

---




**AVAR**  
**SYDNEY 2014**  
NOVEMBER 12-14

---

ORGANIZED BY



ENJOY SAFER  
TECHNOLOGY™



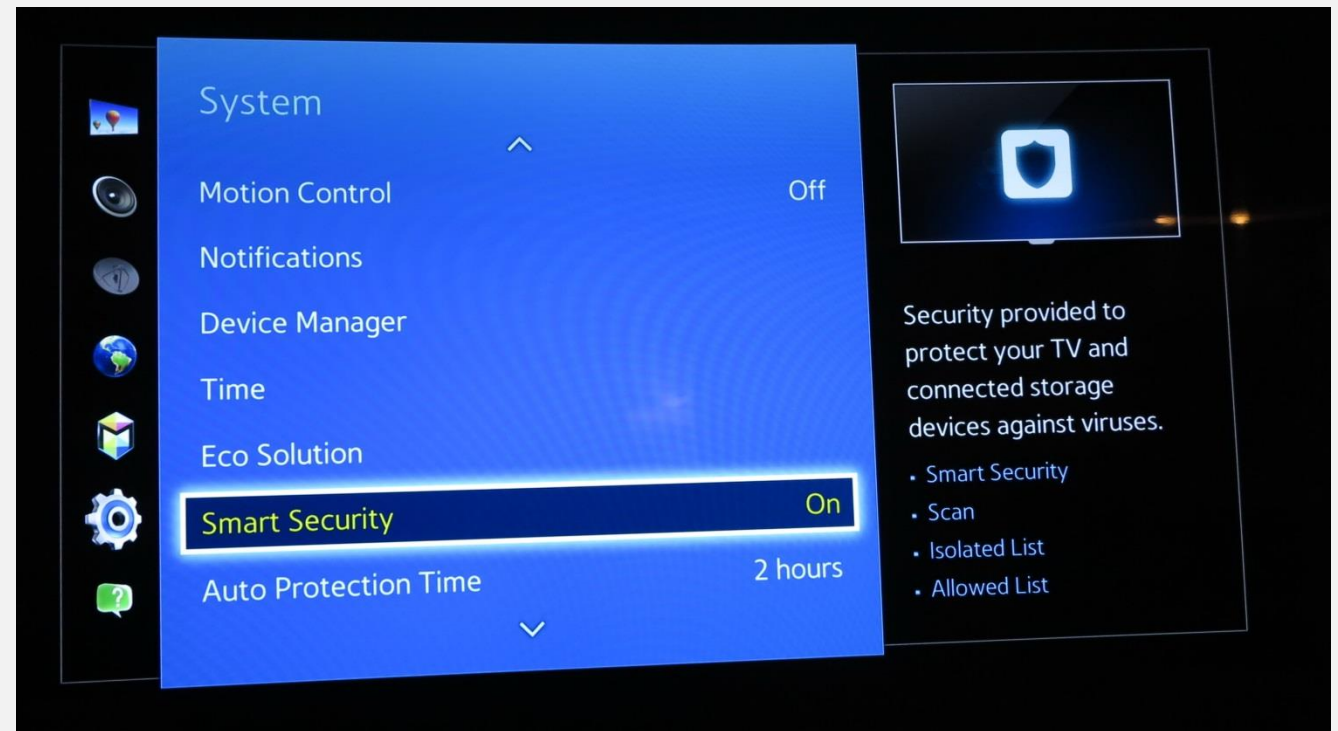
# The Internet of Things – OR – Security: The Forgotten Feature

Andreas Marx  
CEO, AV-TEST GmbH

# Smart Security - a virus scanner on my Samsung TV

[VIDEO]

Is this necessary...  
... or just scary?



# Introduction

- You can sell functionality, but not security
- Everything should be as easy as possible to use
- 'Let's trust everyone' won't work anymore!
- Think about e-mails and the missing basic authentication: Spam!
  - These design mistakes have been made many year ago, but we're still suffering today... every day.

# AV-TEST reviewed Smart Home Starter Kits (I)

- Research by Michael Schiefer, Ulf Lösche & Maik Morgenstern
- Missing encrypted communication (e.g. https instead of http for passwords and control messages)
- Missing authentication (e.g. everyone in the same network has full access)
- Possibility of manipulation by external parties (e.g. control commands, firmware updates)
- Unprotected firmware updates (only MD5 or SHA1 check, but no digital signatures)

# AV-TEST reviewed Smart Home Starter Kits (II)

- Network traffic inspection: it was simple to reverse-engineer the required commands to control the device
  - Some products encrypts the data, but the key is supplied at the same time
  - Outdated Linux kernel versions (not months, but several years: e.g. 2006!)
  - If encryption is used, the selected cyphers are not recommend to use anymore
  - No 'Heartbleed' patch included (not to speak about 'Poodle' at all)
  - Challenging firmware updates (manual installation on a very complex way)
  - Hidden backdoor accounts with full administrator privileges
- **This leaves the door wide open - for everyone!**

# Further Research (2014, Part I)

## **Alex Chapman: vulnerable light bulbs**

- While AES was used as encryption algorithm, the implementation was flawed and the used credentials could be extracted in no time
- Firmware update was released later... for light bulbs!

## **Karsten Nohl and Jakob Lell: USB security**

- Due to unprotected firmware updates, USB keys can be used to infect systems in a very hard-to-detect way
- No software vulnerabilities needed (e.g. unlike Stuxnet)

## **Another example (identified by myself)**

- The firmware updates for Western Digital drives can be applied on any Windows system, even without requiring Windows Administrator privileges



# Further Research (2014, Part II)

## David Jacoby: "How I hacked my home"

- Network-attached storage systems (NAS), Smart TV, satellite receiver, an Internet router from an ISP and a printer.

## Michael Jordon: "Hacking Canon Pixma Printers - Doomed Encryption"

- Unprotected firmware updates: how to play Doom on a Canon printer

## And well, I also have found one more issue:

- Yamaha AV receiver: the iPhone App works in any wireless network, not necessarily my own one
- 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



# Summary (I)

- Likely driven by product management teams, technicians had to focus too much on 'easy-of-use' and 'functionality'
- Security was (and is) not a selling argument and hasn't played a big role
- **BUT:** Would you buy a car today without safety belts and airbags?
- If the industry itself cannot focus more on security, this might sooner or later start government activities which may lead in regulations
  - Who is faster? And what's more painful?

## Summary (II)

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 e.g. be misused for Bitcoin mining. Therefore, we need to be very careful here!

# An Open Letter

Dear product developers and managers,

- Please ensure to use protocols like https instead of http in the right way (obfuscation usually won't work!)
- Do not create any backdoor accounts (not even for testing, as they might be forgotten in the code)
- Use known secure encryptions algorithms and implement them correctly
- Make firmware updates as easy as possible to perform and don't forget to carefully check such updates before installing them on your device!
- 3rd party penetration tests are recommend: you'll be surprised what others can do with your soft- and hardware! :-)



Thank You