Consideraciones de seguridad en una red AMI

Honeywell
Elster Medidores
www.honeywellsmartgrid.com

Introducción

Muchas empresas de servicios eléctricos o planean o ya implementan tecnologías de redes inteligentes. Para esto, la infraestructura de medición avanzada (AMI) es una nueva tecnología que permite cambios radicales en el funcionamiento de la red de distribución. Teniendo en cuenta los nuevos niveles de automatización y ampliado del acceso a la red permitido por AMI, se han planteado cuestiones en relación a la inseguridad dentro de las redes inteligentes, con algunas preocupaciones relativas específicamente a las ofertas de soluciones AMI nuevas y existentes.

Este artículo examina algunos de los problemas de seguridad relacionados con los sistemas AMI y describe las medidas preventivas clave que se pueden adoptar contra cuestiones de seguridad cibernética.

Componentes básicos de AMI

La red de AMI comprende varias redes de comunicación, así como de componentes de software y hardware, tales como los siguientes:

- Una aplicación de gestión de elementos y/o del sistema (en inglés, *head end*) que operan en la red de servicios públicos.
- Una red de área amplia (WAN) (en inglés, *backhaul*) que proporciona comunicaciones desde el *head end* de la compañía eléctrica hacia el campo.
- Acceso al campo o puntos de recogida en el borde de la WAN, proporcionando conexiones y/o consolidación para acceso a datos de medición.
- Una red de malla (en inglés, *red mesh*) conocida como una red de área local (LAN) proporciona sub-redes de medidores, extendiendo el alcance a una mayor población de medidores.

También se están introduciendo las redes de área en el hogar (HAN) para proporcionar interfaces que alienten la conciencia del cliente sobre el consumo de energía y para ampliar el soporte de respuesta de la demanda.

Asegurando la red LAN

Al igual que con la línea de cobre o redes inalámbricas existentes, la primera preocupación gira en torno a las protecciones de seguridad para que los dispositivos como los medidores y los

hardwares asociados de comunicaciones sean fácilmente accesibles.

Ingeniería inversa de dispositivos LAN para atacar la red

Una de las principales preocupaciones es la presunta capacidad de un hacker de aplicar ingeniería inversa a un dispositivo de campo robado o comprado tal como un medidor.

Para reducir considerablemente el riesgo de que un dispositivo de usuario remoto evada la seguridad en el sistema AMI, el fabricante puede bloquear los microcontroladores que contienen el firmware. Esto evita que intrusos puedan leer el firmware del dispositivo.

La infraestructura de medición avanzada (AMI) es una nueva tecnología que permite cambios radicales en el funcionamiento de la red de distribución.

Este enfoque permite también que el firmware sea escrito (clave para que permita actualizaciones remotas de alta eficiencia), aun con la protección contra cambios no autorizados siga de la siguiente manera:

- Una sección de firmware (conocido como el gestor de arranque) es bloqueada y no se puede sobrescribir.
- Independientemente de si una sección o la totalidad del firmware fue escrita, el gestor de arranque verifica la nueva sección descargada, así como toda la imagen. Un pirata informático tendría que satisfacer todos los requisitos de seguridad esperados por el cargador de arranque. Además, para el hacker sería necesario un conocimiento detallado de la completa imagen del firmware con el fin de intentar modificar o cargar una nueva imagen que cumpla con el cargador de arranque de normas de verificación.
- El medidor (el ejercicio de su inteligencia distribuida) no tratará de cambiar la imagen de un nuevo firmware hasta que la nueva imagen sea validada por el gestor de arranque del medidor.

En resumen, debido a que el firmware no se puede leer, cualquiera de los aspirantes a ingeniería inversa está operando a ciegas. Modificaciones parciales o completas escritas en el firmware deben coincidir exactamente con todas las características esperadas para ser validadas para el uso de un medidor.

Actualizaciones remotas OTA seguras

En el caso de un riesgo potencial para la seguridad o incumplimiento en dispositivos remotos, es fundamental que dichos dispositivos sean gestionados de forma remota y actualizados para rechazar la amenaza. Esta capacidad le suma la flexibilidad necesaria al sistema para pruebas a futuro y permite nuevas funcionalidades o parámetros que serán proporcionados, así como mantenerse al día con la evolución de amenazas de seguridad.

El fabricante puede cifrar el firmware para aumentar la seguridad de la transferencia y la descarga en el dispositivo. Esto asegura el nuevo firmware desde el punto de origen y solo permite que el dispositivo inteligente pueda descifrarlo con éxito antes de realizar la validación. El cifrado del firmware debe ser completado con un cifrado único de clave diferente a la utilizada para las comunicaciones cifradas. Todas las comunicaciones deben también estar cifradas (por ejemplo, usando un algoritmo AES-128 bits) para proporcionar una seguridad remota fuerte.

Monitoreo de comportamiento de puntos finales LAN

El monitoreo de comportamiento se basa en la premisa de que observar el comportamiento pasado permite predecir el futuro comportamiento. Los aspirantes a los piratas informáticos pueden monitorear comunicaciones de medidores para aprender comportamientos de mensajería de red que posteriormente permitirían al atacante enviar otros (perturbadores) mensajes a un dispositivo.

Este riesgo se reduce manteniendo al mínimo la cantidad de mensajería (reducción de la vibración) y proporcionando unos pocos ejemplos de mensajes o comportamientos válidos.

Por ejemplo, en la LAN un dispositivo de punto final se programa para originar solo los mensajes de eventos. Un dispositivo de punto final no va a hacer voluntariamente cualquier otra tarea de comunicación a menos que dicha tarea se inicie por una comunicación segura de un dispositivo de recolección. Datos de medida nunca se envían y mensajes de control solamente se envían si son solicitados por un dispositivo de recolección (por ejemplo, firmware dentro de los dispositivos de punto final es incapaz de iniciar mensajes de control a otros dispositivos de red).

Prevención de ataques de comunicación LAN

Existen varias medidas preventivas que se pueden desplegar en paralelo para fortalecer aún más la seguridad de comunicaciones globales de LAN.

Se necesitan conocimientos técnicos, tanto en la medición y redes de bajo ancho de banda, para implementar con éxito la seguridad mejorada dentro del recurso y, como con componentes restringidos de ancho de banda que comprenden la LAN AMI. Factores tales como interferencias de radio, dispositivos operados con pilas y mensajería optimizada deben ser acomodados cuando se diseñen e implementen las soluciones de seguridad de LAN. Algunos medios probados en el campo para mejorar la seguridad de la LAN son citados a continuación:

- Seleccionar un tipo intrínsecamente más seguro de las radiocomunicaciones. Por ejemplo, el ejército de Estados Unidos utiliza comunicaciones con espectro de frecuencias de salto de propagación (FHSS) (que puede ser utilizado en la LAN) ya que proporciona un nivel de seguridad inherente no encontrado en los sistemas de un solo canal. Debido a que utiliza FHSS múltiples canales en una secuencia de salto aleatoria para los datos de transmisión, es muy difícil escuchar a escondidas e interceptar mensajes completos. Cada dispositivo utiliza una diferente secuencia de salto y tiempo, por lo que incluso si un hacker se las arregla para penetrar en un único dispositivo, es imposible extrapolar a cualquier otro dispositivo en el sistema.
- Comunicaciones sin sesión de LAN entre el acceso punto y cada punto final ofrecen una mayor seguridad porque cada comunicación debe estar autenticada antes de que pueda ser objeto de decisiones.
- La comunicación cifrada LAN (por ejemplo, AES-128 bits) proporciona una capa adicional de forma confidencial para cada mensaje entre el punto de acceso y el punto final.
- Más controles se deben proporcionar para añadir datos, comprobaciones de integridad (para confirmar que los datos no han sido manipulado antes de la llegada).
- El uso de claves de cifrado únicos para dispositivo de LAN aumenta la resistencia y disminuye la capacidad de infiltrarse en las comunicaciones de LAN.
- Para defenderse de las amenazas futuras, o simplemente para reunir las políticas de seguridad de la empresa distribuidora, es muy importante ser capaz de gestionar y cambiar las claves criptográficas de forma remota.
- Para defenderse de las amenazas inminentes o activas, es también crítico poder manejar o cambiar rápida y fácilmente las claves a través de una gran red del sistema AMI.

Algunos críticos han dado a entender que un ataque podría iniciarse a través de un medidor o de otros dispositivos de LAN. El escenario imagina que los mensajes de LAN se pueden enviar para cambiar el comportamiento del dispositivo o el control de un dispositivo que causa, por ejemplo, una desconexión masiva de energía residencial. Si se diseña correctamente (es decir, para soportar una configuración maestro a esclavo), un punto de acceso WAN (dispositivo principal), no lo hará aceptar un mensaje

de comando (desde un dispositivo secundario LAN). En arquitectura de sistema jerárquico, el control de un solo punto final no se puede extrapolar para controlar más de una multitud de puntos finales.

La restricción sobre cómo se procesan las comunicaciones del sistema asegura aún más las comunicaciones de LAN. Un ejemplo es limitar el punto final de medición para enviar solo espontáneamente datos de excepción del sistema y eventos tales como alertas de sabotaje o notificaciones de apagones. El medidor recoge y mantiene registros y los datos de intervalo hasta que se recupera mediante una sesión de petición y respuesta de comunicaciones con el recolector de datos.

Este enfoque aumenta en gran medida la protección contra engaños hacia un medidor y autorizaciones para los datos falsos que se presenten al sistema. La adición de comunicaciones cifradas LAN proporciona la confidencialidad de los datos que aseguran aún más la red y evitan la posible suplantación de identidad.

¿Medidores a prueba de manipulación?

Dado que el medidor es un componente expuesto en la red (no solo a los elementos naturales, sino a los atacantes físicos también), existe una preocupación razonable sobre la seguridad cibernética de estos dispositivos de borde para evitar la ingeniería inversa o engaño de medidores. Cada uno de los artículos se discutió anteriormente (arquitectura maestro-esclavo, FHSS, notificación de fraude, autenticación, encriptación, cifrado único, etcétera), todos proporcionan una protección, pero medidas de prevención adicionales se pueden tomar en el diseño del medidor para ayudar a evitar la suplantación de identidad o manipulación.

Para falsificar un medidor, un atacante tendría que saber íntimos detalles acerca de los microcontroladores en el medidor, como así también del firmware. Los atacantes (o consultores de seguridad) crean pruebas únicas o monitoreo de dispositivos con un objetivo en mente: controlar o acceder a la información sobre la propia física del dispositivo con el objetivo de manipular o modificar el medidor (por ejemplo, cambios en datos de facturación, hacer que el dispositivo se desconecte, hacer que el dispositivo haga *broadcast* a través de otros dispositivos, etcétera).

Los microcontroladores contienen el firmware de los medidores que controla la metrología y sus comunicaciones. Mediante el uso de microcontroladores que se pueden bloquear, el fabricante puede prevenir que el firmware pueda ser leído desde un medidor cuando es probado, evitando de este modo que un atacante pueda directamente acceder y leer o descargar el firmware.

El bloqueo frustra la capacidad de un hacker para analizar o manipular y volver a instalar el firmware.

Se requiere la capacidad de escribir (o sobrescribir) el firmware que permite a los dispositivos remotos actualizar in situ cambios adicionales y evolucionar la tecnología de los medidores (futuras pruebas). El siguiente nivel de seguridad es evitar que el firmware se sobrescriba por uno corrupto o uno no autorizado.

Teniendo en cuenta esta necesidad, un método para prevenir la sobrescritura de firmware es tener todos y cada uno un nuevo firmware validado por-integridad y autenticado en la instalación. Ambos, validación y autenticación, deben ser completados antes de la colocación de firmware en el entorno de ejecución (es decir, el cargador de arranque). Este enfoque impide la suplantación de identidad y bloques de inserción de virus.

Además de estas medidas preventivas, la totalidad de imágenes de firmware puede ser cifrada por el diseño del proveedor del equipo. La codificación proporciona confidencialidad y ayuda a mantener la integridad de las nuevas imágenes de firmware permitiendo un transporte seguro a través de la red de servicios públicos en los dispositivos de medición, donde se descifra.

Suponiendo que todas estas medidas preventivas de seguridad de los medidores están en su lugar, y suponiendo que un atacante sea capaz de tener éxito…

- Obtener o modificar una imagen de firmware
- Descifrar el mecanismo de autenticación y validación en la imagen
- Instalar la nueva imagen
- Descifrar y/o cifrar imágenes de firmware
- Encontrar o romper las claves criptográficas únicas para la comunicación cifrado

¿Qué pueden esperar la compañía eléctrica y los consumidores?

Después de haber roto a través de todas estas capas de seguridad, el atacante es capaz de alcanzar un solo medidor/cuenta. Además, se disparará una alerta automática a la compañía eléctrica que puede entonces tomar medidas para investigar y rápidamente actualizar o reemplazar el medidor si se considera necesario.

Asegurando la red WAN

La infraestructura (WAN) de red de área amplia puede ser de propiedad de la compañía eléctrica o de acceso público. Pueden utilizarse opciones propias de las compañías tales como *WiMax*, frecuencia con licencia, o de fibra óptica, se pueden utilizar para la automatización de la compañía eléctrica, así como para AMI. Redes inalámbricas públicas son otras opciones para una WAN.

Debido a que es raro que una sola tecnología soporte todo los requisitos de comunicación de la compañía, el sistema AMI debe ser diseñado para operar con seguridad usando una variedad de tecnologías WAN. Independientemente de la tecnología WAN seleccionada, se debe proporcionar una solución segura.

Comunicaciones WAN

Existen estándares de la industria para las comunicaciones WAN, que se despliegan activamente y se utilizan en la actualidad proporcionando diferentes niveles de seguridad. Dos de los más importantes son las normas ANSI C12.21 y C12.22.

ANSI C12.21 proporciona acceso WAN, autenticación de dos vías mediante el cifrado DES de un token generado aleatoriamente.

El protocolo C12.21 está basado en la sesión, se puede implementar un tiempo de espera para liberar la sesión y reducir la amenaza potencial de denegación de servicio a través de sesiones de agotamiento.

El cifrado C12.21 ANSI es comúnmente proporcionado por portadores de comunicación cuando los datos se transmiten a través de la WAN (GPRS, EDGE, HSDPA, CDMA, 1xRTT, EVDO, etcétera).

ANSI C12.22, si es proporcionada por el proveedor del sistema, añade otro nivel de seguridad al proporcionar acceso WAN, la autenticación y el cifrado de datos usando un algoritmo AES-128 bits (por normas ANSI C12.22). ANSI C12.22 ofrece comunicaciones sin sesión. Cada comunicación debe estar autenticada antes de que pueda actuar en consecuencia.

Para aumentar el nivel de seguridad, cada punto de acceso WAN o dispositivo final debe tener una clave criptográfica única para comunicaciones cifradas WAN. La gestión de clave de encriptación debe ser compatible con las políticas de seguridad de la compañía y estar implementada para acelerar cambios clave en el caso de una identificación de una potencial amenaza.

Atributos de cifrado WAN

Cuando se suministran soluciones de cifrado WAN, muchos vendedores no tienen en cuenta el costo añadido y la complejidad de proporcionar una

solución de gestión de claves (por lo general, los componentes más difíciles de prever en una red AMI).

Dada la naturaleza del sistema AMI, la red de IT de soluciones existentes de seguridad no se ajusta a la necesidad. Una gran variedad de soluciones están siendo propuestas e implementadas por varios vendedores. Al evaluar las distintas ofertas, la compañía eléctrica debe buscar lo siguiente:

- La capacidad de cambiar las claves (el reingreso de información) en la red AMI (como exigen las políticas de seguridad de compañías de servicios públicos).
- Intento único de reintroducción de clave (diferente de la clave de cifrado de datos) utilizado en una base por dispositivo para cifrar la clave nueva, añadiendo una capa adicional de seguridad.
- Mínimo impacto en el rendimiento del sistema y de dispositivos relacionados con el cifrado, descifrado y funciones de reescritura de claves.
- Mínimos costos (no hay manera óptima) de sistemas y dispositivos relacionados para proporcionar cifrado y gestión de claves.

Seguridad del proveedor de la red WAN

Para las WAN inalámbricas, las empresas de telecomunicaciones utilizan redes privadas y cifrado para proporcionar datos seguros en las transmisiones. Si se utilizan módems de WAN inalámbrica, estos deben proporcionar protección por contraseña. Los módems de WAN inalámbrica también deben soportar los nodos de punto de acceso personalizados (APN) que hacen que la dirección IP del módem sea inaccesible desde fuera de la red corporativa (es decir, privada y no expuesta a la Internet pública).

Seguridad del sistema *head-end*

El sistema de cabecera AMI o *head-end* reside dentro de la red de la compañía eléctrica. Como tal, debe integrarse dentro de la red empresarial existente y proporcionar soluciones de seguridad necesarias. Los atributos de seguridad básica a tener en cuenta son:

- Autenticación de acceso
- Coexistencia dentro del firewall de la utilidad
- Gestión de contraseñas de usuarios con acceso opcional a servidores centralizados de seguridad (es decir, LDAP)
- Autorización, controles de nivel de acceso basado en roles
- Umbrales de eventos y alertas
- Auditoría, informes de seguimiento de usuario del sistema y de auditoría
- Interfaces de redes seguras
- Transferencia de datos segura para aplicaciones de red

Estas consideraciones de seguridad son bien entendidas por experimentados profesionales de IT y debe ser incluidas y aplicadas al sistema de cabecera de cualquier solución de AMI.

Resumen

A medida que las compañías de servicios públicos evalúan los sistemas AMI, se deben considerar los requisitos de seguridad básicos de la industria, y el sistema de AMI seleccionado debe proporcionar una seguridad superior.

El sistema de AMI se debe diseñar e implementar pensando en la seguridad. Esta no debe aplicarse simplemente recurriendo a terceros como una superposición (es decir, la seguridad debe ser construida y no agregada). Para ser exitosa, esta requerirá proveedores y empresas de servicios públicos apoyándose por igual, no solo en la seguridad, las comunicaciones y experiencia en redes, sino también en la experiencia detallada y el conocimiento de los componentes de AMI del trabajo, que les permitirán integrar con éxito una solución AMI segura al sistema. La solución del sistema *EnergyAxis* de *Honeywell* está diseñada e implementada con los atributos seguros definidos previamente, proporcionando una oferta AMI segura para satisfacer los más exigentes requisitos. ■