EL RETO DE LA CIBERSEGURIDAD EN INFRAESTRUCTURAS DE MEDICIÓN AVANZADA

Conference Paper · October 2016

CITATIONS
0

READS
161

3 authors, including:

Gregorio López
Universidad Politécnica de Madrid
51 PUBLICATIONS **420** CITATIONS
SEE PROFILE

Jose Ignacio Moreno
University Carlos III de Madrid
131 PUBLICATIONS **960** CITATIONS
SEE PROFILE

EL RETO DE LA CIBERSEGURIDAD EN INFRAESTRUCTURAS DE MEDICIÓN AVANZADA

Miguel Seijo Simó, Investigador, Universidad Carlos III de Madrid
Gregorio López López, Investigador, Universidad Carlos III de Madrid
José Ignacio Moreno Novella, Profesor, Universidad Carlos III de Madrid

Resumen: La importancia de las Tecnologías de la Información y Comunicaciones (TIC) en las Infraestructuras de Medición Avanzadas (AMI) conlleva muchos beneficios, pero también nuevos retos para la distribución eléctrica, siendo especialmente relevantes los relativos a seguridad y privacidad. El objetivo de este artículo es analizar los riesgos de seguridad y privacidad propios de las AMI y presentar una serie de recomendaciones y propuestas para mitigar dichos riesgos en base a un completo estudio del estado del arte, incluyendo la recomendación europea 2012/148/UE, así como la directiva del NIST IR-7628. El artículo también discute la importancia y dificultades del análisis forense en este tipo de escenarios.

Palabras clave: AMI (*Advanced Metering Infrastructure*), Ciberseguridad, Privacidad, Análisis Forense.

INTRODUCCIÓN

Las Infraestructuras de Medición Avanzada (AMI) están siendo ampliamente desplegadas en todo el mundo y especialmente en Europa, donde se estima que se invertirán hasta 45B€ en el despliegue de 200M de contadores para 2020. En España, en particular, se habrá sustituido todo el parque de contadores por contadores inteligentes en el 2018, lo que supone en torno a 30M de contadores.

Las Tecnologías de la Información y Comunicaciones (TIC) juegan un papel crucial en las AMI, lo cual conlleva muchos beneficios, pero también nuevos retos para la distribución eléctrica, siendo especialmente relevantes los relativos a riesgos en seguridad y privacidad. Los riesgos que suponen los ataques a una infraestructura crítica como la red eléctrica son especialmente peligrosos, implicando un impacto mayor en la salud, seguridad o bienestar económico de los ciudadanos o en el eficaz funcionamiento de los estados donde se produzcan dichos ataques (CE, 2004). Estos ataques son especialmente atractivos desde un punto de vista económico (p.ej., manipulación de datos de facturación), para obtener datos que puedan revelar información sensible, o con fines terroristas (p.ej., cortes en el suministro).A pesar de lo reciente de estas tecnologías, ya existen ejemplos que ilustran el interés en atacar las infraestructuras AMI, como el incidente de Malta (SmartGridNews, 2014), donde más de 1000 contadores inteligentes fueron comprometidos entre 2011 y 2012, suponiendo un robo de electricidad por valor de 30M€.

En consecuencia, las autoridades gubernamentales y organismos competentes están tomando medidas para proteger los despliegues de AMI frente a ciberataques. Así, la recomendación europea relativa a los preparativos para el despliegue de los sistemas de contador inteligente (2012/148/UE), hace un especial énfasis en aspectos de seguridad y privacidad (CE, 2012). De igual modo, en los Estados Unidos, la ciberseguridad también representa un tema de capital importancia en este ámbito, existiendo normativa del *National Institute of Standards and Technology* (NIST) y de la *North American Electric Reliability Corporation* (NERC) al respecto (NIST IR-7628 (NIST, 2010), CIP-002 a CIP-009).

El objetivo de este artículo es introducir los principales retos de seguridad en AMI, haciendo especial énfasis en los ataques a la seguridad, a la privacidad y el análisis forense. El resto del artículo se estructura de la siguiente forma. La segunda sección describe el estado del arte en las arquitecturas TIC para AMI, dando una visión general que describe y contextualiza estas arquitecturas. La tercera sección analiza el problema de la ciberseguridad en AMI asociado a las arquitecturas TIC descritas previamente y plantea

soluciones a los problemas descritos. La cuarta y última sección recoge las principales conclusiones de lo expuesto en el artículo y las líneas de trabajo futuras.

ESTADO DEL ARTE EN LAS ARQUITECTURAS TIC PARA AMI

Las AMI pueden definirse como aquellos sistemas que integran contadores inteligentes, redes de comunicaciones y sistemas de gestión, permitiendo la comunicación bidireccional entre la distribuidora y los clientes finales.

Esto permite soportar una variedad de aplicaciones, incluyendo: (1) mejora del control de calidad del suministro; (2) control en escenarios de generación distribuida basada en renovables; (3) mejoras en la facturación; (4) respuesta a la demanda; (5) técnicas contra el fraude; y (6) aplicaciones domóticas.

Las redes de contadores inteligentes tienen una naturaleza heterogénea al existir distinta densidad y distribución de los nodos dependiendo del escenario, observándose grandes diferencias entre áreas metropolitanas y rurales. Por esta razón, además de los principales sistemas que forman las AMI - contadores inteligentes, redes de comunicaciones y sistemas de gestión- es necesario incluir concentradores de datos en los escenarios con un gran número de nodos.

En la Figura 1 se pueden observar tres posibles configuraciones de una red de comunicaciones para AMI. (1) y (2) corresponden típicamente a escenarios con gran densidad de nodos, donde los contadores inteligentes forman una subred con el concentrador de datos, normalmente situado en los centros de transformación secundarios (de media a baja tensión). En el primer caso, el concentrador tiene conexión directa con el sistema de gestión, mientras que en el segundo se utilizan diferentes tecnologías que conectan estos concentradores con la pasarela al sistema de gestión. (3) se utiliza típicamente en escenarios con un número menor de nodos geográficamente más dispersos, teniendo todos ellos conexión directa con el sistema de gestión.

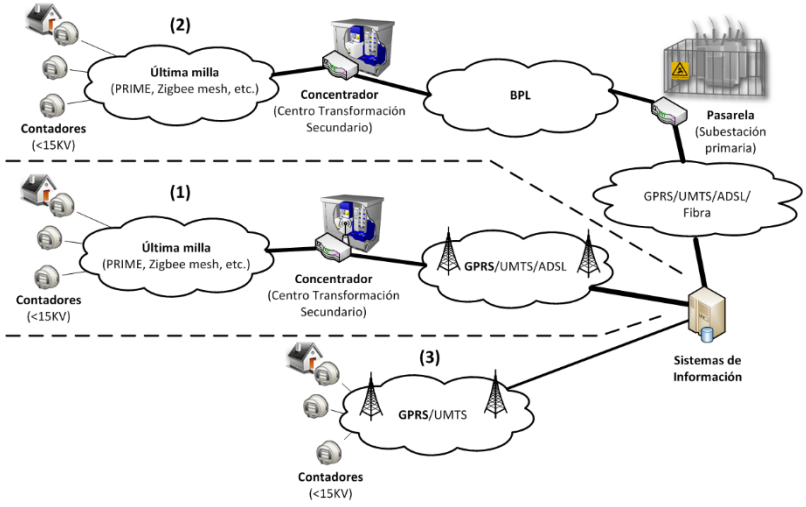

Figura 1. Arquitectura TIC para AMI

Como se puede observar en la Figura 1, la arquitectura tiene forma de árbol (a excepción de los contadores inteligentes, que pueden conectarse entre sí formando una topología mallada), donde cada rama representa una subred independiente, por lo que es posible combinar distintas tecnologías de comunicación en un mismo escenario. Las tecnologías más utilizadas en los contadores inteligentes suelen ser aquellas que no requieren desplegar nuevos canales de comunicación, que son autoconfigurables aun para un alto número de nodos y suponen un bajo coste (p.ej., Zigbee *mesh* o PLC). En las comunicaciones entre los concentradores situados en los centros de transformación y los sistemas de información, se

suelen utilizar tecnologías robustas, de largo alcance y con mayor tasa de transmisión, como pueden ser fibra óptica, xDSL, tecnologías celulares o PLC de banda ancha.

En AMI, tanto la arquitectura como las tecnologías utilizadas dependen de muchos factores, como las características de la infraestructura eléctrica, la regulación existente en cada país o las aplicaciones que se quieran soportar. Esto genera notables diferencias en los distintos despliegues a nivel global.

En Europa, por ejemplo, la implantación de AMI se orienta a proporcionar lecturas al cliente con la finalidad de ahorro energético, proporcionar control y lecturas del contador inteligente en remoto por parte del operador para mejorar la planificación de la red y aceptar sistemas de tarificación avanzados, como queda patente en la recomendación 2012/148/UE (CE, 2012). Esta recomendación también trata ampliamente sobre la seguridad y privacidad de los datos procedentes de sistemas de contador inteligente, centrándose especialmente en temas de privacidad.

En Estados Unidos, sin embargo, la implantación de AMI se extiende también a aplicaciones tales como la detección de cortes de suministro, fraude y pérdidas no técnicas, mejora de la calidad, interfaces prepago, DR y aplicaciones domóticas. En cuanto a las recomendaciones en ciberseguridad, las directivas del NIST tratan también tanto seguridad como privacidad, dando más peso a los aspectos relativos a seguridad (NIST, 2010).

EL RETO DE LA CIBERSEGURIDAD EN AMI

Uno de los mayores retos en cuanto a ciberseguridad en el ámbito de las AMI radica en la imposibilidad de aplicar las tecnologías tradicionales (p.ej., sistemas de detección de intrusiones (IDS), infraestructuras de intercambio de claves (PKI), antivirus, firewalls) sin cambios, dadas las diferencias existentes entre las AMI y las redes de comunicaciones convencionales.

Por un lado, en las AMI la disponibilidad es el máximo requisito de seguridad, mientras que en las redes de comunicaciones tradicionales este requisito aplica mayormente a los servidores centrales, primando la confidencialidad en el resto de nodos. La arquitectura de red también es diferente, siendo predominantemente de árbol en el caso de las AMI (ver Figura 1) y más flexible en las redes convencionales. Los elementos a proteger también son distintos, ya que en AMI puede haber distintos nodos con requisitos de seguridad similares a los del servidor central, mientras que en redes convencionales el servidor central requiere mayor protección. Además, en AMI un gran número de estos nodos, p. ej., concentradores y contadores inteligentes, son sistemas embebidos con mucha menor capacidad de procesamiento que los sistemas de redes tradicionales, características típicas en escenarios del Internet de las cosas. Las tecnologías también son distintas, pudiendo existir una gran variedad de protocolos en una misma red de comunicaciones para AMI.

Seguridad

Debido a las diferencias mencionadas anteriormente, los problemas de seguridad que podemos encontrar en AMI presentan ciertas peculiaridades frente a los encontrados en redes de comunicaciones tradicionales.

Los ataques pueden realizarse contra: (1) los dispositivos, ya sean contadores, concentradores o sistemas de información, (2) la red, en alguno de los tramos que componen su arquitectura, o (3) los datos, alterando su integridad.

Los ataques contra los dispositivos tienen como objetivo comprometer dispositivos de la red y pueden ser el punto de entrada para otros ataques más sofisticados contra la red o a los datos. Este tipo de ataques suele utilizar vulnerabilidades en los distintos nodos para ejecutar ciertos comandos (como puede ser la desconexión remota de una línea eléctrica) o incluso hacerse con el control total del dispositivo, llevando a cabo acciones más sofisticadas (como la alteración de las mediciones). La mayoría de los contadores y concentradores son sistemas embebidos que no tienen capacidad de procesamiento suficiente como para

ejecutar programas que eviten el *malware*, dependiendo únicamente de las actualizaciones del fabricante como medida de seguridad. Sin embargo, estas actualizaciones pueden exponer a los dispositivos a la carga de *firmware* modificado por el atacante (Liu *et al.*, 2012). En el caso de dar servicio a aplicaciones domóticas, se introducen nuevos sistemas embebidos sobre los cuales se tiene un control aún más reducido, pudiéndose introducir con fines maliciosos.

Los ataques contra la red tienen como meta deteriorar o alterar las comunicaciones entre los dispositivos. Al igual que en el caso anterior, este tipo de ataques también pueden aprovechar vulnerabilidades, en este caso en los protocolos de comunicación, para ser llevados a cabo. Uno de los objetivos de estos ataques puede ser mermar la disponibilidad en las comunicaciones con los nodos, lo cual puede ser especialmente efectivo si el atacante tiene conocimiento sobre la topología de la red, para usar un ataque de denegación de servicio coordinado sobre aquellos nodos que resultan más críticos para la conectividad del sistema global (p.ej., concentradores) (Chen *et al.*, 2012).

Otro de los objetivos principales de este tipo de ataques puede ser interceptar, corromper o falsificar los datos transmitidos. En las redes de contadores y concentradores, los nodos tienen un ancho de banda, memoria y almacenamiento limitados, por lo que la gestión de claves de cifrado de datos no es tan robusta como debería (Liu *et al.*, 2012), de manera que al vulnerar uno de los nodos la seguridad del resto se ve comprometida.

Los ataques contra los datos tratan de comprometer el sistema a través de la inyección, modificación o interpretación de los datos en la red. Una vez vulnerada la red y obtenidos los datos de un contador o concentrador que realicen funciones de agregación, el atacante puede desagregar para interpretar la información de cada uno de sus elementos.

Otro objetivo de un ataque contra los datos puede ser falsear los datos para engañar a los sistemas de información, forzándolos a tomar decisiones erróneas y dando al atacante el control de la red (Liu *et al.*, 2012). De esta forma, es posible tomar el control de los sistemas de información sin vulnerarlos directamente, aprovechando el eslabón más débil de la topología.

En cuanto a recomendaciones de seguridad, para mantener la seguridad en los dispositivos, se recomienda un control de acceso estricto basado en roles y permisos sobre atributos para reducir los efectos de los ataques de control remoto de los nodos y el efecto de posibles dispositivos de domótica maliciosos. También es necesario el uso de sistemas de clave pública/privada únicos para cada nodo para el cifrado y verificación de la integridad del *firmware*.

En lo relativo a la seguridad de la red, la adaptación de sistemas de detección de intrusiones (IDS) a escenarios AMI permitiría detectar y evitar ataques a la disponibilidad de los nodos, entre otros. La autenticación de los nodos de la red mediante cifrado de los datos permite mantener su integridad y proporcionar propiedades de no-repudio, permitiendo detectar anomalías y depurar responsabilidades. Para solventar el problema de la gestión de claves, se puede reducir el dominio de claves y que las interacciones entre los distintos dominios se realicen mediante la técnica de *re-signature*.

Por último, para evitar los ataques contra los datos, en (Kim & Poor, 2011) se propone un algoritmo para elegir las medidas óptimas para ser protegidas de forma que el impacto sea mínimo.

Privacidad

La información personal tratada por los sistemas AMI es de carácter sensible, por lo que la protección de la privacidad en este ámbito es especialmente importante, como reflejan las recomendaciones y directivas internacionales (CE, 2012) (NIST, 2010).

De un contador inteligente, no sólo se pueden obtener consumos eléctricos totales, sino que es posible extraer otra información como la información de los dispositivos de domótica incluidos en la vivienda, incluso es posible identificar los electrodomésticos que están en funcionamiento mediante el análisis de la huella de consumo energético de cada uno de ellos. También es posible obtener información sobre los

hábitos de los usuarios, como pueden ser la ocupación de una vivienda o las horas de sueño, la cual es especialmente valiosa para fines publicitarios o incluso delictivos.

Para proteger la privacidad, es importante que la información de alta granularidad (consumos horarios, entre otros) sea utilizada únicamente para el control de la red o la selección de tarifa y se evite que esa información sea transmitida a terceros. Para lograr esto, se propone que los datos de alta granularidad sean anonimizados y agregados usando, p. ej., cifrado homomórfico, de modo que sólo la compañía eléctrica sea capaz de asociar estos datos con los usuarios (Gómez-Mármol et al., 2012), (Li *et al.*, 2010). Existen también técnicas para evitar revelar los hábitos del cliente, como distribuir el consumo en el tiempo mediante el uso de acumuladores. Sin embargo, esta técnica necesita grandes baterías y es demasiado compleja, siendo en muchos casos suficiente con proteger la privacidad del cliente respecto a terceras partes mediante cifrado.

Análisis forense

Las AMI pueden ser cruciales para la investigación y prevención de actividades como el fraude en el consumo eléctrico, ya que los contadores inteligentes incluyen mecanismos de protección y notificación contra la manipulación física y el acceso ilegítimo. El análisis forense puede también, a partir de los datos de consumo provistos por el contador inteligente, descubrir aquellos electrodomésticos y elementos de domótica que perturben el normal funcionamiento de la red.

Sin embargo, este tipo de análisis presenta una serie de retos aún abiertos como pueden ser la seguridad de los datos recogidos, la privacidad de los usuarios o las pérdidas de datos relevantes en la agregación de los mismos, unida a las restricciones en almacenamiento de los sistemas de contador inteligente.

Para hacer frente a esos retos, se recomienda el uso de cifrado y autenticación para mantener la seguridad y privacidad a la hora de obtener pruebas forenses. Es importante que el acceso a los datos solo sea posible mediante orden judicial. También se debe hacer uso de sistemas de agregación avanzados que permitan mantener toda la información relevante sin incurrir en grandes volúmenes de datos (Erol-Kantarci & Mouftah, 2013).

CONCLUSIONES Y TRABAJOS FUTUROS

En este artículo se han presentado los principales retos en seguridad y privacidad que introducen las TIC en entornos AMI, poniendo de manifiesto sus principales diferencias frente a los escenarios TIC tradicionales. Además, se han presentado resumidamente los problemas del análisis forense en este tipo de entornos. Para todos ellos, se han incluido también una serie de recomendaciones para paliar los problemas previamente expuestos. La Tabla I resume los retos y recomendaciones presentados a lo largo del artículo.

Queda patente que las AMI no están exentas de problemas en ciberseguridad, algunos de los cuales aún no han sido solventados. Por esto se recomienda a las distribuidoras y fabricantes de equipos que tomen medidas para proteger la seguridad de sus redes y la privacidad de sus usuarios y las implementen en los actuales despliegues.

Como trabajo futuro se incluye la extensión del presente estudio, analizando las vulnerabilidades de los protocolos de comunicaciones utilizados en AMI, prestando especial atención a la torre de protocolos PRIME/DLMS/COSEM, por estar ampliamente desplegado a nivel nacional, y relacionándolas con los problemas y recomendaciones expuestos en este artículo. Asimismo, sería interesante disponer de laboratorios ciber-físicos que permitan reproducir ataques de seguridad y posibles contramedidas en un entorno controlado.

	Retos	Recomendaciones
Seguridad		
Dispositivos	- Sistemas embebidos, seguridad dependiente de actualizaciones de *firmware*. *Firmware* malicioso. - Aplicaciones domóticas abren la red a dispositivos de terceros potencialmente maliciosos.	- Control de acceso estricto basado en roles y atributos. - Sistemas de clave pública/privada por nodo para verificar la integridad del *firmware*.
Red	- Ataques de denegación de servicio a nodos críticos. - Gestión de claves de cifrado poco robusta debido a limitaciones *hardware*.	- Adaptar sistemas IDS a AMI. - Reducir dominio de las claves mediante *re-signature* para facilitar su gestión.
Datos	- Agregación vulnerable a extracción o inyección de datos. - Inyección/modificación de datos para actuar sobre los sistemas de información.	- Usar algoritmos que permiten proteger los nodos más críticos frente a ataques de inyección/modificación.
Privacidad	- Posibilidad de extraer información personal y hábitos de los usuarios.	- Anonimización de los datos mediante, p.ej., técnicas de cifrado homomórfico. - Distribución del consumo en el tiempo mediante acumuladores.
Análisis Forense	- Seguridad/privacidad de los datos extraídos. - Capacidad limitada de almacenamiento de los nodos.	- Cifrado y autenticación. Se debe requerir orden judicial para el acceso a los datos. - Sistemas de agregación avanzados que permitan mantener toda la información relevante.

Tabla I. Resumen de retos y recomendaciones para seguridad, privacidad y análisis forense en AMI

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el Ministerio de Economía y Competitividad a través del Programa Estatal de I+D+i Orientado a los Retos de la Sociedad dentro del proyecto OSIRIS (RTC-2014-1556-3)

REFERENCIAS

- Chen, P.Y., *et al*., "Smart Attacks in Smart Grid Communication Networks", IEEE Communications Magazine, 2012.
- Comisión Europea. "Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism", 2004.
- Comisión Europea. "Recomendación europea relativa a los preparativos para el despliegue de los sistemas de contador inteligente (2012/148/UE)", 2012
- Erol-Kantarci, M. & Mouftah, H.T., "Smart Grid Forensic Science: Applications, Challenges and Open Issues", IEEE Communications Magazine, 2013.
- Gómez-Mármol, F., *et al.*, "Do not snoop my habits: preserving privacy in the smart grid", IEEE Communications Magazine, 2012.
- Kim, T.T. & Poor, H.V., "Strategic Protection Against Data Injection Attacks on Power Grids", IEEE Transactions on Smart Grids, 2011.
- Li, F., *et al.*, "Secure information aggregation for smart grids using homomorphic encryption", IEEE SmartGridCom, 2010.
- Liu, J., *et al.*, "Cyber Security and Privacy Issues in Smart Grids" IEEE Communications Surveys & Tutorials, 2012.
- NIST IR-7628. "Guidelines for Smart Grid Cyber Security". 2010.
- SmartGridNews – Malta's smart meters scandal: http://www.smartgridnews.com/story/maltas-smart-meter-scandal-41-million-worth-electricity-stolen/2014-02-18 [18-07-2016]