



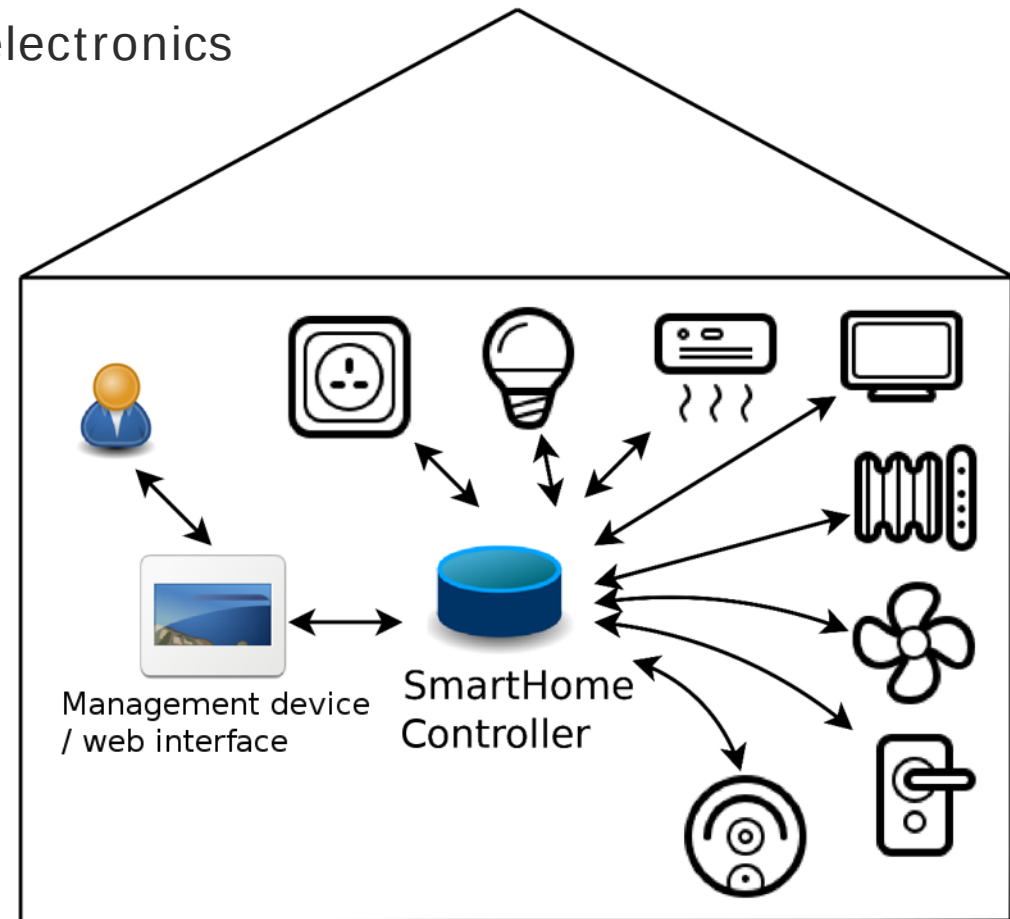
openHPI – Internet Security Privacy: Smart Home and Smart Meters

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Smart Home

Smart Home - Management of a networked house technology by means of controllers

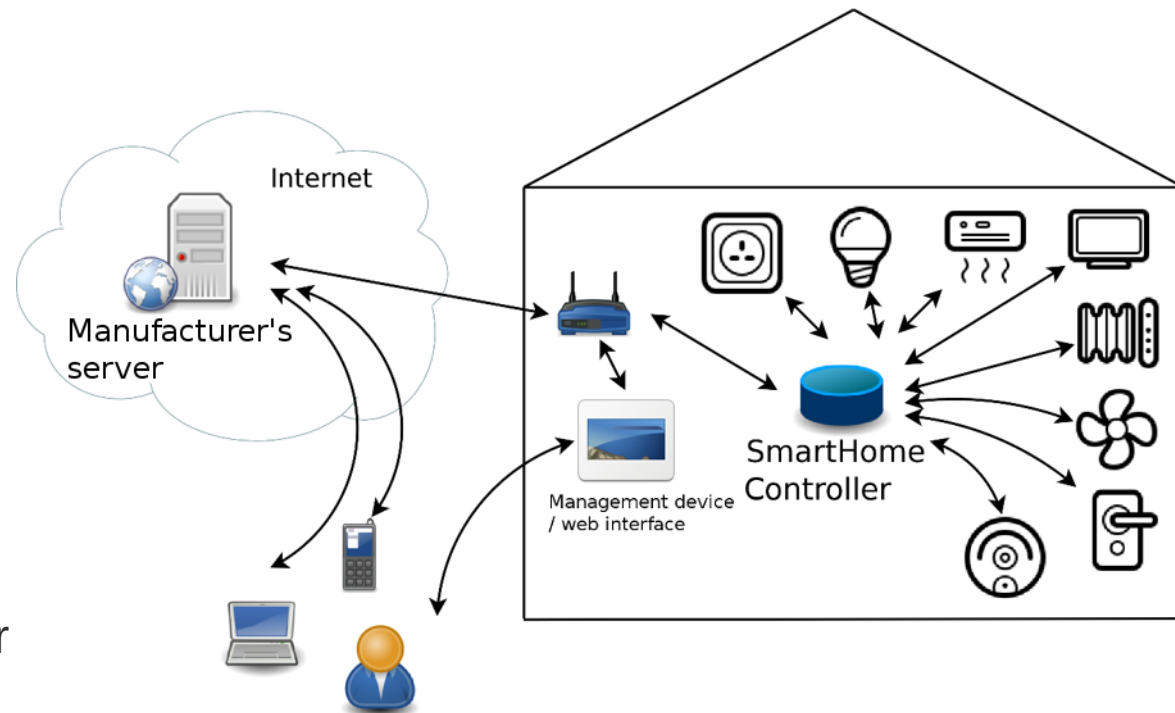
- Lighting and entertainment electronics
- Heating and air conditioning
- Windows and doors
- Alarm system
- Blinds
- ...



Smart Home and Cloud

Modern smart home solutions use cloud technology to facilitate the management of home technology for users

- Controllers of the Smart Home systems are always connected to the manufacturer's server via the Internet
- The user can manage the Smart Home system from any location using the Internet and the server



Smart Home, Privacy and Security

Of course, the manufacturer has access to the user data and can edit it

- SmartHome controllers can also have vulnerabilities, e.g. MiCasaVerde VeraLite
 - CVE-2013-4861: An attacker can read **any data** from the file system (including hashed passwords)
 - CVE-2013-4862: Guest users can **change firmware** and **download all settings**
 - CVE-2013-4863: No authentication is required to run **arbitrary malicious code** from the LAN as an **administrator**
 - CVE-2013-4865 (Cross-Site Request Forgery)
 - the manufacturer has not published any patches for the device (Source: Trustwave SpiderLabs)

- Software is based on obsolete OpenWRT 10.03 operating system
 - all vulnerabilities in OpenWRT 10.03, as well as vulnerabilities of various components and libraries of the Linux system (such as OpenSSL) are also relevant for VeraLite
- VeraLite is accessible through the manufacturer's server (remote maintenance) → another potential gateway for attacks
- The secret key for remote maintenance (via SSH) is the same for all devices (!!!) and stored on the device
 - having knowledge of a valid device ID (may also be guessed - for example, the attacker's number +1), attackers can gain full access to the Smart Home controller

Smart TV

Not only Smart Home controllers, but also other "smart" devices have problems with privacy and security

■ Samsung Smart TV

- listens to all conversation (and other noises) in the room, if voice control is activated
- spoken words are "transmitted to third-party"

■ LG TV

- sends various user data to the manufacturer in order to show Smart Ads (targeted advertising)
- information is also transmitted when the corresponding setting is disabled (!)
- transmitted data: TV channels watched, file lists of connected USB sticks and hard disks, search requests, ...

Smart Meters

Smart meters are consumption meters with a network connection for electricity, gas and water

- Analogue consumption meters are read 1-2 times a year
- Smart meters are constantly connected with energy suppliers and transmit measured data
- Supplier recognizes energy supplies in a timely manner and can optimize tariffs (electricity at night is cheaper, ...)
- They also ease counting procedures, forecasts, invoicing, ...
- Typically, tariffs open up "consumer saving opportunities"



EVb Energie AG, via Wikimedia Commons

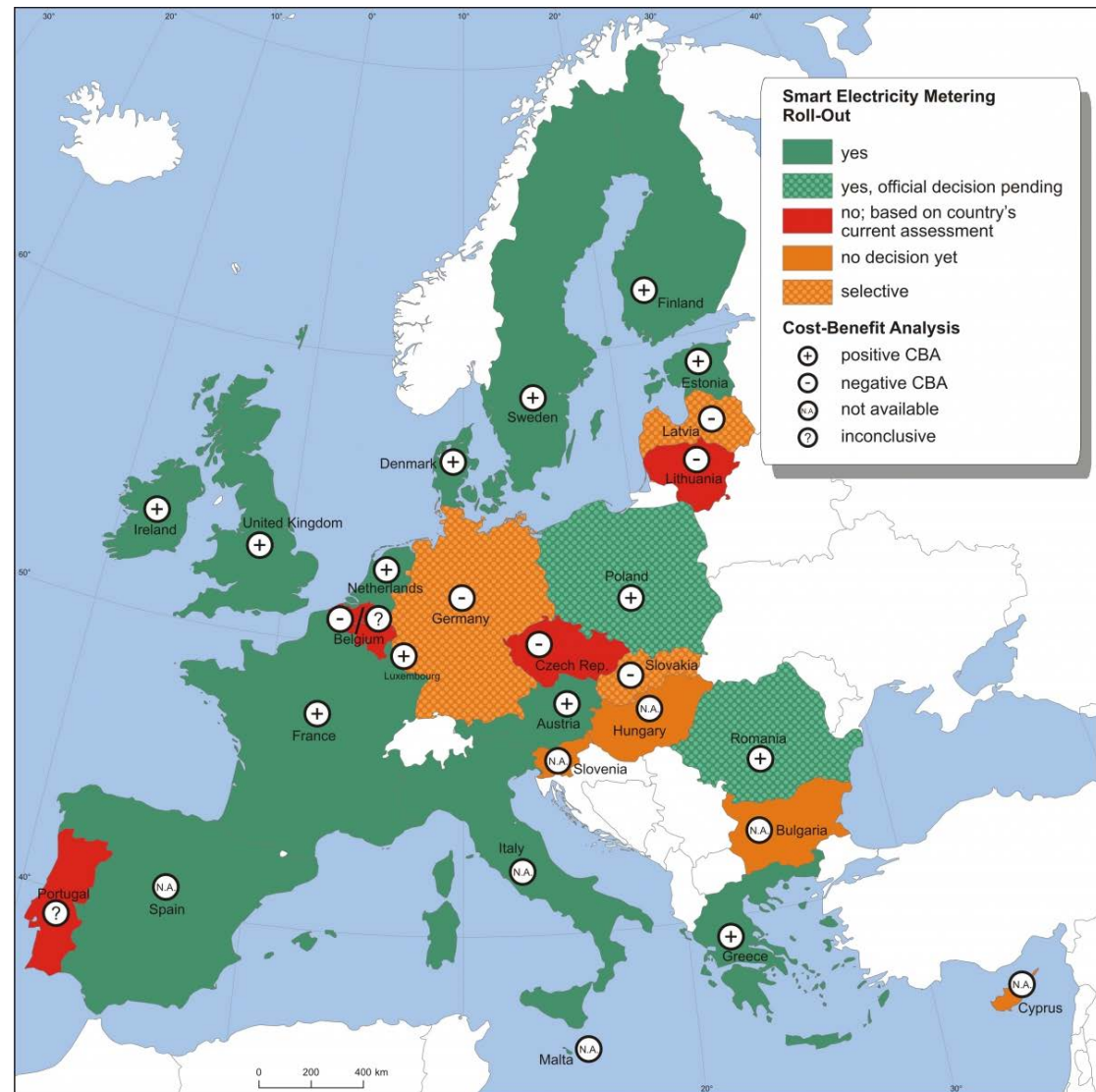
Smart Meters: Privacy and Remote Cut-Off

- Detailed information on energy usage in a household says a lot about residents
 - sleeping hours
 - washing times
 - how many people are at home at any given time
 - cooking times
 - ...
- Police in Texas (USA) use electricity data to detect marijuana plantations
- In Australia, such data was passed on to debt collection companies
- Smart Meters also enable the energy provider to shut down the power supply remotely

Roll-Out of Smart Meters in Europe

European Commission:

- “To date, Member States have committed to rolling out close to **200 million** smart meters for electricity and **45 million** for gas by 2020”
- “By 2020, it is expected that almost **72 % of European consumers** will have a smart meter for electricity while 40% will have one for gas.”



© European Union, 1995-2017