Why hack a thermostat in a hotel?

Antago GmbH | Friedrichstraße 36 | D 64646 Heppenheim
Tel.: +49 . 6252 . 94262 . 0 | Fax: +49 . 6252 . 94262 . 1
E-Mail: sicherheit@antago.info | Web: http://www.antago.info
HRB 89141 | Geschäftsführerin: Frau Silke Thielmann

Sitz der Gesellschaft: Heppenheim | Registergericht: Darmstadt
Steuer-Nr.: 007 228 03 203 | Ust-IDNr.: DE 27 237 9849
Konto-Nr.: 0133 106 971 | BLZ: 508 526 51 | Sparkasse Dieburg
IBAN: DE07 5085 2651 0133 1069 71 | BIC: HELADEF1DIE

Why hack a thermostat in a hotel?

By M.Sc. Alexander Mohammed Dörsam, Head of Information Security/Partner, Antago GmbH

The Internet of Things (IoT) was ranked the second most important strategic technology trend of 2015 by IT research firm Gartner in their world-renowned annual list, after Computing Everywhere, and has been included in many other technology trend lists globally.

IoT is the network of physical objects or "things" that can collect and exchange data with each other and the Internet. Examples are all around us; from the parking sensors in the mall and the carts on the golf course, to almost everything in the car and the Apple watch. It is expected that 50 billion ''things" will be connected to the Internet by 2020, so it's big and here to stay. In the hospitality industry we see first adoptions of IoT, whilst hotels have for years achieved energy savings and managed their buildings by using building automation, lighting control systems and guest room management technologies.

One of the biggest risks and concerns in intelligent buildings and IoT is security, but the problem is that building automation typically doesn't sit within the classic domains of IT security. Why hack a thermostat? The core focus of hotel IT security teams revolves around payment security, guest data and networks in general.

This article illustrates the vulnerability of buildings, including hotels, that use products based on the KNX protocol, which is adopted by more than 400 manufacturers of building automation products globally. KNX is the association that administrates the KNX standard and that provides the backend software ETS, necessary to configure and control the KNX devices from a server. The KNX protocol originates back to the nineties and has ever since gained vast adoption beyond its original application in private homes.

The security flaw affects any KNX device, including light switches, thermostats and even door locks, in any environment where the technology is installed and physically accessible. Thevulnerability makes it possible to alter selected devices connected by KNX and to remotely control them. Can you imagine that someone could take control of a hotel's guest room management system and make all the lights in a hotel go on and off continuously or heat the rooms up to 35°C? A 100% check-out rate within hours is guaranteed.

Since its discovery, the issue has been widely debated on security conferences and specialized industry forums, but it's yet to be resolved. Not only does this vulnerability put thousands of existing buildings, such as hotels, hospitals and airports at risk globally, manufacturers and installers are still selling and installing KNX as if nothing happened.

At Antago we started working on this issue in 2013, but it was only a year later after a hack at a luxury hotel in China due to insecure WiFi, that the issue first received public attention. Since, this has evolved into a hardware hack and today, access to just one light switch or thermostat in any room or public area, is sufficient to gain control over an entire building.

It's surprising that despite all the information that is publicly available, including a security checklist and statement from the CEO of the KNX association, there is so little attention and no solution to this major vulnerability.

As clearly stated in the KNX security checklist, the only way to secure an installation is to ensure there is no physical access by an unauthorized party (anybody other than the hotel management for example) to any of the installed KNX products or cables. Whilst physical access to these devices can be prevented inside a private residential environment, this is by definition impossible to do in any public building such as a hotel.

Having contacted manufacturers that use the KNX protocol for years without success, I decided to raise awareness by reaching out to building automation vendors that don't use the KNX protocol and received a response from INTEREL, a specialist supplier of hotel guest room management systems. Subsequently, when talking to senior IT and engineering hotel executives, we were invited to do a live hack at a luxury hotelin the UAE that uses products based on the KNX protocol.

During the live hack, I demonstrated the weakness of the KNX protocol and the impact it can have on a hotel's operation in three easy steps and in just eight minutes:

1) Armed with a screwdriver and my KNX module with hack software, I checked into the hotel and entered the room

2) I unmounted the thermostat to gain access to the KNX bus cable, read out the KNX commands being transmitted without encryption (sniffing) and installed the hidden device behind the thermostat

3) I checked-out of the hotel and controlled that room as well as other selected rooms remotely (this could have been the entire hotel)

What was I able to do? I could remotely switch the lights of that room, or any other room in the hotel, on and off at random, make them blink, switch the AC on and off and change the temperature.

A senior global IT representative from the hotel chain where the live hack took place said: "We were shocked to see that the hotel's room management system could be hacked in just eight minutes. We are now undertaking a global inventory and audit of our KNX-based systems to understand what steps we have to take to resolve this issue."

Within days of the first hack we were invited by two other hotels in the UAE to demonstrate the vulnerability through a live hack, both of which were successful in just under eight minutes.

Whilst controlled hacks - such as the ones performed at the hotels designed to demonstrate the KNX vulnerability without damaging any systems - require a lot of professional knowledge and experience, regular hacks of this nature can be done by amateurs. The necessary know-how is in the public domain, the entry barriers are low and the hardware used for this hack can be purchased online at less than USD$8. Hacking is no longer exclusive to the professional hacking community and can bedone by amateurs as young as twelve years old, which is the average age of a hacker today.

What can we do to solve the issue? The solution is not to take the "smart" out of smart buildings, but to optimize the security of the systems used and to carefully consider security when selecting new technologies for the hotel. The Internet of Things is here to stay and buildings will become even smarter in the future, the key is to make them more secure as well.

Unfortunately, for the thousands of hotels that have installed KNX-based room management systems there is no proper solution other than to replace the technology with specialist hospitality systems that don't use the KNX protocol. This becomes even more critical for hotels that have their door lock systems connected by KNX as this is an immediate threat to guest safety.

My recommendation to hoteliers and the hospitality IT community is to review their guest room management systems and to make this a priority for 2016.