Are Smart Homes Cyber-Security smart?

ENISA published today the Threat Landscape and Good Practice Guide for Smart Home and Converged Media, a contribution towards the achievement of the objectives of the EU Cyber Security Strategy. The study aims to identify the security risks and challenges, and the countermeasures required for emerging technologies in smart homes, providing a specific and focused approach, with an overview of the current state of cyber security in this emerging domain.

For the compilation of this report, an informal expert group was created to collect input at various stages of the project. In addition, the study takes into account existing assessments and publicly available information sources and deepens into the ENISA annual Threat Landscape.

Within the scope of the study, threat agents have been identified revealing several sources of vulnerability. Cyber criminals are identified as the largest and most hostile threat category, while the potential abuse of smart homes should be considered high with the increasing number of smart devices and homes and particularly converged media. Further, several economic factors generate security vulnerabilities, while design choices are competing against cost and convenience.

Many of the risks will be of a socio-technical type due to the depth and variety of personal information that can be captured and processed, and will produce data on previously unrecorded activities, with a close link between people and their environments. In addition, the interests of different asset owners in the smart home are not necessarily aligned and may even be in conflict, creating a complex environment for security activity.

On the other hand, converged media and television raise security issues in terms of connectivity, embedded functionality, opaque systems and incompatibility with traditional information security approaches, along with issues on privacy, access and copyright. Converged media devices are likely to be some of the first consumer smart home devices introduced to many homes, and will therefore be the terrain for the initial playing out of many of the identified smart home security issues.

Not all smart homes are created equally due to multiple design pathways which result in their own security and privacy peculiarities, sharing issues and vulnerabilities. Just as in many other areas of ICT, applying basic information security can significantly increase overall security in the smart home domain.

Good practices in the sector involve the design of the smart home as a system, careful consideration of the security of cloud-based smart home designs, an application isolation framework (as developed in smart cars), and keeping critical software separate from non-critical apps, network and communications security measures. Similar approaches referred for smart grids may prove to be applicable in the smart home context.
The Executive Director, Udo Helmbrecht commented: “The smart home is a point of intense contact between networked information technology and physical space, and therefore brings together security risks from both the virtual and the physical contexts. Identifying cyber threats is crucial for the protection of the smart home and is therefore a key element in ensuring its successful deployment”.

For full report: Threat Landscape for Smart Home and Media Convergence

For interviews and contacting the authors please use resilience@enisa.europa.eu, media enquires press@enisa.europa.eu

Notes to editors:

Figure 1: Overview of Smart Home and Converged Media Assets p.11
Figure 2: Overview of Threats Assumed for Smart Home Assets p.13
Association between threats and smart home assets p.34
Table 1: Involvement of Threat Agents in the Threats p.38
Table 3: Good Practice Measures against Threat Categories p.51


ENISA thematic threat landscapes:

Threat Landscape and Good Practice Guide for the Internet Infrastructure (2014)
Smart Grid Threat Landscape and Good Practice Guide (2013)