XYO Network (La Red XYO): Riesgos de Seguridad y Mitigaciones

Arie Trouw*, Andrew Rangel, Jack Cable

Febrero 2018

---

1 Introduction

XYO Network es una red de ubicación criptográfica descentralizada y sin confianza que utiliza pruebas de cero conocimiento para establecer un alto grado de certeza con respecto a la verificación de la ubicación. Una de las preocupaciones principales de XYO Network, al igual que con todas las entidades descentralizadas y sin confianza, es la seguridad del sistema. Las vulnerabilidades incluyen, pero no se limitan a: fallas de diseño/arquitectura, errores de codificación, motivación económica incorrecta e ingeniería social. El enfoque principal de este documento se relaciona con los brillos de diseño/arquitectura y la motivación económica.

---

2 Consideraciones Técnicas

2.1 Resumen

Este documento aborda conceptos de alto nivel con respecto a posibles ataques contra XYO Network. Debido al hecho de que la red utiliza un sistema sin confianza, se supone que todos los participantes en la red son vulnerables (por ejemplo, Centinelas, Puentes, etc.). Esta sección detalla algunos de los ataques conocidos a nivel de protocolo junto con las salvaguardas estándar de la industria en su contra. Todos los demás ataques asumen que los dispositivos en el sistema están comprometidos.

2.2 Bluetooth

La mayoría de los dispositivos Bluetooth utilizan una configuración de emparejamiento de "Clave a Largo Plazo" que establece un PIN utilizado para el cifrado. Si la clave fuera descubria mediante una interceptación del proceso de emparejamiento, todo el tráfico futuro podría descifrarse fácilmente. Existen herramientas que podrían comprometer el PIN por fuerza bruta. Incluso los esquemas bien establecidos que establecen una contraseña fuera del protocolo generalmente se ejecutan sin cifrar. Esto permite múltiples vectores de ataque para acceder al protocolo. Además, los dispositivos podrían ser fácilmente suministrados para acelerar estos enfoques.

Para evitar ataques de esta naturaleza, las direcciones MAC de la lista blanca pueden prevenir dispositivos no autorizados que se comuniquen con Centinelas y Puentes. Otra forma de contrarrestar estos ataques es exigir que el usuario presione físicamente un botón de "reinicio" para emparejar el dispositivo, lo que evitaría los ataques de los usuarios que no tienen acceso físico directo al dispositivo.

---

*XYO Network, **arie.trouw@xyo.networK**

2.3 Por el Aire (PA)

Las Centinelas necesitan la capacidad de realizar actualizaciones "Por el Aire" (PA). Las actualizaciones PA permiten parches rápidos para mejorar la estabilidad y la seguridad del dispositivo. Una desventaja de esta característica es la posibilidad de un ataque que parodie esta actualización y agregue códigos maliciosos.

2.3 Hardware

Los dispositivos en la Red XYO están físicamente dispersos en una amplia gama de ubicaciones por todo el mundo. Esto significa que existe un potencial continuo para comprometer un dispositivo físicamente. Esta es una razón integral para que la Red XYO sea una red completamente infiel. La totalidad del sistema se basa en algoritmos complejos que analizan cuidadosamente y diligentemente la historia y el contenido de los datos que ingresan al sistema. Cualquier dato que no pase como datos de cadena larga de alta puntuación se descarta y los dispositivos restantes se penalizan.

---

3 Ataque de Pozo Envenenado

3.1 Resumen

Un Ataque de Pozo Envenenado ocurre cuando un mal funcionamiento o una parte maliciosa crea e inyecta datos corruptos que disminuyen la precisión general y/o la certeza de los resultados generados por el sistema.

3.2 Motivación

En un Ataque de Pozo Envenenado, el objetivo del actor malicioso es interrumpir o envenenar los datos que se envían a una Centinela o Puente en particular. Alcanzar esto les permitiría causar interrupciones económicas tanto a corto como a largo plazo. Dado que la Red XYO es un sistema sin confianza, existe una baja tolerancia para que este tipo de datos incorrectos se ingresen a la red.

Aunque no hay ganancia directa para el actor malo, existen beneficios en el trastorno y/o alteración de la reputación de datos de los demás. Suponga que se utilizó la Red XYO para rastrear la ubicación de las personas bajo libertad condicional a fin de denunciar cualquier violación de los términos de la libertad condicional basada en la ubicación. Si esto se usara para monitorear la cantidad de tiempo que un delincuente reincidente de conducción bajo la influencia de drogas pasa en un bar, un delincuente infractor en libertad condicional podría Envenenar el Pozo alimentando datos malos de un Puente basado en barras hasta que sea eliminado de la red. El delincuente podría violar los términos de su libertad condicional y consumir alcohol en el bar por el tiempo que le plazca. Incluso si los datos proporcionados informaran que el delincuente está en la ubicación del bar, los datos envenenados podrían reducir su certeza hasta el punto de que se invalidaría.

3.3 Análisis Técnico

Los datos de ubicación de una Centinela podrían ser afectados por bloqueadores de GPS o transmisores ilegales de radiofrecuencia que son diseñados para interferir con las comunicaciones de radio autorizadad. Dispositivos de

spoofing GPS [1] tienen la capacidad de enviar datos falsos a los receptores de radio GPS para falsificar la ubicación.

Las Centinelas que se comunican a través de Bluetooth presentan otro vector para este tipo de ataque. Hay varios métodos en los que un dispositivo Bluetooth podría ser falsificado para enviar datos incorrectos [2]. Mientras que las claves privadas creadas por la Red XYO se eliminan inmediatamente, es posible que un dispositivo pueda escuchar la comunicación entre una Centinela y un Puente y copiar los datos que se envían. Este ladrón podría enviar datos erróneos actuando como la Centinela y comenzar a envenenar los datos que el Puente envía a los Archivistas.

3.4 Estrategias de Mitigación de Protocolo

Mientras está activo, un bloqueador GPS se puede reconocer fácilmente debido a la contaminación que causa en el área general a la que apunta. Por ejemplo, cualquier usuario de teléfono celular en el área de destino experimentaría un bloqueo repentino de muchas de las aplicaciones que usan. Sería solo una cuestión de tiempo antes de que varias partes confirmen problemas similares y puedan confirmar que un emisor es el culpable. Dado que este tipo de interrupción es altamente detectable combinado con el hecho de que la FCC ha dictaminado explícitamente que la invocación de bloqueadores es ilegal [5], el alto riesgo asociado con este tipo de ataque hace que la probabilidad de que ocurra sea baja. Aun así, existen sofisticadas técnicas de GPS para evitar el spoofing que se están siendo desarrolladas actualmente tanto a nivel de hardware como de software para una mayor seguridad[1].

Además de estas protecciones, existen tecnologías y estrategias actuales que nos permiten protegernos contra el spoofing y la interrupción de Bluetooth, como la autenticación de claves de enlace con conexiones seguras. [3]

3.5 Estrategias de Mitigación de la Red XYO

La Red Archivista es una red competitiva que devuelve datos verificados al ser consultados por los Adivinos. En el momento en que los archivistas reciben los datos (detallados en papel amarillo), la red comienza a reducir los datos erróneos. La retransmisión de la información almacenada en la cadena al origen permite la detección de datos incorrectos recientemente agregados, incluso con información falsa en una cadena larga. Cada archivista también verifica los datos de otros archivistas para construir un consenso válido para la red. Debido al hecho de que a los archiveros se les paga, junto con Puentes y Centinelas, la criptoeconomía inherente suprime los intentos de envenenar componentes de bajo nivel.

3.6 Conclusión

Teniendo en cuenta que un archivista extrae datos de una amplia región geográfica y que es necesario ubicarlo físicamente en algún lugar para envenenar esa región, este tipo de ataque resultaría que el atacante sea castigado por la red. Esto es lo que hace que un atacante se desincentive económicamente para llevar a cabo dicho ataque en la Red XYO.

4 Ataques de Asesinato

4.1 Resumen

Un Aqtaque de Asesinato es definido por un actor malicioso que intenta discreditar un nodo (difamación) o hacer que otro nodo no funcione (asesinato técnico).

4.2 Motivación

En un Ataque de Asesinato, un atacante está motivado para socavar la reputación de nodos primitivos con el fin de aumentar la credibilidad relativa de otros nodos controlados por el atacante. Como la reputación de Centinelas en la Red XYO es fundamental para una red funcional, es crucial que la reputación de los nodos no se pueda manipular fácilmente.

Considere una situación en la cual un atacante intente transmitir información de ubicación falsa en la Red XYO (más detallada en el Ataque de Campo de Fuerza). En este caso, el atacante debe apuntar primero a los nodos individuales para dañar su reputación. Un método en el que esto podría lograrse es a través de la firma selectiva, donde un atacante proporciona selectivamente información falsa a una Centinela legítima (convirtiendo sus datos en valores atípicos) para hacer que el nodo sea menos consistente con otros nodos en la Red XYO. Esto hace que la reputación de la Centinela se reduzca en relación con otros nodos en la red.

Además, un atacante puede participar en un asesinato técnico de un nodo, tal como destruir físicamente un dispositivo. Este tipo de ataque también se realiza en intentos de falsificar información de ubicación en la red y dar como resultado dispositivos no funcionales.

4.3 Análisis Técnico

Un Ataque de Asesinato en una Centinela requiere que un atacante despliegue al menos un dispositivo para comunicarse selectivamente con la Centinela objetiva. Como otros dispositivos en la red no generan firmas con el nodo malicioso, el nodo malicioso solo es visible en el nodo de destino.

Para los Puentes externos a la red, la información transmitida por el nodo de destino es inconsistente con el resto de la red. Esto tiene el efecto de que el nodo objetivo pierda reputación con respecto al resto de la red, lo que es consistente en no reconocer el nodo malicioso.

4.4 Estrategias de Mitigación de Protocolo

Fundamental para la protección contra un Ataque de Asesinato es el establecimiento de castigar la reputación de un nodo si se involucra en la firma selectiva. En este escenario, los nodos maliciosos participan en la firma selectiva para que parezcan invisibles para otras Centinelas en la red.

El establecimiento de una reputación de cada Centinela de acuerdo con su coherencia con el resto de la red permite castigar a los nodos que participen en la firma selectiva. Un nodo acreditado puede emitir una consulta a un nodo de menor reputación en la red. Si el nodo de menor reputación es legítimo, sería mejor firmar la consulta y hacerse visible en la red, lo que aumentaría su reputación. Por lo tanto, si un nodo fuera a practicar la firma selectiva, el nodo más confiable puede transmitir que el nodo malicioso se negó a firmar su consulta. Esta práctica no puede explotarse en el caso en que un nodo realmente firme la consulta, ya que el nodo legítimo puede luego transmitir su firma para refutar la acusación de firma selectiva.

El acto de castigar la firma selectiva dentro de la Red XYO mitiga los ataques de asesinato de personajes, ya que cada Centinela tiene un mecanismo de defensa para recibir información inconsistente.

4.5 Estrategias de Mitigación de la Red XYO

Establecer una reputación para cada Centinela desalienta a los nodos a participar en la firma selectiva. Esto mitiga los ataques de asesinato de difamación haciendo que cualquier Centinela en la red sea punible por la firma selectiva.

Los ataques de asesinato físicos (por ejemplo, la destrucción de un dispositivo) son más difíciles de prevenir a nivel de red, pero la Red XYO es resistente a los ataques que se dirigen a dispositivos individuales.

4.6 Conclusión

El establecimiento de un sistema de reputación permite a las Centinelas imponerse mutuamente y erradicar a los malos actores. Así es como la Red XYO mitiga los Ataques de Asesinato.

---

5 Ataques de Decepción

5.1 Resumen

Un Ataque de Decepción ocurre cuando un actor malicioso intenta pasar datos incorrectos pero válidos para ser usados en el sistema para beneficio personal.

Una forma de Ataque de Decepción ocurre mediante la forja de cadenas múltiples, donde un atacante mantiene múltiples versiones de su propia cadena que esencialmente podrían existir en múltiples lugares a la vez.

5.2 Motivación

Un atacante podría falsificar información bifurcando su propia cadena de ubicación. Esto podría lograrse enviando la clave privada para un enlace de cadena, que se genera durante la creación de nuevos bloques locales, a uno o más adversarios colusores en diferentes áreas. Esto permite la creación continua de nuevas cadenas de ubicación que se ramifican desde el mismo punto de origen.

Un atacante podría beneficiarse de difundir información falsa sobre su ubicación in situ, donde la precisión de la ubicación es imperativa. Tomemos como ejemplo la intención de establecer una coartada para dar fe de que el atacante estuvo presente en una ubicación específica en un momento dado. Al tener múltiples cadenas, el atacante podría informar selectivamente solo la cadena que transporta información, la cual es más ventajosa para ellos como coartada.

5.3 Análisis Técnico

Un Ataque de Decepción es cada vez más difícil de ejecutar a medida que la cadena crece. A medida que pasa el tiempo, la información de un nodo particular se transmite a través de la Red XYO. Esto significa que cualquier ataque factible permitiría, como máximo, algunos pequeños cambios en una cadena en un punto dado en el pasado.

Este proceso no disminuye por completo el potencial de un ataque. Mientras se sincroniza con un Puente, una Centinela maliciosa podría elegir una de sus cadenas bifurcadas para compartir con el Puente. Dado que ambas cadenas son válidas, el puente y otros dispositivos en sentido ascendente no pueden concluir inmediatamente que la cadena se ha bifurcado. En cambio, es esencial que los nodos realicen una verificación cruzada con los registros de comunicación con otras Centinelas en la red para verificar que el nodo no haya existido en varias ubicaciones a la vez.

5.4 Estrategias de Mitigación de Protocolo

La Red XYO, por naturaleza, puede detectar ataques de cadenas múltiples. Cualquier bifurcación a largo plazo de la cadena de un nodo será inconsistente con el consenso general de la red. Para evitar pequeñas modificaciones, cuando la integridad de los datos de ubicación es primordial, un usuario puede esperar confirmaciones adicionales por Archivistas que contienen firmas de nodos distribuidos. A medida que pase el tiempo, las discrepancias resultantes de una cadena bifurcada se harán evidentes.

5.5 Estrategias de Mitigación de la Red XYO

Los datos se distribuyen a través de los archivistas que contienen registros firmados de las comunicaciones entre las Centinelas. En la práctica, incluso las modificaciones ligeras (aunque válidas) de una cadena existente son detectables. Si una Centinela intenta realizar un ataque de cadena múltiple, otros nodos con historial conflictivo pueden transmitir el conflicto a la red. Como resultado, la reputación de la pícara Centinela disminuirá, obligando que todas sus cadenas sean eliminadas de la red.

Por lo tanto, la Red XYO está diseñada para permitir la verificación cruzada de estas comunicaciones como protección contra este tipo de ataques.

5.6 Conclusión

La redundancia de datos en la Red XYO disuade los intentos de transmitir datos inconsistentes reduciendo la reputación de cualquier otra Centinela a un nivel que la elimine de la consideración en la red.

---

6 Ataque Sybil desde la Misma Máquina

6.1 Resumen

Un Ataque Sybil desde la Misma Máquina ocurre cuando un actor malicioso crea múltiples nodos desde una sola máquina. Debido a que los dispositivos en la Red XYO no tienen identificadores únicos, esto es fácil de lograr. El actor malicioso refuerza la reputación al firmar paquetes entre los nodos simulados para retratar los nodos como orgánicos y puros. El atacante luego permite que los nodos se comuniquen con diferentes grupos de nodos cercanos, de modo que el nodo simulado mantenga información diferente en sus cadenas de prueba de origen. Esto da como resultado que todos los nodos simulados adquieran altos puntajes de cadena de origen. Este ataque permite a los actores maliciosos económicamente producir en masa nodos que pueden usarse para llevar a cabo ataques Sybil en una red local o incluso mundial.

6.2 Motivación

Un atacante puede tratar de participar en un Ataque Sybil desde la Misma Máquina para influir una región en particular. Al crear múltiples nodos falsos desde el mismo dispositivo, se reduce la barrera para ejecutar un ataque Sybil. Es mucho más fácil para un atacante crear muchos dispositivos falsos en una máquina que crear muchos dispositivos maliciosos.

6.3 Análisis Técnico

No es difícil falsificar un dispositivo Bluetooth para que parezca indistinguible del dispositivo [4]. Por lo tanto, un atacante podría crear múltiples dispositivos desde una computadora que actúan y aparecen como dispositivos separados.

Una vez que se han creado varias Centinelas virtuales, un atacante puede operar las Centinelas como si fueran físicamente distintas. Las Centinelas parecen ser orgánicas y proceden a firmar información relacionada con otras Centinelas en su proximidad. Además, un atacante podría crear un mapa virtual de dispositivos que se refleja en las firmas de las Centinelas virtuales.

6.4 Estrategias de Mitigación de Protocolo

La clave para defenderse contra un Ataque Sybil desde la Misma Máquina es la capacidad de detectar datos duplicados mediante el análisis de la potencia de la señal. Una computadora con muchas Centinelas virtuales parece tener el mismo RSSI para cada Centinela. Como resultado, a una Centinela externa, cada Centinela virtual que opera en la computadora parece cerca una de la otra (siempre que haya una cierta fluctuación en la intensidad de la señal). Para prevenir este tipo de ataque, es importante que una Centinela legítima detecte dispositivos empaquetados y trate su información como un solo nodo.

6.5 Estrategias de Mitigación de la Red XYO

El indicador principal de la Red XYO para detectar los Ataques Sybil desde la Misma Máquina es la intensidad de la señal Bluetooth (RSSI). Esta es una métrica de dos vías que puede ser acordada por dos nodos. Como resultado, un nodo que ejecuta un Ataque Sybil desde la Misma Máquina parecerá tener la misma potencia de señal para cada uno de sus nodos virtuales. Los Archivistas reducen la desduplicación de los datos del nodo, lo que hace que todos los nodos virtuales se traten como un solo nodo. Esto hace ineficaz un Ataque Sybil desde la Misma Máquina en la representación de una máquina como varios nodos virtuales.

6.6 Conclusión

La detección de la intensidad de la señal Bluetooth de la red XYO, junto con su capacidad para desduplicación de datos, mitiga un ataque desde una máquina que crea un racimo de nodos virtuales al tratar el racimo como un solo nodo

---

7 Ataques por Campo de Fuerza

7.1 Resumen

Un Ataque por Campo de Fuerza combina un Asesinato con un ataque Sybil tradicional para proporcionar datos falsos a una red. Es un doble ataque: un atacante provee información inconsistente a nodos legítimos mientras permite que la red de nodos del atacante sirva como una red consistente para observadores externos.

7.2 Motivación

Este enfoque toma la forma de una Sybil local, en cual el atacante intenta controlar completamente la autoridad de una determinada ubicación física. Sin embargo, un ataque Sybil puro en la Red XYO requeriría una gran cantidad de dispositivos distribuidos con un historial extenso para superar en número a los nodos de buena reputación existentes. Para sortear este obstáculo, un Ataque por Campo de Fuerza emplea un enfoque híbrido, que primero se dirige a la reputación de los nodos existentes a través de ataques de asesinato para crear inconsistencias entre nodos legítimos..

Considere una situación en cual un atacante desee tener la autoridad completa de una determinada región local. Empleando un Ataque por Campo de Fuerza, el atacante podría primero inundar cada nodo legítimo con información inconsistente. La reputación de estos nodos en la red disminuiría en consecuencia, reduciendo la barrera de calificación de la reputación. Con esta barrera reducida, un atacante podría suministrar su propia red de dispositivos que superan en número a la baja reputación de dispositivos legítimos, estableciendo una autoridad única para la región objetiva.

7.3 Análisis Técnico

Para rendir una red existente incoherente, un atacante utiliza la firma selectiva para disminuir la superposición entre nodos legítimos. Esto podría hacerse al traer nodos maliciosos hacia la red local y luego permitir que cada nodo solo se comunique con dispositivos particulares en la red. Cada Centinela legítima seleccionada transmitirá la ubicación del nodo malicioso con cual se comunica, mientras que el nodo malicioso permanece invisible para las Centinelas circundantes. En gran escala, esto provocaría que cada Centinela tuviera una interpretación muy diferente del estado de la red. Para una fuente externa, como un puente, la reputación de cada nodo se reduciría.

En cuanto que se logre, un atacante podría aprovechar la reputación reducida de todo el sistema para inyectar su propia red de Centinelas. Es posible que estos dispositivos ya hayan existido en la red, simplemente se volverán más importantes a medida que disminuyan las reputaciones de otras Centinelas.

Este método de ataque depende de la cantidad de nodos existentes en la región y se hace cada vez más difícil a medida que crece este número.

7.4 Estrategias de Mitigación de Protocolo

Similar a la prevención de Ataques de Asesinato, la mitigación de los Ataques por Campo de Fuerza se basa en el castigo de la firma selectiva. Un Ataque por Campo de Fuerza emplea la firma selectiva con un cártel de nodos maliciosos para hacer que los nodos legítimos objetivos sean incompatibles con la Red XYO.

Teniendo una encuesta de Centinelas acreditada con menos nodos de buena reputación para firmas y nodos de informes que se nieguen a responder disminuye la capacidad de los nodos para participar en la firma selectiva.

Esto hace que un Ataque por Campo de Fuerza sea mucho más difícil de ejecutar, ya que cualquier reputación construida para ejecutar el ataque se disiparía rápidamente después de participar en la firma selectiva.

7.5 Estrategias de Mitigación de la Red XYO

La Red XYO castiga los nodos que intentan la firma selectiva para no cumplir con el resto del sistema. Esto aumenta el incentivo para que los nodos respondan a solicitudes de firma y aporten datos a la Red XYO. Los nodos incompatibles pierden credibilidad en forma de baja reputación, lo que hace que el componente de Asesinato de un Ataque por Campo de Fuerza sea económicamente inviable. Esto reduce un Ataque por Campo de Fuerza a un ataque Sybil tradicional, que requiere una cantidad desmesurada de dispositivos y poder de cálculo.

7.6 Conclusión

El costo resultante para la reputación de una Centinela en un Ataque por Campo de Fuerza en la Red XYO hace que el ataque sea económicamente impráctico.

---

8 Ataque de Teletransporte

8.1 Resumen

Un Ataque de Teletransporte ocurre cuando un atacante puede falsificar su ubicación "teletransportándose" a otra ubicación a través de la red. Si se utiliza un teléfono inteligente o baliza Bluetooth como la Centinela que proporciona los datos de ubicación de un atacante, un atacante podría falsificar su ubicación enviando su Centinela a otra persona. Si la red se utilizó para establecer una coartada, un actor malicioso podría intercambiar su Centinela con otra persona para falsificar su ubicación informada.

8.2 Motivación

Este tipo de ataque también puede lograrse a nivel de software por un atacante compartiendo su clave privada con uno o más individuos. Si la red se usara para verificar las reseñas de un hotel, solo permitiría que las personas abandonen las reseñas que tenían historial de confianza en la cadena. Un actor malicioso podría compartir remotamente su clave privada con un individuo en el hotel y podría aparecer como si estuvieran ubicados allí sin estar en proximidad física de la zona.

8.3 Análisis Técnico

Si la clave privada se proporciona al usuario, podría compartirse para crear un dispositivo falsificado que aparezca como ese dispositivo del usuario. La utilización de la Radio Definida por Software permitiría a las partes elegibles aparecer como cualquier dispositivo específico en la red, siempre que esté asociado con la clave privada de ese dispositivo. Esto anularía los intentos de validar la ubicación de un usuario. Esto también podría afectar los datos de la cadena de bloques, ya que es teóricamente difícil discernir el viaje legítimo del dispositivo desde un Ataque de Teletransporte.

8.4 Estrategias de Mitigación de Protocolo

Las estrategias de detección contra este tipo de ataque son complejas debido a las interrupciones naturales en la cadena. Por ejemplo, si un teléfono se utiliza como una Centinela y se apaga, no estará en comunicación con la red hasta que se vuelva a encender. Las lagunas en la información que se envía requieren un algoritmo sofisticado para distinguir las lagunas naturales de los puntos de datos potencialmente malos que deben sancionarse.

8.5 Estrategias de Mitigación de la Red XYO

La viabilidad de un Ataque de Teletransporte vacila en el punto donde los Archivistas pueden compartir información entre ellos y verificar la viabilidad de los datos. La cantidad de dispositivos elegibles se reduce aún más en las

etapas iniciales de la Red, donde es realista para los servidores comparar los datos en grandes áreas geográficas. Esto permite a los Adivinos observar datos incorrectos en forma de ubicaciones duplicadas y Teletransporte, que pueden ser filtradas y castigadas con el uso de un algoritmo.

8.6 Conclusión

Aunque un Ataque de Teletransporte es difícil de determinar a nivel de protocolo, los servidores de nivel superior en la Red XYO, como Archivist, permiten la detección y el castigo de datos maliciosos en la Red. El intercambio de información entre estos servidores continuamente construirá y anexará información confiable para filtrar los datos incorrectos del sistema.

---

9 Ataque Sigiloso

9.1 Resumen

Un Ataque Sigiloso se define por un dispositivo que está oculto de la red. Varios casos de uso de la Red XYO requieren que los dispositivos en la red tengan un historial de cadena sólido.

9.2 Motivación

Hay pocos incentivos para que un usuario malicioso realice un Ataque Sigiloso en la Red XYO. La red tiene como objetivo proporcionar certeza de que algo existe en un lugar determinado, no comprobar todas las partes donde ha estado. Esta es una distinción importante, ya que los datos a nivel de protocolo pueden ser imprecisos ya que los nodos no son de confianza.

Aun así, un usuario final podría estratégicamente activar y desactivar los servicios de ubicación de su teléfono o baliza para crear datos de cadena defectuosos que de otra manera serían válidos. Esto les permitiría esencialmente esconderse de la red cuando no desean informar datos y volver a aparecer en la red cuando les resulte ventajoso.

9.3 Análisis Técnico

Se puede lograr un Ataque Sigiloso desactivando un dispositivo en la red. Un enfoque más complicado podría ser emplear una jaula de Faraday que oculte un dispositivo de la red. Un enfoque no físico para este tipo de ataque podría persistir mediante Ataques de Denegación de Servicio.

9.4 Estrategias de Mitigación de Protocolo

La acción contra los Ataques Sigilosos puede ser compleja debido a la capacidad de Bluetooth y otros dispositivos para desconectarse fácilmente de la red. La estrategia principal para aliviar esta vulnerabilidad es la implementación y el uso de una sólida capa de software que penaliza a Centinelas y Puentes que transmiten datos de cadenas interrumpidas. Las capacidades de detección aprenderán y crecerán a medida que el algoritmo mejore para comprender las sutiles diferencias entre los datos válidos y no válidos.

9.5 Estrategias de Mitigación de la Red XYO

Una laguna en el historial de un nodo será inmediatamente sospechosa en los casos de uso que requieran una Prueba de Ubicación continua en la Red XYO. Cuando los datos llegan a los Archivistas, se someten a un riguroso proceso de poda y filtración que puede detectar estas lagunas y castigar las incoherencias. Esta característica principal de la Red XYO le permite proporcionar la ubicación más precisa a pesar de los datos desordenados que son inherentes al mundo físico.

9.6 Conclusión

Un Ataque Sigiloso es económicamente inviable dado los casos de uso para la Red XYO.

---

10 Ataques de Denegación de Servicio

10.1 Resumen

Un Ataque de Denegación de Servicio (DoS) ocurre cuando un actor malicioso o disfuncional causa un corte a nivel local, regional o del sistema.

10.2 Motivación

Un atacante puede intentar interrumpir la Red XYO para evitar que pueda verificar la Prueba de Ubicación.

10.3 Análisis Técnico

Debido a la naturaleza del protocolo Bluetooth, las balizas Bluetooth solo se pueden conectar a un dispositivo a la vez. Esto significa que cualquier dispositivo que acepte comandos no autenticados puede ser fácilmente eliminado de la red. Esto podría lograrse mediante la utilización de una aplicación de teléfono móvil, lo que permitiría que un dispositivo que emite comandos de Bluetooth lo haga continuamente con relativa facilidad. El envío de valores hexadecimales al dispositivo para determinados parámetros, como el parámetro "reproducir sonido" en la mayoría de las balizas, crea una conexión con ese dispositivo. Si se establece esta conexión, bloquea cualquier otro dispositivo para que no se comunique con él. Esto podría ser amplificado por el uso de la Radio Definida por Software que podría ejecutar scripts para transmitir continuamente varios valores hexadecimales a cualquier baliza de red en el rango.

10.4 Estrategias de Mitigación de Protocolo

Los dispositivos Bluetooth en la Red XYO solo deben aceptar comandos autenticados o utilizar una lista blanca de direcciones MAC. Reducir el número de comandos autenticados por escritura minimiza el acceso a este vector de ataque.

10.5 Estrategias de Mitigación de la Red XYO

La Red XYO está compuesta por usuarios que ejecutan servidores Archivista y Adivino. Ambos componentes comparten información y validación con sus compañeros. Esto permite que una consulta seleccione de cualquier "pila" de componentes para recuperar una respuesta. Aunque es posible denegar una pequeña parte del servicio de red a nivel de protocolo, la amplitud y escala de la red hace que esto sea económicamente inviable.

10.6 Conclusión

Debido a la naturaleza distribuida de la Red XYO, la red sigue siendo funcional a pesar de un intento de Ataque de Denegación de Servicio. Como un DoS requiere un gran poder de cómputo y acceso físico para atacar una pila completa, apuntar incluso una pequeña porción de la Red XYO es costoso y económicamente ilógico.

---

11 Reconocimientos

Este documento en rojo es un corolario de seguridad del libro blanco y el papel verde de XYO Network (La Red XYO). Agradecemos a Christine Sako por su atención al detalle y la aplicación de las mejores prácticas en su revisión de este trabajo.

References

[1] Jafarnia-Jahromi, Ali. Ali Broumandan, John Nielsen, and Gerard Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. https://www.hindawi.com/journals/ijno/2012/127072/cta/ International Journal of Navigation and Observation, Alberta, Canada, Mayo 2012.

[2] Padgette, John, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, and Karen Scarfone. Guide to Bluetooth Security. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf U.S. Department of Commerce, National Institute of Standards and Technology, Mayo 2017.

[3] Dunning, JP. Breaking Bluetooth by being bored. https://www.defcon.org/images/defcon-18/dc-18-presentations-/Dunning/DEFCON-18-Dunning-Breaking-Bluetooth.pdf DefCon, Agosto 2010.

[4] haxf4rall. Spoofing a Bluetooth device. http://haxf4rall.com/2016/05/11/spoofing-a-bluetooth-device/ May 11, 2016.

[5] Chief, Enforcement Bureau. FCC Enforcement Advisory. https://apps.fcc.gov/edocspublic/attachmatch/DA-14-1785A1.pdf FCC.gov, 8 Diciembre 2014.

Glosario

exactitud
Una medida de confianza que un punto de datos o heurística está dentro de un margen específico.

Archivista
Un Archivista almacena heurística como parte del conjunto de datos descentralizados con el objetivo de almacenar todos los registros históricos, pero sin ese requisito. Incluso si algunos datos se pierden o se vuelven temporalmente no disponibles, el sistema continúa funcionando, solo con una precisión reducida. Los Archivistas solo almacenan datos brutos y se les paga únicamente por la recuperación de los datos. El almacenamiento siempre es gratis.

Puente
Un Puente es un transcriptor heurístico. Transmite de forma segura los libros mayores heurísticos de Centinelas a Adivinos. El aspecto más importante de un Puente es que un Adivino puede estar seguro de que los libros mayores heurísticos que se reciben de un Puente no han sido alterados de ninguna manera. El segundo aspecto más importante de un Puente es que agregan metadatos adicionales de prueba de origen.

certeza
Una medida de la probabilisas de que un punto de datos o heurística estée libre de corrupción o manipulación.

criptoeconomía
Una disciplina formal que estudia los protocolos que rigen la producción, distribución y consumo de bienes y servicios en una economía digital descentralizada. Criptoeconomía es una ciencia práctica que se centra en el diseño y la caracterización de estos protocolos.

Adivino
Un Adivino responde a una consulta dada mediante el análisis de los datos históricos que se han almacenado por la Red XYO. La heurística almacenada en la Red XYO debe tener un alto nivel de Prueba de Origen para determinar la validez y precisión de la heurística. Un Adivino obtiene y entrega una respuesta al juzgar al testigo en base a su Prueba de Origen. Dado que la Red XYO es un sistema sin confianza, los Adivinos deben ser incentivados para proporcionar análisis honestos de la heurística. A diferencia de Centinelas y Puentes, los Adivinos usan Prueba de Trabajo para agregar respuestas a la cadena de bloques.

Puntuación de la Cadena de Origen
El puntaje asignado a una Cadena de Origen para determinar su credibilidad. Esta evaluación toma en cuenta la longitud, enredo, superposición y redundancia.

Prueba de Cadena de Origen
Una Clave de Transición que combina una serie de entradas del libro heurístico de Testigos Atados.

Centinela
Una Centinela es un testigo heurístico. Observa la heurística y garantiza la certeza y precisión de ellos produciendo registros temporales. El aspecto más importante de una Centinela es que produce registros que los Adivinos pueden estar seguros que provienen de la misma fuente al agregarles Prueba de Origen.

sin confianza
Una característica donde todas las partes en un sistema pueden llegar a un consenso sobre cuál es la verdad canónica. El poder y la confianza se distribuyen (o comparten) entre las partes interesadas de la red (p. ej., desarrolladores, mineros, y consumidores), en lugar de concentrarse en un solo individuo o entidad (p. ej., bancos, gobiernos e institutuciones financieras). Este es un término común que puede ser fácilmente malentendido. Las cadenas de bloque en realidad no eliminan la confianza. Lo que hacen es minimizar la cantidad de confianza que se requiere de un solo actor en el sistema. Lo hacen medicante la distribución de la confianza entre los diferentes actores del sistema a través de un juego económico que incentiva los actores a cooperar con las reglas definidas por el protocolo.

La Red XYO

La Red XYO significa ("XY Oracle Network (Red Oráculo XY). Está compuesta por todo el sistema de componentes/nodos que incluyen Centinelas, Puentes, Archivistas y Adivinos. La función principal de la Red XYO es actuar como un portal mediante el cual los contratos digitales inteligentes se pueden ejecutar a través de confirmaciones de ubicación geográfica.