Implementación de Mecanismos de Seguridad en las Comunicaciones de un Sistema de Gestión de Edificios Dedicado a Tareas de Oficina.

Resumen: *La seguridad en los sistemas de gestión de Edificios (SGE) es de gran importancia, la falsa creencia de que no es un blanco de interés para hackers, o incluso para usuarios o empleados, puede llevar a ingratas sorpresas, que varían desde una consecuencia incómoda, a un verdadero riesgo empresarial. Se debe proteger tanto de amenazas externas como internas. Los estándares de comunicación de SGE como KNX han comenzado en forma reactiva a implementar niveles de seguridad en sus sistemas. En el trabajo, se propone una metodología que permita implementar medidas para brindar seguridad en las comunicaciones de un SGE automatizado con KNX; y que clasifica las amenazas y los sectores vulnerables, implementa mecanismos para contrarrestar o evitar ataques y describe una arquitectura de red segura. La metodología puede ser utilizada también en SGE basados en otros estándares de comunicación diferentes a KNX.*
Palabras Claves: *lSGE; Seguridad; KNX; Comunicaciones*

Abstract: *The security of Building Management System (BMS) has a great relevancy, the false belief that the BMS is safe from hackers attacks or even from users or employees attacks too, can it carrying to unfortunate surprises, from uncomfortable consecuencies to a dangerous empresarial risk. It must give protection for both external threats and internal threats. The comunication Standars such as KNX have began to implement security levels in your systems in reactive way In this article proposes present a methodology that allow to implement actions to give security in the comunication of a automated BMS with KNX.; Classifies threats and vulnerability sectors. Implements mechanisms to counteract or prevent attacks and describes a security net architecture. The methodology can be used in BMS with others communication standards that are different to knx.*
Keywords: *BMS; Security; KNX; Comunication*

Andrés I. Vigil

Grupo de Control y Seguridad Eléctrica (CySE) (Lavaise 610, Santa Fe),
Facultad Regional Santa Fe, UTN
E-mail de contacto: avigil@frsf.utn.edu.ar

INTRODUCCIÓN

Las redes de información de los sistemas de automatización y sus estándares se desarrollaron en su mayoría antes de fin de siglo pasado, en aquellas épocas aún no se había dado la gran expansión de las redes y el auge de internet, que trajo aparejado nuevas vulnerabilidades, amenazas inherentes y virus informáticos. Los sistemas de automatización de edificios, o también denominados Sistemas de Gestión de Edificios (SGE), comprenden desde los sensores y actuadores de campo hasta el software de gestión de las instalaciones del edificio [1]. En principio los SGE parecieron mantenerse al margen de ataques, ya sea por resultar blancos de poco interés o por encontrarse en redes privadas ocultas a internet. No obstante hoy en día la situación de privilegio de los SGE ha cambiado. Un ejemplo de ello es el ataque al Hotel St Regis en la ciudad China de Shenzhen en el 2014. (Ver nota: [2]), donde un huésped con habilidades informáticas y conocimientos sobre el protocolo de comunicación produjo un caos en el servicio de lavandería del hotel. Los estándares en automatización de edificios SGE han comenzado en forma reactiva a implementar niveles de seguridad en sus sistemas. El protocolo KNX (ISO/IEC 14543), mediante sus extensiones KNX AN158 (2014) [3], KNX AN159 (2013) [4], aprobadas en 2015 y el protocolo BACnet (ISO 16484-5) [5] a través de addendum 135-2008g aprobada en 2010 dan cuenta de ello. En el caso de KNX las extensiones mencionadas no han sido aún implementadas en los dispositivos de campo, es por ello que es necesario implementar mecanismos o contramedidas para brindar seguridad. Cavallieri [6], Lechner [7] y Granzer [8,9] abordan el tema clasificando las amenazas y contramedidas de todo el sistema, proponiendo mecanismos para generar un canal seguro a nivel backbone, aunque dejando sin cubrir los otros sectores de vulnerabilidad. Por otra parte Antonini [10] y Granzer [9] resaltan vulnerabilidades en el resto de los estándares de comunicación de automatización de edificios. El trabajo propone una metodología para implementar medidas de seguridad en las comunicaciones de un SGE automatizado con KNX. La metodología:

- clasifica las amenazas
- clasifica los sectores vulnerables
- implementa mecanismos para contrarrestar o evitar ataques
- describe una arquitectura de red segura.

La metodología puede ser utilizada en SGEs basados en estándares de comunicación diferentes a KNX.

METODOLOGÍA

Arquitectura básica de un SGE

La arquitectura básica de KNX para un SGE consta de:

- Dispositivos de campo (Actuadores, Sensores, Controladores)
- Red de campo (1er nivel): Compuesto por el BUS KNX que interconecta los dispositivos de campo.
- Red de backbone (2do nivel): En la actualidad compuesta por una red TCP/IP típica.
- Software o Servidor de gestión (BMS Server por su sigla en inglés): Servidor que brinda la gestión y la interfaz de monitoreo centralizada de todo el edificio.

Una arquitectura de 2 niveles (red de campo + backbone) es suficiente en un edificio de oficinas. La interconexión entre los 2 niveles de la red se realiza mediante un Gateway IP/KNX que hace de interfaz entre los diferentes protocolos de cada una de las redes. La posibilidad de utilizar routers a nivel de campo es descartada por razones de seguridad y de diseño de la arquitectura, dejando la interconexión de redes bajo responsabilidad del BMS Server.

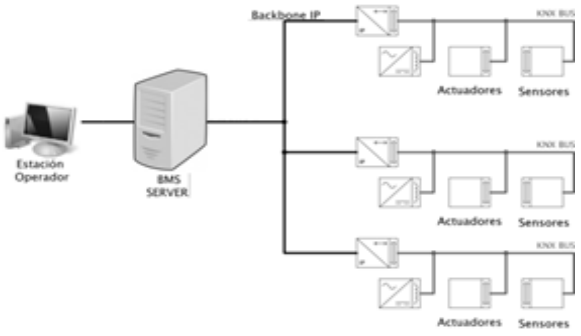

Figura 1. Arquitectura de un SGE de 2 niveles.

Amenazas, ataques, mecanismos de seguridad y servicios

Un trabajo realizado por Stallings [11] define:

- Amenaza: Una potencial violación de seguridad, la cual existe cuando hay una circunstancia, posibilidad, acción o evento que podría violar la seguridad y causar daño. Una amenaza es un posible peligro que podría explotar una vulnerabilidad.

- Ataque de seguridad: Cualquier acción que compromete la seguridad de información propia de una organización.

- Mecanismo de seguridad: Un mecanismo que es diseñado para detectar, prevenir o recuperarse de un ataque de seguridad.

- Servicio de seguridad: Un servicio que mejora la seguridad de un sistema de procesamiento de datos y la transferencia de información de una organización. Los servicios son destinados a contrarrestar los ataques de seguridad, y ellos hacen uso de uno o más mecanismos de seguridad para proveer el servicio.

En un SGE un ataque se puede producir accediendo a la red o a los dispositivos de campo. Una clasificación completa de los ataques puede verse en la figura 2.

Las amenazas pueden ocurrir a nivel de dispositivos, red de campo, red de backbone (amenazas internas) y BMS Server (amenazas externas) Figura 3.

KNX no ofrece mecanismos de seguridad para protegerse de ataques de red.

Propuesta de seguridad

Se propondrá estrategias de seguridad para cada una de las partes de la arquitectura previamente clasificadas.

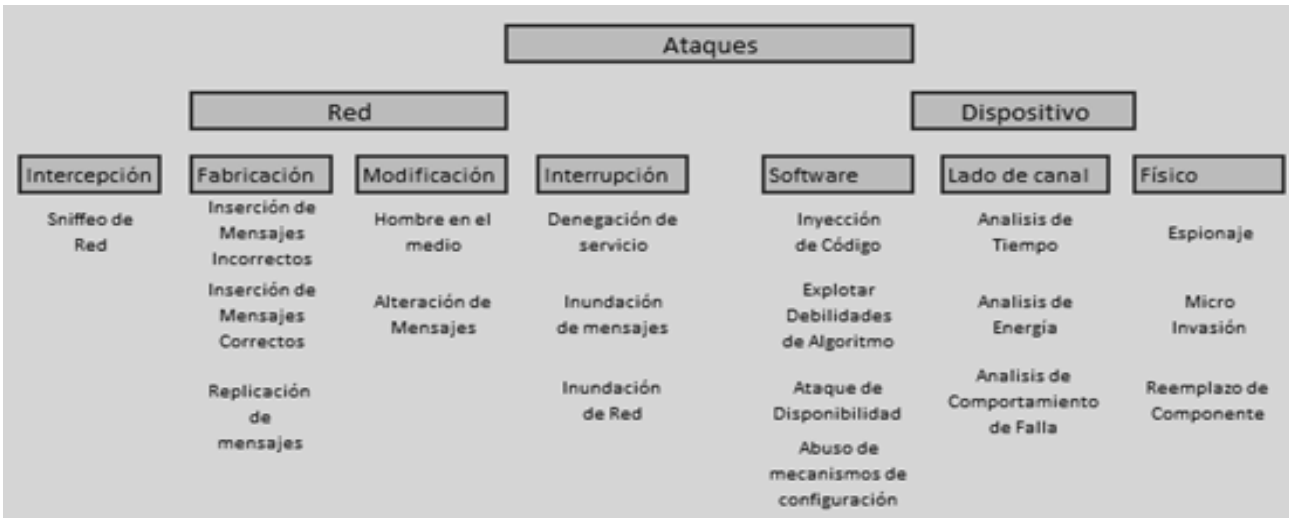

Figura 2: Ataques de Seguridad en un SGE Granzer [8].

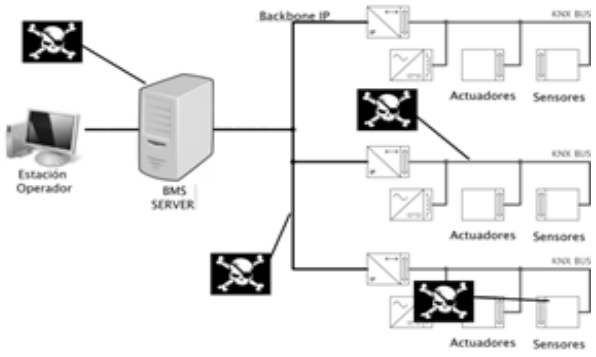

Figura 3. Amenazas en un SGE.

Dispositivos

Los dispositivos de automatización son normalmente dispositivos embebidos con recursos limitados de sistema como memoria o poder de proceso, que se alimentan vía BUS o batería. Los mecanismos de seguridad (particularmente algoritmos de encriptación) son computacionalmente caros y no están disponibles en ellos. Además se debe tener en cuenta que muchos de los dispositivos se encuentran físicamente expuestos al alcance de cualquier atacante o incidente, por ejemplo un sensor de presencia que es una pieza necesariamente expuesta, no solamente podría sufrir una ataque de modificación de configuración o firmware sino que también puede ser reemplazado intencionalmente por otro (impostación), ser robado o ser violentado (ataque de disponibilidad) con o sin intención (incidente).

Ante estas condiciones poco favorables, en este nivel sólo se puede proveer mecanismos físicos que contrarresten estas debilidades (contramedidas).

- Ocultar y proteger todos los dispositivos que no necesiten estar expuestos dentro de racks, centro de datos o tableros eléctricos que posean seguridad física y control de acceso.

- Mantenerlos vigilados u observados con cámaras de seguridad.

- De ser posible restringir el acceso a los sectores vulnerables de los dispositivos expuestos, empotrándolos en la mampostería y cubriendo con etiquetas de seguridad la clema de conexión y el botón reset.

Bus de campo.

A nivel de Bus de campo, KNX tampoco ofrece mecanismos de seguridad ante ataques de Red siendo vulnerable a ataques como sniffeo de red, impostación de activos, generación de tráfico o denegación de servicio. Descripto por: Antonini [11].

Los mecanismos de seguridad otra vez se reducen a una protección física del recurso, los objetivos serán aislar el acceso a esta red y ocultarla para evitar que un atacante pueda tener acceso a ella (seguridad por oscuridad). Para aislar los puntos de acceso a la red se tomarán las siguientes medidas:

- Sectorizar el edificio en unidades pequeñas (sub redes) para disminuir el impacto de un ataque de denegación de servicio o de un sniffeo de red a una sola subred y no se pueda propagar.

- Evitar el uso de routers KNX/IP en cambio utilizar Gateway KNX/IP (cuya única función es la conversión de protocolos). El Gateway arma una conexión unicast con el BMS, se evita de este modo la interconexión vía KNX de las diferentes subredes. Todo el tráfico de red accede por el gateway (único punto de choque).

- Restringir el ingreso a la red mediante un Firewall con mecanismo de detección de ataques de inundación de red, lista blanca de acceso, etc. (Una explicación detallada de la configuración del firewall será dada más adelante)

Los tres puntos anteriores tratan sobre como limitar los accesos vía red, no obstante también deberemos proteger el acceso físico al BUS.

- Aislar el BUS de las demás redes de datos.

- Proteger al BUS físicamente dentro de un caño o cablecanal cerrados que en caso de ser vulnerados dejen marcas inocultables de que su aislamiento ha sido violado.

- Evitar el uso de dispositivos KNX con conexión de radiofrecuencia a este nivel, donde cualquier atacante sin la necesidad de estar físicamente cerca podría tomar contacto directo con el BUS.

No existe a nivel de BUS la posibilidad de incluir dispositivos de detección de intrusos (IDS), firewalls o proxys, además el Gateway KNX/IP carece de capacidad de procesamiento para incluir mecanismos de seguridad o de control de acceso, por eso es vital anteponerle al Gateway de ingreso un firewall dedicado que brinde los mecanismos de seguridad.

A pesar de las debilidades nombradas una de las ventajas de KNX es que al tratarse de hardware no convencional (no es una red TCP/IP) un atacante requiere de software y hardware particular. Por ejemplo aunque un atacante pueda tener acceso a la clema del dispositivo o al BUS de datos, de no tener una interfaz y un software preparado para KNX no podría realizar modificaciones a ningún dispositivo.

Backbone IP

Se puede suponer que esta es la red más propensa a sufrir ataques debido al extenso uso de redes IP y que sus falencias y debilidades son ampliamente conocidas.

Se puede generar un canal seguro entre dispositivos de una red TCP/IP utilizando [13]:

- IPSEC: Es una extensión al protocolo IP que permite construir un canal seguro de comunicación entre dos entidades, funciona a nivel de capa de red, utiliza mecanismos de encriptación (DES, 3DES, AES), de autenticación (IKE, HMAC-SHA1) y brinda los servicios de autenticación mutua, integridad de datos, freshness y confidencialidad.

- SSL/TLS: Security Socket Layer y su sucesor Transport Layer Security son protocolos de capa de transporte desarrollados para asegurar la comunicación entre dos aplicaciones. Brinda servicios de confidencialidad, integridad, freshness y autenticación, para conseguirlo se basa en mecanismos de autenticación (HMAC-MD5, RSA, TLS_DH), cifrado (AES). La principal desventaja de TLS es que no puede ser utilizado en arquitecturas multicast, no obstante como se ha descripto previamente para el caso en cuestión no se utilizará la opción multicast.

- VPN: Es una tecnología que permite construir una red lógica segura sobre un medio de comunicación que no es seguro, principalmente se utiliza para asegurar conexiones de usuarios remotos que necesiten acceso y privilegios de red local dentro de una organización. VPN hace uso de SSL/TLS o IPSec. La realización de VPN's dentro de una red local se conoce como VPN over LAN y se utiliza para aislar zonas y servicios de redes internas de una organización, este es el caso de estudio.

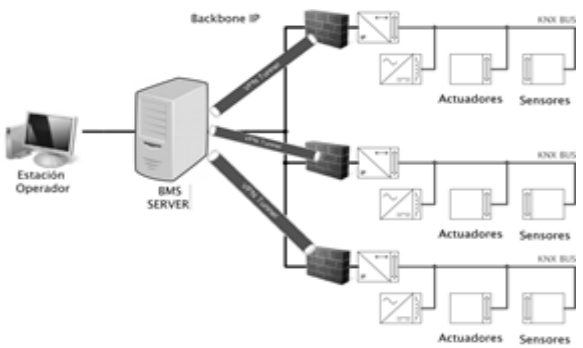

Figura 4. Arquitectura con seguridad a nivel Backbone.

La implementación de VPN necesita que cada entidad cliente que se conecta construya una conexión con una entidad servidora centralizada.

Un túnel VPN se realiza desde cada Firewall (cliente VPN) que antecede a los Gateway KNX/IP hasta el BMS

Firewall VPN						
dirección MAC origen	puerto origen	dirección MAC destino	puerto destino	Tráfico	flags	acción
BMS Server	BMS Server app	Gateways habilitados	KNX puertos	entrante	*	permitir
Gateways habilitados	KNX puertos	BMS Server	BMS Server app	saliente	*	permitir
Gateways habilitados	KNX puertos	BMS Server	BMS Server app	saliente	syn	denegar
*	*	*	*	*	*	denegar

Tabla 1. Tabla de Filtro Firewall Cliente VPN.

Server en donde se implementará un Servidor VPN. Ver Figura 4. Los dispositivos KNX no poseen la capacidad de implementar VPN por eso es fundamental antecederlos con un activo de Red que pueda actuar como cliente VPN.

Consideraciones de Firewall:

- Funciona como único punto de choque de acceso a la red de campo. Todos los mecanismos de seguridad de acceso se aplican aquí.
- Actúa como Cliente VPN.
- Acceso por lista blanca. Tabla 1.
- Restringe el tráfico de puertos permitiendo el paso solo a aplicaciones utilizadas. Tabla 1.
- Deniega conexiones provenientes de la red interna
- Implementa mecanismos contra ataques de inundación [13].

BMS Server

A nivel BMS Server los conceptos de seguridad se extienden a otros niveles de aplicación, no es la intención de esta propuesta salirse de los conceptos de seguridad en redes. No obstante es inevitable proponer cambios a la estructura del BMS para poder implementar la solución.

Los siguientes conceptos serán utilizados para entender la estructura segura del BMS Server:

- Arquitectura MVC: Es una arquitectura de software que separa los datos y la lógica del negocio de la interfaz de usuario.

- DMZ: (zona desmilitarizada) es una zona segura que aísla la red externa (internet) de la red interna de la organización. Se utiliza principalmente para ubicar servidores que deben ser accedidos desde la red externa y sólo estos servidores pueden realizar peticiones a la red interna.

Se propone separar al software en capas (Interfaz/ Lógica + datos) y se abre la posibilidad de migrar la capa de interfaz (la expuesta al público) a una DMZ Figura 5.

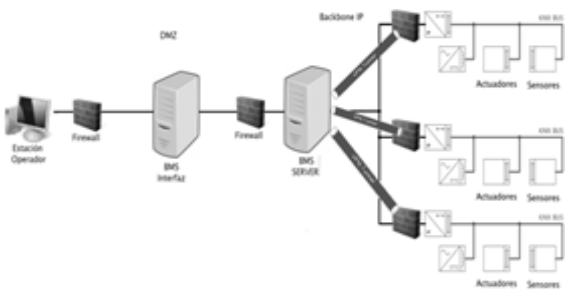

Figura 5. Arquitectura de seguridad de un SGE.

Los firewall que conforman la DMZ deben ser de diferente marca y modelo para disminuir el riesgo de un ataque que explote una vulnerabilidad particular de algún modelo de firewall.

El último punto a considerar para la seguridad es la redundancia de servidores que aumenta la disponibilidad del servicio.

Firewall 1						
Dirección MAC origen	puerto origen	Dirección MAC destino	puerto destino	Tráfico	flags	acción
Host habilitados	BMS interfaz aplicacion cliente	BMS interfaz	BMS interfaz aplicación servidor	entrante	*	permitir
BMS interfaz	BMS interfaz aplicación servidor	Host habilitados	BMS interfaz aplicacion cliente	saliente	*	permitir
BMS interfaz	BMS interfaz aplicación servidor	Host habilitados	BMS interfaz aplicación cliente	saliente	syn	denegar
*	*	*	*	*	*	denegar

Tabla 2. Tabla de Filtros de Firewall 1.

Firewall 2						
dirección MAC origen	puerto origen	Dirección MAC destino	puerto destino	Tráfico	flags	acción
BMS interfaz	BMS Server aplicación cliente	BMS Server	BMS Server aplicación servidora	entrante	*	permitir
BMS Server	BMS Server aplicación servidora	BMS interfaz	BMS interfaz aplicación cliente	saliente	*	permitir
*	*	*	*	*	*	denegar

Tabla 3. Tabla de Filtros de Firewall 2.

RESULTADOS

Lo más conveniente en un sistema de seguridad es ser completamente consciente de que amenazas se han suprimido, cuales se han mitigado y cuales simplemente se han asumido. En otras palabras que se ha conseguido evitar y a que consecuencias habrá que atenerse. Se podría asegurar que un atacante utilizando el camino de conexión convencional no podría obtener acceso directo ni al BMS Server ni a los dispositivos de campo a excepción que encuentre vulnerabilidades del propio software BMS (Ej. Backdoors), esta clase de vulnerabilidades no fue abordada en este artículo.

Se ha puesto un importante esfuerzo en aislar las diferentes subredes que conforman la arquitectura tanto lógica como físicamente, incluso eliminando el acceso inalámbrico. Aunque no se puede asegurar absolutamente la posibilidad de un acceso intruso.

Las tablas 4, 5 y 6 muestran los Servicios brindados y los mecanismos utilizados para conseguirlo en cada uno de los niveles.

	BMS				
Servicios	Control de Acceso	Autenticación	Integridad	Confidencialidad	Disponibilidad
Mecansimos	Lista Blanca				
	Autenticación Software				
		Encripción (propia del Soft BMS)			
		Firma Digital (propia del soft BMS)			
					Control de tráfico

Tabla 4. Mecanismos y Servicios a nivel BMS.

	Backbone				
Servicios	Control de Acceso	Autenticación	Integridad	Confidencialidad	Disponibilidad
Mecansimos	Lista Blanca				
		Encripción			
		Firma Digital			
				Oscuridad	
					Control de tráfico

Tabla 5. Mecanismos y Servicios a nivel Backbone.

	Nivel de Campo			Dispositivos	
Servicios	Control de Acceso	Confidencialidad	Disponibilidad	Control de Acceso	Confidencialidad
Mecansimos	Lista Blanca			Lista Blanca	
	Etiqueta de Seguridad			Vigilancia	
		Oscuridad		Etiqueta de Seguridad	
			Control de tráfico		Oscuridad

Tabla 6. Mecanismos y Servicios a nivel de Campo y Dispositivos.

DISCUSIÓN

Se ha clasificado y analizado las amenazas; también se ha propuesto medidas de seguridad para todos los sectores que componen el SGE, cumpliendo el objetivo del trabajo. También se ha hecho referencia a las dificultades para proteger el acceso al medio vía red de campo en la sección 2.3.2, transformándose el control de acceso a la red de campo en el punto crítico de la seguridad. Para contrarrestar el punto crítico, se propuso la inclusión de subredes y la eliminación de los routers KNX/IP, que junto al anexo de firewalls hacen de muro de contención frente a los ataques provenientes de un sector, evitando que se propaguen a otros sectores y disminuyendo el rango de acción de un atacante a una sola subred. Objetivo diferente es el buscado por Granzer y Cavalieri cuya intención es proponer una revisión y cambios al estándar incluyendo seguridad nativa a nivel de campo y backbone.

Sorprende que uno de los más importantes estándares mundiales de automatización como KNX haya esperado a sufrir un ataque informático para tomar las acciones pertinentes que lo protejan ante vulnerabilidades. Se espera que en los años venideros la seguridad nativa provista por los estándares sea suficiente y el trabajo futuro se concentre sólo en la protección física de los dispositivos como en la sección 2.3.1 y en proteger el acceso a la interfaz que es la que estará en contacto directo con los usuarios como en la sección 2.3.4.

El punto más importante conseguido en la propuesta, fue reducir el rango de acción de un posible ataque. Por ejemplo si un atacante toma control del bus de campo, sólo podrá hacerlo, si ha tenido contacto físico con el medio; y sólo podrá ver (sniffear) información relativa a esta subred. Tampoco podrá obtener información del BMS Server que quedará oculta tras el o los firewall, ni tomar control de otra subred ya que el BMS server es quien se encarga de la conexión en alto nivel de las subredes. Si se lanzara un ataque de denegación de servicio sólo se afectaría a una subred, y sería fácilmente detectable. En resumen un atacante debería vencer varios mecanismos de seguridad para conseguir control global del sistema.

CONCLUSIONES

En este artículo se ha construido una metodología que permite brindar seguridad en una arquitectura de red que carece de ella. Las redes de los SGE interactúan con diferentes tecnologías de comunicación y los mecanismos para conseguir seguridad son diversos, tanto lógicos como físicos. Es destacable, por otro lado que la metodología puede ser utilizada también en SGE, basados en otros estándares de comunicación diferentes a KNX, debido a que las vulnerabilidades, falencias y arquitecturas backbone son similares.

En cada uno de los niveles, los mecanismos y las propuestas de seguridad fueron diferentes, por ejemplo: A nivel de BMS, Se separó en capas al Software de SGE y se expuso al público solo la interfaz brindando altos niveles de seguridad lógica y física, incluso para acceso remoto. A nivel Backbone se incluyó una VPN que es una reconocida y confiable solución de seguridad en redes. En cambio a nivel de campo la seguridad sólo fue posible evitando el acceso físico al medio y a los dispositivos.

REFERENCIAS

Wang, S. (2010). Intelligent Buildings and Building Automation. Londres: Spon Press Págs .

Zetter, K. (2014). Web: http://www.wired.com/2014/07/hacking-hotel-room-controls/

KNX Org. (2014). KNX Data Security. Applicaction Note 158/13 v02. KNX CERTIFICATION AND LICENCE SYSTEM.

KNX Org. (2013). KNX KNXnetIP Secure. Applicaction Note 159/13 v04. KNX CERTIFICATION AND LICENCE SYSTEM.

ANSI/ASHRAE. (2008). BACnet Addendum 135-2008g. AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS, INC.

Cavalieri, S. Cutuli, G. (2009). Realising secured data transmission in KNX. Industrial Informatics, 2009. INDIN 2009. 7th IEEE International Conference on (págs 626-631). Cardiff, Wales: IEEE.

Lechner, D. Granzer, W. Kastner, W . (2008). Security for KNXnet/IP, KNX Scientific Conference. Sint-Katelijne-Waver, Belgium.

Granzer, W. Praus, F. (2010). Security in Building Automation Systems. IEEE Transactions on Industrial Electronics, Vol 57. Nro 11: IEEE

Granzer, W. Neugschwandtner, George. Praus F. (2006). Security in Networed Building Automation Systems Factory Communication Systems, 2006 IEEE International Workshop on (283-292). Torino, Italy: IEEE.

Antonini, A. Maggi, F. Zanero, S. (2014). A Practical Attack Against a KNX-based Building Automation System. 2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014). St Pölten, Austria: BCS.

Stallings, W. (2010). Cryptography and Network Security. Londres: Prentice-Hall. Págs (-)

Granzer, W. Lechner, D. Praus F. (2009).

Securing IP Backbones in Building Automation Networks, Industrial Informatics, 2009. INDIN 2009. 7th IEEE International Conference on (págs. 410-415). Cardiff, Wales: IEEE.

Granzer, W. Reinisch, C. Kastner, W. (2008). Denial-of-Service in Autiomation Systems. Emerging Technologies and Factory Automation, 2008. ETFA 2008, IEEE International Conference on. (págs 468 – 471). Hamburgo, Alemania: IEEE.

FECHA DE PRESENTACIÓN: 22/02/16
FECHA DE APROBACIÓN: 10/08/16