AVAR 2014 Paper: "The Internet of Things – Or – Security: The Forgotten Feature"

Andreas Marx, CEO, AV-TEST GmbH

Address: Klewitzstr. 7, 39112 Magdeburg, Germany

Phone: +49 391 6075460, E-Mail: amarx@av-test.de

About the Author

Andreas Marx has a diploma degree in Business Informatics. He is the CEO of AV-TEST GmbH and represents the company in dealings with institutions and customers. The AV-TEST Institute is home to more than 30 specialists which all strive to achieve a common goal, namely: to establish progressive data and to quickly react to the needs of all target groups and support them with highly relevant IT security analyses.

Abstract

Criminals are exploring the next possibilities to spread their malware on and to broaden their criminal business model. This is where The Internet of Things comes into play. Criminals are aware of the potential of these devices. Anything that adds comfort and is easy to use will be loved by the user, forgetting about security concerns. Smart Home kits have the potential to be one of the ice breakers and may bring the Internet of Things, and the associated security problems, into millions of households.

AV-TEST examined several different Smart Home Kits to show their problems and vulnerabilities. We will explain where these kits fail to implement security and what that means for the home user and which criminal business models may follow out of that. In addition we will propose options to increase the security of these devices and discuss opportunities for vendors of AV soft- and hardware to lend a hand to the user.

Introduction

A lot of things in the Internet world are built with functionality, but not with security in mind. Just think about the e-mail concept and the missing (basic) authentication which allows spammers to send billions of junk e-mail around the globe -- every day! Such fundamental 'let's trust everyone' principles might have worked some decades ago, but everyone should know better today. Anyway, still security is not a feature someone can sell, just functionality is. And everything should be as easy as possible to use.

AV-TEST recently reviewed various Smart Home Starter Kits and more than half of the products failed in basic security testing [1]. This includes, but is no limited to, missing encrypted communication (e.g. using https instead of http for passwords and control messages), missing authentication (e.g. everyone in the same network has full access), the possibility of manipulation of all data by external parties (e.g. control commands, firmware updates) and the like. The firmware update files, for example, are checked against a set of supplied MD5 or SHA1 hashes before they are applied, but an attacker can easily create a new hash for the modified version and that's everything required -- no digital signatures are used.

Looking at the actual packets transferred and protocols used, it was simple to reverse-engineer the required commands to activate or deactivate a specific device. While some products encrypts the data, the key is usually supplied at the same time. A few products are using Linux as operating system, but the Kernel version used dates back to the year 2006. If encryption libraries are actually used, the selected cyphers are not recommend to use anymore. Besides this, the systems were not patched for many months after the Heartbleed bug [2] was discovered, or the firmware updates had to be installed manually on a usually very complex and challenging way.

Last but not least, some products have (hidden) backdoor accounts with full administrator privileges. This leaves the door wide open - for everyone!

Further Research

Alex Chapman presented further research regarding light bulbs in July 2014 [3]. While actually a strong encryption algorithm - AES - was used, the implementation was flawed and the used credentials could be extracted in no time. While a fix was later released by the vendor, it leaves some strange feelings regarding the requirement of firmware updates on light bulbs.

Just a bit later, Karsten Nohl and Jakob Lell presented their findings about USB security at Black Hat [2]. Due to unprotected firmware updates, the USB devices (and especially USB keys) can infect systems in a very hard-to-detect way [3]. The author of this AVAR 2014 paper also made some own discoveries, for example, the firmware update for Western Digital drives can be applied on any Windows system, even without requiring Windows Administrator privileges [6].

Finally, in August 2014, David Jacoby published an article about how he hacked his home [7]. The detailed analysis includes attacks for network-attached storage systems (NAS), his Smart TV, satellite receiver, an Internet router from his ISP as well as his printer. At home, I also had an interesting experience with my own Yamaha AV receiver which offers a full remote management via an iPhone app. Unfortunately, there is absolutely no authentication, so everyone with this app on his smartphone and who is in the same wireless network has full access to the system. In the easiest case, one can turn on or off the device, but an attacker can also try to play his favorite tunes on the maximum possible volume.

Some products - like many NAS systems - are automatically downloading the latest firmware once you're about to setup the box. This is good news, however, 'latest' doesn't necessarily mean the 'latest available' version. For example, at the time of writing this paper, the Synology NAS systems are updating itself to version 5.0-4493 (released on 4th June 2014), but the very latest version is indeed 5.0-4493 Update 5 (released 10th September 2014) [8]. In 'Update 5' security patches to prevent attacks by the 'SynoLocker' ransomware were included [9], what can make a big difference to the user. While the system is regularly checking for new updates, the firmware still needs to be applied manually, which includes a reboot of the device to get everything running.

With the possibility to hack products, you can also bring additional functionality to them, so formerly unavailable features can now be used. For example, the SamyGO project [10] for Samsung Smart TVs allows to use an alternative firmware or enable 'hidden' features like TV recording, thanks to a vulnerability in older versions of the software and the Skype application. Besides this, old hardware can be recycled and get a new life. The 'XBOX Media Center' (XBMC, now called Kodi) [11] is a good example.

During the IFA 2014 fair in Berlin, Germany [12], many new 'smart' devices by companies from all over the world were presented in September 2014. However, some features were a bit surprising.

For example, the latest Ultra-High Definition TVs by Samsung are now much more secure, I was told, because of a new build-in function called 'Smart Security'. Actually, this is a virus scanner. On a Smart TV! Definition updates are to be released regularly as part of the firmware updates. OK, but I was not feeling better due to this feature, but I found it quite scary...

The future?

For many years, technicians focused too much on 'easy-of-use' and 'functionality', most likely driven by their product management teams. Security hasn't played a big role yet. However, nobody would buy a car today without safety belts and airbags. If the industry cannot focus more on security, one needs to keep in mind that this might sooner or later start government activities which may lead in regulations.

The current products are really nice to use, they offer a lot of functionality, but at the end, they can be hacked too easily and finally misused. Right now, people might question 'why should someone hack my smart home', but the same question was previously asked already: 'why should someone hack my PC, I have no important data on it' or 'why should someone hack my phone'?

While the potential 'black hat' business models might not be lucrative or practical enough (e.g. espionage, extortion), such people will always find a way to make money. Usually a lot of money. Many years ago, it has started with spam, and today, hijacked devices can also be misused for Botcoin mining [13]. Therefore, we need to be very careful here!

If you develop products, please ensure to use protocols like https instead of http (obfuscation usually won't work!), do not create any backdoor accounts (not even for testing, as they might be forgotten in the code), use well-known secure encryptions algorithms in the right way, and make firmware updates as easy as possible to perform. However, don't forget to carefully check such updates before installing them on your device!

Besides this, 3rd party penetration tests are strongly recommend -- you'll be surprised what others can do with your soft- and hardware! :-)

References

[1] Michael Schiefer, Ulf Lösche, Maik Morgenstern. Test: Smart Home Kits Leave the Door Wide Open – for Everyone. Summary: http://www.av-test.org/en/news/news-single-view/test-smart-home-kits-leave-the-door-wide-open-for-everyone/ Full paper: http://www.av-test.org/fileadmin/pdf/avtest_2014-04_smart_home_deutsch.pdf

[2] The Heartbleed Bug. http://heartbleed.com/

[3] Alex Chapman. Hacking into Internet Connected Light Bulbs. http://contextis.com/resources/blog/hacking-internet-connected-light-bulbs/

[4] Karsten Nohl & Jakob Lell. BadUSB - On Accessories that Turn Evil.

https://www.blackhat.com/us-14/briefings.html#badusb-on-accessories-that-turn-evil

[5] Andy Greenberg. Why the Security of USB Is Fundamentally Broken

http://www.wired.com/2014/07/usb-security/

[6] My Passport Ultra firmware update for Windows users. http://www.wdc.com/wdproducts/wdsmartwareupdate/firmware.asp?id=wdfMP_Ultra&os=WIN

[7] David Jacoby. How I hacked my home. http://securelist.com/analysis/publications/66207/iot-how-i-hacked-my-home/

[8] Synology DS211j Release Notes. https://www.synology.com/en-global/releaseNote/DS211j

[9] Synology Continues to Encourage Users to Update. https://www.synology.com/en-us/company/news/article/470

[10] SamyGo. http://www.samygo.tv/

[11] Kodi (software). http://en.wikipedia.org/wiki/Kodi_(software)

[12] IFA 2014, Messe Berlin. http://b2b.ifa-berlin.com/

[13] Botcoin: Bitcoin Mining by Botnet. http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/