White Paper

Antago hacks Gira home and facility server

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 | Managin Director: Mrs. Silke Thielmann

Registered Office: Heppenheim | Register Court: Darmstadt
Tax no.: 007 228 03 203 | VAT ID no.: DE 27 237 9849
Acc no.: 0133 106 971 | Sort Code: 508 526 51 | Sparkasse Dieburg
IBAN: DE07 5085 2651 0133 1069 71 | BIC: HELADEF1DIE

Introduction

Since a couple of years and in the context of different research projects Antago GmbH has been dealing with the security of EIB/KNX based systems besides classical digital penetration.

In 2014, as a result of this research, „Erebos" (http://bit.ly/1jWDDu5) was introduced on various security exhibitions as the first professional appliance for attacks against building management systems. Many months of research and the cooperation with manufacturers of the section of EIB/KNX had been preceding. In addition and as the next „evolutionary step" „Thanatos" (http://bit.ly/1jWDlxV) was finally published. Both attacking tools require physical access to the building to be attacked. However, Antago succeeded in developing Thanatos to a component that small to be suitable behind previously installed light switches.

This very development enabled Alexander Dörsam, heads of Information Security Antago, to present results according to security in the section of EIB/KNX on international platforms; inter alia the VDS. Furthermore, a cooperation with VDS has started for developing standards for a "safe" EIB/KNX installation.

The vision

Despite the extending opportunities of Erebos and Thanatos a one-time physical access to the building to be attacked was required. As a consequence it would be necessary to perform the same attacks on light/climate and alarm systems via the Internet. The vision would be to access administratively thousands of building control systems via automatically working software.

One of the largest providers for Smart Buildings – linked via the Internet – is Gira. It was obvious to analyze their very product with regard to vulnerability. Such an attack was not been executed up to this point thus it was late-breaking and quite dangerous.

Tip:
The following parts of this statement will not deal with the very issues of KNX Bus. If there is any interest you can consult white papers on http://knx-security.de/. In fact, the following parts will be about the vulnerability of transferring from KNX to IP-based systems.

Function of the systems

If you are a customer of Gira or comparable producers of visualization solutions for building control systems you will be provided different concepts of remote access.

In case of home and facility servers you will be provided remote access via Gira by using an exposed web portal. There will be the opportunity to connect to the building with the help of a unique serial number or using an alias awarded by yourself. Besides the actual user this function is often used by commissioned installers to maintain the buildings.

Either you would use the alias or the unique serial number, there would be forwarding to the very building. Then your home or facility server would provide a website for your login.

Your server would sign on Gira in regular intervals to connect this connotation and to transmit your latest IP-address, whereby you will be able to log in to your server (by using your identification) and to operate by remote control.

Attack

It is important to ensure the identification of buildings as well as accessing to attack such systems.

Identification of buildings

It is essential for a comprehensive attack to identify multipliers that are accessible for many target systems. Gira provides the described web portal whereof you can reach all active home and facility servers. The IP-addresses of all the client systems are centrally filed in a database. There are various approaches to read out this certain database: We used the Brute-Force-Approach which is about guessing an alias or a serial number by just attempting. There, we found out that last names used as an alias would deliver fast results but in very low numbers. In conclusion, we tried to create valid serial numbers which succeeded in identifying valid prefix serial numbers. Therefor, we used a recall campaign (initiated by Gira) in which the affected customers were contacted on the basis of the serial number sections. Quickly, we found a pattern in the serial numbers usable to create a program generating those serial numbers.

In the context of this research we generated 16^4 serial numbers whereof we extracted 16^3 (thus 4096 serial numbers) as a representative amount. Due to some programming weaknesses in the implementation of the web portal we were able to verify the created serial numbers (automatically and in a huge amount) by Gira. About 1000 serial numbers out of the 4096 could be identified as valid serial numbers.

The next step of the attack was to connect the real connotation to the certain home and facility servers. Therefor, we expanded the software to request thousands of serial numbers including the particularly related IP-adresses within a few seconds via the web portal.

On the one hand the issue is the predictability of the serial numbers and on the other hand the plentiful inquiries of their validity and the actual associated IP-addresses.

As a conclusion of this part of the project we had a software able to generate a huge amount of serial numbers and delivering an overview of all active home and facility servers and their IP-addresses.

Penetration into the surface

After it had been possible to use a multiplier to identify a variety of "Smart Buildings". The next step would be to gain access to the previously identified home and facility servers. As a lab environment we used our own home server installations.

While examining it was eye-catching that the surfaces did not have any type of encription. This would only be an important help if we attacked the building's users. We were aware of this scenario and those were excluded from testing.

Again we would use the Brute-Force-Approach as the obvious tool for penetration and developed a software implementing different ways of Brute-Force-Approach against our home server. During this process we profited by common dictionaries which we tested against the servers. There were hardly any barriers.

At the end of this part of the project we had a software that ensures an administrative remote access to home and facility servers (accessible via Internet). The software generates a screen shot of the invoked surface as a documentation for the access.

Summary

At the end of this research project both software components were transferred into one program. It is obvious that (besides all previous issues of KNX-Bus) additionally IT-typical weak points are detectable in those buildings. Certain issues of web-applications show up. It is possible to identify thousands of active buildings within a few minutes by means of our developed software, to attack automatically and variously and to build the base for comprehensive attacks from afar. Afterwards we luckily had the opportunity -upon approval by the end customer- of testing our software against real

installations. After all, the rate of success was huge. We reduced this result on the fact that normally, installers or end customers are using very simple passwords or that one which is given in the instructions by Gira and never changed.

The practicability of comprehensive attacks and the remote control of tens of thousands of "Smart Buildings" was proved by Antago GmbH.

There are various attack scenarios with extensive consequences, such as

- switching off and blocking buildings
- switching off the heating systems during winter time
- deactivating alarm systems and
- manipulation of locking systems

The attack described above was executed at Gira but it cannot be excluded that other producers do have comparable weak points. The consequences would not be imaginable if the software was exerted on others than our volunteering test customers. (You can find more details of KNX attacks in our white papers.)

We informed Gira about the weaknesses and the obvious approaches by telephone as well as in written form on June, 23rd 2015. Moreover, we conducted a free workshop in the Gira head quarter.

Perspective

The focus of the described attack was to make possible comprehensive access to building control systems. We proved that case undoubtedly.

As a forecast it would be imaginable uniting the capability of Erebos with our software. Then we would be able to expand the KNX attacks, initiated by Erebos, into hundreds of thousands of buildings. We have already built prototypes, based on a generic protocol, allowing Erebos to remote control the corresponding buildings from a distance.

Some time ago, we published attacks, done by Erebos and iPad on our youtube channel (https://www.youtube.com/user/AntagoVideoChannel) which are workable for thousands of buildings at the same time.

Author:
M.Sc. Alexander Mohammed Dörsam,
Head of Information Security / Partner, Antago GmbH
More information and contact: Antago GmbH, sicherheit@antago.info,
https://www.antago.info