Asegurar Sistemas de Automatización y Control de Edificios contra Ataques Cibernéticos

Autor: Ferdinand Melendez Torres
Mentor: Dr. Nelliud Torres
Department of Computer Science

Resumen

Los ataques cibernéticos a sistemas de IT o tecnologías de la información son comunes y generalmente se originan en la Internet. Los sistemas de automatización y control de edificios (SACE) a menudo están conectados a la Internet, pero carecen de una protección sólida contra estos ataques: contraseñas débiles y / o predeterminadas, comunicación no encriptada, falta de protección contra cambios no autorizados en los datos y utilización de programación básica o de conocimiento público, por mencionar algunos. En este artículo discutimos cómo los SACE pueden protegerse contra ataques cibernéticos. Esto incluye una evaluación de las características de seguridad en sistemas de información según estándares como ISA/IEC-62443 y ASHRAE 135 (BACnet) entre otros.

Introducción

Los edificios más modernos contienen tecnologías para regular automáticamente la temperatura, controlar la entrada de luz y la intensidad de la iluminación. La recopilación de datos en medidores permite la optimización del consumo energético; sensores adicionales como los detectores de movimiento pueden apagar la luz cuando el cuarto, oficina o área de trabajo no esta siendo utilizada, maximiza la vida útil de los equipos, reducen costo asociados a mantenimiento, entre otros. Una alternativa adicional que proveen estas tecnologías es ayudar a mantener el edificio seguro de intrusos o acceso a personas no autorizadas con la intención de hacer daño a la operación del negocio. La seguridad se garantiza mediante el uso de dispositivos electrónicos, p. ej., enrutadores, “firewalls”, “switches”, controladores, etc. La operación automática en general funciona cuando los sensores recopilan datos y los actuadores (dispositivo mecánico cuya función es proporcionar fuerza para mover o “actuar” otro dispositivo mecánico), permiten el cambio de posición según datos obtenidos de los sensores, accionando y regulando piezas móviles como válvulas o interruptores. Estos sensores y actuadores se controlan mediante controladores que se utilizan para la automatización de edificios; juntos forman un sistema de automatización y control de edificios (SACE).

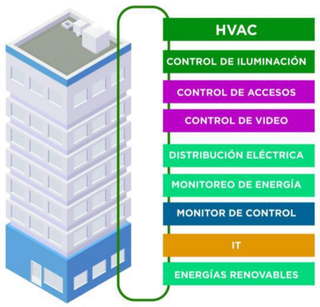

Figura 1
Diagrama típico de un Sistema de Automatización y Control de Edificios.

Componentes del SACE

Los equipos que componen un SACE generalmente se agrupan en tres niveles. La automatización en el nivel de campo (nivel donde se encuentran los equipos mecánicos, eléctricos), es el más bajo y se logra mediante la comunicación directa entre los sensores, interruptores y actuadores como, por ejemplo, el interruptor de control de la luz o pasando por un elemento del CPU como un controlador lógico programable (PLC) o control digital directo (DDC). Los tres niveles pueden incluir equipos de la siguiente manera:

• Nivel de campo: sensores, actuadores interruptores, etc.
• Nivel de automatización: los controladores (PLC o DDC) permiten el control de los sistemas de calentamiento, ventilación y aire acondicionado (HVAC); control para funciones como iluminación de pasillo y control de luz para fachadas. Una funcionalidad de control simple son los controladores de luz de las oficinas que regulan la intensidad de la iluminación, así como los aspectos de las unidades de aire (HVAC) de un área de trabajo. Estos controladores pueden hacer uso de equipos de nivel de campo para recopilar datos p. ej. medidores de uso, y poder utilizar dicha información para evaluaciones de la gerencia para futuras mejoras en eficiencia energética.
• Nivel de monitoreo: aquí es donde los datos se recopilan, se almacenan en bases de datos y se muestran a los usuarios que operan estos equipos a través de pantallas (HMI) o estaciones de trabajo (WS), incluyendo alarmas, historial de condiciones, reportes, etc. Aquí también encontrará interfaces de configuración y programación para el sistema.

Ataques Comunes

Los ataques comunes en los sistemas de información se enfocan en servidores y computadoras, así como en la infraestructura de la red o equipos IoT “Internet of Things”. Los servidores son atacados por su presencia en la web; estar expuestos a la Internet por diseño significa que tienen una "superficie de ataque" o “punto de vulnerabilidad”.

Los ataques generalmente funcionan probando contraseñas “brute force", lo que le permite al hacker intentar varias contraseñas en una sesión de correo electrónico (emails) o “website logins” hasta lograr obtener la correcta. También utilizan debilidades en páginas de la internet creados por ejemplo con CMS “Content Management System”, es una aplicación de software que permite manejar, crear y desarrollar el contenido digital en los websites. Aplicaciones de CMS que se utilizan con frecuencia son WordPress, Joomla, Drupal y Squarespace entre otros.

Otro método popular es instalar un virus que encripta o elimina archivos importantes del usuario y luego muestra un mensaje de “ransom” o de pagar para recuperarlo. Para recuperar los archivos (que puede o no que realmente los recuperes), el usuario debe pagar dinero al hacker a través de la Internet. Programación o software malicioso que utiliza los hackers en este tipo de ataques se conoce como "malware" o "ransomware", y en la mayoría de los casos, se distribuye por correo electrónico en un archivo adjunto que utiliza vulnerabilidades en la seguridad de aplicaciones como MS Office o Acrobat Reader. Estos ataques también son posibles a través de los websites utilizando vulnerabilidades en el navegador (web browser) o sus complementos (plugins). Los ataques son más fáciles cuando se instalan los “plugins”, p. ej., Adobe, Java y web browsers como Internet Explorer, Chrome o Firefox. Estos “plugins” son componentes de software que añaden una característica específica a un programa de computadora existente. Cuando un programa admite estas extensiones o complementos, permite personalizar la experiencia que el usuario tiene durante el uso de la aplicación o durante la navegación en un website. Plugins permiten realizar funciones adicionales además de las funciones predeterminadas por las cuales fue diseñado originalmente. Una vez dentro de una red local (LAN), el malware a menudo puede propagarse fácilmente, aprovechándose de las vulnerabilidades en la seguridad o políticas de acceso en los sistemas operativos.

La mayoría de los ataques contra Internet of Things (IoT) y equipos dentro de una infraestructura de una red se enfocan en enrutadores de cable o DSL y cámaras con IP. Estos equipos están conectados a la Internet 24 horas al día. A menudo carecen de la configuración de seguridad adecuada, no tienen, o tienen una contraseña predeterminada de fácil acceso, o tienen otras vulnerabilidades de seguridad. Suplidores de hardware no solucionan problemas de seguridad en equipos actualmente en uso, específicamente en equipos legacy si modelos recientes salieron al mercado. En muchas ocasiones los usuarios desconocen de la necesidad de nuevos firmwares, creando una vulnerabilidad en la seguridad estos equipos. Una vez el hacker tiene acceso, utiliza estos equipos para acceder a otros equipos o sistemas en la red implantando un gusano “worm” y poder crear un botnet.

Un botnet es un número de equipos conectados a la Internet, cada uno de los cuales ejecuta uno o más bots (aplicaciones de software que corren instrucciones automáticamente en la Internet). Botnets se pueden utilizar para realizar ataques de negación de servicio distribuida (DDoS), robar datos, enviar spam y permitir que el hacker acceda a otros equipos y sistemas. El hacker puede controlar el botnet utilizando el software de comando y control (C&C) (figura 2). La palabra "botnet" es un acrónimo de las palabras "robot" y "network". El término generalmente se usa con una connotación negativa o maliciosa.

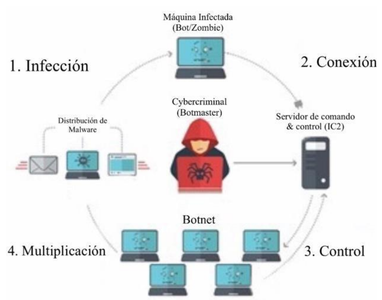

Figura 2
Cómo funciona un botnet

Como Asegurar un SACE

Para que los SACE sean más seguros contra los ataques cibernéticos, es necesario establecer un proceso que rija la producción, cadena de suministro, instalación, configuración/programación, operación y mantenimiento. Los estándares internacionales como el ASHRAE 135 (BACnet) anexo g e ISA/IEC 62443 pueden ayudar a cubrir muchos aspectos de seguridad y hacer que los sistemas sean operables conforme a estos estándares de seguridad.

BACnet es un protocolo de comunicación de datos que estandariza las comunicaciones entre equipos electrónicos de automatización de edificios de diferentes fabricantes, lo que permite compartir datos y que los equipos trabajen juntos fácilmente. BACnet define los objetos de datos, sus propiedades y los servicios para la comunicación. A diferencia de otros estándares (como Modbus), este se ha escrito específicamente para sistemas de automatización de edificios, no para sistemas de automatización y control en general. Esto significa que tiene todas las definiciones y tipos de datos necesario facilitando también la documentación y análisis. Su comunicación basada en IP (BACnet/IP) se basa en UDP/IP, mientras que la mayoría de los estándares más seguros de comunicación y autenticación (como TLS y SSH) (en su forma estándar) se basan en TCP/IP. ASHRAE 135g define sus propios mecanismos de protección, lo que hace que su implementación sea más compleja. La seguridad se realiza en la capa de la red y se define para todos los medios, como MS/TP, BACnet/IP, etc. y todos los tipos de equipos (figura 3). También funciona para todos los servicios/paquetes, incluyendo mensajes confirmados y no confirmados, difusión uno a uno “unicast”, uno a todos “broadcast” y uno a varios “multicast”.

Figura 3 Capas de Comunicación BacNet

ASHRAE 135g permite el uso de hash MD5 y SHA-256 (SHA2 con 256 bits). Para la confidencialidad mediante encriptación, permite encriptación simétrica con el estándar AES-128, que también es bueno según los estándares de seguridad actuales. ASHRAE 135g requiere un manejo de claves o llaves algo complejo, por lo que permite la protección de capas del acceso al bus (comunicación), datos (confidencialidad) y configuración del equipo.
AES también se utiliza para firmas digitales como prueba de autenticidad de datos y acceso. La autenticación normalmente se realizaría con un algoritmo de encriptación con clave o llave pública (es decir, asimétrico) como RSA, como se usa en estándares como HTTPS, PGP, etc. La verificación de autenticidad, así como la protección de acceso mediante claves o llaves, también pueden evitar el cambio no autorizado de datos, programación y firmware, que es una característica importante.

IEC 62443 estándar fue creado originalmente como ISA-99 por la Sociedad Internacional de Automatización (ISA), pero ahora es desarrollado por la Comisión Electrotécnica Internacional (IEC).
IEC 62443 está organizado en las siguientes cuatro categorías: General, Políticas y Procedimientos, Sistema y Componentes:

• General: proporcionan una visión general del proceso de seguridad industrial e introduce conceptos esenciales.
• Políticas y procedimientos: destacan la importancia de las políticas: incluso la mejor seguridad es inútil si las personas no están capacitadas y comprometidas a apoyarla.
• Sistemas: debido a que la seguridad solo puede entenderse como un sistema integrado, los documentos del sistema proporcionan una guía esencial para diseñar e implementar sistemas seguros.
• Componentes: los documentos de componentes describen los requisitos que deben cumplirse para componentes industriales seguros.

IEC 62443 cubre un área amplia, que incluye muchas recomendaciones para procesos comerciales según las mejores prácticas en la industria, desde infraestructura y control de acceso hasta copias de seguridad para garantizar la disponibilidad.

Otros Aspectos en la Seguridad Cibernética

Al considerar la seguridad de un SACE, las técnicas presentadas en los estándares y las mejores prácticas en la industria del mundo de IT deben implementarse.
Por ejemplo, si se necesita acceder a un SACE remotamente, ya sea para mantenimiento, acceso a datos o control, se puede usar VPN (Red Privada Virtual). Se puede implementar un acceso VPN en un enrutador de la red instalado en sitio. Los equipos del SACE se configurarían y conectarían de manera tal que no fuera posible el acceso externo directo, sin embargo, se conectarían al router (o por medio de él). Entonces, se podría usar VPN para acceder al router desde el exterior utilizando un canal encriptado y seguro. Una vez obtenido este acceso a un equipo o sistema, el router prácticamente lo convierte en parte de la red local, lo que permite la comunicación con todos los componentes del SACE.
También se pueden usar técnicas de endurecimiento “hardening” como las utilizadas en servidores y redes, por ejemplo:

• Reducir el acceso físico y electrónico al mínimo requerido para un funcionamiento adecuado.
• Cierre, deshabilitación y eliminación de puertos no utilizados en la red, software y servicios no necesarios, incluyendo, pero no limitado a telnet, Modbus y servicios de configuración/programación y controladores de puertos
• Elegir buenas contraseñas de acceso individual y distintos niveles de usuario, p. ej., para visualización, configuración/control y reprogramación
• Inhabilitar la posibilidad de adivinar las contraseñas rápidamente mediante el uso de la fuerza bruta, limitando la cantidad de intentos cuando se inicia una de sesión y activando bloqueos automáticos después de cierta cantidad de intentos.
• Separar partes de la red que no necesitan comunicarse, p. ej., redes de oficinas, redes de invitados, redes de WiFi, SACE, etc. mediante el uso de VLANs, y utilizando DMZ (zonas desmilitarizadas) para restringir el acceso en línea
• Utilizar firewalls buenos y bien configurados para filtrar el tráfico entrante y saliente
• Mantener seguras otras computadoras en el mismo sitio, así como las computadoras portátiles que se usan para mantenimiento.

Conclusión

La seguridad cibernética para los edificios es cada vez más importante a medida que avanza la tecnología, dándole más recursos a los hackers, por lo tanto, aumentando los ataques a estos sistemas. Las soluciones y tecnologías de seguridad presentadas son las que se incluyen en los estándares actuales de seguridad de redes y las más utilizadas en la industria. Se pueden utilizar equipos/sistemas más robustos como los que se adaptan al estándar de ASHRAE 135g (BACnet) y tener como complemento la implementación de los aspectos de seguridad para monitoreo y control según IEC 62443. Implementar una seguridad eficiente y efectiva contra los ataques cibernéticos es difícil y costosa, pero es un activo si lo comparas con la posible pérdida de información o interrupción de operaciones de una manufactura o negocio.

Referencias

[1] M. Nast, B. Butzin, F. Golatowski y D. Timmermann, "Performance Analysis of a Secured BACnet/IP Network", 15th IEEE International Workshop on Factory Communication Systems (WFCS), Sundsvall, Suecia, 2019, pp. 1-8, doi: 10.1109/WFCS.2019.8758009.

[2] N. A. Khan y H. Ahangar, "Use of Open Content Management Systems in Government Sector," 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS), Noida, 2018, pp. 183-187, doi: 10.1109/ETTLIS.2018.8485191.

[3] C. Easttom, Computer Security Fundamentals, 3a ed. Indiana: Pearson, 2016.

[4] Energy management systems – Requirements with guidance for use, ISO 50001, 2018.

[5] Building Automation And Control Systems (BACS) – Part 5: Data Communication Protocol, ISO 16484-5, 2017.

[6] BACnet: A Data Communication Protocol for Building Automation and Control Networks, ANSI/ASHRAE 135, 2016.

[7] Network and System Security for Industrial Process Measurement and Control, ISA/IEC 62443, 202[10] “5G Network Slicing in 5GTANGO,” 5GPPP. [Online]. Available: https://5g-ppp.eu/5g-network-slicing-in-5gtango/