Securing the Lifecycle of Smart Home Environments

Dr. Cédric Lévy-Bencheton | NIS Expert

Validation Workshop | Berlin| 6 October 2015

Summary

1 Definition of the context

2 Methodology of the study

3 Results of the study

4 Challenges and next steps

Definition of the context

What is a Smart Home?

Connected devices

- Data acquisition and processing
- Actions on the environment

Connected users

- Interface for command & control
- Adaption to the environment

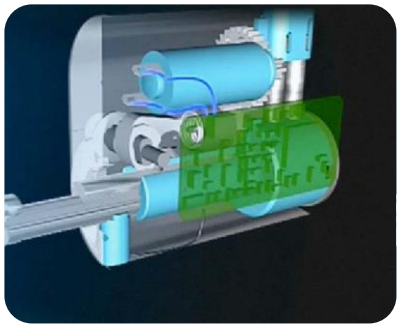
Towards an automation of the home
for an improved quality of life (comfort, energy reduction…)

ENISA Threat Landscape for Smart Homes

TV recording all conversations

No device is fully secured

- Dependency to external services
- Design of IoT/connected devices
- Vulnerabilities of protocols



Hacking Smart Locks to open doors

Non-technical threats

- Cost reduction during design/manufacturing
- Economical model (*e.g.* selling private data…)
- Potential risks on health and safety

By design, a Smart Home is prone to several threats

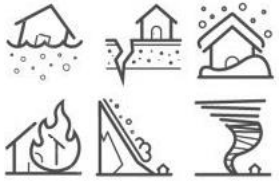
Real physical threats

Impact on life, health and safety

- Failure or attack on devices?

Criminal usage of IoT and Smart Homes

- “Virtual” crime
- Physical crime difficult to prove (e.g. robbery with no proof)



Continuity of service in case of a disaster

- Impact on the Smart Home environment?

Usage in case of emergency?

- How could IoT devices help first aid / emergency services?

A lack of legal framework defining liabilities in Smart Homes

A questionable approach of security

Technical

- Choice and implementation of protocols

Economical

- Low incentive to integrate security
- Long term support of devices vs rapid evolution

Cultural

- Functionalities before security (product before end-user)
- Lack of collaboration industry/research. On the contrary, several lawsuits were initiated against security researchers.

No major attack to this day

⇨ Limited integration of security in the lifecycle of IoT

Methodology of the study

ENISA's work to secure Smart Homes

Secure the lifecycle of IoT devices and services

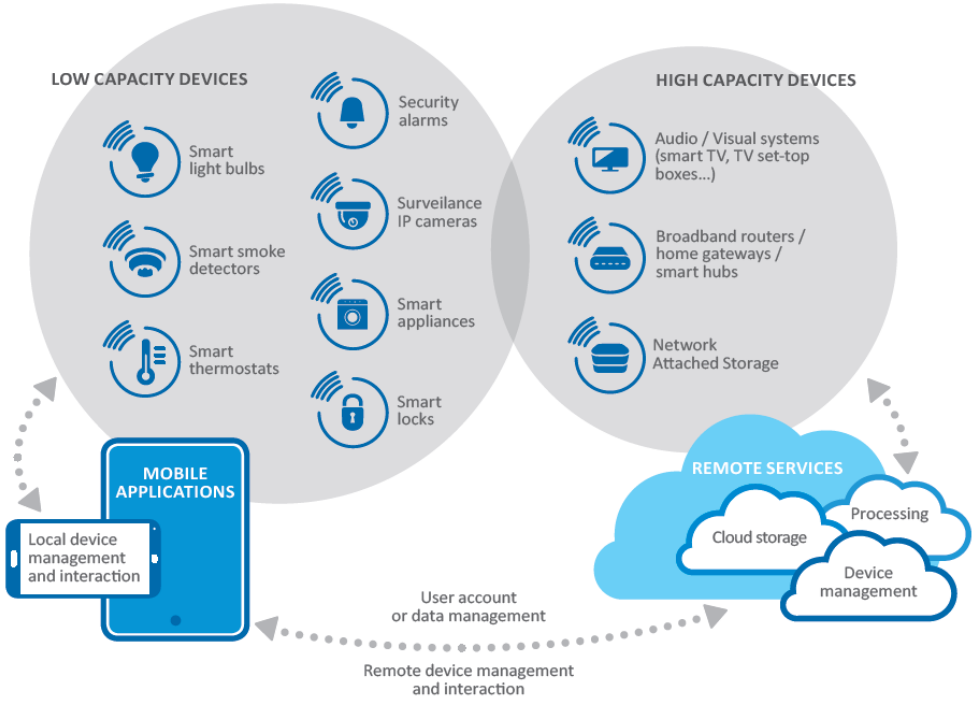
- Raise awareness
- Promote good security practices
- Propose recommendations to stakeholders

Target audience

- Manufacturers and third-party developers
- Service and solution providers
- Electronic communications providers
- Other stakeholders may find interest in the study

ENISA work shall enhance cyber security in IoT devices
⇨ Limit risks on life, health and safety

Scope and target audience



Devices

- Constrained devices [RFC 7228]
- High-capacity devices

Data exchange with

- Mobile applications
- Remote services

[RFC 7228] https://tools.ietf.org/html/rfc7228

Project Methodology

Desktop research

- Public sources + ENISA threat landscape for smart home (2014)
- Objective: update important threats, collect good practices

Survey and interviews

- Vendors, developers, researchers…
- Objective: validate good practices and understand gaps

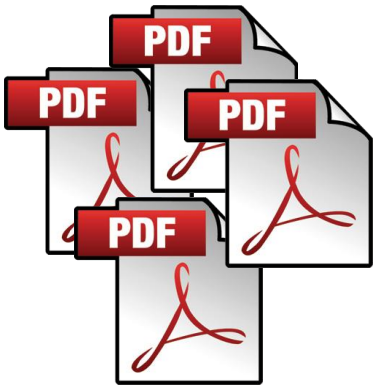
Analysis

- List of good practices
- Findings and Recommendations

Validation workshop – Today

- Review of the draft report by experts
- Objective: validate the study before publication

Desktop research



Update threats and collect security measures

- Over 100 sources analysed: threat analyses, white papers, technical documentation…
- Analysis, aggregation and correlation of results

References for IoT and Smart Home

- Security level is generally low
- No real solution, only recommendations

References for security solutions

- Usually very specific solutions (specific product, protocol…)
- Applicability of security measures from other domains?

Survey and interviews

Online survey

- Not very fruitful (6 answers)
- All respondents involved in IoT (5/6 in Smart Home)
- Mostly big companies: 250+ people (4/6)
- Survey too specific or security not a domain of interest?

Phone interviews

- Good participation (12 answers)
- Several types and size of stakeholders
- Highlight on existing good practices
- Understand the needs of the sector

How to define Good practices?

Good practices = security measures

- Technical or non-technical
- Applicable to the lifecycle of devices and services
- Evaluation throughout the project
- Objective: define what to do and when to do it

Difference between good practices that

- Are applicable ⇨ desktop research
- Are already applied ⇨ survey and interviews
- Should be applied ⇨ recommendations

Presentation of good practices

Categorisation of good practices

- Inspired by Common Criteria
- Objective: facilitate understanding

Applicability defined for

- Remote services (e.g. Cloud)
- High-capacity devices only
- Class 0 (~10 KiB RAM), Class 1 (~100 KiB storage) or higher
- Any device

Example of Good Practices

USE SECURE DESIGN PRINCIPLES	REMOTE SERVICES, CLASS 1 DEVICES AND HIGHER
Use defense in depth Designers should assume that their security measures will be compromised at some point – and they should therefore provide redundancy by the means of layered security measures. It also means that error and attack scenarios should be taken into account during the design (not limiting the design to nominal cases)	
Separate security functions from other functions Consequently security functions should have clear and limited interfaces to the "non-secure" functionality. It enables to review thoroughly the secure parts of the product and to avoid security functions to be bypassed by a loosely reviewed "non-secure" function. It also enables to separate development teams and focus the task of security experts only on secure parts.	
Consider third-party review by security specialists for developers with limited security experience A third-party review is recommended for the whole design, and absolutely crucial for cryptography, in order to select the appropriate algorithms and associated functions, and know-how to implement or configure them correctly. This should be a mandatory step during the design stage, since cryptographic operations might put resource conditions that have a significant impact on components procurement.	

Findings and Recommendations

Findings

- Detailed analysis of security in Smart Homes
- Current hard points to tackle

Recommendations

- Objective: overcome findings
- Target specific stakeholders
- Detail incentives

Results of the study

Analysis of survey and interviews (1/2)

Threats are real and have manifested

- Remote attacks (web-based interfaces, local network)
- Attack using other devices (smartphone, PC, other smart home devices...)

Liabilities not well defined

- Vulnerability disclosure / dissimulation
- Who is responsible in case of an incident?

Need for Security requirements

- Minimum security requirements per device
- For their development, operation and maintenance
- Definition by a public or trans-national body
- Yet regulation not desired

Analysis of survey and interviews (2/2)

Supply chain is a real concern

- Re-use of third-party hardware and software (OS, API…)
- No possibility to assess security

Security label or certification

- Not a guarantee for security: in-house testing still needed
- Should not hamper business (usually too long to get certified)

Current security practices for development and maintenance (internal)

- Operational guidelines
- In-house testing and validation

Overview of Good Practices

Development of smart home devices and services

Development Security

- ❑ Design
- ❑ Development
- ❑ Testing

Security functions for hardware and software

- ❑ Security Audit
- ❑ Communication protection
- ❑ Cryptography
- ❑ User Data Protection
- ❑ Identification, authentication, authorization
- ❑ Self-Protection

Integration of devices in the Home Area Network

Resilience of the HAN

- ❑ Ensure a minimum level of reliability for devices
- ❑ Define trust relationships
- ❑ Use additional HAN protection measures

Usage until end-of-life

Protection of data exchange

- ❑ Segregate the Smart Home Networks and the AMI
- ❑ Leverage on gateways

Operational security and maintenance

- ❑ Vulnerability survey
- ❑ Security updates
- ❑ Remote interfaces protection
- ❑ Security management system for support infrastructures
- ❑ Secure deletion of data when end-of-life is reached

Device vendors and service providers

Electronic communication providers

End-users

Main findings (1/2)

Smart Home assets' sensitivity is underestimated

- “Not a target” attitude
- Functionalities over security
- Asset owner is not well informed of risks

Vendors lack incentives to enhance security

- Security requires organisational changes
- Lifecycle of devices/services too short to invest
- And there is no customer demand…

Smart home strengths are not always leveraged upon

- Improve security thanks to the architecture of Smart Home

Main findings (2/2)

Smart Home devices and services implement few security measures

Smart home causes new security challenges

- Potential risks on health and safety

IoT vulnerable “building blocks” cause vulnerabilities to be shared at large scale

IoT pervasiveness and dynamicity bring new threats

IoT brings new constraints on security

- Several risks for data exchange
- Requires a global effort and interoperability

Recommendations

1. All stakeholders should reach a consensus on security requirements
2. Industry actors should support security-driven business models
3. All actors should contribute to raise security awareness
4. Industry actors should develop security assessment methods or frameworks
5. Policy Makers should clarify the legal aspects of Smart Home Environments
6. Industry actors should integrate cyber security in Smart home R&D projects

Challenges and next steps

Challenges of IoT

Security of IoT for Smart Homes is important

- Rapid technological evolution
- Many vulnerabilities with impact on EU citizens
- Security required for the whole lifecycle of IoT products and services

Main challenges to overcome

- Security is difficult to assess (3rd-party APIs…)
- No incentive for developers and manufacturers to integrate security
- Users not ready to pay for more security… yet?

Next steps

Enhance IoT security

- Definition and harmonisation of minimum security features
- Integration of security in research projects (H2020, industrial)
- Evaluation framework for IoT security (type “5 stars” framework)

ENISA proposes a pragmatic approach

- Technical guidance
- Reference groups
- Awareness raising

Cyber security for IoT requires a global effort

Objectives of Session 2

Validate the good practices

- Detail and applicability of security measures
- Completeness of the list
- Should some proposals not be considered good practices?

Validate recommendations

- Pertinence of recommendations
- Priorities?

Thanks

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu