



IV CONGRESO EDIFICIOS INTELIGENTES

Madrid 19 Junio 2018

CIBERSEGURIDAD ABSOLUTA, TAMBIÉN PARA EL CONTROL Y LA AUTOMATIZACIÓN DE VIVIENDAS Y EDIFICIOS

Casto Cañavate Fernández

Marketing Manager and Business Developer

KNX Association International



GRUPOTECMARED



IV CONGRESO
EDIFICIOS INTELIGENTES
Madrid 19 Junio 2018

SITUACIÓN ACTUAL

Smart home hacking is easier than you think



Scary stories of hacking Internet of Things devices are emerging, but how realistic is the threat?

By Colin Fiegale | 10:00 NetworkWorld | Apr 2, 2015 4:34 AM PT

RELATED TOPICS: Security, Internet of Things

Last March, a very satirical cover of the *Harvard* MIT Thermostat led a product review on Amazon.com that shed some light on an unexpected benefit of the smart home — revenge.


Smart home devices could put you in danger

Cade Thompson | Jul 15, 2015, 11:59 PM | 258

Smart home products are supposed to help keep you safe, but some of these connected devices could put you in danger.

As home automation products flood the market, there's growing concern that these internet connected devices — like smart cameras and thermostats — are an easy target for hackers because they lack basic security measures.

"Really, the state of security on these things right now is pretty atrocious," Colby Moore, a security research engineer at the cybersecurity firm Snyack, told Business Insider.



Poor security on smart home devices can enable hackers to know when you aren't at home.

How Hackers Violate Privacy and Security of the Smart Home

POSTED IN HACKING ON SEPTEMBER 11, 2015

The Technology Invades Our Living Room

The rapid growth of the paradigm of the Internet of Things is influencing in a significant way our concept of "house." Modern homes are full of smart devices and new generation of smart appliances promises to make our life easier and more comfortable, but we cannot underestimate that risk of cyber attacks.

The solutions for home automation are flooding the market, but these devices in the majority of cases lack security; security experts are aware that smart cameras and meters are an easy target for hackers.

Samsung Smart Home flaws let hackers make keys to front door

Don't rely on SmartThings for anything security related, researchers warn

by Dan Goodin - May 2, 2016 8:31pm CEST




Enlarge

Computer scientists have discovered vulnerabilities in Samsung's Smart Home automation system that allowed them to carry out a host of remote attacks, including digitally picking connected door locks from anywhere in the world.

The attack, one of several proof-of-concept exploits devised by researchers from the University of Michigan, worked against Samsung's SmartThings, one of the leading Internet of Things (IoT) platforms for connecting electronic locks, thermostats, ovens, and security systems in homes. The researchers said the attacks were made possible by two intrinsic design flaws in the SmartThings

HERE'S HOW EASY IT COULD BE FOR HACKERS TO CONTROL YOUR HOTEL ROOM



A view of the SL Regis Shenzhen hotel. © SL Regis

SHENZHEN IS THE Silicon Valley of mainland China. Situated about 50 minutes north of Hong Kong, the modern city is home to the Shenzhen Stock Exchange and numerous high-

SOLUCIÓN IDEAL VS REAL

- Sin conexión de ningún tipo



- Conectado en todo momento



CASO REAL

- Publicado en: wired.com

Caso real en hotel 5 estrellas

“... control of the thermostats, lights, TVs and window blinds in all of the hotel's 250-plus rooms, as well as alter the electronic "Do Not Disturb" lights outside each door...”



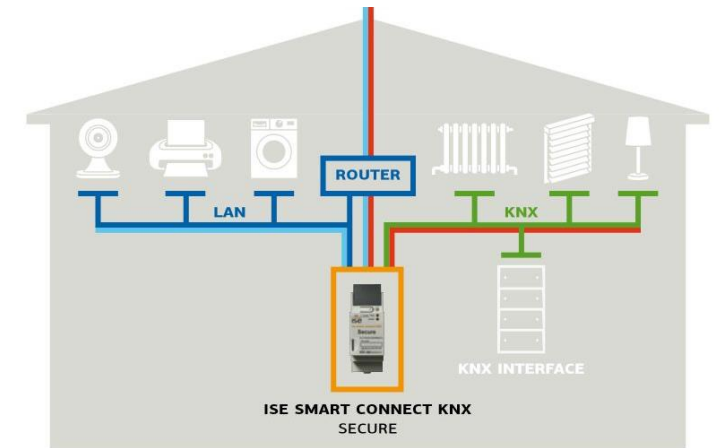
CASO 2

Caso típico de acceso a una instalación

“tras desmontar un producto de una instalación se puede llegar a controlar la misma, de forma cableada o WiFi”



¿CÓMO EVITAR ESTAS SITUACIONES?

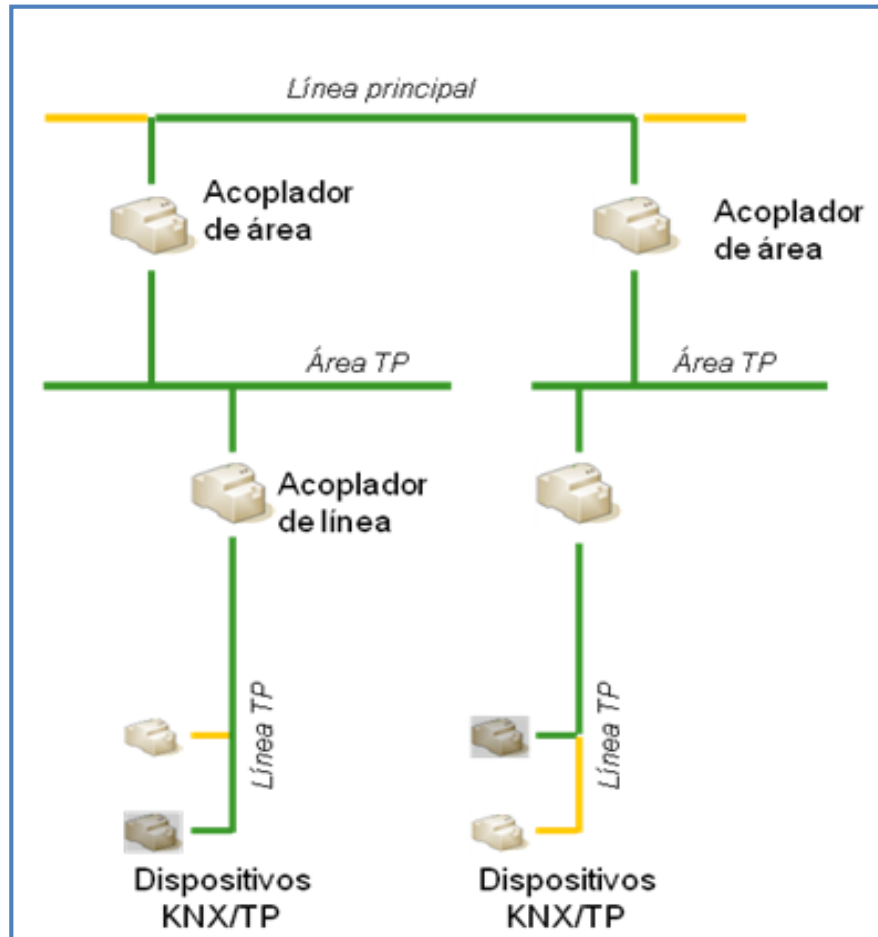


¿CÓMO EVITAR ESTAS SITUACIONES? (II)

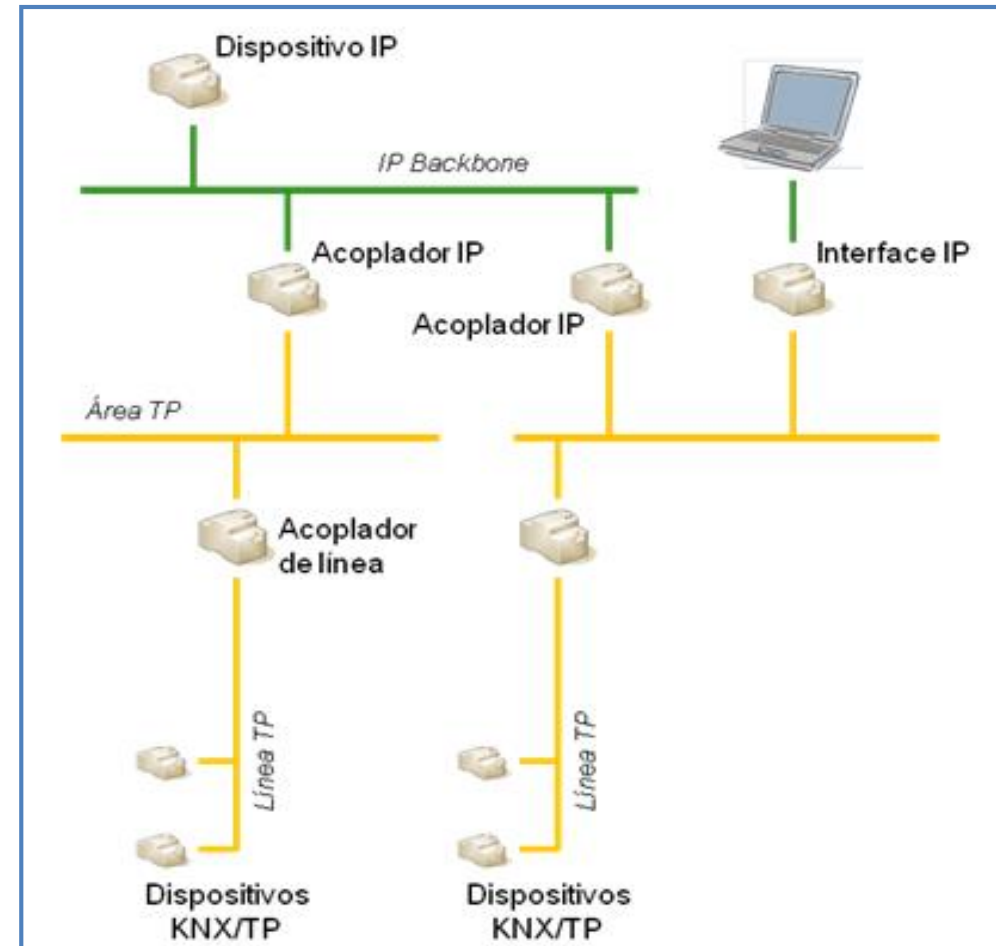
AES
encryption

¿CÓMO EVITAR ESTAS SITUACIONES? (III)

Instalaciones Aisladas



Instalaciones Conectadas



RECOMENDACIONES Y CONCLUSIÓN

Conozca bien los punto vulnerables de su sistema



La seguridad es un proceso



Use un estándar (EN 50090-4-3 conforme a ISO 18033-3)





IV CONGRESO EDIFICIOS INTELIGENTES

Madrid 19 Junio 2018

Casto Cañavate Fernández

Casto.canavate@knx.org

Móvil (BE) +32.487.523.216



Smart home and building solutions.
Global. Secure. Connected.

