o revocar permisos de acceso a los Socios.

Esto puede venir en la forma de una API autenticada, o una GUI que permite controles simples: “Sí o No” en general, y por socio en concreto.

8.3.1 Riesgo

Sin la capacidad de los usuarios para controlar qué datos aportan a un proveedor de servicios de IoT, corren el riesgo de que sus datos se expongan en caso de una violación de seguridad, ya sea en el proveedor de servicios o en uno de los socios que trabaja con el proveedor de servicios. Dado que ciertos usuarios corren un riesgo mucho mayor que otros, cada usuario debería poder ajustar sus restricciones de privacidad de acuerdo con sus

necesidades personales. Hacer que esta interfaz esté disponible ayuda a garantizar que la capacidad esté ahí. El usuario debe encargarse de ajustar los controles para adaptarlos a sus necesidades. Por ejemplo, oneM2M (a través de TS-0003) permite al usuario establecer las preferencias de privacidad para un proveedor de servicios determinado.

8.4 Defina un Modelo para la Evaluación de Falsos Negativos o Falsos Positivos

Si bien el análisis de un “falso positivo” es un tema extremadamente complejo, existe una manera simple de identificar si una tecnología tiene más probabilidades de sufrir falsos positivos. Esto es mediante la evaluación de los siguientes elementos:

- ¿Es confiable la fuente de los datos?
- ¿Se puede alterar o falsificar la fuente de los datos?
- ¿Es la fuente de los datos del dominio analógico?
- ¿Pueden los datos corroborarse a partir de múltiples puntos de origen?
- ¿Existen fuentes de datos en el sistema de Dispositivos Periféricos y que estos a su vez los corroboren?
- ¿Se pueden falsificar o alterar las fuentes de datos corroboradas en el sistema?
- ¿Hay herramientas disponibles para manipular la fuente de los datos?
- ¿Qué nivel de experiencia o costo se requiere para manipular la fuente de los datos?
- ¿Es fiable el dispositivo que se conecta a la fuente de los datos?

Todos estos atributos, y más, se pueden usar para evaluar si los datos son fiables. Esto es extremadamente importante, ya que las decisiones críticas que afectan el mundo físico pueden generar situaciones potencialmente dañinas en los datos. Es imperativo que el equipo de ingeniería cree un modelo de fiabilidad y lo aplique a cada fuente de datos involucrada en la toma de decisiones críticas. Si el peso de la fuente de datos es tal que no se puede confiar ella, se debe implementar el recurso más racional y más seguro.

Es importante tener en cuenta que el equipo de ingeniería no es la única entidad que debe tomar esta clase de decisiones. Los directivos empresariales, el equipo de abogados y el equipo de seguros deberían participar en la planificación de las acciones precisas a ejecutar en escenarios potencialmente peligrosos. Los ingenieros deben codificar el proceso correcto de toma de decisiones en la tecnología de una manera verificable y reproducible.

Este proceso es muy complejo ya que exige la atención de toda la organización sobre cómo debería reaccionar la tecnología en escenarios críticos. La fiabilidad es un atributo complejo que se debe aplicar a tecnologías concretas, especialmente aquellas que están integradas en los sistemas hardware.

8.4.1 Riesgo

Sin un modelo de evaluación para falsos positivos, los ingenieros pueden pasar demasiado tiempo analizando eventos normales mientras ocurren eventos más críticos en paralelo que deben analizarse con mayor detenimiento. Esto puede dar como resultado un mayor riesgo de que las métricas analizadas por la organización no proporcionen una dirección clara sobre qué tipos de eventos ocurren en producción y funcionamiento normal. Esto devalúa la infraestructura de registro y supervisión, y disminuye la capacidad de la organización de utilizar estos costosos recursos para su beneficio en situaciones críticas.

9 Resumen

En resumen, casi todos los riesgos de seguridad en un producto o servicio de IoT pueden combatirse con una arquitectura bien definida, utilizando entes inteligentes en el sistema para identificar los riesgos antes y durante los eventos relacionados con la seguridad, y las políticas y procedimientos para manejar dichos eventos. Al analizar qué conceptos de seguridad de alto nivel son importantes para el proveedor de servicios de IoT, se pueden revisar las “preguntas frecuentes” de seguridad. Esto debería indicar al equipo de ingeniería que recomendaciones son más relevantes para resolver las brechas en su arquitectura de seguridad.

A medida que el equipo progresa en la definición de la arquitectura, puede revisar las recomendaciones independientes a medida que sus preguntas y preocupaciones de seguridad se vuelven más exclusivas de su propia implementación.

En general, cada equipo de ingeniería se enfrentará a riesgos muy parecidos. Es imperativo que la organización elija compartir sus inquietudes con sus socios en la implementación para construir una base de conocimiento común tanto para los riesgos como para las estrategias de respuesta y reparación. Juntas, las organizaciones pueden construir una tecnología y conocimientos para ayudarse mutuamente en la construcción de tecnologías de IoT seguras.

Annex A Gestión del Documento

A.1 Historia del Documento

Version	Fecha	Breve Descripción de los cambios	Aprovación Autoridad	Editor / Compañía
1.0	08-Feb-2016	New PRD CLP.12	PSMC	Ian Smith GSMA & Don A. Bailey Lab Mouse Security
1.1	07-Nov-2016	Se agregaron referencias al esquema de evaluación de seguridad de IoT de GSMA. Correcciones editoriales menores.	PSMC	Ian Smith GSMA
2.0	29-Sep-2017	Se Agregaron referencias adiciones de oneM2M	Grupo de Seguridad IoT	Rob Childs GSMA

A.2 Otra Información

Tipo	Descripción
Dueño del Documento	GSMA IoT Programme
Contacto	Rob Childs – GSMA

Es nuestra intención proporcionar para su uso un producto (documento) de calidad. Si encuentra algún error u omisión, contáctenos y háganos llegar sus comentarios. Puede notificarnos a esta dirección: prd@gsma.com.

Sus comentarios o sugerencias serán siempre bien recibidas.