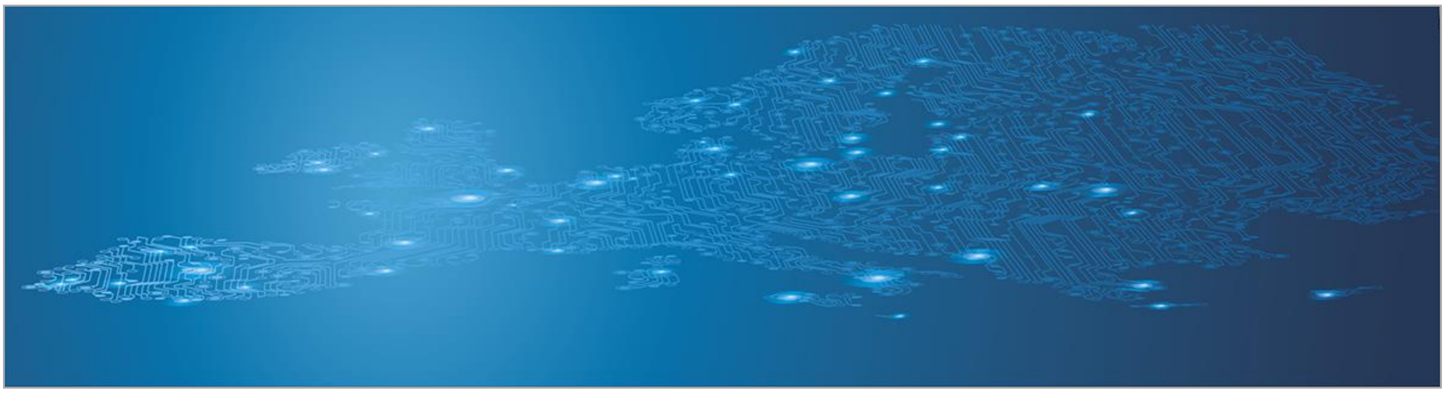

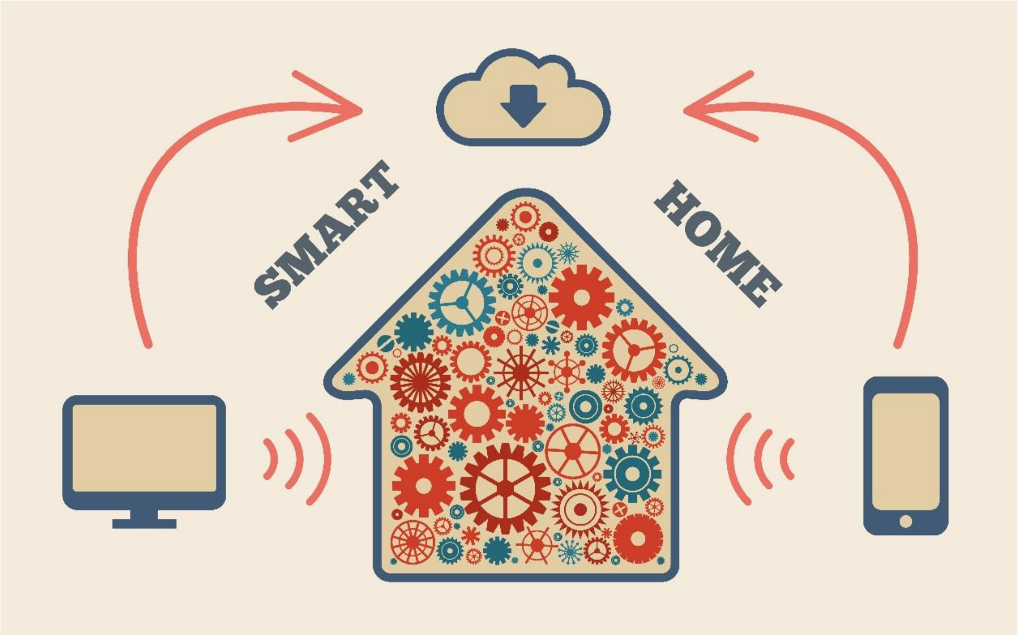

Threat Landscape and Good Practice Guide for Smart Home and Converged Media

1 December 2014

enisa

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

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

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu

Acknowledgements

The analysis in this document was produced in collaboration with Trilateral Research & Consulting (www.trilateralresearch.com).

Acknowledgement should be given to the ENISA colleagues who provided support with the compilation of this report, and in particular to Adrian Pauna for his valuable contribution.

The report also benefited from the participation and contribution of the following members of the Expert Group. ENISA would like to thank all involved individuals for their valuable input that made possible the creation of this deliverable, and in particular:

- Behrang Fouladi, Microsoft Security Response Center, United Kingdom
- Kai Kreuzer, Deutsche Telekom, Germany
- Annica Kristoffersson, Center for Applied Autonomous Sensor Systems (AASS), Örebro University, Sweden
- Massimo Mecella, Sapienza Università di Roma, Research Center of Cyber Intelligence and Information Security (CIS) and Dipartimento di Ingegneria Informatica Automatica e Gestionale (DIAG), Italy
- Benjamin Schwarz, CTO innovation Consulting, France

Cover page image from http://www.shutterstock.com - Image ID: 162180008 - Copyright: Macrovector

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-096-3, doi: 10.2824/33134

Executive summary

Smart homes are homes equipped with technology that provides the occupants with comprehensive information about the state of their home and allows them to control all connected devices, including remotely. In addition to this consolidated and remote control of the home, a smart home may also be able to “learn” the preferences of its inhabitants and adapt to them. Examples of smart home devices include: smart fridges, smart electricity meters, smart blinds, and automatic pet feeders. Important components of the integrated smart home are converged media - media characterised by the merging of traditional broadcast services with the Internet - in particular in the form of smart TVs and related devices such as media centres. Home automation has increased over the years due to the fact that the various smart home components, devices and systems have reached a level of technological development and maturity suitable for entry into the market. Furthermore, smart home devices have nowadays become more affordable. Due to the proliferation of interconnectivity and intelligence related to living habits, coupled with the digitalization of important utilities, smart homes constitute an attractive field for developments and future deployments.

Smart home technology aims to increase efficiency and quality of life, for example through assisted living for ageing populations. However, besides benefits, smart home also bears cyber security risks. This *Threat Landscape and Good Practice Guide for Smart Home and Converged Media* provides an overview of the current state of cyber security in this domain. In particular it identifies commonly used assets, exposure of these assets to cyber threats, threat agents, vulnerabilities and risks, as well as available good practices in the field. In addition to the input from the members of the ENISA informal Expert Group (EG) created for this effort, existing assessments and publicly available information have been taken into account.

The study identifies threats to all asset classes, across the several alternative design pathways to smart homes. As it develops, the smart home will exhibit a high cyber security risk profile for the individual context, with additional systematic effects on broader information security. Highlights of this study are:

- **Not all smart homes are created equally**. There are multiple design pathways that lead to functional smart homes, ranging between localised and integrated home-automation systems. These pathways have their own security and privacy peculiarities, but also have shared issues and vulnerabilities.
- **Smart homes will have significant privacy and data protection impacts**. The increased number of interlinked sensors and activity logs present and active in the smart home will be a source of close, granular and intimate data on the activities and behaviour of inhabitants and visitors.
- Several **economic factors may lead to poor security** in smart home devices. Companies involved in the smart home market include home appliance companies, small start-up companies, and even crowd-funded efforts. These groups are likely to lack security expertise, security budgets and access to security research networks and communities.
- **The interests of different asset owners in the smart home are not necessarily aligned** and may even be in conflict. This creates a complex environment for security activity.
- Just as in many other areas of ICT, **applying basic information security would significantly increase overall security** in the smart home domain.

The smart home is a point of intense contact between networked information technology and physical space. This will create new yet unknown threat and vulnerability models that are result of bringing together both the virtual and physical contexts.

Table of Contents

1 Introduction

Scope

A threat landscape is a collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends. Threat landscapes can be broad, including the entire range of cyber threats, or targeted at a particular sector, such as the financial sector, critical infrastructure or smart homes.

Threat landscapes can also vary by the particular time horizon involved, including current threat landscapes, emergent threat landscapes and future threat landscapes. Emerging threat landscapes reflect threat exposure of deployments of new technology, often characterised by a low maturity regarding technical vulnerabilities. Emerging threat landscapes also involve mapping existing threats onto emerging technologies to better understand how the particular context is exposed to these threats.

The scope of this threat landscape is smart home environments, with a particular focus on converged media and television.

Smart homes can be considered a sub-category of the Internet of Things (IoT), which has recently been identified as an emerging digital battlefield for information security[1]. Smart homes are also an emergent technology, which has reached a level of technological development suitable for entry onto the market and are therefore a relevant subject for an emergent threat landscape. The popularity and affordability of smart homes has been increasing in recent years due to reductions in costs and integration with mobile phones and tablets[2]. 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.

Goal

This threat landscape deepens the generic threat assessment of the ENISA Threat Landscapes 2012[3] and 2013[4], by taking into account the specificities of the area of smart home environments, with a particular focus on converged media and television. It does so by following the same approach adopted by ENISA for other thematic threat landscapes, such as the *Smart Grid Threat Landscape and*

[1] ENISA, *ENISA Threat Landscape 2013: Overview of current and emerging cyber threats*, European Network and Information Security Agency, Heraklion, 11 December 2013, p.iii. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats [accessed 27 October 2014}

[2] Booton, J., "Why the 'Smart Home' Market is about to Take Off", *Foxbusiness*, 21 January 2014. http://www.foxbusiness.com/technology/2014/01/21/why-smart-homes-might-actually-be-here-to-stay/ [accessed 27 October 2014]; Warman, M., "Everything Connected: the smart home in 2014", *The Telegraph*, 31 December 2013. http://www.telegraph.co.uk/technology/Internet/10542550/Everything-connected-the-smart-home-in-2014.html [accessed 27 October 2014]

[3] ENISA, *ENISA Threat Landscape 2012: Responding to the Evolving Threat Environment*, European Network and Information Security Agency, Heraklion, 08 January 2013. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape [accessed 27 October 2014]

[4] ENISA, *ENISA Threat Landscape 2013: Overview of current and emerging cyber threats*, Op. cit.. p.7 http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats [accessed 27 October 2014]

Good Practice Guide from 2013[5] and *Threat Landscape and Good Practice Guide for the Internet Infrastructure*[6], a work conducted by ENISA in parallel in 2014. This *Threat Landscape and Good Practice Guide for Smart Home and Converged Media* is one of the deliverables (Work Package 1.1 - Deliverable 2) foreseen in the ENISA Work Programme 2014 under the Work Stream "*Support EU policy building*"[7].

The purpose of ENISA's work on threat landscapes is to provide stakeholders with information about developments in the cyber-threat landscape and to identify threat trends for the near future. This is in support of the EU Cyber Security Strategy[8]. In this context, this report aims to:

- Identify security challenges, associated risks and required countermeasures, for emerging technologies in smart homes, in particular, for converged media and television[9].
- Consider political, social, economic and technical threats, in addition to technical threats.
- Take into account input from experts and the members of the ENISA informal Expert Group (EG) established to support the compilation of the current *Threat Landscape for Smart Home and Converged Media*.
- Take into account existing assessments, publicly available information sources and the perspectives of involved stakeholders.

Policy context

The EU Cyber Security Strategy[10] stresses the importance of threat analysis and emerging trends in cyber security. The ENISA *Threat Landscape and Good Practice Guide for Smart Home and Converged Media* contributes towards the achievement of objectives formulated in this Communication, in particular, to the identification of emerging trends in cyber-threats and understanding the evolution of cyber-crime (regarding the proposed role of ENISA, see in particular section 2.4 of this Communication).

Moreover, the ENISA Regulation[11] mentions in its Recital (24) the necessity to analyse current and emerging risks (and their components), stating that for this purpose the Agency should, "*in*

[5] ENISA, *Smart Grid Threat Landscape and Good Practice Guide*, European Network and Information Security Agency, Heraklion, 9 December 2013. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide [accessed 27 October 2014]

[6] ENISA, *Threat Landscape and Good Practice Guide for the Internet Infrastructure*, European Network and Information Security Agency, Heraklion, 19 December 2014. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl [accessed 19 December 2014]

[7] ENISA, *Work Programme 2014*, 29 November 2013. https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014 [accessed 27 October 2014]

[8] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final, of 7 February 2013, on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1413446331633&uri=CELEX:52013JC0001 [accessed 20 October 2014].

[9] ENISA Work Programme 2014. http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014, p. 19 [accessed 27 October 2014]

[10] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final, of 7 February 2013, on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1413446331633&uri=CELEX:52013JC0001 [accessed 20 October 2014].

[11] European Parliament and the Council, Regulation (EU) No. 526/2013, Concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, 21 May

cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information". In particular, Article. 3 (Tasks), d), ii), states that one of the tasks to be performed by the Agency is to "*support research and development […] by […] advising the Union and the Member States on research needs in the area of network and information security with a view to enabling effective responses to current and emerging network and information security risks and threats, including with respect to new and emerging information and communications technologies* […]".The ENISA Threat Landscape is contribution to the EU Cyber Security Strategy, by streamlining and consolidating available information on cyber-threats and their evolution. Detailing the ENISA Threat Landscape for various emerging areas, such as smart homes, should contribute to existing policy measures established by the European Commission.

Furthermore, the Commission has issued a recommendation[12] regarding energy efficiency by means of intelligent buildings encompassing "*ICT-based innovations that may provide one of the potentially most cost-effective means to help Member States achieve the 2020 (energy) targets*". Although being an indirect consequence of this recommendation, such innovations will be the catalyst for the introduction of smart home environments, as they play an important role in increasing energy efficiency of buildings. This is an indirect, rather than a direct context. But it will result in smart functionality being introduced in smart buildings and smart homes. This study is a first contribution towards cyber-security issues of these environments.

Target audience

The target groups of this document are specialists and individuals who are concerned with the development and evolution of threats in cyber space, primarily security experts interested in assessing the "external environment" and "internal environments" in the framework of threat and risk assessments. This information might be interesting when formulating security policies or creating protection profiles. Interested decision makers and users of IT components may find information of help in defining their risk appetite and in making informed investment decisions and for the protection of potentially valuable assets and of help. This *Threat Landscape and Good Practice Guide for Smart Home and Converged Media* provides non-security experts with information to better understand dependencies and developments in the area of cyber-security.

The document will also be of interest to policy-makers as, in addition to providing an overview of the threat landscape and good practices in smart home and coverged media, it identifies existing policy measures supporting smart home security and further action that may be required for various stakeholders.

Finally, the document is intended to serve as a basis and a resource for further research in the area of smart home security.

2013, OJ. L 165/41. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF [accessed 17 October 2014]

[12] Commission Recommendation, C(2009) 7604 final, on Mobilising Information and Communications Technologies to facilitate the transition to an energy-efficient, low-carbon economy, of 9 October 2009. http://ec.europa.eu/information_society/activities/sustainable_growth/docs/recommendation_d_vista.pdf [accessed 27 October 2014]. Regarding encouraging energy efficient buildings, see also High Level Advisory Group and REEB Consortium, *ICT for a Low Carbon Economy: Smart Buildings*, European Commission, Information Society and Media, July 2009. http://ec.europa.eu/information_society/activities/sustainable_growth/docs/sb_publications/smartbuildings-ld.pdf [accessed 27 October 2014]

Structure of this document

The rest of this document is structured into the following sections (the subheadings of which are in bold face):

- **Smart home infrastructure with a special focus on converged media and television** sets out a rationale for the smart home landscape, and sets out the boundaries and applicability of the threat landscape.
- **Methodology** then provides information on the methods used to identify sources for the threat landscape, including the involvement of the expert group.
- **Valuable assets in smart homes and converged media** identifies and depicts valuable assets that are likely to be part of a smart home environment, as based upon common models of smart homes.
- The subsequent section depicts the **Threats** to which smart home assets are potentially exposed.
- The **Specific smart home threats** section draws upon the evidence provided by the documentary analysis to identify the specific threats (from the broader typology of potential threats) that apply to smart home assets.
- **Smart home assets exposure to cyber threats** maps the association between the identified threats and the smart home and converged media assets.
- The **Threat agents** potentially responsible for cyber security threats to smart home assets are identified, described, and mapped against threat categories.
- The report then examines **Vulnerabilities and risks in smart homes** and also provides a brief overview of some particular issues raised for converged media.
- The report then identifies a set of available **Good practices in smart home and converged media security measures** and their roles in responding to threats, vulnerabilities and risks.
- Based upon the preceding vulnerabilities and good practices, the report conducts a **Gap analysis**, identifying further areas of research.
- In the **Conclusions,** the report provides cross-cutting findings from the study.

2 Smart home infrastructure including converged media and television

The fundamental concept of a smart home is one fitted or equipped with a range of interconnected sensors (light, temperature, motion, moisture, pressure, etc.), systems (heating, lighting, security, etc.), and devices (media devices, appliances, washing machines, fridges, home robotics, etc.), which can be automated, monitored and controlled, e.g., through a computer or smart phone, including from outside the home, or via the Internet. Smart homes can either be the result of integrated design, or the accumulation of interconnected components over time, perhaps in response to changing needs or availability of technology[13]. The intent is to provide the occupants with sophisticated information about the state of their home, and to allow them to control the connected devices. In addition to consolidated and remote control of the home, a smart home may also be able to "learn" the preferences of its inhabitants and adapt to them. In this case, the control interfaces may fade into the background. This shift is seen as critical to avoid overloading the household with the task of monitoring and programming the smart home[14]. A smart-home-connected refrigerator might be able to monitor its contents, and use this information to suggest potential menus or to order replacements. A smart electricity meter connected to the smart grid might be able to respond to fluctuations in the per-unit cost of energy by slightly adjusting the temperature of the house, or by starting the washing machine at a later time[15]. A smart home might respond to the presence of certain occupants by changing desired lighting levels. Smart homes have also been identified as particularly beneficial for assisted living for ageing populations[16].

Smart homes combine a set of currently developing technologies. Whilst the development of these technologies is not fixed, trends are discernible. This threat landscape report focuses on the most likely patterns of development in smart homes[17].

Early approaches to home automation assumed a cohesive and harmonised model, in which a single system would provide automation of a building, most likely provided by a single supplier, and potentially integrated with the building at the time of its construction. Current approaches suggest a more complex smart home environment, composed of multiple technologies from multiple manufacturers and service providers, and often integrated on an *ad-hoc* basis with existing legacy technologies and systems. This complex environment may take a range of models.

In a fully decentralised smart home, each device is autonomous, making use of the existing home network to connect to the Internet, and transmits data to the service provider in the cloud. This is the model adopted, for instance, by the NEST smart thermostat[18]. Each device has its own control interface or app. The home network provides secure transmission of data in the home. Any integration or interaction between services is accomplished by communication between different service providers, either through a central service (such as IFTTT[19]), or through direct peer-to-peer integration.

[13] Edwards, W.K., and Grinter, R.E., "At home with ubiquitous computing: Seven challenges" in Abowd, G.D., Brumitt, B., and Schafer, S.A.N., (eds.), *Ubicomp*, 2001, pp. 256-272.

[14] Davidoff, S., Lee, M.K., Yiu, C., Zimmerman, J., and Dey, A. K., "Principles of Smart Home Control" in Dourish, P., and Friday A. (eds.), *Ubicomp 2006*, Springer-Verlag, Berlin, 2006, pp. 19-34.

[15] In this manner, smart homes are closely linked to the concept of the smart grid, especially those implementations of smart grids that intend to reduce energy used through variable pricing schemes.

[16] Arcelus, A., Jones M. H., Goubran, R., and Knoefel, F., "Integration of Smart Home Technologies in Health Monitoring System for the Elderly", *21st International Conference on Advanced Information Networking and Applications Workshop (AINAW'07)*, 2007.

[17] For information on the identification and collection of sources, see Section 3: Methodology.

[18] https://nest.com/uk/ [accessed 20 October 2014]

[19] https://ifttt.com/ [accessed 20 October 2014]

In this context, security and privacy are not guaranteed by a single manufacturer but rather the whole network has to be considered.

An alternative option enables local connectivity between smart devices, without the use of connections to cloud services and without a central gateway. In this model, all devices are able to discover each other and automatically form a smart solution by recognising their peers and their capabilities. This model faces strong technological barriers and suffers from the absence of shared protocols and communication standards, as well as ways of incorporating individual devices designed to connect to the Internet.

A third alternative is a system based around a central hub or gateway of some form. A central software system (deployed on a home desktop, a set-top-box, a smart TV) co-ordinates all the devices, integrating their services in order to provide added value, more complex services. In this case, as the data is confined to the home itself, security and privacy can be protected. Many approaches to home automation adopt a home gateway (such as the GIRA Homeserver[20], the QIVICON Home Base[21], the Insteon Hub[22], the SmartThings Hub[23], the Revolv Hub[24] and the Ninja Sphere[25]). In addition to these fixed devices, other devices such as smart phones, tablets, laptops and wearable technology enter and leave the house.

We consider that the most likely and feasible scenario for the common installation of smart homes will not be a pure form of one of these three models. One potential location for smart home gateway or hub will be the smart media device, typically a converged media device such as a smart television. Smart televisions have a number of attributes that contribute towards this role, which are discussed in more detail in Section 9, Subsection: Particular issues raised for converged media. Smart phones, which should also be considered as media devices in this context, will also play a role in controlling the smart home.

We can gain additional insights into the likely smart home infrastructure from parallel infrastructure. For example, hotels worldwide have been installing a range of room-automation, entertainment and management systems for the comfort of their customers as well as for their own management, billing and profit maximisation (for example, selling premium media content). Smart TVs are often a key element of these systems, allowing visitors to the hotel to order services, access entertainment, and view billing details. This can include TV over IP[26]. These systems are of a larger scale than the typical home automation set-up, but utilise many of the same technologies. The large transient population of hotels, including international business travellers and other high-value customers, makes them a tempting target for fraudsters and for espionage, and therefore potentially exposes a large number of people to victimise through the exploitation of information security vulnerabilities in these systems. Hotels can be seen as leading the way in introducing these systems, and provide a perspective on how these issues might play out as smart home technology becomes more diffuse and dispersed.

Digital convergence is the coming together of the media, telecommunications and consumer electronics sectors, driven by several trends, including increases in processing speed, storage capacity,

[20] http://www.gira.com/en/gebaeudetechnik/systeme/knx-eib_system/knx-produkte/server/homeserver.html [accessed 20 October 2014]
[21] https://www.qivicon.com/qivicon-prinzip/qivicon-home-base/ [accessed 20 October 2014]
[22] http://www.insteon.com/2242-222-insteon-hub.html [accessed 20 October 2014]
[23] http://www.smartthings.com/ [accessed 20 October 2014]
[24] http://revolv.com/ [accessed 20 October 2014]
[25] http://ninjablocks.com/pages/home [accessed 20 October 2014]
[26] Leyden, J., "Hotel hacking could pump smut into every room", *The Register*, 22 August 2005. http://www.theregister.co.uk/2005/08/22/hotel_hacking_reloaded/ [accessed 20 October 2014]

transmission speed, compression techniques and standardisation[27]. Despite the increasing popularity of consuming media through other devices such as smart phones and tablets, television remains an important media channel for European citizens. This is expanded by the increased uptake of smart TVs, which offer Internet connectivity, as well as other devices (such as Google Chromecast, Apple TV, Roku streaming devices and games consoles such as the PlayStation and Xbox) that connect to non-smart TVs to grant them certain elements of smart functionality. Smart TVs are capable of broadcasting both linear (traditional broadcast television) and non-linear (downloaded or streamed) audio-visual content, bringing about a convergence between traditional and online media. The smart TV offers the potential for a device, which replicates the functionality of existing TV, media player, home cinema, music and gaming systems, connected to the Internet and a range of online services, and may well be integrated with home automation systems as part of a smart home. Internet connectivity and home networking also allow a range of media devices within the home to share content with each other, streaming media to different devices[28]. This general convergence of media creates a dynamic situation in which the information processed and produced by converged home media centres will be significant, will run through a shifting set of publishers, broadcasters, search providers, connection providers, etc., and will be highly applicable to the profiling of individuals within the household. As networked forms of interactive communication become pervasive, they enhance and expand monitoring practices as they can gather information about user activity[29]. Whilst this convergence brings advantages to the consumer in terms of access to a wide variety of media content on flexible terms, these systems may well not be under the full control of the user. For example, in 2013, a tech blogger reported that he discovered that some smart TVs were transmitting unencrypted information on viewing habits, as well as the names of files stored on an external USB drive[30]. In addition to social issues around privacy, access and copyright, converged media and television raise related security issues to smart homes in terms of connectivity, embedded functionality, opaque systems and incompatibility with traditional information security approaches, and can be understood as a particular instance of the principles behind smart homes.

Smart homes raise security concerns. First, small, low cost, interconnected devices may not have mature security functions, having been designed primarily for ease of set-up, use and interconnection and having relatively low processing capability. Communication within the smart home may use a range of protocols (WiFi, Bluetooth, NFC, ZigBee and others), and therefore have a number of open vectors for exploitation. Devices which were previously considered secure (or not even within the ambit of information security) may become vulnerable to attack, either against the device itself, or to harness the device to propagate further malicious attacks. Your smart kettle might, without your knowledge, participate in a botnet[31]. Furthermore, many current information security approaches have been developed in the context of enterprise computing, and may not be perfectly applicable to the context of a distributed smart home, set up and inhabited by individual consumers. Second, smart homes will be a key point of intersection between people and technology, and as such an approach to

[27] Van Oranje, C., Cave, J., Van der Mandele, M., Shindler, H. R., Hong, S.Y., Illiev D. I., and Vogelsang, I. *Responding to Convergence: Different approaches for Telecommunications Regulators*, 30 September 2008. http://ssrn.com/abstract=2142015 or http://dx.doi.org/10.2139/ssrn.2142015 [accessed 27 October 2014]

[28] Arabo, A., and El-Mousa F., "Security Framework for Smart Devices", *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),* 28 June 2012. http://ssrn.com/abstract=2173343 [accessed 27 October 2014]

[29] Lyon, D., "Surveillance Studies: An Overview", Cambridge, *Polity*, 2007, p. 25.

[30] DoctorBeet, "LG Smart TVs logging USB filenames and viewing info to LG servers", *DoctorBeet's Blog*, 18 November 2013. http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html

[31] Sharwood, S., "Don't brew that cuppa! Your kettle could be a spambot", *The Register*, 29 October 2013. http://www.theregister.co.uk/2013/10/29/dont_brew_that_cuppa_your_kettle_could_be_a_spambot/ [accessed 27 October 2014]

information security (and in particular to understanding the threat landscape) in this context requires a particular input from social, political and economic perspectives. Privacy issues in smart home are not limited to confidentiality and access control. Smart home sensors in particular will generate a large amount of highly personal data about activities within the home. The multiple streams of data combined together in a smart home system create the possibility of deeper contextual background and reveal patterns of behaviour of the inhabitants[32]. The visibility of the smart home occupant is increased by the large network of third parties who may be involved in providing smart home functionality. Smart home functions may have serious impacts upon privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of location, and privacy of association[33]. The role of an information industry becomes particularly important in the shift to ubiquitous computing[34]. Smart home systems may include embedded features that are opaque to the user, and do not inform the user about the status of their operation. They may also be difficult to update and patch in response to identified vulnerabilities. Smart homes may include sensitive systems related to the occupants' healthcare, finances and systems related to the physical security of the home[35], which may be open to dangerous manipulation by attackers.

Responses to the security and privacy risks of smart homes will include layering effective privacy controls, and user-centric solutions on top of other effective information security measures, adapted to the domestic context of smart homes[36]. Security services, such as authentication and access control, have to be non-intrusive, intelligent and able to adapt to the rapidly changing contexts of the spaces[37]. Smart home control and management systems will have to take security into consideration. This is likely to include decisions about the architecture of smart home systems, as well as the broader policy and legal context.

[32] Davies, N., and Langheinrich, M., "Privacy by Design", *IEEE Pervasive Computing*, vol. 12, No. 3, April-June 2013, pp. 2-4.

[33] Finn, R. L., Wright, D. and Friedewald, M., "Seven Types of Privacy" in Gutwirth, S., et al (eds.), *European Data Protection: Coming of Age*, Dordrecht, Springer, 2013.

[34] Andrejevic, M., "Ubiquitous Surveillance", in Ball, K., Haggerty, K., and Lyon, D. (eds.), *Routledge Handbook of Surveillance Studies*¸ Routledge, Abingdon, 2012, pp. 91-98.

[35] Wolf, M., "Here are 4 industries about to be completely disrupted by the smart home", *Forbes*, 18 March 2014. http://www.forbes.com/sites/michaelwolf/2014/03/18/here-are-4-industries-about-to-be-completely-disrupted-by-the-smart-home/ [accessed 27 October 2014]

[36]Arabo, A., Brown, I., and El-Moussa, F., "Privacy in the age of Mobility and Smart Devices in Smart Homes", *Fourth IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT)*, 4 September 2012. http://ssrn.com/abstract=2173360 [accessed 27 October 2014]

[37] Al-Muhtadi, J., Ranganathan, A., Campbell, R., and Mickunas, M.D., "Cerberus: a context-aware security scheme for smart spaces", *Proceedings of the first IEEE International Conference on Pervasive Computing and Communications*, 26-9 March 2003.

3 Methodology

This study is based upon a variety of open sources of information relevant to smart homes and converged media, which were collected during the period of the study. In addition, ENISA established an informal expert group to collect input at various stages of the project. The group comprised five experts in the field who, on a voluntary basis, provided their expertise, e.g., for the identification of the relevant assets, associated risks, past incidents and existing good practices. The expert group contributed to the finalisation of this report. This section provides an overview of the methods of collection and the information collected as well as some of the issues encountered during this process.

Documentary sources

This report identifies the majority of sources consulted; the details of all documentary sources consulted during the study are available on request by contacting resilience@enisa.europa.eu. 166 documentary sources were identified through a number of search methods, including specialist search engines for academic sources and journal articles. The sources collected are primarily in English, but also include documents in other European languages.

Interviews and groups discussion with the expert group

The study team conducted a series of semi-structured expert interviews with each of the members of the study's expert group. The aim of these interviews was to access these experts' knowledge of the field of smart home security and to identify additional documentary material for the study. The interviews also allowed for the cross-checking of information from the documentary sources. A semi-structured approach starts with initial questions and topics for discussion but does not use a fixed standardised question schedule. This allows the interviews to address emergent and unexpected topics, whilst still covering the necessary material. The interviews lasted between thirty minutes and one hour and allowed for detailed examination of specific issues and threats. The study team supplemented individual interviews with expert group discussions and answers to written questions. The study team provided the expert group with drafts of the report, as well as key components, such as the valuable assets diagram, for consultation throughout the drafting process.

Issues in data collection on the specific topic

Security issues in smart homes, and those focused upon converged media and television, overlap with other areas of research, in particular, information security, the Internet of Things, home automation, communications, cloud security, privacy and data protection. The Internet of Things is an area attracting attention from the general and specialist press. In some cases, relatively minor press releases, reports or studies on smart home security have been taken up by numerous other blogs and content aggregators, creating something of an echo-chamber, where the same basic claim is repeated by several sources, and later appears as fact without citation. As is common with other areas of information security, data on vulnerabilities and potential technical exploits are much more easily available than verifiable information on actually occurring threats.

4 Valuable assets in smart homes and converged media

The figure below (Figure 1: Overview of Smart Home and Converged Media Assets) provides an overview of smart home assets. An asset is anything that has value and therefore requires protection[38]. Owners value assets and wish to minimise risks to those assets. Threat agents wish to abuse, co-opt and/or damage assets, and thereby give rise to threats that increase risk to assets.

Any such typology or categorisation exercise is variable, reflecting the purpose behind the categorisation. As such, several different approaches to categories could have been identified, with individual assets potentially placed within multiple categories. When such a decision was required, it was guided by the exposure of the assets to related threat families. This categorisation therefore serves to underpin the following threat landscape. Many of these assets could be further decomposed into components and sub-processes, and the categorisation here attempts to strike a balance between covering key significant categories and relevant detail.

In this threat landscape the following assets groups have been identified: Sensors, Software, Human-machine interface devices, Home networking, Audio/Visual, Information Storage, Home appliances, Integrated Home services, Robotics, Tags and markers, Building security, connected transportation, Medical, Information, Management/operation, and People/living. Identified assets and sub-assets are categorised and listed under these assets groups. E.g., under the asset group Sensors, the assets Temperature, Lights, Microphones, etc. are listed.

This asset list has been developed from an examination of common models of actual and potential smart homes, guided by the development scenarios outline in the previous section. Given the modular and potentially idiosyncratic nature of real-world smart home set-ups, the study team does not suggest that all smart homes will necessarily contain all of these assets. Individual set-ups will be determined by a mixture of occupant or owner choices and requirements, budgets, available technology, and compatibility with existing or legacy systems. Smart homes might be understood as sitting somewhere on a continuum from those with a small number of such assets to those that include the full range. Regardless, the different classes of assets result in complex environments even within a single home, since they are produced by different manufacturers and may be installed in an *ad hoc* manner.

Smart home technology, including converged media and television, is still developing, and new applications are being developed. The study team hopes this categorisation of assets will remain relevant for some years due to the selected level of abstraction and the capacity of several categories to accept new assets.

The asset list includes non-ICT assets where these assets are exposed to potential harm from ICT assets and where those assets may be a potential route to attack ICT assets.

[38] ISO/IEC 27005:2011 Information technology – security techniques – Information security risk management.

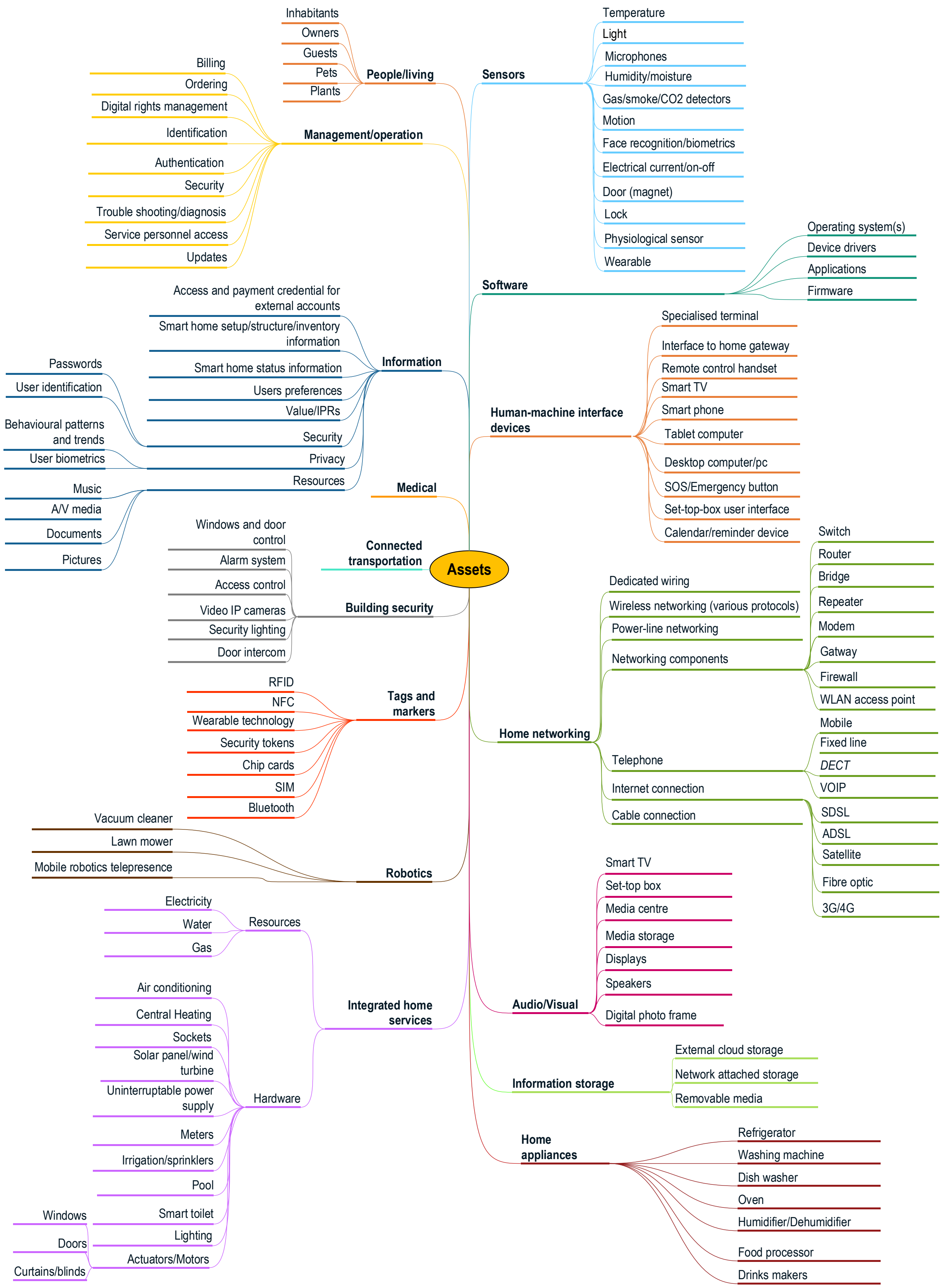

Figure 1: Overview of Smart Home and Converged Media Assets

5 Threats

For the purpose of the smart home threat landscape, a general threat-taxonomy has been developed. The threats included in this collection of threats are all applicable to the smart home assets presented in the previous section. The presented threat taxonomy covers mainly cyber-security threats, that is, threats applying to information and communication technology assets. Some additional non-IT threats have been assumed in order to cover threats to physical assets that are necessary to operate the considered ICT-assets. This threat taxonomy draws upon the threat taxonomies developed for the *ENISA Threat Landscape* 2013[39] and the *Smart Grid Threat Landscape and Good Practice Guide*[40]. Please note that the use of colour is to distinguish between threat categories, and does not signify any correlation between threats in this figure and assets in the previous figure.

In this threat landscape the following threats groups have been identified: Physical attacks, Unintentional damage (accidental), Disasters, Damage/Loss (IT assets), Failures/Malfunctions, Outages, Eavesdropping/Interception/Hijacking, Nefarious activity/Abuse, and Legal.

Identified threats and sub-threats are categorised and listed under these threat groups. E.g., under the threat group Unintentional damage (accidental), the threats Information leakage or sharing, Erroneous use or administration of devices and systems, Using information from an unreliable source, etc. are listed.

The specific smart home threats are described in Section 6.

[39] ENISA, *ENISA Threat Landscape 2013: Overview of current and emerging cyber threats*, Op. cit, 2013. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats [accessed 27 October 2014]

[40] ENISA, *Smart Grid Threat Landscape and Good Practice Guide*, Op. cit., 2013. https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide [accessed 27 October 2014]

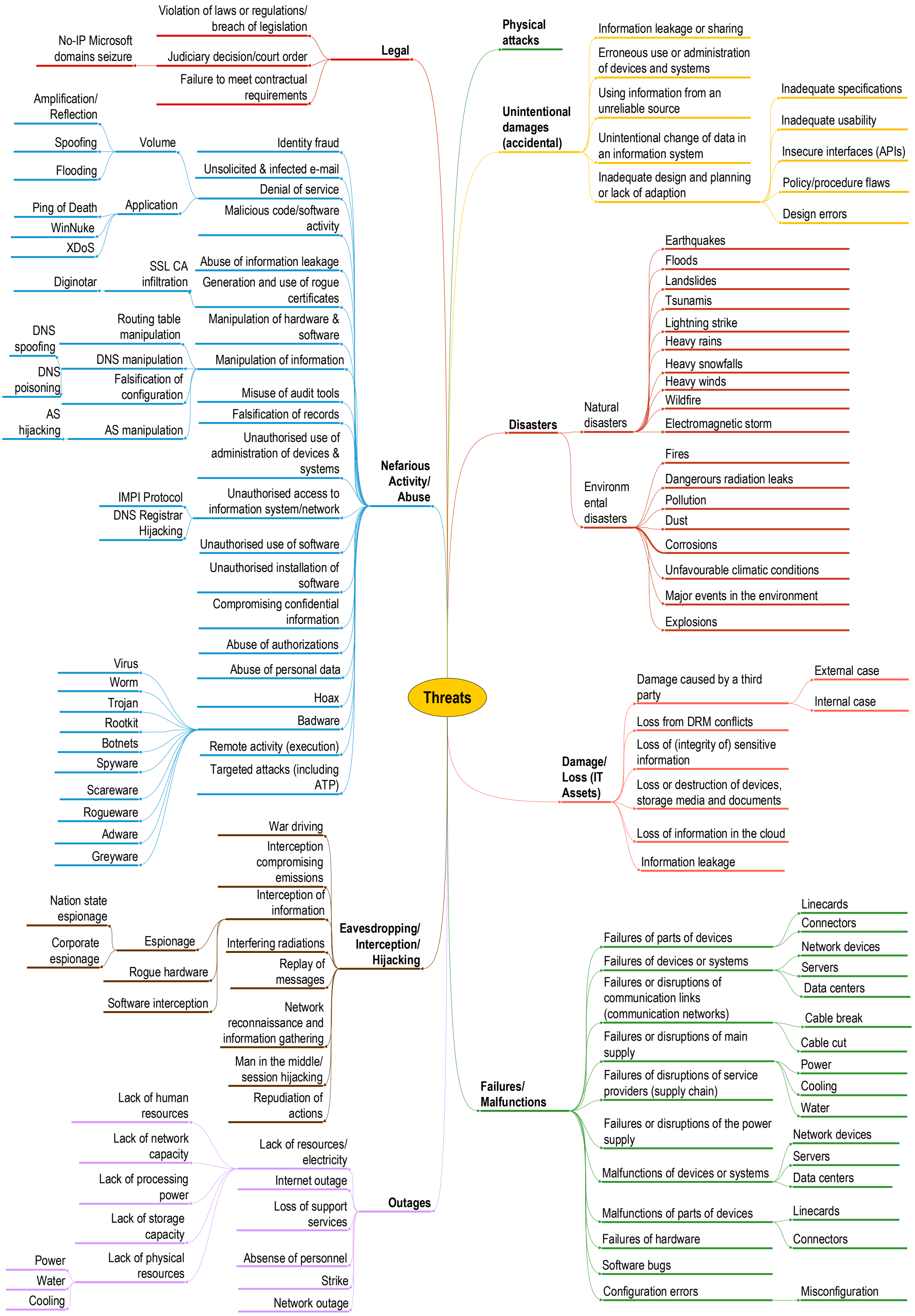
Threats
Legal
Violation of laws or regulations/ breach of legislation
No-IP Microsoft domains seizure
Judiciary decision/court order
Failure to meet contractual requirements
Nefarious Activity/ Abuse
Amplification/ Reflection
Spoofing
Flooding
Volume
Ping of Death
WinNuke
XDoS
Application
Identity fraud
Unsolicited & infected e-mail
Denial of service
Malicious code/software activity
Abuse of information leakage
SSL CA infiltration
Diginotar
Generation and use of rogue certificates
Manipulation of hardware & software
Routing table manipulation
DNS spoofing
DNS manipulation
DNS poisoning
Falsification of configuration
AS hijacking
AS manipulation
Manipulation of information
Misuse of audit tools
Falsification of records
Unauthorised use of administration of devices & systems
IMPI Protocol
DNS Registrar Hijacking
Unauthorised access to information system/network
Unauthorised use of software
Unauthorised installation of software
Compromising confidential information
Abuse of authorizations
Abuse of personal data
Virus
Worm
Trojan
Rootkit
Botnets
Spyware
Scareware
Rogueware
Adware
Greyware
Hoax
Badware
Remote activity (execution)
Targeted attacks (including ATP)
Eavesdropping/ Interception/ Hijacking
War driving
Interception compromising emissions
Interception of information
Nation state espionage
Corporate espionage
Espionage
Rogue hardware
Software interception
Interfering radiations
Replay of messages
Network reconnaissance and information gathering
Man in the middle/ session hijacking
Repudiation of actions
Outages
Lack of human resources
Lack of network capacity
Lack of processing power
Lack of storage capacity
Lack of physical resources
Power
Water
Cooling
Lack of resources/ electricity
Internet outage
Loss of support services
Absense of personnel
Strike
Network outage
Physical attacks
Unintentional damages (accidental)
Information leakage or sharing
Erroneous use or administration of devices and systems
Using information from an unreliable source
Unintentional change of data in an information system
Inadequate design and planning or lack of adaption
Inadequate specifications
Inadequate usability
Insecure interfaces (APIs)
Policy/procedure flaws
Design errors
Disasters
Natural disasters
Earthquakes
Floods
Landslides
Tsunamis
Lightning strike
Heavy rains
Heavy snowfalls
Heavy winds
Wildfire
Electromagnetic storm
Environm ental disasters
Fires
Dangerours radiation leaks
Pollution
Dust
Corrosions
Unfavourable climatic conditions
Major events in the environment
Explosions
Damage/ Loss (IT Assets)
Damage caused by a third party
External case
Internal case
Loss from DRM conflicts
Loss of (integrity of) sensitive information
Loss or destruction of devices, storage media and documents
Loss of information in the cloud
Information leakage
Failures/ Malfunctions
Failures of parts of devices
Linecards
Connectors
Failures of devices or systems
Network devices
Servers
Data centers
Failures or disruptions of communication links (communication networks)
Cable break
Cable cut
Failures or disruptions of main supply
Power
Cooling
Water
Failures of disruptions of service providers (supply chain)
Failures or disruptions of the power supply
Network devices
Servers
Data centers
Malfunctions of devices or systems
Malfunctions of parts of devices
Linecards
Connectors
Failures of hardware
Software bugs
Configuration errors
Misconfiguration

Figure 2: Overview of Threats Assumed for Smart Home Assets

6 Specific smart home threats

By analysing existing literature on smart home and converged media security (See Section 3: Methodology), we have identified specific threats that have been taken into account in existing assessments. These threats include some widely applicable cyber security threats, which manifest in particular ways in the smart home environment, as well as threats that emerged from the specific smart home research.

The threats analysed include those that are applicable to the specific smart home with a focus upon converged media infrastructure, as set out in Section 2. The specific smart home threats encountered in the analysed literature are structured below, according to the categories mentioned in Figure 2: Overview of Threats Assumed for Smart Home Assets. They are presented by means of threat details of particular threats and threat groups.

The sequence of the specific smart home threats presented below is not prioritised because the analysed material has not provided any information that would allow prioritising threats. Given the fact that no significant experience exists in this domain from existing implementations (i.e., through incident statistics in this area), no attempt has been made to introduce any priorities for these threats.

Threat Group: Physical attacks

The majority of smart home assets are physically located objects, which can be physically damaged, and many have a financial value motivating theft. These smart home assets are therefore potentially vulnerable to physical attacks, which may remove or damage the assets, degrading or preventing their functionality. Physical attacks can also disrupt the communications between smart home components.

Some smart home assets, such as smart phones, tablets, removable storage media and computers, may physically move in and out of the home making them more vulnerable when outside. Smart homes may feature sensors on the exterior of the building, which may make them more vulnerable to sabotage or damage than internal components.

Physical access to smart home assets is important as many manufacturers assume that only the device owner will have physical access to the device, thus ensuring security. Physical access to smart home devices can allow for uploading new software[41], adding hardware components, changing device settings, and even extracting encryption keys[42].

Threat Group: Unintentional damage (accidental)

Threat: *Information leakage or sharing*

Smart homes are complex networks of sensors and collect significant information on inhabitants. Inhabitants and visitors may reveal more information to the smart home sensors than they intend or anticipate, and may further share information through incorrect security settings[43].

[41] Lawler, R., “Nest Learning Thermostat has its security cracked open by GTV Hacker”, June 23rd 2014. http://www.engadget.com/2014/06/23/nest-thermostat-rooted/ [accessed 20 October 2014]
[42] Bowers, B., “ZigBee Wireless Security: A New Age Penetration Tester's Toolkit”, 9 January 2012. http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4 [accessed 20 October 2014]
[43] Ward, M., “Why your washing machine is a security risk”, BBC, 4 August 2014. http://www.bbc.com/news/technology-28582479 [accessed 20 October 2014]

Many smart home and converged media devices lack dedicated security software and secure encrypted communications (due to a lack of processing or electrical power, the added cost and decreased convenience of adding encryption, or the difficulty of correctly establishing secure communications). This increases the likelihood of unintentional information leakage.

The way the smart home is organised impacts upon the probability of information leakage. For example, smart home technologies that make use of cloud services for information storage are reliant upon the security of those services to prevent information leakage, in addition to securing information inside the smart home. The greater the number of external connections, the greater the chance of information leakage.

Additionally, the service providers that collect and process smart home data may be acquired by other companies in a way that is unanticipated by the data subject. These companies may then process the data collected in unanticipated ways, and potentially against the interests and wishes of the data subject[44].

Threat: *Erroneous use or administration of devices or systems*

Smart homes are complex systems with multiple devices and technologies, and with complex interoperability between them, through different protocols, which can make administration a difficult task. Smart homes are further complicated through any form of automation or learning, which can be hard to anticipate. Smart home systems can be powerful (heating, lighting, water, physical access) and erroneous use of these can therefore cause physical damage to the systems themselves or to the home environment generally. Despite attempts to make smart home interaction "natural", many of the design techniques and cues that simplify interaction with a graphical user interface are not available with sensor-based systems[45]. For example, multiple errors can occur through voice-controlled smart home systems[46].

Threat: *Using information from an unreliable source*

Automated smart home systems that respond to the behaviour of inhabitants (for example, heating that comes on when an inhabitant arrives home) may be activated on the basis of unreliable sensor readings, leading to un-required activation. Compromised devices can be redirected towards unreliable sources. Smart TVs that allow the broadcaster control over the purported origin of web content would allow a malicious broadcaster to inject any script of his choice into websites accessed through the TV[47] [48].

[44] Davies, S., "Google takes a dangerous stride from your hear to your home". http://www.privacysurgeon.org/blog/incision/google-takes-a-bold-stride-from-your-head-to-your-home/ [accessed 20 October 2014]

[45] Bellotti, V., Back, M. W., Edwards, K., Grinter, R. E., Austin Henderson and Christina Lopez, "Making sense of sensor systems: Five Questions for Designers and Researchers", *Ubiquity*, 20-25 April 2002. http://www3.nd.edu/~cpoellab/teaching/cse40827/papers/bellotti.pdf [accessed 27 October 2014]

[46] Oulasvirta, A., Engelbrecht, K.P., Jameson A., and Möller, S., *Communication Failures in the Speech Based Control of Smart Home Systems*, 2007. http://dfki.de/~jameson/pdf/OulasvirtaEJ+07.pdf [accessed 20 October 2014]

[47] Oren Y., and Keromytis, A. D., "Attacking smart TVs". http://itsecurity.co.uk/2014/06/attacking-smart-tvs/ [accessed 20 October 2014]

[48] Oren, Y., and Keromytis, A. D., "From the Aether to the Ethernet – Attacking the television using Broadcast Digital Television", *23rd Usenix Security Symposium*, 20-22 August 2014. http://iss.oy.ne.ro/Aether.pdf [accessed 20 October 2014]

Threat: *Unintentional change of data in an information system*

As with any complex information system, unintentional changes in data can cause failure, errors and improper functioning within the smart home.

Threat: *Inadequate design and planning or a lack of adaptation*

Inadequate design and planning are key issues for smart homes as they can cause security and privacy problems. Inadequate design can occur at the level of smart home components and services, and at the level of the general installation and integration of the smart home as a whole.

At the component level, poor security design can range from a lack of security methods to poor implementation of security. For example, incorrectly set up Secure Sockets Layer certificates may mean that information is transmitted without encryption[49]. Or a device might ship with unchangeable default passwords[50]. Smart home components may be developed by manufacturers with limited experience of security design, as they add connectivity to their existing products. Alternatively, security features may be limited in order to keep the cost of the devices affordable. Smart TVs may have a combination of over-the-air updates, and a lack of firewalls[51].

With the increase in stand-alone smart gadgets that connect to existing Wi-Fi networks, smart home functionality can be created piece-by-piece in an *ad-hoc* manner by inexperienced users. These users may not plan for the security of the smart home as a whole. The absence of privacy-by-design[52] measures in the smart home also exposes the smart home to unwanted information leakage and its potential misuse.

Threat Group: Disasters (natural, environmental)

Threats from disasters are not particularly prevalent in the current literature on smart home security, with the exception of the potential role of flood detection systems and general emergency alert systems. However, physical smart home assets are as vulnerable to these threats as any other physical device. Smart home components are often integrated into the structure of a building, or otherwise installed in appropriate locations within it (for example, wall mounted sensors). They can also be quite large (e.g., integrated smart heating system) and are therefore difficult to move in response to a disaster. Smart home and converged media systems are sensitive electronics networked together in a complicated arrangement and are therefore vulnerable to changes in the environment. Fire, flood, pollution, dust, corrosion, lightning[53], water, violent physical movement and unfavourable climatic conditions are likely to significantly degrade or prevent smart home functionality and decrease the

[49] Wisniewski, C., *Smart meter hacking can disclose which TV shows and movies you watch*, 8 January 2012. http://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/ [accessed 20 October 2014]

[50] Chirgwin, R., "SmartTV, dumb vuln: Philips hard-codes Miracast passwords", *The Register*, 2 Apr 2014. http://www.theregister.co.uk/2014/04/02/smarttv_dumb_vuln_philips_hardcodes_miracast_passwords/ [accessed 20 October 2014]

[51] Roberts, P., "Samsung Smart TV: Like A Web App Riddled With Vulnerabilities", 1 August 2013. https://securityledger.com/2013/08/samsung-smart-tv-like-a-web-app-riddled-with-vulnerabilities/ [accessed 20 October 2014]

[52] About "privacy-by-design", see, for instance, *Privacy and data protection by design --- bridging policy and technology* (provisional title), a work conducted by ENISA in 2014, to be published on the ENISA website. See also, "7 Foundational Principles". www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles [accessed 20 October 2014]

[53] http://forum.smarthome.com/topic.asp?TOPIC_ID=11132 [accessed 20 October 2014]

lifespan of, or destroy, components. Building management systems may be placed under particular strain from extreme changes in climate and environment. Natural disasters are likely to cause outages in services necessary for the smart home, including Internet connection and electrical power[54] [55]. Additionally, natural disasters can have long lasting impacts[56].

In contrast with physical components, virtual assets in a connected smart home with converged media, can be better protected from physical threats due to external storage in the cloud. The specific location of threat is important for determining the vulnerability of an asset. For example, external information storage is not vulnerable to natural disaster in the location of smart home, but is vulnerable to natural disaster in the location of the server.

Threat Group: Damages or loss (IT assets)

Threat: *Damage caused by a third-party*

(Similar to Threat Group: Physical attack, see above).

Threat: *Loss from DRM (Digital rights management) conflicts*

Media content use in the smart home and converged media environment may be protected by digital rights management methods, both in software and in hardware. Hardware devices can be protected against tampering through certificates and tamper-switches. Improperly implemented DRM might result in the blocking or deletion of legitimately owned media content or in extreme cases to damage to hardware ("bricking")[57]. DRM policies may also prevent access to desired functions[58].

Threat: *Loss of (integrity of) sensitive information*

Smart homes and converged media devices potentially collect and store large amount of sensitive information and this increases the attack surface and the opportunity for information leakage. This can be exacerbated by poor security design, implementation or management and by a lack of encrypted communication[59]. Additionally, it may not be immediately obvious to smart home users what information can be collected by the smart home, and how sensitive this information might be (and therefore what is the appropriate level of protection). Many smart home and converged media devices lack dedicated security software and secure encrypted communications (due to a lack of

[54] Heidemann, J., Quan, L., and Pradki, J., "A Preliminary Analysis of Network Outages during Hurricane Sandy", *USC/ISI Technical Report, ISI-TR-685b*, February 2013. ftp://ftp.isi.edu/isi-pubs/tr-685.pdf [accessed 27 October 2014]

[55] Erjongmanee, S., Chuanyi, J., Stokely J. and Hightower N., "Interference of Network-Service Disruption upon Natural Disasters", *Knowledge Discovery from Sensor Data*, Springer, 2010. http://users.ece.gatech.edu/~jic/katrina.pdf [accessed 27 October 2014]

[56] ENISA, *Annual Incident Reports 2013*, 16 September 2014. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013, p. iii.

[57] North, D., *Using piracy devices could brick your Nintendo 3DS*, 3 July 2011. http://www.destructoid.com/using-piracy-devices-could-brick-your-nintendo-3ds-195895.phtml [accessed 20 October 2014]

[58] Cushing, T., "LG Will Take the 'Smart' Out Of Your Smart TV If You Don't Agree To Share Your Viewing And Search Data With Third Parties", 20 May 2014. https://www.techdirt.com/articles/20140511/17430627199/lg-will-take-smart-out-your-smart-tv-if-you-dont-agree-to-share-your-viewing-search-data-with-third-parties.shtml [accessed 20 October 2014]

[59] Goodin, D., "Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords", 7 July 2014. http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/ [accessed 20 October 2014]

processing or electrical power, the added cost and decreased convenience of adding encryption, or the difficulty of correctly establishing secure communications). This increases the likelihood of unintentional information leakage.

Threat: *Loss or destruction of devices, storage media, and documents*

Smart home and converged media systems are likely to store significant media and documents. Unless stored in external cloud storage systems, these are likely to be retained in the home itself. Documents and media in the smart home may include both physical and digital media. Some smart home devices are mobile and may be exposed to damage or loss outside the smart home, where data leakage resulting from device loss of threat is one of the highest risks[60].

Threat: *Loss of information in the cloud*

Loss of smart home-related information (sensor records, activity, preferences and settings, account details) stored in the cloud can lead to the loss of functionality of cloud-based services[61], or the system to return to factory default. Information in the cloud also likely includes media content, documents and files, which are valuable, and may be either costly, or impossible to replace. Cloud service providers themselves may go out of business, making stored information inaccessible[62].

Threat: *Information leakage*

The smart home offers significant opportunities for surveillance, espionage, law enforcement, social surveillance (voyeurism) and other potential invasions of privacy. In addition to the nefarious activity/abuse threats described below, information could leak from improper destruction of smart home components, particularly memory and storage[63].

Threat Group: Failures/malfunctions

Smart homes and converged media devices are complex systems, reliant upon a number of different inputs, and are vulnerable to failures and malfunctions[64]. In many cases failure or malfunction will result in the smart home service being unavailable. In some cases this will be a minor nuisance, for example being unable to access media, but in others could result in costly damage, for example, a defrosted freezer, or doors that cannot be opened without repair. Impacts will be dependent upon the failure states of the devices and how they are designed to deal with disruption of service, power supply or communication links. Cloud-based smart home and media services are reliant upon the Internet connection for services and may be nearly useless without it. Recovery from failure can be

[60] See: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks [accessed 20 October 2014]

[61] Dabbs, A., "Cloud computing is FAIL and here's why", *The Register*, 16 May 2014. http://www.theregister.co.uk/2014/05/16/cloud_computing_is_fail_and_heres_why/ [accessed 20 October 2014]

[62] Lawton, S., "When Cloud Providers Fail: Creating A Cloud Storage Backup Plan", 7 January 2014. http://www.tomsitpro.com/articles/cloud-storage-backup-plan,1-1529.html [accessed 20 October 2014]

[63] Doner, K., "Information Security and Computer Disposal", *Property Professional*. https://www.npma.org/Archives/Vol.18-1-Donner.pdf [accessed 20 October 2014]

[64] Kapitanova, K., Hoque, E., Stankovic, J. A., Whitehouse K., and Son, S. H., "Being SMART about Failures: Assessing Repairs in Smart Homes", *Ubicomp 2012*, 2012. http://www.cs.virginia.edu/~stankovic/psfiles/ubicomp2012-2.pdf [accessed 27 October 2014]

complicated by the design of the system. For example, a device might have to be physically reset or rebooted by the user, who may be physically remote.

A particular issue for smart home services, and for devices in general, is that if the service or vendor company goes out of business then the device may no longer be supported and updated, and spare parts may not be available. This may leave vulnerabilities un-patched or remove particular functionality from the smart home. This may be a particular risk in a relatively emergent market with a large number of start-up companies, which may be at high risk of failure and leave users without services[65].

As with other areas of electronics, the quality of smart home components may be variable and some devices may be more likely to malfunction than others within a category[66]. Smart gadgets might be appealing to counterfeit manufacturers.

Exploiting failure states can facilitate other threats. For example, if a component that has lost network connectivity it may search for other networks to connect to, which may allow it to be hijacked.

Threat Group: Outages

Smart homes are reliant upon a range of resources and services to provide sophisticated functionality. Outages in these inputs can have a negative impact upon the functionality of the smart home.

Threat: *Lack of resources/electricity*

Smart home and converged media systems require electricity. Whilst some of the smaller components can operate on battery power, the larger systems, including integrated home services, and most audio-visual and home networking, will require mains power. Functionality of these devices will be significantly degraded or stop entirely, with a loss of electricity. Major home integrated services such as heating and plumbing also require input from external services to function.

In some cases short term outages will be a minor nuisance, for example being unable to access media, but in others could result in costly damage, for example, a defrosted freezer. The level of disruption is dependent upon the failure states of the devices and how they are designed to deal with disruption of service, power supply or communication links. Recovery from outages can be complicated by the design of the system. For example, a device might have to be physically reset or rebooted by the user, who may be physically remote or unaware of the problem.

Threat: *Internet outage*

Internet outage to the smart home will prevent any remote access to the smart home systems from outside, and will prevent the smart home from accessing an external resources dependent upon an active Internet connection. In particular for converged media, this will include any media content delivered over IP or stored in the cloud.

Threat: *Loss of support services*

Support services includes any cloud services, any monitoring, security or analytics services not locally hosted, and support services (including call centres and helplines) for audio-visual services. This can

[65] https://www.youtube.com/watch?v=WHdU4LutBGU [accessed 20 October 2014]

[66] Hnat, T. W., Srinivasan, V., Lu, J., Sookoor, T. I, Dawson, R., Stankovic, J., and Whitehouse, K., “The hitchhiker’s guide to successful residential sensing deployments”, *InSenSys*, 2011.

also include the business failure of service providers, or their decision to withdraw a particular service. Loss of support services may make the routine operation of the smart home more difficult, but are likely to be particularly problematic in the event of another failure or problem, as the absence of support services will complicate recovery, as advice, guidance, and potential service replacement, may not be available.

Threat: *Absence of personnel*

In the domestic smart home context described in section two, the knowledge and skills required to manage the smart home are likely to be unevenly distributed amongst the inhabitants; for instance, some members of a family may not know how to operate the smart home, or may not be allowed to. The absence of the owner/controller of the smart home, or other knowledgeable inhabitants, may complicate general operation, recovery from error, or response to attacks and threats.

Threat: *Strikes*

In this context, strikes as a threat are most likely to manifest as outages in electricity, support services, or other resources, with impacts as above. Some warning may be available.

Threat: *Network outages*

Network outages in the smart home with converged media may occur as a result of hardware failure or software error, interference, deliberate attack, or power failure. The result would include a loss of local connectivity between smart home components, with a resulting near total loss of smart home functionality. Additionally, network outages outside the home might degrade functionality, depending upon what services, capabilities or information are stored or provided externally.

Threat Group: Eavesdropping/interception/hijacking

Eavesdropping, interception and hijacking are key threats to smart homes and converged media. The large number of sensors, as well as devices that log fine-grained details of the behaviour of people in the home, produces significant information on the inhabitants such as their regular habits, consumer activity, presence or absence, health, and preferences. This information is valuable for several actors, both illegal and illegal. Secondly, smart homes feature high levels of communication between different devices over a range of protocols and technologies. These increasingly include wireless protocols such as Wi-Fi, Z-wave[67], Zigbee, Bluetooth and others.

End devices do not have the processing power (or energy if on batteries) for encryption in the home, which makes them very vulnerable to sniffing, replay attacks, man in the middle and taking control of the gadgets when in physical proximity. Smart TVs and other converged media devices may themselves log viewing habits, and may transmit these logs to the manufacturer, or to a service provider[68]. The physical location of the smart TV, often in the centre of a home, provides a good position for monitoring a location and the activity within it[69].

[67] Fouladi, B., and Ghanoun, S., "Security Evaluation of the Z-wave Wireless Protocol." http://research.sensepost.com/cms/resources/conferences/2013/bh_zwave/Security%20Evaluation%20of%20Z-Wave_WP.pdf [accessed 27 October 2014]

[68] McAllister, N., "You THINK you're watching your LG smart TV - but IT's WATCHING YOU, baby
Phones home with the names of videos you watch, too", *The Register*, 20 Nov 2013. http://www.theregister.co.uk/2013/11/20/lg_smart_tv_data_collection/ [accessed 20 October 2014]

[69] Ferrante D., Auriemma, L., Smart TV IN~~security~~, 2014, http://revuln.com/files/Ferrante_Auriemma_SmartTV_Insecurity.pdf [accessed 20 October 2014]

Lifestyle data gathered from the smart home is likely to be very attractive to advertisers and data-miners[70].

Threat: *War driving*

War driving involves seeking out vulnerable wireless communications in a mobile manner (for example from a moving vehicle or walking with a portable device). The wireless communications protocols in the smart home may extend some distance from the house itself, making them vulnerable to war driving. It is likely that multiple smart homes will be located in the same area, making these areas an attractive target for war driving. If wireless networks are accessed through war driving, then the attackers may be able to effect physical and visible changes to the smart home (e.g. turn lights on/off) that will confirm the physical location of the identified network. War driving may serve as a relatively slow way of identifying unsecured building automation systems[71]. War driving has been demonstrated for the ZigBee protocol[72].

Threat: *Interception of compromising emissions*

It is possible to detect what TV programme is being watched based upon monitoring the electricity consumption of a smart TV[73].

Threat: *Interception of information*

As threats for the general category of Eavesdropping/Interception/hijacking. Smart home and converged media environments contain large amounts of information, which is communicated through multiple protocols with differing levels of security. For example, signals from video-over-IP cameras can be intercepted and received by an attacker[74].

It is difficult to learn that much about individual behaviour from a single smart device, but with multiple devices and some contextual knowledge it becomes easier to make inferences about behaviour. At least sufficient to support aggressive advertising, reminders, deals etc. and this can influence the inhabitants' way of living.

Threat: *Interfering radiation*

Multiple smart home devices from different manufacturers, using different wireless communication protocols may potentially interfere with each other, or compete for bandwidth. Multiple smart homes in close proximity may experience interference between Wi-Fi on the same channel causing the signal

[70] Ward, M., Op. cit., http://www.bbc.com/news/technology-28582479 [accessed 20 October 2014]

[71] Storm, D., "Botnets coming soon to a smart home or automated building near you", Computerworld, 4 June 2014. http://www.computerworld.com/article/2476386/cybercrime-hacking/botnets-coming-soon-to-a-smart-home-or-automated-building-near-you.html [accessed 20 October 2014]

[72] Goodsspeed, T., "Wardriving for Zigbee", 23February 2012. http://travisgoodspeed.blogspot.co.uk/2012/02/wardriving-for-zigbee.html [accessed 20 October 2014]

[73] Brinkhaus, S., Carluccio, D., Greveler, U., Justus, B., Löhr, D., Wegener, C., "Smart Hacking For Privacy". http://events.ccc.de/congress/2011/Fahrplan/attachments/1968_28c3-abstract-smart_hacking_for_privacy.pdf [accessed 20 October 2014]

[74] Larose, C., Veness, A., "Internet Peeping Toms and The Internet of Things Face New Hurdles: FTC Settles with TRENDnet, Inc.", 10September 2013. http://www.privacyandsecuritymatters.com/2013/09/Internet-peeping-toms-and-the-Internet-of-things-face-new-hurdles-ftc-settles-with-trendnet-inc/ [accessed 20 October 2014]

quality to degrade. Deliberate jamming of smart home communications may also be possible[75], and jamming devices designed for common smart home frequencies are available for sale[76].

Threat: *Replay of messages*

Replay attacks involve replaying captured packets back to a smart home network in order to replay the previous activity. Smart home wireless communications protocols, including ZigBee have minimal protection against replay attacks[77]. These can attack wireless communication components from within radio range of the smart home[78]. Replaying control signals in smart homes may allow for the bypassing of locks and other security systems.

Threat: *Network reconnaissance and information gathering*

Network reconnaissance in the smart home and converged media context involves building up a model of the smart home network, its systems and services, and its vulnerabilities. Network reconnaissance may be the precursor to other forms of attack. Internet connected devices with poor security (including smart TVs[79]) may facilitate reconnaissance of other devices connected to the same network.

Threat: *Man-in-the-middle/session hijacking*

Man-in-the-middle attacks involve an attacker making independent connections with two parties or devices and relaying communications between them. This allows the attacker to eavesdrop on communications and control other elements of the communication. In this smart home context this might include common devices which lack properly implemented encrypted communications[80] [81]and end point authentication, such as unencrypted wireless access points, and baby monitors [82]. Vulnerabilities that could allow man-in-the-middle attacks have been identified in the ZigBee and Z-Wave protocols[83].

[75] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G., "A survey on jamming attacks and countermeasures in WSNs", *Communications Surveys & Tutorials*, IEEE, vol.11, no.4, pp.42, 56, Fourth Quarter 2009.

[76] See for instance: http://www.jammer-store.com/868mhz-car-remote-control-jammer.html [accessed 20 October 2014]

[77] Bowers, B., "ZigBee Wireless Security: A New Age Penetration Tester's Toolkit", 9 January 2012. http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4 [accessed 20 October 2014]

[78] Reuter, T., *Security analysis of wireless communication standards for home automation*, Der Technischen Universität München, 15 November 2013, p.5 https://www.sec.in.tum.de/assets/Uploads/MAThomasReuter.pdf [accessed 27 October 2014]

[79] Oren Y., and Keromytis, A. D., "Attacking smart TVs", Op. cit. http://itsecurity.co.uk/2014/06/attacking-smart-tvs/ [accessed 20 October 2014]

[80] Petró, D., Vesztergombi, G., and Fritsch, L., *D.3.2 Threat Analysis*, uTRUSTit, 30 April 2011. http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D3.2_Threat_Analysis_final.pdf, p.37[accessed 27 October 2014]

[81] Reuter, Op. cit., p.5.

[82] Hill, K., "Welcome to The Not-So Private Parts where technology & privacy collide", *Forbes*, 29 April 2014. http://www.forbes.com/sites/kashmirhill/2014/04/29/baby-monitor-hacker-still-terrorizing-babies-and-their-parents/ [accessed 20 October 2014]

[83] Fouladi B., Ghanoun, S., Op. cit. http ://research.sensepost.com/conferences/2013/bh_zwave [accessed 20 October 2014]

Devices with insecure failure modes can facilitate session hijacking, for example when removed from a trusted network, which then allows attackers to take control of the device[84].

Threat: *Repudiation of actions*

Repudiation of actions involves the malicious manipulation or falsification of the identification of actions, often involving the deletion of logs. Within the smart home and converged media this would allow for attackers to cover their involvement in an action, including access to smart home services, or to attribute actions to others, including smart home inhabitants[85] [86].

Threat Group: Nefarious activity/abuse

Threat: *Identity fraud*

Smart homes systems may store and manage credentials for various functions and services which the home provides and makes use of. These credentials may be for use internally (identity, user accounts, permissions, preferences and settings or access conditions) or externally (media accounts, cloud storage, billing and home delivery, security alarms, external management or analytics). These credentials are likely to include payment details (credit card or account numbers) which are desirable targets for financially motivated cyber criminals[87]. Information about user behaviour, preferences, habits, travel, media consumption etc., collected and stored in the smart home, may assist more detailed forms of impersonation fraud. A more local form of identity fraud can include the unauthorised use of smart home user accounts belonging to other inhabitants.

Threat: *Unsolicited and infected email*

Smart home devices may have their own email accounts (this is common for web-connected printers and for e-reader devices) and this can be exploited to send messages to these devices, potentially as a form of spam[88], but also as a delivery vector for malware.

Threat: *Denial of service*

Traditional denial of service and distributed denial or service attacks on information systems can be threats to the smart home, given Internet-connected components[89]. Such attacks may be the first step

[84] Upton, L., “Rickmote: Rickrolling Chromecast users”, 16 July 2014. http ://www.raspberrypi.org/rickmote-rickrolling-chromecast-users/ [accessed 20 October 2014]
[85] Mantas, G., Lymberopoulos, D., and Komninos, N., “Security in the Smart Home Environment”, *Wireless Technologies for Ambient Assisted Living and Healthcare,* 2011. http://www.igi-global.com/chapter/wireless-technologies-ambient-assisted-living/47126 [accessed 27 October 2014]
[86] Krishnamurthy, P., Kabara, J., and Anusasamornkul, T., (2002). Security in Wireless Residential Networks. *IEEE Transactions on Consumer Electronics*, *48*(1), 157‑166.
[87] Bodnar, C., “Don’t Shop or Bank With a Smart TV”, 13February 2014. https://blog.kaspersky.co.uk/dont-shop-or-bank-with-a-smart-tv/ [accessed 29 October 2014]
[88] http://www.darkreading.com/risk/printers-could-be-vulnerable-to-spam/d/d-id/1129229 [accessed 20 October 2014]
[89] Fouda, M. M., Fadlullah Z. M., and Kato, N., “Assessing Attack Threat Against ZigBee-based Home Area Network for Smart Grid Communications”, Proceedings of the 6th IEEE International Conference on Computer Engineering and Systems, 30 November – 2 December 2010. http ://www.mostafafouda.com/Pub/Conf/2010.ICCES%2710.pdf [accessed 27 October 2014]

in removing a smart home component from a network, in order to exploit a vulnerability in its disconnected failure state.

The physical elements in the smart home environment also offer the possibility of physical denial of service attacks[90]. If an attacker can gain control of smart home components then she could activate these in order to deny access and use to legitimate users (for example, repeatedly turning lights on and off, lock all access to and from the building[91], turning off heating, changing media source, playing loud music, etc.).

Threat: *Malicious code/software activity*

Malicious code and software activity underpin many of the other threats to the smart home and converged media. Many smart home devices are essentially computers, often running a variant of Linux and with the capacity to perform other functions[92] [93]. They can therefore be reprogrammed by an attacker with access to run software that the attacker desires. This generative functionality has been demonstrated on multiple devices from large manufacturers[94] and is likely to also affect home-built or custom smart environments. This opens up a wider range of threats, including monitoring network traffic, controlling other devices, and extracting information stored in the system (including both sensitive personal data and media content). In addition to accessing the information systems in the smart home, the Internet connected devices can potentially be used for external functions desired by the attacker, for example, hosting malware or illegal websites, operating as part of a botnet, or sending spam emails[95] [96]. For some smart home devices, physical access is advantageous for installing malicious code.

Threat: *Abuse of information leakage*

See also “Information leakage” under “Physical attacks”, and “Unintentional damage”. Information leakage can be exploited for further nefarious activity including crime and surveillance[97].

[90] Wendzel, S., Zwanger, V., Meier, M., and Szlósarczyk, S., “Envisioning Smart Building Botnets”, *Sicherheit 2014*. http://www.wendzel.de/dr.org/files/Papers/EnvisioningSmartBuildings.pdf [accessed 27 October 2014]

[91] Storm, D., “Botnets coming soon to a smart home or automated building near you”, Computerworld, 4 June 2014, http://www.computerworld.com/article/2476386/cybercrime-hacking/botnets-coming-soon-to-a-smart-home-or-automated-building-near-you.html [accessed 20 October 2014]

[92] Stross C., *Trust Me (I’m a kettle)*, December 12, 2013, http://www.antipope.org/charlie/blog-static/2013/12/trust-me.html [accessed 20 October 2014]

[93] Leyden, J., “Patch Bash NOW: ‘Shellshock’ bug blasts OS X, Linux systems wide open”, *The Register*, 24 September 2014, http ://www.theregister.co.uk/2014/09/24/bash_shell_vuln/ [accessed 20 October 2014]

[94] HP, *Internet of Things Research Study*, July 2014. http ://fortifyprotect.com/HP_IoT_Research_Study.pdf [accessed 20 October 2014]

[95]Proofpoint Inc., “Your Fridge is Full of SPAM, part II: Details”, 21 January 2014. http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-part-II-details.php ; Goodin, D., “Is your refrigerator *really* part of a massive spam-sending botnet?”, 17 January 2014. http://arstechnica.com/security/2014/01/is-your-refrigerator-really-part-of-a-massive-spam-sending-botnet/ ; Thomas, P., “Despite the News, Your Refrigerator is Not Yet Sending Spam”, 23 January 2014. http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam [All accessed 20 October 2014]

[96] Hussein, E., Talmat, S., “Behind ADSL Lines: How to Bankrupt ISPs While Making Money”, 28 March 2013. http://blog.ioactive.com/2013/03/behind-adsl-lines-how-to-bankrupt-isps.html [accessed 20 October 2014]

[97] Titlow, J. P.,·“Smart Homes: Our Next Digital Privacy Nightmare”, 18 March 2013. http://readwrite.com/2013/03/18/smart-homes-our-next-digital-privacy-nightmare [accessed 20 October 2014]

Threat: *Generation and use of rogue certificates*

The exploitation of rogue certificates can undermine device signing and encryption and allow attackers access to smart home asserts and communications[98]. This can then be used to force updates, potentially containing malware or undesired functionality, to smart home components.

Threat: *Manipulation of hardware and software*

Vulnerabilities have been identified in many smart TV systems from different manufacturers, which allow for the software running on the TV set to be altered[99]. Smart home hardware may potentially be pre-manipulated during production to include undesired functions, spyware, or hardware backdoors[100]. Smart home inhabitants many manipulate their own hardware (for example, hacking a set-top box to receive additional TV services[101]), which may violate license conditions if this hardware is not fully owned, or is required to be in a particular state to receive services.

Threat: *Manipulation of information*

Smart home sensors could be fed false information, which could be particularly important for access or for bypassing security measures (biometric sensors or facial recognition). Falsification of records could be part of blackmail, fraud or escalation of privileges. Smart home audio-visual systems could be used to display false data. HbbTV broadcasts allow for an attacker to insert malicious content over a large geographical footprint[102].

Threat: *Misuse of audit tools*

Audit tools, such as system logs[103] will collate a large amount of information on behaviour in the smart home from which information on the inhabitants could be extrapolated.

Threat: *Falsification of records*

Falsification of records could be used to plant false records in order to embarrass or blackmail inhabitants, as well as to hide other nefarious behaviour (theft, illegal access, etc.) from the system owner. This is necessary for long-term misuse of smart home assets and is a component of rootkits[104].

[98] Bodnar, C., Op. cit. https://blog.kaspersky.co.uk/dont-shop-or-bank-with-a-smart-tv/ [accessed 20 October 2014]

[99] "European HbbTV Smart TV Holes Make Sets Hackable", http ://it.slashdot.org/story/13/06/05/1216232/european-hbbtv-smart-tv-holes-make-sets-hackable [accessed 20 October 2014]

[100] Sharwood, S., "Don't Brew That Cuppa! Your Kettle Could Be A Spambot", *The Register*, 29 October 2013. http://www.theregister.co.uk/2013/10/29/dont_brew_that_cuppa_your_kettle_could_be_a_spambot/ [accessed 20 October 2014]

[101] Lynn, G., "Davey, E., Pirated Sky TV sold for £10 a month", 10 February 2014. http ://www.bbc.co.uk/news/uk-england-london-26052012 [accessed 20 October 2014]

[102] Oren Y, and Keromytis, A. D., Op. cit., http://www.cs.columbia.edu/~angelos/Papers/2014/redbutton-usenix-sec14.pdf [accessed 27 October 2014]

[103] See, for instance, http://www.smarthome.com/fingerprint-id-door-lock-deadbolt-w-audit-trail-right.html [accessed 20 October 2014]

[104] For more information regarding rootkits, see, for instance, http://www.microsoft.com/security/portal/mmpc/threat/rootkits.aspx [accessed 20 October 2014]

Falsification of records may be used to frustrate computer forensics efforts in law enforcement.[105]

Threat: *Unauthorised use or administration of devices and systems*

In the smart home context admin devices and systems are often either controlled through physically located devices (remote control, tablet, dedicated terminal or hub, smart TV) or control at a distance through smart phone or cloud-based applications. These provide access to control over the smart home's functions. Exploitation of app-based control methods for smart devices is possible to gain access to and control over the device[106]. In some contexts, for example elder-care and medical devices, administration tools might be located off-site to administer a number of smart homes together. Gaining access to these administrative credentials would allow an attacker to control multiple smart homes at the same time.

Threat: *Unauthorised access to the information system/network*

Unauthorised access to the information system in the smart home context allows for the extraction of information about the inhabitants, including their behaviours, preferences, and credentials. It allows the attacker to change settings, and install or manipulate software. Unauthorised access allows the user to replicate all the activity available to the legitimate user, and therefore for act as an inhabitant. They can then access media and other information, cause operations and effect physical changes[107] (including remotely), and can cause downloads, purchases etc., feed false information to sensors, and access information and records. Depending upon the extent to which the smart home design has integrated different accounts and services, then access to the smart home administration potentially offers access to a number of different services. Access can be facilitated by poorly set-up access controls[108].

Threat: *Unauthorised use of software*

Unauthorised use of software that is legitimately installed on smart home components could include remote activation, as well as event logging, identification/authentication methods, use of any installed apps, visualisation tools or web-based control panels. Unauthorised use of existing software could include the exploitation of very common pieces of software[109] [110].

[105] Emspak, J., "A Phone That Lies for You", 1 June 2014. http://www.scientificamerican.com/article/a-phone-that-lies-for-you-an-android-hack-allows-users-to-put-decoy-data-on-a-smartphone/ [accessed 20 October 2014]

[106] Ward, M., Op. cit. http://www.bbc.com/news/technology-28582479 [accessed 20 October 2014]

[107] http://www.theregister.co.uk/2013/08/13/wave_goodbye_to_security_with_zwave/ [accessed 20 October 2014]

[108] Ray, B., "Revealed: Simple 'open sesame' to unlock your home by radiowave", 13 Aug 2013. http://www.hotforsecurity.com/blog/vulnerability-in-vaillant-heating-systems-allows-unauthorized-access-5926.html [accessed 20 October 2014]

[109] Heilman, D., "Hackers Exploit Shellshock, Much More Trouble Awaits", 29 September 2014. http://www.toptechnews.com/article/index.php?story_id=00100018PJ5T [accessed 20 October 2014]

[110] Zolfagharifard E., Woollaston, V.,"Bash bug could be worse than Heartbleed': 'Catastrophic' flaw may threaten the security of millions of internet-connected devices", 24 September 2014. http://www.dailymail.co.uk/sciencetech/article-2769514/Bash-bug-worse-Heartbleed-Catastrophic-flaw-threaten-security-millions-Internet-connected-devices.html [accessed 20 October 2014]

Threat: *Unauthorised installation of software*

See "Badware" (below) for likely threats emerging from unauthorised installation of software. Unauthorised installation of software by inhabitants might compromise licensing agreements or might expose the system to trojans or backdoors included in cracked versions of software[111].

Threat: *Compromising confidential information*

The sensors in the smart home (microphones, video, face recognition, biometrics) in physical space, as well as the activity logging through various devices and accounts allows for the collection of highly granular confidential information on inhabitants and visitors[112] [113]. This information may be stored locally, or transmitted over local networks, and even into cloud storage. This also applies to confidential documents that might be stored on the home network. Attackers could compromise this confidential information through access to any of the relevant components, but particularly through access to physical and remote storage, the network router, or the smart home hub. Attackers may also compromise this confidential information by undermining security measures, including encryption.

Threat: *Abuse of authorizations*

The smart home and converged media context offers a large number of potential user accounts for media services, as well as external smart home services. This increases the number of authorizations that could be misused. This would include the sharing of accounts within or between households when this is not authorised by the content provider. A common example in converged media is the use of one streaming media account by multiple people in different locations[114].

Threat: *Abuse of personal data*

The significant personal data on inhabitants and visitors that could be collected by the sensors and system logs in a smart home[115] could be valuable for a range of purposes that may not be desired by the smart home owner. These purposes include targeted advertising, profiling and categorisation, identity fraud, disclosure of personal information, espionage, journalism, law-enforcement, and general invasions of privacy.

Threat: *Hoax*

The smart home with converged media can support hoax activity in three ways. Firstly, it contains a number of information sources, which could be fed false information, in order to propagate a hoax.

[111] Reisinger, D., "Could your printer be a Trojan horse? Researchers say yes!", 29 November 2011. http://www.cnet.com/uk/news/could-your-printer-be-a-trojan-horse-researchers-say-yes/ accessed 20 October 2014 [accessed 27 October 2014]

[112] O'Hara, K., "Privacy and the Internet of Things", *Internet of Things Ecosystem – the Next 40 Billion Devices*, NESTA, 3 June 2014. http://eprints.soton.ac.uk/365545/1/PRIVACY%20AND%20THE%20INTERNET%20OF%20THINGS.pdf [accessed 27 October 2014]

[113] http://readwrite.com/2013/03/18/smart-homes-our-next-digital-privacy-nightmare [accessed 20 October 2014]

[114] http ://gigaom.com/2012/02/13/tv-everywhere-password-sharing/ [accessed 20 October 2014]

[115] Haowen, C., and Perrig, A., "Security and Privacy in Sensor Networks", *IEEE Computer,* 36(10), October 2003. https ://sparrow.ece.cmu.edu/group/pub/chan_perrig_secure_sensor_article.pdf [accessed 27 October 2014]

For instance, the system that inserts adverts into streamed content on a smart TV could be exploited to push hoax content to the viewer, or web-enabled displays in the home could display false information. Secondly, an attacker could falsely trigger alarm systems in the home[116]; alarms for invisible, odourless dangers such as carbon monoxide would be particularly effective for this. Thirdly, attackers with access to the smart home components could fake a system crash or error, or virus, and then offer to repair this as a method of gaining physical access to the home or further access to other components.

Threat: *Badware*

As many smart home components are functional computers, they can be affected by the full range of malicious software, although some may need to be customised to take full advantage of the smart home context. This can include spyware, adware, ransomware, key and activity logging, traffic monitoring software[117] [118]. As many smart home components lack the capacity to run security software and even lack a graphical display, the presence and activity of this malicious software can remain undetected for long periods of time. It may be possible to utilise the broadcast network to place badware on smart TVs through the HbbTv protocol[119].

Threat: *Remote activity (execution)*

Part of the core selling point of many smart home applications is the ability to remotely activate integrated home systems (heating, lighting, irrigation, etc.) from outside the home. This functionality, if unsecured, or attacked, can allow physically distant attackers to potentially activate any of the remote functions in the smart home[120]. Unwanted activation could be used for denial of service attacks and harassment.

Threat: *Targeted attacks (including Advanced Persistent Threat)*

If attackers are seeking to attack a particular target, rather than any available unsecured victim, then the smart home is highly useful for this. It will often physically surround the target with a sensor infrastructure, collects sensitive information on them, manages permissions for other accounts and services belonging to the target, and potentially allows for control of their environment. Access to the smart home will provide targeted attackers with information on their target useful for reconnaissance as well as potential ways to influence the target’s behaviour. The sensors in a smart home, if compromised, could be particularly useful for the reconnaissance component of Advanced Persistent Threat (APT), whilst the greater attack surface presented by multiple devices could facilitate an attacker gaining presence[121].

[116] http://www.wired.co.uk/news/archive/2014-07/24/home-alarm-hacking [accessed 20 October 2014]
[117] http://www.wired.com/2011/08/hacking-home-automation/ [accessed 20 October 2014]
[118] Wendzel et al, Op. cit. http://www.wendzel.de/dr.org/files/Papers/EnvisioningSmartBuildings.pdf
[119] Oren Y., Keromytis A. D., “From the Aether to the Ethernet – Attacking the television using Broadcast Digital Television”. http://iss.oy.ne.ro/Aether [accessed 27 October 2014]
[120] http://www.wired.com/2014/07/hacking-hotel-room-controls/ [accessed 20 October 2014]
[121]http://resources.infosecinstitute.com/advanced-persistent-threats-attack-and-defense/ [accessed 20 October 2014]

Threat Group: Legal

Threat: *Violation of laws or regulations/breach of legislation*

Smart homes are buildings, and therefore they must be compliant with building regulations, as appropriate to the country in which the building is located. Software controlled systems must remain compliant with these requirements.

Third-party data processing services for the smart home must be compliant with data protection law. This is required for all parties collecting and processing personal data, but in the smart home and converged media context it is particularly significant for cloud services and information storage companies. Part of the requirements of data protection law with the EU is that appropriate security measures must be taken[122] [123].

Threat: *Failure to meet contractual requirements*

Smart home, converged media, and related services offered by third-party companies, may fail to meet contractual requirements promised to the subscriber. This is a particular problem given the small and under-resourced nature of many smart home start-up companies[124]. Smart home inhabitants may themselves fail to meet their contractual requirements in relation to these services, most likely through failure of payment, but also by breaking conditions of use (for example, using HDMI splitters to circumvent a TV provider's single-room license arrangement, or by "jailbreaking" or "rooting" devices).

Smart home technology, presented as a closed-source "black box", may include additional functions and capabilities and they might represent legal risks of which the user may be unaware.

Threat: *Unauthorised use of copyrighted material*

The converged media environment may allow inhabitants to make unauthorised use of copyrighted material such as audio and visual media (films, TV, music, sport) and software[125]. Unauthorised use might include downloading and storing streamed media, storing and displaying pirated content, or accessing content with geographical access restrictions over a virtual private network or proxy[126] [127]. Some smart home communication protocols are proprietary. Manufacturers may include compatibility with these protocols without obtaining the appropriate licensing agreement.

[122] Whitehouse, O., *Security Of Things: An Implementers' Guide to Cyber-Security for the Internet of Things Devices and Beyond*, NCC Group, 2014, p.6. https://www.nccgroup.com/media/481272/2014-04-09_-_security_of_things_-_an_implementers_guide_to_cyber_security_for_Internet_of_things_devices_and_beyond-2.pdf [accessed 27 October 2014]

[123] EU Media Futures Forum, *Fast-forward Europe: 8 Solutions to thrive in the digital world, final report*, September 2012. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753

[124] https://www.youtube.com/watch?v=WHdU4LutBGU [accessed 20 October 2014]

[125] http://inside.org.au/convergence-only-one-part-of-the-media-problem/ [accessed 20 October 2014]

[126] De Kosnik, A., *Piracy is the Future of Television*, C3 Research Memo, 2010. http://www.convergenceculture.org/weblog/2010/12/c3_research_memo_2010_piracy_i.php [accessed 27 October 2014]

[127] http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/forum_final_report_en.pdf [accessed 20 October 2014]

7 Smart home assets exposure to cyber threats

This section presents the threat exposure of smart home assets. The following table (Table 1: Association between Threats and Smart Home Assets) shows the association between the assumed threats from Figure 2: Overview of Threats Assumed for Smart Home Assets and the smart home and converged media assets from Figure 1: Overview of Smart Home and Converged Media Assets.

The table below establishes the relationship between threats and the assets to which these threats apply. To this extent, the table shows the exposure of smart home assets to the assessed threats.

Threat groups are listed in the first column of the following table. Related threats in the second column. Associated assets groups are in the third column. The last column, only when relevant, provides information on some particular assets or some more details on some specific issue. E.g., under the threat group Unintentional damage (accidental) (first column), the threat Information leakage or sharing is listed (second column). An association is made between such threat and the following asset groups (third column): Human-machine interface devices, Information storage, Integrated home services, Information, and Management/operation. The Asset/Detail field (fourth column) is empty here because in this specific case no furher detailed information needed to be mentioned.

This information contained in the table below is important in the process of identification of countermeasures that will reduce the exposure surface of assets. This threat-to-assets association is made on the basis of an initial assessment done within the project. More detailed assessments can follow when additional asset details and/or new threats are being considered. To this extent, the association performed in this report is non-exhaustive and subject to refinements, according to particular smart home and threat environments.

The table below details threats identified in the preceding literature review. Threats that can be logically assumed to apply to smart homes, but for which we did not identify evidence, are not included in this table, but are included in a fuller table available by contacting resilience@enisa.europe.eu . The fuller table has been created as a side-product of this work and may be used as basis for detailed risk assessments in the area of smart homes.

Threat group	Threat	Asset groups	Asset/Detail
Physical attacks (deliberate/ intentional)			
Unintentional damage (accidental)		All physical assets	
	Information leakage or sharing	Human-machine interface devices, Information storage, Integrated home services, Information, Management/operation	
	Erroneous use or administration of devices and systems	All assets (excepting people/living things)	

Threat group	Threat	Asset groups	Asset/Detail
	Using information from an unreliable source	Human machine interface devices, Home networking, Audio/Visual, Information storage, Building security, Information, Management/operation, People/living things	
	Unintentional change of data in an information system	Human-machine interface devices, Home networking, Audio/visual, Information storage, Integrated home services, Tags and markers, Building security, Medical, Information, Management/operation.	
	Inadequate design and planning or lack of adaptation	All assets	
Disasters (natural, environmental)			
Damage/Loss (IT Assets)			
	Damaged caused by a by a third-party	All physical assets	
	Damage from DRM conflicts	Software, Human-machine interface devices, Audio/visual, Information storage, Home appliances, Tags and markers, Information, Management/operation	
	Loss of (integrity of) sensitive information	Audio/Visual, Information storage, Medical, Information	
	Loss or destruction of devices, storage media, and documents	All assets	
	Loss of information in the cloud	Information storage, Information, Management/operation	External cloud storage
	Information leakage	All assets	

Threat group	Threat	Asset groups	Asset/Detail
Failures/ Malfunctions			
Outages			
	Lack of resources/electricity	All assets (excepting people/living things)	
	Internet outage	Home networking, Information storage, Management/operation	Internet connection, External cloud storage. Additionally any smart home systems that rely on cloud services will be unavailable.
	Loss of support services	Medical, Management/operation	
	Absence of personnel	Building security, Management operation.	
	Strikes	Integrated home services Management/operation,	Resources
	Network outages	Home networking	Cable connection, Wireless networking, Telephone
Eavesdropping/Interception/ Hijacking			
	War driving	Sensors, Home networking (particularly wireless networking), Tags and markers,	
	Intercepting compromising emissions	Sensors, Human machine interface devices, Home networking, Audio/visual, Home appliances/white goods, Integrated home services, Robotics, Building security, Connected transportation, Information	
	Interception of information	All assets	
	Interfering radiation	Sensors, Audio/visual, Information storage, Tags and markers,	

Threat group	Threat	Asset groups	Asset/Detail
	Replay of messages	All assets	
	Network reconnaissance and information gathering	Home networking, Information, Management/operation	
	Man in the middle/ Session hijacking	All assets	
	Repudiation of actions	All assets	
Nefarious Activity/ Abuse			
	Identity fraud	Human-machine interface devices, Audio/visual, Tags and markers, Information, Management/operation	(set top box)
	Unsolicited and infected e-mail	Human-machine interface devices,	
	Denial of service	Sensors, Human machine, Interface devices, Home networking, Audio/visual, Information storage, Building security, Management/operation	
	Malicious code/ software activity	All assets (excepting people/living things)	
	Abuse of information leakage	Software, Human-machine interface devices, Home networking, Information storage, Information, Management/operation	
	Generation and use of rogue certificates	All assets (excepting people/living things)	
	Manipulation of hardware and software	All assets	
	Manipulation of information	All assets	
	Misuse of audit tools	All assets (excepting people and living things)	
	Falsification of records	All assets (excepting people and living things)	
	Unauthorised use or administration of devices and systems	All assets (excepting people and living things)	

Threat group	Threat	Asset groups	Asset/Detail
	Unauthorised access to the information system/network	All assets (excepting people and living things)	
	Unauthorised use of software	Software	
	Unauthorised installation of software	All assets (excepting people and living things)	
	Compromising confidential information	Information storage, information, human machine interface devices.	
	Abuse of authorisations	All assets (excepting people and living things)	
	Abuse of personal data	People/living things	
	Hoax	People/living things	
	Badware	All assets (excepting people and living things)	
	Remote activity (execution)	Software, Home networking, Audio/visual, Information storage, Home appliances/white goods, Integrated home services, Robotics, Building security, Management/operation	
	Targeted attacks (including APT)	All assets	
Legal			
	Violation of laws or regulations / breach of legislation	Software, Human-machine Interface devices, Home networking, Audio/visual, Information storage, Integrated home services, Robotics, Building security, Medical, Connected transport, Information, Management/operation, People/living things	
	Failure to meet contractual requirements	Management/operation, Hone networking, Integrated home services	Internet connection, Telephone, Electricity, Water, Gas
	Unauthorised use of copyrighted material	Software, Audio/visual, Information storage, Information,	

Table 1: Association between Threats and Smart Home Assets

8 Threat agents

Threats emerge from groups of threat agents. It is important for smart home and converged media asset owners to know which threats emerge from which threat agent group. This information is significant to decide on the kind of risks that should be mitigated: threat agent groups are indicative of the energy behind launched attacks and capability level. The smart home environment, as depicted in our initial scenarios, differs in some significant ways from other cyber security contexts, and this has implications for the nature of the threat agents. The typology of threat agents draws upon but adapts the typology presented in previous ENISA threat landscape reports[128].

Corporations

Corporations are private legal entities, generally motivated by the pursuit of profit and organised accordingly, but this category can include not-for-profits and charitable organisations. The sources of threat from corporate actors can range from the impacts of poor implementation or design of smart home technologies, business models that are not aligned with the interests of smart home inhabitants, through to illegal practices. Corporate actors can be potentially well resourced and competent if the threat emerges from the deliberate actions of the organisation, but corporations can also include elements of insider threat from employees who may have their own divergent agendas. Corporate threat agents can be sub-divided into three categories. The categories are not mutually exclusive and can overlap.

Data miners and advertisers

These threat agents operate with business models that are reliant upon the collection and processing of data from smart home technology, which can also include personal data of individuals. They therefore have an interest in the information that a smart home can produce about its inhabitants and how this can inform the creation and promotion of advertised products and services. They may themselves be service providers, or may be interested in data produced by service providers. The primary threats from these actors include the use and abuse of intentionally shared or unintentionally leaked information from the smart home. Inhabitants may be unaware of how such information may be utilised by corporate actors, and these actors may therefore have strong impacts upon privacy and data protection. These actors may also collect significant personal data, which may then become a valuable asset itself in need of security protection.

Technology vendors and service providers

Service providers and technology developers for the smart home may themselves become threat agents to other smart home assets. The key sources of threat here are in the unintentional category, such as errors in design, installation, administration, maintenance of devices and systems as well as obsolescence of technology over time, and the possibility of these agents being unable to fulfil their commitments (loss of service, a smart home service provider going bankrupt or stopping support for a widely installed product). Failures and malfunctions (including unintended information leakage) can result from design decisions on the part of these actors. Technology vendors and services providers are in an influential position in the smart home context and their actions can have significant impacts upon smart home assets, including their security capabilities. In the context of smart media, threats to smart home assets can emerge from digital rights management or revenue-protection actions.

[128] ENISA, *Smart Grid Threat Landscape and Good Practice Guide*, Op. cit.. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide [accessed 27 October 2014]

Journalists and media

These agents are primarily motivated by the information on people available from the smart home. Their interests are likely to focus upon smart home inhabitants who are in some way notable (celebrities, politicians).

Cyber criminals

Cyber criminals are the largest and most significant hostile threat category in relation to smart homes with a special focus upon converged media.

Financial criminals

Cyber criminals are primarily motivated by financial interest, and threats to smart home assets arise from criminal attempts to extract value from these assets. The full range of potential cyber-criminal activity directed at other types of information systems are also applicable to the smart home, including identity and credential theft, ransomware, malware, using smart home assets to conduct other illegal activity (spam, bot nets, etc.).

Content pirates

In the particular context of converged media and television, media piracy and related types of crime are highly relevant.

Other actors may overstep their legal boundaries and technically become cyber criminals, but their motivations will vary. Cybercriminals can be organised on a local, national or even international level. It should be taken as given, that a certain degree of networking between cybercriminals is being maintained.

Traditional criminals

Traditional criminals are criminal actors that conduct crimes that are not primarily mediated through information technology, but may increasingly contain a technological aspect, and this aspect makes them a threat to smart home assets. For example, a physical burglar, who makes use of a method for circumventing a smart lock, or jamming a video-over-IP system, fits into this category. In the smart home context, traditional criminals are most likely relatively local, and their activity is categorically defined by their physical interaction with the smart home. Their primary motivation is financial, but this category can include other types of socially-motivated crime such as assault, voyeurism or harassment. Threats to smart home assets from this category of threat agent primarily emerge from circumvention of smart home security measures, exploitation of smart home systems to gain information about the home, or theft of valuable smart home components themselves.

Inhabitants

Inhabitants of a smart home may be considered threat agents to assets, which may be located in the smart home, but which the inhabitants themselves do not control or own. Examples of such assets might include licensed audio-visual media, proprietary software in smart home devices, or smart home devices on lease or license. Threats to assets from inhabitants can also be the result of mistakes and errors in set-up and use. Furthermore, the interests of all inhabitants in a single smart home may not necessarily coincide. Inhabitants may use the information gathering capability of the smart home to invade the privacy of other inhabitants, or attempt to overcome content or access restrictions placed on particular media content.

Nation states

Threats to smart home assets from nation states can arise from the state where a smart home is located, as would be the case in law enforcement, or from other countries, in the case of espionage or cyber warfare. Depending upon national context, nation states threat to smart home may be restricted by legal frameworks. Nation states can have offensive cyber capabilities and use them against an adversary. Nation states are becoming a prominent threat agent due to the deployment of sophisticated attacks that are considered as cyber weapons. From the sophistication of these malware it can be confirmed that some nation states have a plethora of resources and they have a high level of skills and expertise. It is too early to determine if smart homes (rather than for example critical national infrastructure) would be perceived as either an effective or legal target for offensive cyber operations.

Hacktivists

Hacktivists are politically and socially motivated individuals who use computer systems in order to protest and promote their cause (but stopping short of terror-provoking violence). Moreover, they usually target high profile websites, corporations, intelligence agencies and military institutions. Threats to smart home assets from hacktivists may include intelligence and information gathering, sabotage, destruction of information, or denial of service attacks.

Terrorists

There is little evidence for a terrorist-conducted cyber attack having occurred, and much terrorist use of the Internet is in the realm of communications activity. It is debatable if cyber attacks would be an effective means for politically or religiously motivated terrorists to achieve their goals. However, it is feasible that terrorist groups or individuals might be motivated to attempt to attack smart home assets. The extent to which this would result in fear-related behaviour change is relatively minimal as the smart home context provides little opportunity for wide-spread damage, injury or destruction. Non-violent actions against smart home assets in this context can be treated as activity by hacktivists.

Threat agents and threat categories

Based on these short threat agent profiles, the threats presented in this document can be assigned to relevant groups. This assignment is based on the threat agent group profile and in particular on assumed motives. The table below (Table 2: Involvement of Threat Agents in the Threats) presents the potential involvement of threat agent groups in the threats considered for smart grid assets.

	Corporations			Cyber criminals		Traditional criminals	Inhabitants	Nation States	Hacktivists	Terrorists
	Data miners	Technology vendors & service providers	Journalists and media	Financial	Content pirates					
Physical attacks		√		√		√	√	√	√	√
Unintentional damage	√	√		√	√	√	√	√		
Disaster										
Damage/Loss (IT-Assets)		√		√		√	√	√	√	√
Failures/ Malfunction		√								
Outages		√		√				√	√	√
Eavesdropping /Interception /Hacking	√		√	√		√	√	√	√	
Nefarious activity/abuse	√		√	√	√	√	√	√	√	
Legal		√					√			

Table 2: Involvement of Threat Agents in the Threats

9 Vulnerabilities and risks in smart homes

This section builds upon the previous accounts of assets, threats, and threat actors, as well as the documentary sources and input from the expert group, to provide an account of the vulnerabilities and risks in smart homes. Risks are understood as emerging when threats abuse the vulnerabilities of assets to generate harm.

It should be noted that the smart home environment is at a relatively early stage of development and adoption. This has implications for mapping vulnerabilities and risks. It is possible to draw from experiences of vulnerabilities and risk in related fields such as home automation and media content provision, however, the nature of the current smart home environment is likely to re-cast some of these risks and vulnerabilities. This section therefore includes consideration of the sources of vulnerabilities in smart home security.

Vulnerabilities

There have been many demonstrations of vulnerabilities in individual smart home components. These have been identified across most of the relevant asset categories in Figure 1: Overview of Smart Home and Converged Media Assets, including IoT devices[129] [130], home automation technologies[131] [132], television[133] [134] [135] and media[136] [137], and in several widely used communications protocols[138]. The majority of these vulnerabilities have been demonstrated by security researchers in lab-based contexts, rather than culled from "real-world" examples. Researchers have then used their judgement, and experiences in other contexts, to extrapolate from these vulnerabilities to the potential harms and impacts that could result from their exploitation. As smart homes are comprised of multiple types of technology (including radio communications, networking, software, hardware, operating systems, protocols, Internet and cloud services, audio/visual etc.), known and unknown vulnerabilities in all these areas are relevant to smart home security.

[129] HP, Op. cit. http://fortifyprotect.com/HP_IoT_Research_Study.pdf [accessed 20 October 2014]

[130] Goodin,D., http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/ [accessed 20 October 2014]

[131] Chirgwin, R., "Nasty holes found in Belkin's home automation kit", 19 Feb 2014. http://www.theregister.co.uk/2014/02/19/wemo_home_automation_is_insecure_ioactive/ [accessed 20 October 2014]

[132] Botezatu, L., "Vulnerability in Vaillant Heating Systems Allows Unauthorized Access", April 16, 2013. http://www.hotforsecurity.com/blog/vulnerability-in-vaillant-heating-systems-allows-unauthorized-access-5926.html [accessed 20 October 2014]

[133] Kuipers, R., Starck, E., Heikkinen, E., "Smart TV Hacking: Crash Testing Your Home Entertainment". http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-smart-tv-fuzzing.pdf [accessed 20 October 2014]

[134] Mocana Corporation, *Vulnerability Assessment of [redacted] Internet-Connected* HDTVs, 14 December 2010. storage.pardot.com/7062/128784/tv.pdf [accessed 27 October 2014]

[135] Darren, P., "Samsung TVs, Blu-ray vulnerable to eternal boot loop", 20 April 2012. http://www.itnews.com.au/News/297710,samsung-tvs-blu-ray-vulnerable-to-eternal-boot-loop.aspx [accessed 20 October 2014]

[136] "DRM Security Issues DRM system cracks: DRM security software & hardware solutions", http://www.locklizard.com/drm_security_issues.htm [accessed 20 October 2014]

[137] Doctorow, C., "What happens with digital rights management in the real world?", 5 February 2014. http://www.theguardian.com/technology/blog/2014/feb/05/digital-rights-management [accessed 20 October 2014]

[138] Fouladi B., Ghanoun, S., Op. cit. http://research.sensepost.com/conferences/2013/bh_zwave [accessed 20 October 2014]

Vulnerabilities arising from business models and economic incentives

Several sources of vulnerability arise from the way that the smart home market is currently configured. The traditional model for home automation was based around a single technology from a single provider, with components integrated through a bus or hub. In this model the main security concerns arise from the security or vulnerability of this hub. A newer model involves connecting together multiple types of devices, often on an existing home network, and making use of cloud services to provide mobile access to these smart systems. This model is gaining popularity because the reduction in cost of low-power processors, memory and networking components has reduced the costs of entry to the smart home market. The cost of adding network connectivity capacity to a device is now around €20 but current customer demand does not yet allow for substantial prices increases for "smart" connectivity. This has brought new entrants to the smart home market, both in terms of large appliance manufacturers adding connectivity to existing home appliances (fridges, washing machines, TVs) as well as smaller start-up companies producing new types of devices. However, these developers may have little experience in security engineering, and/or little budget to devote to security[139]. They are likely to adopt standard, generic hardware and firmware, which may have well-known but unpatched vulnerabilities, or unknown vulnerabilities which, when discovered, will apply to a huge range of different devices.

Secondly, the heavy use of cloud computing resources, for storage and the provision of services, introduces new vulnerabilities[140] [141] [142]. Hacking the cloud server becomes a very effective way of getting access to large numbers of smart homes, and could be done through relatively simply methods of social engineering, phishing, etc. The use of cloud services may include transfers of data across national and jurisdictional boundaries, with resulting implications for data protection and privacy regulation[143]. Although cloud providers are putting effort into cloud security,[144] domestic consumers, or smart home services marketed at consumers, may not adopt more costly cloud security methods and services, or be able to scrutinise the security methods of cloud providers[145].

Vulnerabilities arising from ownership and administration models

Smart homes have an administrative model much closer to that of the home PC and home network than that of enterprise IT. They are unlikely to have dedicated IT or IT security personal, but rather this will be the responsibility of a likely untrained occupant with limited attention and capacity to identify security risks to the smart home or to take action against them. An increased number of non-integrated smart devices connected to cloud services may also increase problems with authentication

[139] https://www.youtube.com/watch?v=WHdU4LutBGU [accessed 20 October 2014]

[140] ENISA Op. cit., 2013, p.49 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats [accessed 27 October 2014]

[141] Subashini, S., and Kavitha, V., "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, 34(1), January 2011. http://www.sciencedirect.com/science/article/pii/S1084804510001281 [accessed 27 October 2014]

[142] Svantesson, D., and Roger Clarke (2010) "Privacy and consumer risks in cloud computing", *Computer Law and Security Review*, 26 (4), 391-397.

[143] Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing, WP196*, 1 July 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [accessed 27 October 2014]

[144] Pucher, A., and Dimopoulos, S., "A Survey on Cloud Provider Security Measures", http://www.cs.ucsb.edu/~koc/ns/projects/12Reports/PucherDimopoulos.pdf [accessed 20 October 2014]

[145] http://www.darkreading.com/cloud/cloud-security-measures-too-opaque-for-customers/d/d-id/1139143 Accessed 20 October 2014 [accessed 27 October 2014]

and password management in this context. For many users, the security models and activity of smart home technology, including devices they may bring into their homes, will be opaque[146]. Many smart devices lack graphical users interfaces, or have limited display capability, making it hard to determine if they are functioning incorrectly or have been compromised. Additionally, smart home technology, particularly sensors, can itself be low profile and not particularly visible. Therefore, occupants will be interacting with smart home devices even when they are not consciously *using* them[147].

The marketing models of smart homes create a picture of smart homes being organised by and for their inhabitants, in order to increase the quality of life of the latter and respond to their needs and problems (such as security, convenience, comfort, entertainment and home administration). This is not the only model for the home automation and monitoring functions of smart homes. Other models may be primarily of benefit to landlords and building owners wishing to mandate or prescribe certain types of behaviour from their tenants. Smart buildings are also likely to be used in business contexts where functions might be used for cost-reduction, environmental sustainability or physical security, but have implications for the privacy of employees.

Many smart home devices and components are vulnerable to an attacker with physical access to the device. Often this will allow the attacker to access stored passwords or cryptographic keys, changes settings, access data, and upload new software. The working assumption appears to be that only asset owners will have this level of physical access, or that the interests of all smart home occupants are the same, and therefore devices do not need to be secured against physical attacks. Physical access to one device of a type (which can be quite affordable) may also be highly advantageous for an attacker targeting that whole range of devices.

In addition, ownership (and therefore responsibility for security) in the smart home context is not always clear. Common beliefs about ownership may not match the legal model. Depending upon particular ownership models, some of the assets in the home may be owned by third-parties (cable and set-top boxes are physical examples of this, and digital media can be rented or supplied with access controls and use limitations). This complicates vulnerability mapping. In some context the inhabitants may be a security risk to the externally owned asset (for example copying and distributing pirated media content), and in others, the external party may be a security risk to the smart home inhabitants. This situation may change the economic incentives to take security action to the extent that additional security vulnerabilities are created.

Pervasive and persistent insecurity

Smart homes increase the number of vulnerable devices within an environment. This is particularly true in comparison with a non-smart home, but also in comparison with a more traditional home network supporting a small number of dedicated computers. This proliferation of devices increases the attack surface for the home. Further, a single compromised device in a smart home may be able to eavesdrop on network traffic and be used as a starting point to compromise other devices. The smart home is therefore as vulnerable as its most vulnerable component and every additional device might introduce a security vulnerability.

[146] O'Hara, Op. cit., http://eprints.soton.ac.uk/365545/1/PRIVACY%20AND%20THE%20INTERNET%20OF%20THINGS.pdf

[147] Nixon, P.A., Wagealla, W., English, C., Terzis, S., *Security, Privacy and Trust Issues in Smart Environments*, p.2. http://www.smartlab.cis.strath.ac.uk/Publications/techreports/SPTPaperFinal.pdf [accessed 20 October 2014]

Given this proliferation of devices, smart home device designers may be tempted to over-rely upon security through obscurity[148], assuming that the range of available targets will obscure their own devices from attackers. The existence of methods for finding and identifying Internet of Things devices, such as the Shodan search engine, suggest this is unwise. Shodan is a search engine for Internet connected devices, including searches based upon known software exploits[149] [150].

As embedded hardware, smart home components can potentially have long service life-spans.[151] They may also be difficult to update or patch if vulnerabilities are discovered[152]. This can leave assets vulnerable for long periods of time. This can be exacerbated by developers no longer supporting an embedded device, going out of business, and having no requirement or economic incentive to continue to update and produce patches[153].

Risks

Understanding risks in the smart home requires an understanding of context and the position of the inhabitants and asset owners. It also requires understanding of the potential harms that can arise from the exploitation of smart home assets.

Crime risks

As set out in Section 5, smart home assets are exposed to threats which can either facilitate criminal actions, or are themselves be a form of crime (e.g. physical damage or theft, unauthorised access to smart home assets). Whilst smart homes may be at risk of crime, it was not possible to comprehensively assess this risk based upon documentation collected. Interviewed experts believe that the current risk of criminal activity directed at the smart home is currently relatively low, given the relatively small number of smart homes. However the increasing number of homes with some kind of Internet connected smart functionality, as well as the corresponding value of identity information, financial tokens and credentials stored in the smart home, may increase financial motivations for crime.

Privacy, surveillance and data protection risks

Smart homes are intended to exploit combinations of small distributed sensing and computational nodes, to identify and deliver personalised services to the users, when they are interacting and exchanging information with the environment[154]. Internet of Things data is high in quantity, quality

[148] Ferrante D., Auriemma, L., Op. cit. http://revuln.com/files/Ferrante_Auriemma_SmartTV_Insecurity.pdf [accessed 20 October 2014]

[149] http://www.shodanhq.com/ [accessed 20 October 2014]

[150] Hill, K., “The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors and Power Plants”, 9 April 2013. http://www.forbes.com/sites/kashmirhill/2013/09/04/shodan-terrifying-search-engine/ [accessed 20 October 2014]

[151] Grossman, W., “Software is forever”, 30 May 2014. http://www.pelicancrossing.net/netwars/2014/05/software_is_forever.html [accessed 20 October 2014]

[152] Roberts, P., “Beware the next circle of hell: Unpatchable systems”, 2June 2014 http://www.infoworld.com/article/2606438/endpoint-protection/beware-the-next-circle-of-hell--unpatchable-systems.html [accessed 20 October 2014]

[153] Fleishman, G., “Security cruft means every exploit lives forever”, 25 September 2014. http://boingboing.net/2014/09/25/security-cruft-means-every-exp.html [accessed 20 October 2014]

[154] Nixon et al, Op. cit.,, http://www.smartlab.cis.strath.ac.uk/Publications/techreports/SPTPaperFinal.pdf [accessed 27 October 2014]

and sensitivity[155]. Given the depth and variety of personal information that can be captured and processed within the smart home, and the potential for privacy violations, potential harms are far from purely technical matters and social context therefore becomes particularly important in assessing risk. Many of the risks presented by the smart home will be of this socio-technical type. Smart homes will produce data on previously unrecorded activities and have a close link between people and their environments[156]. The data produced by activity within a smart home is likely to be perceived as valuable to a number of actors and additional applications may be found, not initially envisaged by designers, service providers or asset owners[157]. This expansion of the uses of smart home data can be understood as a form of "function creep". It complicates understanding potential risks because new uses of previously captured data also produce new risks that were not considered at the time of either device installation, or the point of data capture. Precisely because of the personal, behavioural and granular nature of the data, smart home data is likely to be seen as having predictive value for applications including market segmentation, risk classification, assessments of insurability, and policing and crime control[158]. This type of data processing, can lead to what is known as "social sorting", where people are assigned to different categories, assigned worth or risk, in ways which have significant impacts upon their life chances[159]. These practices can have collective social justice implications as well as individual privacy risks.

Particular issues raised for converged media

From the threat analysis conducted in this study, converged media can be understood as a particular instance of the principles behind smart homes. To the extent that the converged media devices can be understood as a computer, the security and risk profile of converged media resembles that of computing more broadly. The security differences therefore arise from implementation, administration and use models as much as from the underlying technological principles. This section presents specific reflections upon threats, vulnerabilities and other security issues in relation to converged media. In addition to issues around privacy, access and copyright, converged media and television raise related security issues to smart homes in terms of connectivity, embedded functionality, opaque systems and incompatibility with traditional information security approaches.

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. Internet-connected smart televisions in particular have a number of attributes which contribute towards their envisaged role in the smart home.

- **Commonly present**. Televisions are a common feature in many homes and other buildings. They are also often centrally located in commonly used areas of the building.

[155] Kohnstamm, J., and Madhub, D., Mauritius Declaration on the Internet of Things, *36th International Conference of Data protection and Privacy Commissioners*, 14 October 2014. http://www.privacyconference2014.org/media/16421/Mauritius-Declaration.pdf [accessed 27 October 2014]

[156] O'Hara, Op. cit., http://eprints.soton.ac.uk/365545/1/PRIVACY%20AND%20THE%20INTERNET%20OF%20THINGS.pdf [accessed 27 October 2014]

[157] Higginbotham , S., "The Internet of things isn't about things. It's about cheap data", 9 June 2014. https://gigaom.com/2014/06/09/the-Internet-of-things-isnt-about-things-its-about-cheap-data/ [accessed 20 October 2014]

[158] Gandy, O. H., *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*, Farnham: Ashgate, 2009, pp.12-16.

[159] Lyon, D., "Introduction", in Lyon D., (Ed) *Surveillance as social sorting: Privacy, Risk and Digital Discrimination*. London & New York: Routledge, 2003,p.1.

- **Larger display**. In contrast to many other smart devices and home appliances, televisions have larger and higher quality screens which may be better suited to the management and control of other devices, as well as the display of information.
- **Capacity and processing power.** In comparison with smaller, dedicated devices, a larger gateway can support increased processing power, memory and storage capacity. The additional capacity offers some potential to support additional security software.
- **Multi-functionality.** Smart TV offers the potential for a device which replicates the functionality of existing TV, media play, home cinema, music and gaming systems, is connected to the Internet and a range of online services, and may well be integrated with home automation systems as part of a smart home.
- **Integration with other devices**. Smart TVs are capable of being linked to a range of devices (set top boxes, media players, games consoles, external memory) that could potentially be expanded. Internet connectivity and home networking also allow a range of media devices within the home to share content with each other, streaming media to different devices[160].
- **Manufacturer interest.** Smart TV manufacturers have exhibited interest in a broad range of functionalities, including the use of the smart TV as a home gateway[161] [162]. This interest is linked to the potential for the smart TV (including set-top boxes) to provide the broadcaster with greater control over quality and content, and for positive branding[163]. The ability to distinguish new TVs from previous models is also of interest to manufacturers.

The corollary of these attributes is that if smart TV becomes a common coordinating hub for the smart home, as well as supporting multiple media services and account credentials, then it will become a likely target for cyber crime. If this is the case then it should therefore equally be a focus for security efforts[164]. Data on media consumption is particularly attractive for business in this field, both for advertising and revenue purposes.

Specific vulnerabilities have been identified in converged media devices[165] [166]. These have been highlighted in Section 6: Vulnerabilities, but include incorrect security implementation, (for example hard coded passwords[167]), backdoors, mechanisms for the insertion of content[168], remote reporting

[160] Arabo, Abdullahi and Fadi El-Mousa, “Security Framework for Smart Devices”, *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),* 28 June 2012. Available at SSRN: http://ssrn.com/abstract=2173343 [accessed 27 October 2014]

[161] Smart TV Alliance, *Smart Home White Paper*, January 2014 https://sdk.smarttv-alliance.org/download.php?file=Smart_TV_Alliance_Smart_Home_White_Paper.pdf [accessed 27 October 2014]

[162] Hunter, P., “Smart home gateway emerges at Broadband World Forum”, http://www.v-net.tv/smart-home-gateway-emerges-at-broadband-world-forum [accessed 20 October 2014]

[163] “STB and Smart TV Survey 2013”, http://advanced-television.com/wp-content/uploads/2013/08/Euro0813.pdf [accessed 20 October 2014]

[164] Sutherland, I., Read, H. and Xynos K., “Forensic analysis of smart TV: A current issue and a call to arms”, *Digital Investigation*, 11(3), September 2014, http://www.sciencedirect.com/science/article/pii/S1742287614000620 [accessed 27 October 2014]

[165] Ashford, W., “ICO investigates claims of data breach by LG smart TVs”, 21 November 2013. http://www.computerweekly.com/news/2240209447/ICO-investigates-claims-of-data-breach-by-LG-smart-TVs [accessed 23 October 2014]

[166] storage.pardot.com/7062/128784/tv.pdf [accessed 23 October 2014]

[167] Chirgwin, Op. cit, http://www.theregister.co.uk/2014/04/02/smarttv_dumb_vuln_philips_hardcodes_miracast_passwords/ [accessed 23 October 2014]

[168] Darren, P., “HbbTV holes make tellys hackable”, 5 June2013. www.scmagazine.com.au/News/345632,hbbtv-holes-make-tellys-hackable.aspx [accessed 23 October 2014]

of viewing habits, security by obscurity[169], and other security flaws[170] [171]. Many smart TVs, for example, use custom user interfaces and operating systems which may allow little security control to the user, or may have undiscovered vulnerabilities. For example, an on screen web-browser might obscure the URL of a visited webpage, allowing for easier spoofing. If smart media devices have the capacity to install third-party applications then this raises the danger of spyware hidden in malicious apps, as has been experienced on smart phones.

The field of converged media is a point of contention between different actors in the smart home with potentially different security interests and incentives. Converged media is typified by a wide and shifting set of publishers, content producers, content providers, distribution channels, and hardware manufacturers[172]. Security conflicts can emerge between the industry and users, with digital rights management and revenue protection activities being a particular source of contention if these are not handled sensitively, and with an eye to general security. The result of this environment is that the converged media device is unlikely to be under the full control of the user[173]. This raises the question of who carries responsibility for security in this environment, and the extent to which converged media actors can and should act in this role.

[169] Ferrante D., Auriemma, L., Op. cit. http://revuln.com/files/Ferrante_Auriemma_SmartTV_Insecurity.pdf [accessed 23 October 2014]

[170] Roberts, P., https://securityledger.com/2013/08/samsung-smart-tv-like-a-web-app-riddled-with-vulnerabilities/ [accessed 23 October 2014]

[171] http://blog.kaspersky.com/dont-shop-or-bank-with-a-smart-tv/ [accessed 23 October 2014]

[172] OECD, "Connected Televisions: Convergence and Emerging Business Models", *OECD Digital Economy Papers*, No. 231, OECD Publishing, 2014. http://www.oecd-ilibrary.org/science-and-technology/connected-televisions_5jzb36wjqkvg-en [accessed 27 October 2014]

[173] https://www.techdirt.com/articles/20140511/17430627199/lg-will-take-smart-out-your-smart-tv-if-you-dont-agree-to-share-your-viewing-search-data-with-third-parties.shtml [accessed 23 October 2014]

10 Good practices in smart home and converged media security measures

The following section presents good practices in smart home and converged media security measures that have been identified in the literature search and in discussion with the expert group. This report has not independently evaluated these measures and so cannot necessarily recommend these measures. Rather, the report presents an overview of efforts and recommendations in the field. The good practices are structured according to the type of security measure.

Smart home and converged media design and architecture choices

Several good practices for security measures involve making good choices and decisions at the level of the design of the smart home as a system, including how the various components are to be integrated together. These good practices suggest ways in which the smart home might be designed in order to increase security and reduce impacts upon privacy. They are therefore directed at smart home designers and owners.

Design considerations include: careful consideration of the security of cloud-based smart home designs, and maximising the extent to which automation and data storage can remain local and under control of the smart home owner; reducing the number of external services used in the smart home design may decrease the attack surface; using a single type of smart home technology may minimise the points of vulnerability that arise from mixing together multiple technologies and protocols; the choice of Open Source protocols over closed-source or proprietary protocols so that the implementation can be inspected and the communications behaviour understood; better interface design so that smart home users can better understand the operation of their devices and exert better control over their activity; and limiting the proliferation of passwords that results from multiple services and accounts.

Another architectural choice can include an application isolation framework (as is developed in smart cars[174]), to keep critical software separate from non-critical apps. In the context of the car, this keeps the music player or climate control from running on the same system as the brakes or steering; in the smart home it might separate media and music systems from security or integrated appliances. Architectural choices can also include the adoption of privacy-by-design approaches to developing the smart home and converged media. These approaches have been detailed for smart grids[175] and approaches may also be applicable in the smart home context. The NCC Group report, *Implementers guide to cyber security of Internet of things devices*, provides design and implementation advice, including considerations for smart homes[176].

[174] Dietzel, S., Kost, M., Schaub, F. and Kargl, F., "CANE: A Controlled Application Environment for Privacy Protection in ITS", *Proceedings of the 12th International Conference on Intelligent Transport Systems Telecommunications,* 2012. http://www.dbis.informatik.hu-berlin.de/fileadmin/research/papers/conferences/2012_11_Dietzel_Kost_Schaub_Kargl_ITST.pdf [accessed 27 October 2014]

[175] Cavoukian, A., *Smart Meters in Europe: Privacy by Design at its Best*, April 2012. http://www.privacybydesign.ca/content/uploads/2012/04/pbd-smartmeters-europe.pdf [accessed 27 October 2014]

[176] Whitehouse, O. *Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond*, 2014, An NCC Group Publication https://www.nccgroup.com/media/481272/2014-04-09_-_security_of_things_-_an_implementers_guide_to_cyber_security_for_Internet_of_things_devices_and_beyond-2.pdf [accessed 27 October 2014]

Good practices for the consumer include choosing systems that allow secure communication, local access, are not dependent upon cloud services and use security features when they are available (which may well be deactivated by default).

Architecture and design good practices may contribute towards mitigating threats from physical attack, unintentional damage, Failures and malfunctions, eavesdropping/interception/hijacking, nefarious activity, outages and disaster. They may contribute in particular to threats from information leakage, loss of support services, inadequate design and planning, or lack of adaption.

Device security measures

A second set of good practices in security measures involve measures at the level of the individual smart device. These measures are directed towards the device manufacturers, but can also guide the selection of devices by smart home designers and owners. Given the Internet-connected nature of many smart home devices, these practices overlap somewhat with network and communications security measures below, and also involve measures on the part of the device vendor and associated service providers. An example of this is HP's account of its activity in protecting Internet-connected printers from spam. In this context this includes restricted access to the printer, deletion of printer content, and activity monitoring conducted by the service provider as well as management tasks delegated to the user, such as not publicly posting the email address of the printer and keeping the printer physically secure[177]. Security measures at the device level can also include improved user interfaces, as well as activity and state alerting (for example, an alert when a device has failed). Many of these good practices include the application of basic information security measures to smart home components[178], including:

- Design with security in mind
- No fixed, default passwords
- No storage of default passwords in the device firmware
- Use encrypted communication with proper implementation
- Secure IP gateways
- End-to-end authentication, no http access without authentication
- Strong key implementation
- Apply updates to apps and firmware as available[179]
- Message authentication[180]

Device security measures may mitigate against threats from unintentional damage, failures/malfunctions, eavesdropping/interception/hijacking, nefarious activity/abuse, and damage/loss of IT assets.

[177] HP, "Protecting Your Web-Connected Printer from Unwanted Email", http://h10025.www1.hp.com/ewfrf/wc/document?cc=us&lc=en&docname=c03600177#N55 [accessed 20 October 2014]

[178] Ward, M., "How to hack and crack the connected home", 17 August 2014. http://www.bbc.com/news/technology-27373328 [accessed 20 October 2014]

[179] "Belkin fixes WeMo security holes, updates firmware and app", 19 February 2014. http://www.networkworld.com/article/2226374/microsoft-subnet/belkin-fixes-wemo-security-holes--updates-firmware-and-app.html [accessed 20 October 2014]

[180] Brown, J., Bagci, I. E., King, A. and Roedig, U., "Defend your Home!: Jamming unsolicited messages in the smart home", *Proceedings of the 2nd ACM workshop on hot topics in wireless networking security and privacy,* 2013, http://dl.acm.org/citation.cfm?id=2463185 [accessed 27 October 2014]

Network and communications security measures

The third category of good practices involves network and communications security measures in the smart home and converged media. These good practices relate to how the various smart home assets are interconnected, and how they communicate and are therefore addressed to both smart home technology manufacturers and vendors, as well as to smart home installers, designers and owners. Several sources emphasise the importance of ensuring that security measures provide for the maintenance of the following essential properties[181] [182]:

- Confidentiality
- Integrity
- Authentication
- Authorisation
- Non-repudiation
- Availability

Similarly, Duo Security identified the following security areas as starting points for Internet of Things security[183]:

- Proper encoding of web service credentials
- Secured local video streaming
- Easy-to-manage firmware upgrades
- Mobile device access and authentication
- Strong password policies for device authentication
- Strong WiFi security
- Secured 3rd party service connections
- Encrypted storage of customer data
- Customer data segmentation with back end systems

Some sources recommend that given the proliferation of connected devices in the smart home, the focus of security should be upon the control of key access points such as the residential gateway, home hub, or smart TV if performing this function. The argument is that security may be better performed at the network level rather than at the end point due to the variety of devices of different types and the limited support for end point security functions on those devices[184].

Various network security measures have been identified as appropriate for increasing security in the smart home, such as white lists for external access to smart home devices, and secure profile management[185]. Remote logging of activity on smart home components and event management software to detect and prevent anomalous or undesired activity may be desirable.

[181] Mantas, G., Lymberopoulos, D., and Komninos, N., Op. cit. http://www.igi-global.com/chapter/wireless-technologies-ambient-assisted-living/47126 [accessed 20 October 2014]

[182] Whitehouse, O., Op. cit. https://www.nccgroup.com/media/481272/2014-04-09_-_security_of_things_-_an_implementers_guide_to_cyber_security_for_Internet_of_things_devices_and_beyond-2.pdf [accessed 20 October 2014]

[183] Martins, F., "How PKI Can Fix Security in the Internet of Things", August 13, 2014. https://blog.digicert.com/how-security-can-fix-Internet-of-things/ [accessed 20 October 2014]

[184] Spencer, L., "IoT security under scrutinity as Apple looks at smart home systems", 27 May 2014. http://www.zdnet.com/iot-security-under-scrutiny-as-apple-looks-at-smart-home-system-7000029859/ [accessed 20 October 2014]

[185] Ziegler, M., Mueller, W., Schaefer, R. and Loeser, C., " Secure Profile Management in Smart Home Networks", *Sixteenth International Workshop on Database and Exert Systems Applications*, 2005. http://adt.cs.upb.de/wolfgang/sun2005a.pdf [accessed 27 October 2014]

Various specific security models for smart homes have been proposed, particularly in the academic literature. Examples include product-based security models[186], and context-aware approaches to authentication and access control[187]. The uTRUSTit project aimed to test user trust perception in the Internet of Things and provide guidance on producing trusted IoT. The project created a set of collected threat and control objectives which are applicable to smart homes[188].

Finally, there are measures which propose to take advantage of the smart home assets and infrastructure to increase privacy. In one case, this involves using the smart home as privacy proxy for the individual, acting as an intermediary and enforcing the use of desired privacy policies[189].

Network and communication security measures may primarily mitigate threats from eavesdropping/interception/hijacking and nefarious activity/abuse, as well as from legal; failures/malfunctions; and unintentional damage.

Policy measures, including standardisation

In addition to the technological and design best practices, several policy measures have been identified that seek to improve smart home and converged media security. Many of these are certification or standardisation approaches that seek to make good practices more widespread through the smart home industry, but others are political or economic activities. The latter case includes the argument for placing economic pressure upon Internet service providers to increase security[190].

The Consumer Electronics Association and Computer Technology Industry Association introduced a new “Digital Home Technology Integrators” certification for individuals and companies installing home networks and connecting consumer electronics devices to a central PC, which has particular relevance to audio-visual installation[191].

CENELEC (The European Committee for Electrotechnical Standardization) established a SmartHouse Roadmap project, to provide strategic direction and co-ordination for the standardisation activities of the European standards organisations (ETSI, CEN and CENELEC), in relation to smart homes[192]. The intent of this roadmap is to identify relevant standards in the area and encourage interoperability. The

[186] Pishva, D., Takeda, K., “Product based security models for smart home appliances“, *Aerospace and Electronic Systems Magazine, IEEE,* Vol 23, No. 10. 2008 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4665323&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4665323 [accessed 27 October 2014]

[187] Al-Muhtadi, J., Ranganathan, A., Campbell, R., Mikunas, M.D., “Cereberus: A context aware security scheme for smart spaces“, *Pervasive Computing and Communications*, 2003. http://faculty.ksu.edu.sa/jalal/PublishingImages/cerberus.pdf [accessed 27 October 2014]

[188] Petró, D., Vesztergombi, G., and Fritsch, L., Op. cit. http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D3.2_Threat_Analysis_final.pdf [accessed 20 October 2014]

[189] Bagüés, S. A., Zeidler, A., Valdivielso F., and Matias I. R., “Sentry@Home - Leveraging the Smart Home for Privacy in Pervasive Computing”, *International Journal of Smart Home*, 1(2), July 2007, http://journal.sersc.org/IJSH/vol1_no2_2007/IJSH-2007-01-02-05.pdf [accessed 27 October 2014]

[190] Roberts, P. Op. cit. https://securityledger.com/2013/08/samsung-smart-tv-like-a-web-app-riddled-with-vulnerabilities/ [accessed 20 October 2014]

[191] Kolbasuk McGee, M., “In-Home Techies Get New Professional Status”, 12 March 2007. http://www.informationweek.com/in-home-techies-get-new-professional-status/d/d-id/1053208 [accessed 20 October 2014]

[192] CENELEC, *SmartHouse – the way forward: Project SmartHouse Roadmap*, ftp://ftp.cencenelec.eu/CENELEC/SmartHouse/SmartHouseBrochure.pdf [accessed 20 October 2014]

Roadmap project addressed security standards that CENELEC considered relevant for smart homes[193], including authentication-related standards[194]. CENELEC has developed, in cooperation with the European Commission Directorate-General for Enterprise and Industry (DG ENTR), a Code of Practice for Smart Houses. Section 3.4 of the Code of Practice engages with system security, and the Code of Practice recommends that security services and model should be selected according to threats, needs, knowledge and costs, and that users should read and adopt user security guidelines. Following the project the coordination of the standardisation activities around SmartHouse were taken over by CLC/TC 205 "Home and Building Electronic Systems (HBES)" Working Group 2, which was tasked with coordinating the introduction of the output of the SmartHouse Roadmap project into the regular standardisation work of CENELEC.

Similarly, the ICTSB (the Information & Communications Standards Board) has conducted a review of existing standards, which may be applicable to smart homes. For the ICTSB, standards for smart homes should be seen in conjunction with standards for digital broadcasting, mobile communications, Internet, PCs, Protected distribution systems, and voice services[195].

IEC *Technical Specification IEC TS 62045-1 Multimedia Security – Guidelines for privacy protection of equipment and systems in and out of use*[196], is intended to respond to the increase in consumer multimedia products that store users' private information, which should be protected from unauthorised or illegal use. The technical specification describes the system model and general methods for the user's privacy protection of data storage, equipment and systems, both in and out of use.

Finally, good practices have been identified that relate to the structure of the smart home industry and how this can be better coordinated in order to improve security. BuildItSecure.ly is a US-based initiative, which aims to improve the interaction between small Internet of things developers and vendors on one hand, and the security research community on the other. The initiative aims to create mechanisms that allow for security researchers to communicate security vulnerabilities that they have identified, to the vendors, and to facilitate knowledge transfer between the two communities[197].

Policy measures, including standardisation, may mitigate threats from unintentional damage, failures/malfunctions, eavesdropping/interception/hijacking, legal, nefarious activity/abuse, outages, damage/loss, and disaster.

[193] Ibid.

[194] CENELEC Work Shop - Smart House, Final Report, July 2003. http://www.ictsb.org/activities/Smart_House/Documents/Annex_Authent.pdf [accessed 20 October 2014]

[195] ICTSB, *Design for All – Final Background Report*, 15 May 2000, http://www.ictsb.org/activities/Design_for_All/Documents/15%20Smart%20Housing.pdf

[196] IEC, Technical Specification IEC TS 62045-1 "Multimedia Security – Guidelines for privacy protection of equipment and systems in and out of use". http://webstore.iec.ch/preview/info_iec62045-1%7Bed1.0%7Den.pdf [accessed 27 October 2014]

[197] For more information, see: http://builditsecure.ly/ [accessed 20 October 2014]

	Design and architecture	Device security measures	Network and communications	Policy measures/ Standardisation
Physical attacks	√			
Unintentional damage	√	√	√	√
Disaster (natural/environmental)	√			√
Damage/loss of IT assets		√		√
Failures/malfunctions	√	√	√	√
Outages	√			√
Eavesdropping/interception/ hijacking	√	√	√	√
Nefarious activity/abuse	√	√	√	√
Legal			√	√

Table 3: Good Practice Measures against Threat Categories

11 Gap analysis

The study has identified the follow areas of smart home threats, security, and good practice where further research and investigation is required.

- **The role of the smart home in emergency response.** To what extent can the capabilities of smart homes be harnessed to support emergency responses, either in the context of an individual location, or across locations in the case of a larger incident? To what extent can information from the smart home be securely shared with incident responders whilst respecting occupant privacy? Might smart home systems cause additional difficulties for emergency response, and would this require additional training or design consideration?
- **The impacts of natural disasters upon the smart home**. As complicated electronics, smart home components are likely to be vulnerable to the impacts of natural disasters, however more research may be necessary to determine the particular impacts and to increase the resilience of smart homes. This research should also consider the way in which smart homes may contribute towards mitigating the impacts of natural disasters.
- **The criminology of the smart home.** In a similar manner to how computing opens up the potential for new types of crime as well as new approaches to traditional crimes, the smart home will have impacts upon criminal behaviour in relation to the home. Understanding the changes in criminal behaviour (and associated policing practices) will reduce the negative impacts of smart home crime and allow designers to take mitigating steps.
- **The role of the smart home in critical infrastructure.** Smart homes will be associated with smart grids, but will also be connected to other elements of critical infrastructure. Can the smart home play a role in contributing to the protection of critical infrastructure, or will the differential demands of the smart home place new pressures upon critical infrastructure that was designed around the needs and requirements of the non-smart home?
- **Liability and insurance issues related to the smart home.** Liability is a particular issue for smart homes involving automation and learning behaviour, where systems are likely to make decisions or act as proxies for their owners. Given that smart homes might include electricity, heating, lighting, and water services which can be damaging and costly, the implications might be significant. Insurance policies might encourage the adoption of particular smart home technologies (for example connected fire, smoke or flooding alarms) in order to reduce policy costs. The implications, processes and extent to which alternative approaches are available should be considered. Related to liability, are questions of contract law, lock-in, and the ability to change service providers for smart home functions.
- **Law, policy and the smart home.** The extent to which existing laws and policies are impacted by developments in the smart home, and the bearing these laws and policies have upon smart home security, should be considered. Of particular interest is the extent to which existing cyber security policies, including national cyber security strategies, encompass smart homes. As international law on cyber conflict develops, consideration should be given to increasingly smart homes.
- **Baseline requirements for manufacturers** should be explored, to ensure that smart home components meet existing and newly developed standards for home appliances and infrastructures. To what extent would product, device, protocol, or service certification improve the standards of smart home security? What should be the contents of such certification and where can it best be targeted? The content of standards should be regularly revised as technology develops. The possibility of technology forcing through standards and regulation should be investigated.

- **User education for the smart home.** As complex interconnected systems, smart homes may require users to be educated in home to operate their smart home safely, securely, and maintain their desired level of privacy and data protection. User education approaches may need to differ from those addressed to home PCs or enterprise IT and these requirements should be explored and addressed. What are the limits of user education in relation to smart home privacy, and what behaviour can be reasonable expected?
- **Training at various levels.** To what extent are existing information security training approaches applicable to and relevant to the smart home, and in particular to the design of smart home components and appliances? Do new training approaches need to be developed, and if so, for whom? What training is available for smart home vendors and installers and is this training creating an adequate level of smart home security?
- **Further development of good practices.** The previously identified good practices address some areas of smart home security, and if applied more widely would have significant impact. However these practices should be further developed and explored. Mechanisms for sharing and expanding good practices in smart home security should also be explored. In a related manner, what work is necessary to make existing security measures and approaches smart home ready?
- **Smart home security diagnostic and forensic methods.** To what extent are existing methods for understanding security events and discovering the source of these events suitable for use in the smart home context? Do new approaches (including processes and procedures) need to be developed? Can methods and systems be developed which allow smart home inhabitants to better understand the security behaviour of their smart home?
- **The interface between the smart home and the smart city.** Smart cities are developing in parallel with smart homes and utilise some shared technologies. To what extent are the smart home and the smart city connected, integrated or communicating, and what issues of security and privacy does this relationship raise?
- **Security management methodologies**, including better approaches to patching, updates, provision of information to asset owners, incident logging and report, should be developed that specifically cater to the smart home context.
- **Longer term studies** of the impacts of smart home security and particularly the impacts upon privacy. It is currently too early in the wide-scale deployment of smart homes to fully understand the implications, however research should attempt to identify the practical implications upon privacy and the effects of security failures, in order to supplement and expand the information available on potential vulnerabilities and to allow trend mapping.

12 Conclusions

Based on the experience gained within this activity and in addition to the asset, threat and vulnerability assessment pursued through the report, the study has identified additional cross-cutting conclusions on threats to the smart home and converged media.

The study identified **threats to all of the asset classes** and high threat exposure across all devices, including to humans inhabitants. A smart home will likely contain a large, complex and diverse attack surface. The potential for abuse of smart homes should be considered high. The smart home offers personalised and context-informed attack vectors. The increasing number of smart homes, and smart devices within homes, particularly converged media, will increase the return of targeting smart home vulnerabilities. The security management of these assets is not yet mature and requires further attention.

Not all smart homes are created equally. There are multiple design pathways that lead to functional smart homes (ranging between localised and integrated home-automation systems, to sets of devices based upon a shared interoperability protocol, and cloud-based gadget-and-app approaches with *ad-hoc* integration). These pathways have their own security and privacy peculiarities, but also have shared issues and vulnerabilities. Design choices in the make-up of the smart home are likely to have significant impacts both on individual security and upon the collective security ecosystem. For example, a cloud provider might become a single point of access for multiple smart homes as a result of individual design choices, with the result that that provider's security decisions will have widespread impact.

We might be unaware of how "smart" the home already is. In many ways, the underlying technologies and **elements of the smart home are already available** and increasingly in place. This is particularly the case in relation to converged media devices. Further services and products are likely to be developed based upon these technologies. The smart home is not just about objects, but about a variety of connected IT devices and services with some relation to the home. This includes tethered devices which move in and out of the physical space, such as smart phones and laptop computers, as well as cloud, media and social network services and accounts in regular use in the home. **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**. As the cost of smart functionality decreases, home appliances will increasingly have some form of computing functionality and connectivity. Individual users may easily be unaware of the potential of the devices and systems in their home. Moreover, their mental models of what is a "computer" (and as such is in need of information security) may be outdated and in need of change.

Several **economic factors generate security vulnerabilities** in smart home devices. First, companies involved in the smart home market include home appliance companies, small start-up companies, and even crowd-funded efforts. These groups are likely to lack security expertise, security budgets and access to security research networks and communities. For some devices, smart functionality is not a core function but may be an additional function or serve to differentiate between models at different price points. Security and privacy can be an afterthought, following on from getting the smart functions to work and be interoperable. The market does not currently appear to support greatly increased cost for adding smart functionality, which further limits the resources that can be devoted to developing and testing for security. Second, data-mining and analytics are a business model for some smart offerings, which will create additional economic incentives for smart home system vendors to collect data from sensor systems. Design choices are competing against cost, convenience, as well as security and privacy.

Applying basic information security could have significant impacts in the smart home domain. Some devices are so lacking in security measures and secure engineering that implementing relatively well known security measures (such as encrypted communication, non-default passwords, user authentication) would increase smart home security. This study has identified specific and focused approaches specifically for smart home security that are being developed in academia and in industry research, but these approaches may require further evaluation and testing beyond the scope of this study.

The interests of different asset owners in the smart home are not necessarily aligned and may even be in conflict. This creates a complex environment for security activity. For example, media content owners may view occupants' attempts to access licensed media content through alternate channels as a threat to their assets, whilst occupants may interpret digital rights management measures as barriers preventing them from accessing their assets. Different service providers and technology vendors may be in competition with each other for both bandwidth and data.

There is **a developing research base for smart home vulnerabilities**, but this is limited and requires further development and expansion. Much of the available information regards technical vulnerabilities and exploits discovered in research labs. The potential real world impacts (including upon privacy) are less well evidenced, and impacts have to be inferred from these vulnerabilities and contextual knowledge. Some knowledge can be transposed from parallel and linked industries, such as cable and satellite TV, hotel systems and wireless security. The research base has some constitutive limits, for example, there is not much information available on the vulnerability of smart homes to natural disaster and physical harm. There is more information available on information leakage than on sociological and legal impacts of information leakage. Several areas requiring further research have been identified.

Smart homes will impact privacy and data protection significantly. The increased number of interlinked sensors and activity logs present and active in the smart home will be a source of close, granular and intimate data on the activities and behaviour of inhabitants and visitors. The home is a key site of consumption, and given the intimate, non-public context, behaviour in the home may be seen as more meaningful or authentic that public activity. This means that the data produced by such environments will have commercial and law enforcement value and there will be resulting privacy and data protection debates arising from this. The risks that arise from smart home privacy are probabilistic rather than deterministic, and can therefore be hard to communicate. Function creep is highly likely in the smart home context. Much of the smart home literature, and particularly the promotional and marketing literature for smart devices, starts from the assumption that the occupant of the smart home is the owner. In many cases, such as rented accommodation and commercial building automation, this will not be the case. In these contexts, smart homes provide for surveillance, and for automatic enforcement of policies set by the owner. Smart homes also provide the capacity for potentially intense surveillance of other family members.

TP-02-14-997-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN: 978-92-9204-096-3
doi: 10.2824/33134

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu