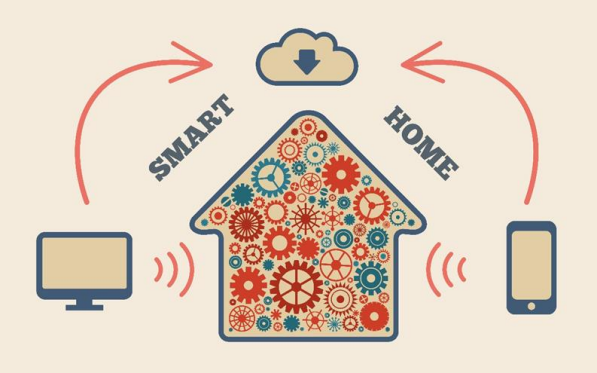
ENISA Thematic Landscape on Smart Homes

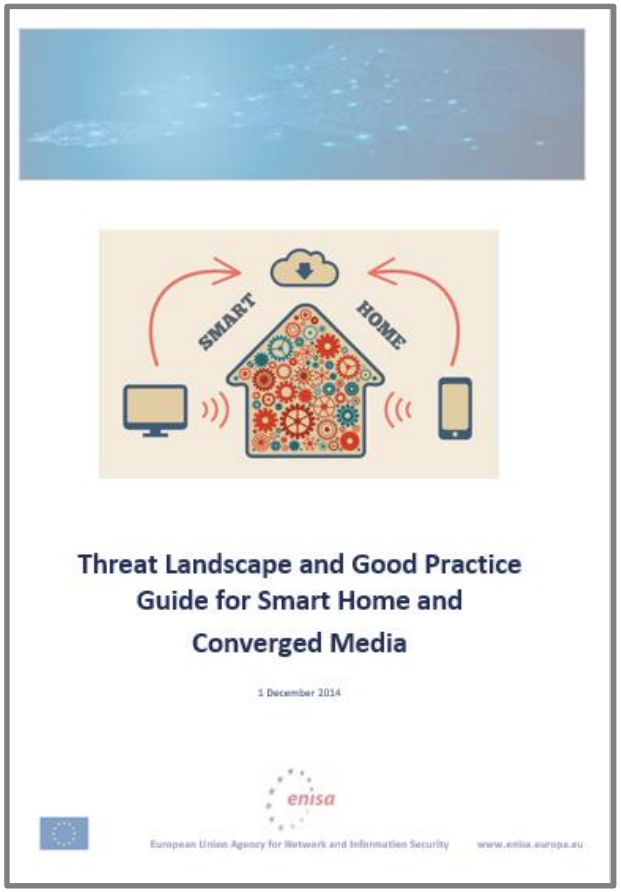


Dr. Silvia Portesi

NIS - Research and Analysis Expert

ENISA

Authors of the study and acknowledgements



Authors

- David Barnard-Wills (Trilateral Research & Consulting)
- Louis Marinos (ENISA)
- Silvia Portesi (ENISA)

Acknowledgements

- Colleagues
- Informal expert group

Agenda

- Introduction
- Scope and goal of the report
- Methodology
- Identified valuable assets
- Identified threats
- Identified vulnerabilities and risks
- Existing good practices
- Next steps
- Conclusions

Introduction

- Smart home and home automation
  - Remote control and users' preferences
  - Increase of home automation over the years
  - More affordability of smart home devices

- Policy context
  - EU Cyber Security Strategy
  - ENISA Regulation
  - COM Recommendation on energy efficiency

Scope and goal of the report

- Focuses on (cyber-) threats related to smart home with particular focus on converged media and television
- Deepens the annual ENISA Threat Landscape
- Follows similar approach of other ENISA thematic threat landscapes
- Aims to identify security challenges, associated risks and required countermeasures

Methodology

- Documentary sources – publicly available information
  - 166 documents processed
  - Documents in several languages
  - Search engines for academic sources and journal articles also used

- Interview and group discussion with the expert group
  - Five experts from academia and industry sector
  - Semi-structured interviews to gather experts' knowledge

Identified valuable assets

- Asset groups identified
  - Within each asset group, specific assets identified
- Example:

Sensors

Audio/Visual

Home Appliances

People/Living

Identified threats

- Threats' groups identified
  - Within each threat group, threats identified
- Example:

Unintentional damage (accidental)

Outage

Eavesdropping / Interception / Hijacking

Identified vulnerabilities and risks

- Vulnerabilities arising from
  - Business models and economic incentives
  - Ownership and administration models
  - Home being smart (pervasive and persistent insecurity)
- Risks
  - Crime
  - Privacy, surveillance and data protection

Existing good practices

- Smart home and converged media design and architecture choices
  - Careful consider security of cloud-based smart home design
  - Keep critical software separate from non-critical apps
  - Choose systems that allow secure communication
- Device security measures
  - Design with security in mind
  - No fixed, default passwords
- Network and communications security measures
  - Secure local video streaming
  - Secure 3rd party service connections
- Policy measures, including standardisation
  - Certifications for individuals and companies installing home networks
  - CENELEC SmartHouse Roadmap project

Next steps

- Taking this threat landscape as a reference and follow-up on cyber security measures
  - Good practices and recommendations for smart homes

- Security of exchange with other smart infrastructures

Smart Grid: energy optimization

Smart Cities: information hub and data provider

Smart Health: monitor health and improve quality of life

Conclusions (1/3)

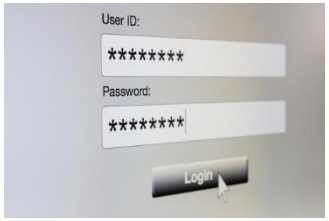
- Not all smart homes created equally
  - Traditional home automation / Interoperability protocols (smart TV as hub is a sub-set of this) / Isolated smart gadgets
  - These routes have their own peculiarities but also shared issues and vulnerabilities
  - Design choices here likely to have significant impacts upon both individual security and collective security in the ecosystem

- Threats identified to all asset groups
  - All groups of threats found some application across the asset groups and all asset groups had threats identified to them

Conclusions (2/3)

- Economic factors generates vulnerabilities
  - Start-ups, small electronics companies, kickstarters, and large scale appliance and utility companies
    - Lack security expertise
    - Lack security budget
    - Lack security research networks
  - “Smart” as add on to core function, security and privacy a distant afterthought
  - Market doesn’t seem to tolerate “smart” costing too much more than “non-smart”

- Applying “basic” information security could have big impacts

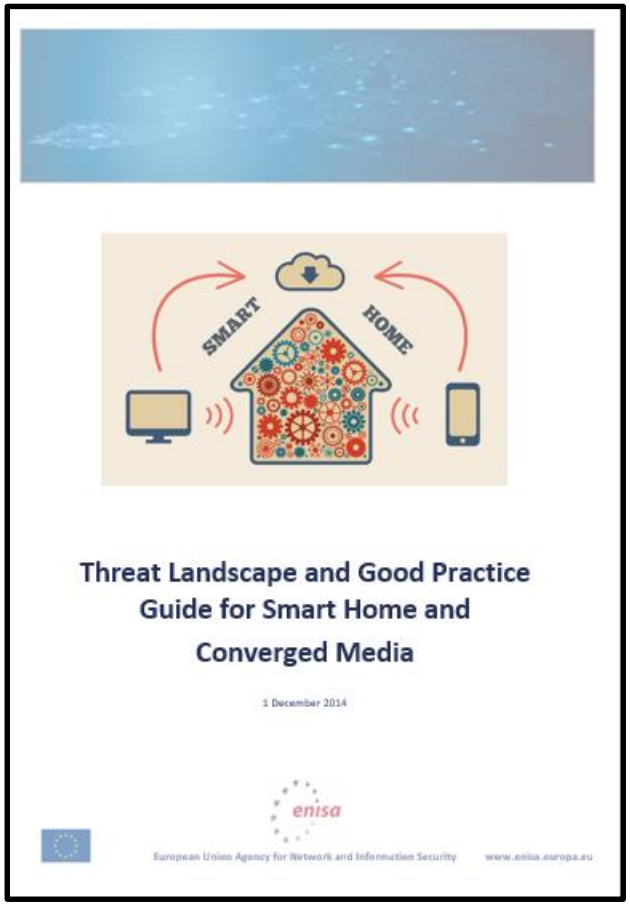


Conclusions (3/3)

- Interests of different assets owners in the smart home are not necessarily aligned
- Some research and experience from parallel more established or linked industries (e.g. cable/satellite TV, hotels, Wi-Fi) but still need for further research, e.g. in the following areas:
  - Role of smart home in emergency response
  - Impact upon smart home of natural disasters
  - Criminology of smart home
  - Liability and insurance issues related to smart home

- Smart home will be significant for privacy
  - Set of sensors in a smart home will be a source of close, granular and intimate data on inhabitants and visitors
  - Data has commercial, law enforcement value

https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-for-smart-home-and-media-convergence/



For more information, please contact:
resilience@enisa.europa.eu

Thank you for your attention

Follow ENISA: