Seguridad de la red inteligente de suministro eléctrico: ¿cruzamos los dedos?

Por Steve Norman

RENESAS
www.renesas.eu/

Steve Norman es Director de Marketing de Energía Inteligente, Grupo de Negocios Industrial, Renesas Electronics Europe.

El año pasado, un informe publicado por Pike Research indicaba que el mercado de la seguridad de la red inteligente de suministro eléctrico (en inglés, smart grid) tendría un valor de hasta 21.000 millones de dólares dentro de cinco años, que equivale aproximadamente al 15% de la inversión global en la red inteligente. Un año antes, los piratas informáticos demostraron la importancia que tiene este asunto en EE.UU. debido a las "intrusiones en compañías de suministro, seguidas de extorsiones", según reveló un analista de la CIA, Tom Donahue, incluyendo cortes de suministro en varias ciudades. A menos distancia, en el Reino Unido, se ha dado a conocer que a principios de este año las bandas criminales han obtenido de manera fraudulenta 7 millones de libras mediante claves de recarga pirateadas en contadores de prepago y que sin duda acaban siendo pagadas por el clientes de prepago conectados a la línea.

En mi opinión, estas anécdotas confirman de manera muy concisa que la seguridad en la red inteligente de suministro eléctrico exige mucho más que añadir criptografiado a un contador inteligente. Y aunque esto pueda resultar sorprendente para muchos lectores, es la cuestión que centra a menudo la atención acerca de la seguridad.

¿Qué es entonces lo peor que puede ocurrir? No es el fraude en el contador; esto sólo cuesta unos pocos miles de millones de euros cada año. El peor caso es que perdamos el control de la red de contadores. En 2009, Mike Davis y su equipo en IOActive desarrollaron un gusano para contador inteligente: un trozo de código muy listo que fue capaz de extenderse de contador en contador. Utilizaron una red de contadores punto a punto simulada para demostrar cómo puede extenderse de forma alarmantemente rápida por una zona urbana entera, hasta provocar finalmente el corte del suministro y cambios en la calibración del contador que en la práctica los pusieron fuera de servicio. También desactivaron la actualización remota, lo que en el mundo real exigió visitar cada propiedad para reprogramar el contador, con el enorme impacto económico y la mala imagen para la marca de muchas personas. Tan solo fue una simulación, pero el gusano era real y fue desarrollado para un contador inteligente también real.

Ya hemos citado dos motivaciones para los ataques a la red, pero pensemos en ellas de nuevo. En primer lugar, queda potencial para el robo de datos, tanto a escala individual como a gran escala. También existe el valor puramente malicioso que tiene desconectar a alguien de la electricidad o el gas; pensemos en un ejemplo relacionado de forma indirecta como la "malicia" dirigida recientemente a Sony y su Playstation Network. También existe un beneficio financiero, bien sea por parte de una persona incentivada por el encarecimiento de los precios del combustible, por el propietario de una plantación de cannabis que consume mucha electricidad o a través del crimen organizado en su intento de influir sobre la cotización de las acciones a través del conocimiento previo del evento o por su explotación. Finalmente, se encuentra el ciberterrorismo, cuyo potencial para un ataque sincronizado podría provocar un caos sin precedentes; como nota al margen, el ataque antes mencionado en EE.UU. en 2009 se dio a entender que había tenido su origen en el extranjero… pero mi parte más cínica piensa que lo hubieran dicho de todas formas.

En resumen, lo que se desea evitar es leer el titular de un periódico (a la luz de una vela, suponiendo que hayan sido capaces de imprimirlo) en el cual se nos explique que centenares de miles de personas están sin suministro de energía eléctrica; que ningún país europeo se encuentra a salvo del pirateo que sufre el país X; que el precio de las acciones está cayendo en picado; y que no hay una solución inmediata. No queremos días de oscuridad.

La cuestión es cómo disminuir el riesgo de que ocurra lo peor. En breve adoptaremos el (necesario) punto de vista más amplio, pero empecemos por el contador con una lista de medidas sencillas que ayudarán a rechazar los ataques.

El uso de criptografía es un punto de partida muy evidente en cumplimiento de la autenticación, proporcionando así criptografiado y firma de datos, pero esto solo es una parte de la solución. Antes de la instalación deben implementarse unos rigurosos procedimientos de diseño y test para evitar vulnerabilidades del software como la sobrecarga del buffer, que consiste en la violación de la seguridad de la memoria por medio de la escritura de datos procedentes del buffer deseado a un área adyacente de la memoria. Al pasar a la fase de instalación, y de hecho a lo largo de todo el ciclo de vida del contador, deben aplicarse más controles con el fin de mantener la integridad del contador y de sus contenidos una vez activados, incluso después de su retirada de servicio y de su eliminación, sea cual sea la forma que pueda asumir esta última. La práctica que debería estar extendida actualmente es la detección, registro y generación de informes en caso de manipulación, así como garantizar el almacenamiento seguro y el uso de

claves criptográficas asociadas; y no olvidemos que también nos referimos a las claves y los certificados que se encuentran en el propio contador. Y un aspecto final sobre las claves criptográficas: deben asignarse claves separadas para usos separados.

Todo esto parece increíblemente simple, y mientras escribía gran parte del párrafo anterior me preguntaba si estaba explicando algo bien conocido ya por todos, pero resulta difícil implementar una buena seguridad.

Recordemos que en última instancia incluso los contadores inteligentes tienen una capacidad de proceso limitada, pese a integrar de manera predominante microcontroladores de 32 bit de gama relativamente alta, por lo que deben incorporar un potente criptografiado que se considere una parte del microcontrolador. Dentro del proceso de criptografiado ya he mencionado diferentes claves para diferentes usos y el desafío que represente el almacenamiento seguro de claves, pero ¿qué hay de la cuestión de renunciar a las claves? Éste supone un enorme problema que no se tratará a fondo en este artículo, pero la cuestión es que debe fijarse una estrategia que no deje al sistema vulnerable y que al mismo tiempo cumpla los compromisos que puedan tener lugar desde el momento en que se produzca la causa de renuncia a la clave, por ejemplo en el caso de una clave criptográfica robada a un instalador de contadores o un terminal portátil de instalación que se haya extraviado.

Es de prever que se instalen millones de estos contadores inteligentes teniendo en cuenta los principales planes de instalación de redes inteligentes o de los propios contadores inteligentes, y esto añade por sí mismo el reto de restringir y controlar la disponibilidad de los contadores a instalar, y más tarde – lo cual seguramente será aún más complicado – controlar su eliminación cuando llegue el fin de su vida operativa. Hay que valorar también lo que ocurre cuando el contador está instalado y se ha dejado en manos del consumidor; la seguridad física supone otro desafío a añadir a nuestra lista.

Volviendo al plano de lo no físico, todos sabemos que la parte inteligente de un contador inteligente significa comunicaciones que idealmente aporten interoperatividad (aunque eso es harina de otro costal), lo cual implica medidas de seguridad punto a punto que se analizan ampliamente. ¿Pero en realidad no deberíamos estar analizando la seguridad de extremo a extremo? ¿O es que realmente la comodidad es más importante para nosotros que la seguridad? Y hablando de comunicaciones, ¿podría enfatizar que algo nuevo no implica necesariamente que sea mejor en cuanto a vulnerabilidades de la seguridad?

Lo que se analiza no es nada nuevo si miramos hacia el exterior del contador inteligente o de la red inteligente de suministro eléctrico; podemos citar algunos ejemplos de otros sectores. La Gestión de Derechos Digitales (Digital Rights Management, DRM) del DVD fue pirateada por un joven de 16 años; el contenido de Blu-Ray fue pirateado de manera parecida apenas días después de estar disponible. El pirateo antes citado de la Playstation Network de Sony sigue vigente, pero no nos olvidemos del enorme perjuicio sobre los beneficios de Nintendo y de sus empresas desarrolladoras debido al pirateo de su consola portátil de juegos DS. ¿Y qué hay de las máquinas de votación? "Diseño seguro" pero también pirateadas; están diseñadas para evitar la inyección de código, pero se construyó una técnica de pirateo que utilizó las colas de subrutinas ya existentes para minar el sistema por completo, todas ellas halladas fácilmente utilizando una unidad de segunda mano comprada en una subasta administrativa; para ser políticamente correctos, dejaremos en el anonimato el nombre del gobierno en cuestión. En el ámbito de los teléfonos móviles y las tarjetas de crédito, los vendedores insisten en la tecnología de la tarjeta inteligente como requisito mínimo. ¿Podemos tomarnos de forma menos seria la aplicación del contador inteligente y de la red inteligente de suministro eléctrico?

Empecemos a pensar en lo que se puede hacer…

Este comentario puede resultar extraño por parte de alguien que representa al mayor fabricante mundial de microcontroladores y líder en el suministro al mercado de contadores, pero la respuesta no estará probablemente en un microcontrolador estándar. Al igual que no se cierra la cerradura de una puerta de alta seguridad y luego se deja la llave debajo del felpudo, no hay que dejar las claves criptográficas desprotegidas. No se puede confiar en que los microcontroladores estándar almacenen las claves de forma segura, y también podrían copiar las claves en una RAM mientras se utilizan; existen numerosas técnicas para que los piratas informáticos accedan a las claves de un microcontrolador estándar. También hay que tener en cuenta su capacidad para la clave y la generación de números aleatorios; es posible efectuar muchos ataques por fallos en la generación, implementación o uso de números aleatorios.

Muchos microcontroladores estándar ofrecen la capacidad de fijar una señal de aviso o fusible de protección para "evitar" la lectura de los datos almacenados, pero no es una solución adecuada. Éstos son algunos de los riesgos potenciales: los análisis de potencia mediante resistencias pueden permitir el acceso a información clave; el análisis de tiempos también puede proporcionar información clave; las interferencias de tensión pueden superar comprobaciones de seguridad; la reinicialización de fusibles mediante láseres, flashes de cámara, etc., pueden permitir la lectura de código; el borrado del chip por medio de JTAG puede permitir la lectura de los datos que contiene la RAM; y se puede aplicar el análisis de entropía a la identificación de claves.

No obstante, un microcontrolador seguro de tipo dedicado puede aportar la solución.

Un microcontrolador seguro puede ofrecer resistencia frente al ataque físico por medio del análisis o muestreo, con su trazado aleatorio del chip inherente, apantallamiento metálico, codificación de datos de memoria y una tecnología avanzada de proceso que aporte un almacena-

miento seguro de la clave en un entorno seguro. La asignación aleatoria de tiempos y la capacidad de enmascarar las operaciones, junto con el criptografiado de los datos de hardware y la generación de números aleatorios integrada en el chip, pueden evitar las perturbaciones de sincronización y de corriente que acaben en un ataque. Un ataque ilegal por tensión, ruido, temperatura, señal de reloj o de tipo óptico puede verse mitigado frente a la detección automática de manipulación, que apagará el dispositivo tras los intentos de acceso ilegal, así como protección mediante EEPROM de tipo dedicado y coproceso para generación de números aleatorios y criptografía para acelerar estas operaciones.

En resumen, un microcontrolador seguro proporciona un almacenamiento seguro de la clave ya que ésta nunca sale del microcontrolador y nunca reside en una RAM insegura; proporciona aceleración de hardware para operaciones criptográficas; evita el copiado; proporciona un almacenamiento y registro seguro de la información de crédito; integra la generación de claves y de números aleatorios; y se validan por completo los algoritmos criptográficos.

Y por último una serie de consideraciones finales. Tal como se ha señalado antes, la seguridad de "Extremo a Extremo" o E2E es más seguro que la seguridad "Punto a Punto" o P2P; P2P solo es tan segura como el eslabón más débil de la cadena, y crea vulnerabilidades en cada punto en el cual los datos se descriptografían y recriptografían. Para la seguridad E2E, el contador y el centro de datos deben implementar algoritmos compatibles, lo cual nos conduce a los marcos regulatorios y de estandarización. Existen unos niveles mínimos establecidos de seguridad criptográfica, pero permanece la cuestión de la comodidad de P2P frente a la seguridad de E2E, al igual que el impacto de las cuestiones relativas al consumo de energía, cuya importancia es crítica en los contadores alimentados mediante batería y determinados por la potencia de la criptografía empleada y la frecuencia de las lecturas. Existe asimismo la incertidumbre relativa a las patentes que cubren algunos algoritmos criptográficos como ECC (Elliptic Curve Cryptography), donde haría falta una solución para interoperatividad sin violación de patente. Por desgracia, si bien no puede haber dudas sobre los requisitos, la seguridad no es algo sencillo, sino que debe tenerse en cuenta desde un principio en los programas que contemplen contadores inteligentes y la red inteligente de suministro eléctrico, y no a posteriori.

Como punto final, en el momento de redactar este artículo la Casa Blanca acaba de anunciar su Marco Político sobre la Red Inteligente de Suministro Eléctrico para EE.UU. Se ha citado la ciberseguridad como unas de las cuatro máximas prioridades para garantizar la protección del sistema eléctrico frente a ciberataques, con la garantía de recuperación ante ataques así como el desarrollo y mantenimiento de sistemas de alarma, directrices y estándares.

En Europa debemos hacer lo mismo.