COMPUTER LAW & SECURITY REVIEW 42 (2021) 105542

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards

Stanislaw Piasecki[1,*], *Lachlan Urquhart*[2], *Professor Derek McAuley*[3]

The University of Nottingham, Nottingham Geospatial Building, Triumph Rd, Nottingham NG7 2TU, United Kindom

ARTICLE INFO

Keyword:
Internet of Things
Smart homes
Standards
Security
Cloud
Edge computing

ABSTRACT

This paper analyses the assumptions underpinning a range of emerging EU and UK smart home cybersecurity standards. We use internet of things (IoT) case studies (such as the Mirai Botnet affair) and the criminological concept of 'routine activity theory' to situate our critique. Our study shows that current cybersecurity standards mainly assume smart home environments are (and will continue to be) underpinned by cloud architectures. This is a shortcoming in the longevity of standards. This paper argues that edge computing approaches, such as personal information management systems, are emerging for the IoT and challenge the cloud focused assumptions of these standards. In edge computing, data can be stored in a decentralised manner, locally and analysed on the client using federated learning. This can have advantages for security, privacy and legal compliance, over centralised cloud-based approaches, particularly around cross border data flows and edge based security analytics. As a consequence, standards should start to reflect the increased interest in this trend to make them more aspirational and responsive for the long term; as ultimately, current IoT architectures are a choice, as opposed to inherent. Our paper unpacks the importance of the adoption of edge computing models which could enable better management of external cyber-criminality threats in smart homes. We also briefly discuss challenges of building smart homes that can accommodate the complex nature of everyday life in the home. In addition to technical aspects, the social and interactional complexities of the home mean internal threats can also emerge. As these human factors remain unresolved in current approaches to smart home cybersecurity, a user's security can be impacted by such technical design choices.

1. Introduction

The objective of this paper is to analyse the technical and social assumptions shaping principles in emerging cybersecu-

* Corresponding author.
E-mail addresses: stanislaw.piasecki@nottingham.ac.uk (S. Piasecki), lachlan.urquhart@ed.ac.uk (L. Urquhart), derek.mcauley@nottingham.ac.uk (P.D. McAuley).
[1] Master's degree in law, economics and management and LL.M. Masters of Law, PhD Student, Horizon Centre for Doctoral Training, University of Nottingham.
[2] Lecturer in Technology Law, school of law, University of Edinburgh
[3] Professor of Digital Economy, Faculty of Science, University of Nottingham.

https://doi.org/10.1016/j.clsr.2021.105542
0267-3649/

rity standards. These shape the design of smart home technologies, indicate industry practice and act as 'soft' regulatory tools. The risk of poorly secured domestic Internet of Things (IoT) devices can create both situational, physical and informational harms to citizens. Accordingly, understanding how different industry standardisation attempts view and are proposing to address these risks is important. Such standards can provide certainty to IoT vendors, and have cross jurisdictional reach, thus the values and norms they perpetuate is important. As a consequence, we proceed by asking: how can standards, and the technology architectures on which they are based, better respond to cybersecurity threats caused by IoT products?

Even though extensive research has been conducted in the field of IoT, its definition continues to be blurry and varies greatly. Each stakeholder's definition tends to differ as it reflects the perspective and objectives of a particular organisation, business or individual.[4] The IEEE mapped state of the art definitions as proposed by standardisation organisations, white papers, books, academia, national initiatives and other sources, in an attempt to create an all-inclusive definition of IoT. It has concluded that "An IoT is a network that connects uniquely identifiable "Things" to the Internet. The "Things" have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the "Thing" can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything."[5] IoT devices can be, for example, factory machinery, medical equipment or domestic appliances.[6] In our work, we will concentrate on domestic IoT.

The omnipresence of IoT devices is already a reality in many countries and its further expansion worldwide seems set for the longer term. According to current industry estimations, there will be 21.5 billion products connected to the internet by 2025 (7 billion in 2018) .[7] These estimates vary but the trend of rapidly increasing numbers of IoT products appears to continue. Data breaches and attacks linked to IoT devices are also likely to rise, partly due to exploits targeting cloud-based architectures and poor security practices on devices (for example, default passwords not being changed). The number and high profile of recent security breaches suggest this will happen.[8]

In response, there are a range of policy initiatives emerging.[9] In October 2018, the United Kingdom Department for Digital, Culture, Media and Sport (DCMS) aggregated different standard setting sources in its "Code of Practice for Consumer Internet of Things (IoT) Security"[10] and the associated "Mapping of IoT security recommendations, guidance and standards to the UK's Code of Practice for Consumer IoT Security".[11] Concurrently, the European Union Agency for Network and Information Security (ENISA) also mapped requirements to standards in its "IoT Security Standards Gap Analysis" .[12] These documents helped us to identify and analyse the assumptions upon which many cybersecurity standards have been written. In terms of standards, our main source was the European Telecommunications Standards Institute's (ETSI) EN 303 645 standard on Cyber Security for Consumer Internet of Things.[13] It references various important works including the DCMS's and ENISA's documents mentioned above. The interplay between different standards as soft regulatory tools is complex. Formally, a standard is a "technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory" .[14] Even though they do not have any legally binding force, standards have a substantial impact on the workings of the IoT sector. They influence how public and private organisations act and require others to act. The DCMS work, for example, has fed into the ETSI IoT standard, but has also shaped the UK government emerging legislative efforts.[15]

This paper analysed in detail one of the assumptions upon which standards have been written – namely, that IoT devices and services will continue to use primarily cloud-based architectures. Whilst this may be the case currently, long term,

[4] IEEE, 'Towards a Definition of the Internet of Things (IoT)' (2015) <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf> accessed 27 October 2020

[5] H. C. Lin and N. W. Bergmann, 'IoT Privacy and Security Challenges for Smart Home Environments' (2016) 7 Information 44

[6] Ibid

[7] IoT Analytics, 'State of the IoT 2018: Number of IoT Devices now at 7B – Market Accelerating' (2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> accessed 27 October 2020

[8] N. Neshenko and others, 'Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations' (2019) 21 IEEE Communications Surveys & Tutorials 2702

[9] I. Brass and others, 'Standardising a Moving Target: The Development and Evolution of IoT Security Standards' (Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, June 2018)

[10] DCMS, 'Code of Practice for Consumer IoT Security' (2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf> accessed 12 May 2020

[11] DCMS, 'Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security' (2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774438/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf> accessed 12 May 2020

[12] ENISA, 'IoT Security Standards Gap Analysis' (2018) <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis> accessed 12 May 2020

[13] ETSI, 'EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements' (2020) <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf> accessed 20 July 2020

[14] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance

[15] DCMS, 'Proposals for Regulating Consumer Smart Product Cyber Security - Call for Views' (2020) <https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views> accessed 17 December 2020

there is an increasing turn to integrating edge computing approaches.[16] As such standards should reflect these aspirations to enable longevity. The other assumption that we have identified is that standards seem to consider home environments as safe spaces. This is not always the case and we wanted to raise awareness that in-home threats linked to smart devices may not be addressed by standards.

We recommend that principles in standards should recognise the value of edge computing, local data storage and analytics approaches. Edge computing is in part driven by the IoT and its need for increased data collection and analysis. It refers to "a network with distributed computing resources (including data storage and processing) where some of the physical infrastructure that hosts these resources is located in close geographical proximity to where data are generated or needed for processing" .[17] Edge computing brings benefits of new mechanisms for data protection compliance and in home security management[18].[19] In this paper, we often refer to the Databox research project[20] as a prototype edge computing system (not yet commercialised) and a model personal information management system (PIMS) built with data protection in mind.[21] Provisions in the General Data Protection Regulation (GDPR), such as Article 32, mandate the use of organisational and technical measures to create more secure systems that address risks to rights and freedoms of individuals.[22] Concurrently, there has been significant interest in PIMS from EU Data Protection Compliance bodies, such as the European Data Protection Supervisor, as they enable greater control over personal data, and put the user at the centre of decisions around processing.[23] Databox, as a specific PIMS, is defined "as a protective container for personal data where data may actually be located in different geographical locations. However, the Databox will act as a virtual boundary (or as a gatekeeper) where it controls how, when, what data is shared with external parties" .[24] In conjunction with DADA, this can attempt to prevent impacts of cybercrimes and data breaches in homes. We will return to this later.

To illustrate, further explain and justify our argument, we have used case studies and used the lens of routine activity theory (RAT) in order to unpack how cybercrimes occur, and what edge approaches might offer to ensure more secure systems are built. According to RAT, a criminal act occurs upon the condition of convergence in time and space of "motivated offenders, suitable targets and the absence of capable guardians" .[25] In current IoT architectures, there is a lack of capable guardian, and the devices remain suitable targets as they have poor security. Edge based security analytics can help address those.

After presenting the background of the problem related to harms arising in insecure smart homes (both internal and external) (2), we will discuss the importance of standards, the assumptions upon which they are based, and how the edge computing Databox model (instead of centralised cloud architectures) could be an effective solution to the issues identified above (3). Case studies and the RAT approach will be used to further analyse how Databox and standards could have helped in preventing security breaches, as 'capable guardians' (4). Finally, we will identify any remaining gaps and give potential directions for future research (5).

2. The insecurity of smart homes and routine activity theory

A smart home can be described as "a contemporary application of ubiquitous computing that incorporates intelligence into dwellings management for comfort, healthcare, safety, security, and energy conservation" .[26] Among smart home technologies, we find monitors, sensors, appliances, devices and interfaces all present on the same network to allow for automation and control of home technologies locally or remotely.[27] A smart home device is truly smart "when all data about the environment is collectively stored and analysed, patterns extracted, and decisions made without the user's intervention" .[28] Any device could potentially be smart. Perhaps one of the most well-known examples are smart TVs but people can also buy smart washing machines, fridges, kettles, doors, thermostats, speakers, lighting or IP cameras. The vision of these devices is to make people's lives more efficient, convenient and safer. The dominant technical architecture to provide a cheaper IoT device in situ is for personal data to be gathered, sent to the cloud to be analysed remotely, and then

[16] He Li, Kaoru Ota and Mianxiong Dong, 'Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing' [Institute of Electrical and Electronics Engineers (IEEE)] 32 IEEE Network 96

[17] UK Parliament, 'Edge Computing, Postnote 631' (2020) <https://post.parliament.uk/research-briefings/post-pn-0631/> accessed 17 December 2020

[18] EDPS, 'Opinion on Personal Information Management Systems' (2016) <https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf> accessed 17 December 2020

[19] Lachlan Urquhart and Jiahong Chen, 'On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity' arXiv pre-print server

[20] H. Haddadi and others, 'Databox' (2020) <https://github.com/me-box/databox/blob/master/README.md> accessed 17 July 2020

[21] L. Urquhart, A. Crabtree and T. Lodge, 'Demonstrably Doing Accountability in the Internet of Things' (2018) 27 International Journal of Law and Information Technology 1

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[23] EDPS, 'Opinion 9/2016 on Personal Information Management Systems' (2016) <https://edps.europa.eu/data-protection/our-work/publications/opinions/personal-information-management-systems_en> accessed 12 May 2020

[24] Charith. A Perera and others, 'Valorising the IoT Databox: Creating Value for Everyone' (2016) 28 Trans Emerging Telecommunications Technologies

[25] Lawrence E. Cohen and Marcus Felson, 'Social Change and Crime Rate Trends: A Routine Activity Approach' (1979) 44 American Sociological Review 588

[26] D. Mocrii, Y. Chen and P. Musilek, 'IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security' (2018) 1-2 Internet of Things 81

[27] D. J. Cook, 'How Smart is your Home?' (2012) 335 [6076] Science 1579

[28] Mocrii, Chen and Musilek

results are fed back to the device to enable the service to be delivered in the home. For example, the computation of data gathered and sent by sleep robots to the cloud can be used to identify sleeping patterns and habits, and smart speakers can inform about various personal preferences and voice patterns of individuals.[29] Often devices do not function without internet connectivity (a security threat in itself, for say a smart lock).

Ordinary users are often unaware of the dangers created by the devices they use, not to mention the lack of technical capacities to set up a secure smart home system.[30] They often experience difficulties both with network management and devices management. For this reason, smart homes should be given particular attention by policy makers and those designing IoT products. Citizens will only be able to successfully manage their networks (and their devices) if they are supported by technology that makes this easy for them.[31] If such home network management systems do not exist, the risks associated with using smart home devices will be higher than the benefits they provide. In this context, the "Homework" project studied the future of home network management through the lens of the needs of the user.[32] Various research traditions were brought together to create new, more user-centred approaches to the use and management of the home networking infrastructure. As a consequence, protocols, architectures and models of the in-home setting were reinvented. This kind of work is crucial to raise awareness and support citizens living in smart homes.[33]

IoT standards have been published recently, but arguably, current standards mainly present best practice requirements of what should have been done from the beginning. Threats related to smart home devices are not new and some are well-known for many years. To give an example, back in 2014, the Article 29 Data Protection Working Party (former EU data protection advisory body, now the European Data Protection Board) identified several threats to the security of our personal data linked to IoT devices. These include users becoming increasingly monitored by third parties and losing control over the use of their data. There are risks associated with changing the original purpose of processing users' data as well as profiling people and receiving knowledge about their behaviour patterns. It is also much more difficult for owners of smart home devices to remain anonymous even if they want to.[34]

Smart homes lead to many security threats if smart devices are not made and deployed correctly. Peppett, for example, argued that the propensity of security issues with IoT is partly due to non IT manufacturers building these systems and lacking familiarity with security issues; and difficulties of patching IoT devices in the wild.[35] In response to these, Manwaring has argued that we need to look beyond privacy frameworks and consider liability and safety to help manage security issues of IoT.[36] This is echoed by Anderson et al., who argue the need for finding practical mechanisms for integrating safety engineering practices with security engineering for the IoT.[37] Similarly, Rosner and Keneally state that there is a lacking incentive structure for manufacturers to invest in security, due to the low cost/profit margin of devices.[38] Singh has argued use of cloud for IoT raises security concerns in relation to chain of responsibility, particularly who is legally meant to implement security mechanisms and the enforcement of liability mechanisms or notification processes when things go wrong e.g. data breaches.[39]

There are both situational and informational harms this type of technology could lead to.[40] Cybercriminals are constantly inventing new ways to overcome security barriers. In 2018, various malicious actions were undertaken by botnets (such as Darkai and AESDDoS) .[41] This resulted in an increase of the number and impact of DDoS attacks during the first quarter of 2018 even though preventive measures following previous attacks have been taken.[42] The cyberthreat landscape is currently wide and there are many other concerns such as the more recent cryptojacking or more traditional (but prevalent) malware campaigns.[43] This highlights how current architectures and standards need to do more to respond effectively to IoT threats as the latter keep materialising.

As we have mentioned in the introduction, there are also threats related to the fact that smart homes are not always safe spaces. A project conducted over a 7 years long period analysed over 2000 American families to learn more about violent behaviour within the family. The study showed that homes can be unsafe spaces, in particular for people who are

[29] L. Urquhart, H. Schnädelbach and N. Jäger, 'Adaptive Architecture: Regulating Human Building Interaction' (2019) 33 International Review of Law, Computers & Technology 3

[30] K. Heuvel, 'Securing the Smart Home' (Masters thesis, University of Amsterdam 2018)

[31] A. Adams and M. A. Sasse, 'Users are Not the Enemy' (1999) 42 Commun Acm 40

[32] Homework, 'Homework User-Centred Home Networking' (2012) <http://homenetworks.ac.uk/> accessed 7 January 2021

[33] Ibid

[34] WP29, 'Opinion 8/2014 on the Recent Developments on the Internet of Things' (2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 27 October 2020

[35] Scott R. Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent' (2014) 93 Texas Law Review 85

[36] Kayleen Manwaring, 'Emerging Information Technologies: Challenges for Consumers' (2017) 17 Oxford University Commonwealth Law Journal 265

[37] R. Anderson, E. Leverett and R. Clayton, 'Standardisation and Certification of the 'Internet of Things'' (16th Annual Workshop on the Economics of Information Security (WEIS 2017), California, June 2017)

[38] G. Rosner and E. Kenneally, 'Clearly Opaque: Privacy Risks of the Internet of Things' SSRN Electronic Journal

[39] Jatinder Singh and others, 'Twenty Security Considerations for Cloud-Supported Internet of Things' (2016) 3 Ieee Internet Things 269

[40] B. Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World* (Norton 2018)

[41] A. Rayome, 'Major DDoS Attack Lasts 297 Hours, as Botnets Bombard Businesses' (2018) <https://www.techrepublic.com/article/major-ddos-attack-lasts-297-hours-as-botnets-bombard-businesses/>

[42] ENISA, 'Threat Landscape 2018' (2019) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018> accessed 12 May 2020

[43] Ibid

traditionally marginalised or considered to be at risk.[44] The latter are often reticent to take part in research related to connected devices, which makes manufacturers and the research community not aware of the harms those devices can cause when they end up being controlled by the wrong person.[45] Furthermore, those who share access to devices may also be a threat to others in the home,[46] an issue compounded by shared device or family accounts.[47]

Since ordinary devices have become connected to the Internet, regulators need to think about security as well as safety as harms are now physical, as well as informational.[48] Whilst a standardised reference architecture allowing for personal data to be stored safely and securely is needed,[49] despite various reference architectures advanced to enable industry wide standardisation for IoT security, none have been widely adopted yet.[50]

Routine activity theory

In Section 4, we use a criminological concept, the routine activity theory (RAT), to analyse what kind of technical architecture and what kind of standards are the most effective in terms of protecting users of smart home devices against human and technical external threats as well as internal technical threats. To do so, we will use case studies, including the Mirai Botnet and Hello Barbie doll examples.

RAT was developed to analyse trends and cycles in criminal activities more effectively. Instead of focusing on the characteristics of those committing the crimes, this approach concentrates on the circumstances in which the criminal acts have been executed. According to the routine activity theory, a criminal act needs the convergence in time and space of *three factors*: "motivated offenders, suitable targets and the absence of capable guardians" .[51] Capable guardianship concerns "the capability of persons and objects to prevent crime from occurring" .[52] This can be achieved either through "their physical presence alone or by some form of direct action" .[53] Direct intervention is not necessary as routine activity theorists "see the simple presence of a guardian in proximity to the potential target as a crucial deterrent" .[54] The absence of any of the RAT conditions is enough to prevent crimes from happening. If there is convergence in space and time of these factors, this can cause crime rates to rise without any kind of modification in the structural conditions that drive people to commit crimes.[55]

Most discussions on whether criminological theories developed for the "real" world can be applied to the "virtual" one has focused on RAT.[56] There are various reasons for this. RAT is a well-known, effective and widely used theory to examine different forms of criminal behaviour.[57] RAT is also quite intuitive and easy to apply in different scenarios, giving clear focal points for effective policy making and crime prevention strategies. Situational crime prevention strategies are often the result of RAT analysis,[58] where design decisions are taken about an environment to try and mitigate opportunities for crime. It can be criticised for not really engaging with the causes of crime, but for our purposes of understanding how to build more secure information systems, it helps to contextualise the threat landscape and the human factor in cybersecurity management. In particular, as it is difficult to know the motivations of the cyber offender, it can be assumed they will be motivated, and instead we can consider the suitability of targets and absence of capable guardians to mitigate. In the IoT domain, the insecurity of devices and lack of design guidance certainly feeds into the pool of suitable targets. Similarly, the poor organisational and technical practices of IoT vendors and service providers, coupled with opacity of device functionality limiting oversight by end users, means there are often no capable guardians.

3. IoT cybersecurity standards and from the cloud to the edge?

Firstly, we will briefly discuss the nature of current smart home cybersecurity standards (3.1) and explain why standards are important as well as their relationship with law (3.2). We will then challenge the assumption about cloud-based architectures for IoT products and services and explain why we advocate for standards to reflect edge computing approaches (3.3). Thirdly, we will discuss the thirteen principles derived

[44] M. Straus, R. Gelles and S. Steinmetz, *Behind Closed Doors Violence in the American Family* (1 edn, Routledge 2017)
[45] S. Zheng and others, 'User Perceptions of Smart Home IoT Privacy' (2018) 2 Proceedings of the ACM on Human-Computer Interaction 1
[46] D. Freed and others, '"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology' (CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, April 2018)
[47] M. Goulden, '"Delete the Family": Platform Families and the Colonisation of the Smart Home' [2019] Information, Communication & Society 1
[48] R. Anderson, E. Leverett and R. Clayton, 'Standardisation and Certification of the Internet of Things' (16th Annual Workshop on the Economics of Information Security (WEIS 2017), La Jolla, California, June 2017)
[49] Mocrii, Chen and Musilek
[50] B. Di Martino and others, 'Internet of Things Reference Architectures, Security and Interoperability: A Survey' (2018) 1-2 Internet of Things 99
[51] Cohen and Felson
[52] A. Tseloni and others, 'Burglary Victimization in England and Wales, the United States and the Netherlands: A Cross-National Comparative Test of Routine Activities and Lifestyle Theories' (2004) 44 British Journal of Criminology
[53] L. E. Cohen, M. Felson and K. C. Land, 'Property Crime Rates in the United States: A Macrodynamic Analysis, 1947-1977; With Ex Ante Forecasts for the Mid-1980s' (1980) 86 American Journal of Sociology 90
[54] M. Yar, 'The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory' (2005) 2 European Journal of Criminology 407
[55] Cohen and Felson
[56] E. R. Leukfeldt and M. Yar, 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis' (2016) 37 Deviant Behavior 263
[57] J. M. Mannon, 'Domestic and Intimate Violence: An Application of Routine Activities Theory' (1997) 2 Aggression and Violent Behavior 9
[58] Leukfeldt and Yar

from the mapping of cybersecurity standards done by various organisations (3.4). Finally, we will raise awareness about the fact that standards do not take into consideration internal human threats (3.5).

3.1. *Overview of the sources of standards applicable to smart homes*

There is a wide array of organisations developing standards at international (ISO, ITU etc.), regional (ETSI etc.) and national levels (for example, the US National Institute of Standards and Technology) in addition to private sector organisations and governments. In our paper we have concentrated on the mapping of consumer IoT cybersecurity standards done by the UK government and EU organisations.

The UK Government's Department for Digital, Culture, Media and Sport's (DCMS) "Code of Practice for Consumer Internet of Things (IoT) Security"[59] and the associated "Mapping of IoT security recommendations, guidance and standards to the UK's Code of Practice for Consumer IoT Security"[60] offer an overview of what the UK government considers as the most important security issues and how they can be addressed in the context of consumer IoT. The DCMS's documents have been one of the main sources of information in our work. At the moment, the Code of Practice is voluntary but the Government is considering making some of its elements legally enforceable in the future.[61]

We also draw on the 2018 ENISA's "IoT Security Standards Gap Analysis, Mapping of existing standards against requirements on security and privacy in the area of IoT" .[62] ENISA was an EU agency, now rebranded as EU Agency for Cybersecurity. The DCMS and ENISA have mapped standards from different sources. For example, ENISA has included standards of the International Organization for Standardization (ISO) whereas the DCMS has omitted to do so.

The European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) are the main European Standardization Organizations at the EU level, working together on issues of mutual interest (as coordinated by the Joint Presidents' Group (JPG)). In 2020, ETSI updated its first globally applicable standard for IoT cybersecurity after the European Commission tasked ETSI to produce this document[63].[64] This standard has taken into account all major documents related to consumer security in the IoT field including the DCMS and ENISA reports mentioned previously. ETSI's work has been the main source of our analysis.

3.2. *The importance of standards and their interaction with law*

Standards can be applied in a voluntary way. Compliance with standards is frequently treated as proof of due diligence and best practice in a particular industry.[65] This is in itself an incentive for organisations to respect standards and there is an argument that those following standards might be more reliable and reputable.[66] For example, the company LIMS which specialises in software to manage laboratory testing promotes on its website the fact that it complies with ISO 27001 standards concerning safety and security.[67]

Standards can also be negotiated or imposed on actors in the field of IoT by legal private and public mechanisms.[68] Public law can impose standards through legal requirements or guidance on how to apply those requirements. Governments often use standards to write legislation and best practice guides (at the EU level, the European Commission has even published a guide on how to reference standards in legislation and it has done so in many EU laws) .[69] Compliance with standards can help an organisation in proving that it also complies with laws.[70] If they are violated, this might result in administrative or criminal sanctions. In private law, standards are often negotiated and enforced through contracts.[71]

Standards can be divided into three main categories.[72] Technical standards provide details "of a format, protocol, or interface and describe how to make things work in an interoperable manner" .[73] They are usually written by industry actors and, as a result, are more often under the umbrella of= private law. Their influence on the way organisations and people behave may be as important as other types of laws and regulations.[74] Informational standards "set parameters for types of information to be communicated about a product, such as

[59] DCMS, 'Code of Practice for Consumer IoT Security'

[60] DCMS, 'Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security'

[61] T. Reeve, 'Government Could Regulate IoT Security as it Launches Industry Code of Practice' (*SC Media*, 2018) <https://www.scmagazineuk.com/government-regulate-iot-security-launches-industry-code-practice/article/1496163> accessed 12 May 2020

[62] ENISA, 'IoT Security Standards Gap Analysis'

[63] ETSI, 'ETSI Releases First Globally Applicable Standard for Consumer IoT Security ' (2019) <https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security> accessed 12 May 2020

[64] ETSI, 'EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements'

[65] N. Gleeson and I. Walden, ''It's a Jungle Out There'?: Cloud Computing, Standards and the Law' (2014) 5 European Journal of Law and Technology

[66] BSI, 'Standards and Regulation' (2019) <https://www.bsigroup.com/en-GB/standards/Information-about-standards/standards-and-regulation/> accessed 12 May 2020

[67] D. Colantuono, 'We are ISO 27001 Certified!' (*EUSoft*, 2019) <https://www.eusoft.co.uk/we-are-iso-27001-certified/> accessed 12 May 2020

[68] Gleeson and Walden

[69] European Commission, 'Methods of Referencing Standards in Legislation with an Emphasis on European Legislation' (2002) <https://ec.europa.eu/growth/content/methods-referencing-standards-legislation-emphasis-european-legislation-0_en> accessed 18 July 2020

[70] Gleeson and Walden

[71] Ibid

[72] Ibid

[73] N. Borenstein and J. Blake, 'Cloud Computing Standards: Where's the Beef?' (2011) 15 Ieee Internet Comput 74

[74] Gleeson and Walden

labelling standards" .[75] Evaluative standards "test and certify the proper use of best-known practices" .[76] Evaluative and informational standards usually influence a higher number of stakeholders, including lawmakers and regulators.[77]

Certification procedures are also proof of the significance of standards, both for consumers and manufacturers of smart home devices. Certification serves often to determine compliance with a set of standards. It can be defined as "conformity assessment" during which "a person or a body will evaluate compliance of persons, products and/or processes with a given set of requirements" .[78] Concerning evaluative standards which demonstrate that particular levels of security or quality have been achieved, certification procedures include an objective evaluation of compliance by third parties.[79] These procedures increase trust among smart home devices buyers as it proves to them that the product respects certain standards .[80]

This is another reason why adopting effective standards is crucial. The buyers of smart home devices could be influenced by certification schemes such as the recently published Kitemark for IoT devices and some of them might think that in the presence of this Kitemark, they do not have to worry about security or safety risks.[81] Indeed, "Standards and certificates can be a synonym of reliability and assurance to the end user and citizen" .[82] Recently, the government has started working on a new labelling scheme for consumer IoT product security, which could have a strong impact on the IoT sector.[83]

Notwithstanding all the benefits and significance of standards, there are issues around them that all stakeholders should strive to overcome. Firstly, standards are not developed fast enough and are written in a way that does not allow to successfully respond to threat levels.[84] Sometimes, there is also a lack of awareness about the existence of certain standards among various stakeholders such as small and medium enterprises or public authorities.[85] Finally, standards development organisations are not communicating with each other effectively about their work which leads to a multiplication of standards on particular topics and a shortage of standards on others.[86]

In our paper, we argue that due to assumptions about the widely adopted cloud architecture model, the nature of the current standards does not guarantee the security and safety of smart home environments, although they are a step in the right direction. Lessig drew attention to regulation through code, and that the design and architecture of technologies are regulatory tools that can enforce certain norms. As a consequence, adopting the right standards and architecture is important because they influence how people behave and how they can interact with their smart devices.[87] As Reidenberg affirmed back in 1997, standards organisations, part of "the technical community, willingly or not, now" have "become a policy community, and with policy influence comes public responsibility" .[88] More than 20 years on, we are still attempting to parse what this role for designers looks like in practice.

3.3. *The choice of a cloud architecture and the edge computing databox alternative*

Back in 2012, one of European Commission's concerns was insufficient standards written in the field of IoT data protection and security.[89] The Commission referred only to cloud-based services. It has called for "publicly available cloud offerings ("public cloud") that meet European standards" .[90] Since then, an impressive number of standards have been developed to support such services. The way the ETSI standard as well as standards mapped by ENISA and the DCMS are currently written, they are making assumptions about the design of IoT products and services, and rather predictable statements (such as the no default passwords requirement). They seem to accept as a necessity that data is removed from the device and stored in the cloud. Citizens' data is currently mined and stored in databases. Indeed, when thinking about IoT, we usually think of goods that send data to the cloud.[91] The current trends in computing are reflected in smart homes, "particularly big data, cloud computing and machine learning, with personal data collected by IoT devices typically being distributed to the cloud for processing and analytics" .[92] There is no inherent need to design IoT devices using cloud infrastruc-

[75] OECD, 'OECD Policy Roundtable on Standard-Setting' (*OECD*, 2010) <http://www.oecd.org/daf/competition/47381304.pdf> accessed 12 May 2020

[76] Borenstein and Blake

[77] Gleeson and Walden

[78] ENISA, 'Security Certification Practice in the EU' (2013) <https://www.enisa.europa.eu/publications/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study> accessed 27 October 2020

[79] Gleeson and Walden

[80] I. Kamara, T. Sveinsdottir and S. Wurster, 'Raising Trust in Security Products and Systems through Standardisation and Certification: The Crisp Approach' (2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, December 2015)

[81] BSI, 'BSI Launches Kitemark for Internet of Things Devices' (2018) <https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-internet-of-things-devices/> accessed 12 May 2020

[82] Kamara, Sveinsdottir and Wurster

[83] DCMS, 'Consultation on the Government's Regulatory Proposals regarding Consumer Internet of Things (IoT) Security' (2020) <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security> accessed 27 October 2020

[84] ENISA, *Guidance and Gaps Analysis for European Standardisation* (2018)

[85] Ibid

[86] Ibid

[87] L. Lawrence, *Code: Version 2.0* (Basic Books 2006)

[88] R. J. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 Texas Law Review 553

[89] European Commission, 'Unleashing the Potential of Cloud Computing in Europe COM (2012)' (2012) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF> accessed 12 May 2020

[90] Ibid

[91] M. Hung, 'Leading the IoT: Gartner Insights on How to Lead in a Connected World' (*Gartner*, 2017) <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf> accessed 27 October 2020

[92] Urquhart, Crabtree and Lodge

tures - this is a design choice, one that may have cost-based justifications but also enables the data harvesting infrastructure that underpins many IoT business models. Why do we advocate for an edge computing solution that goes against current cloud-based trends?

Firstly, from a GDPR perspective, international data transfers to third countries where remote servers are based make compliance difficult. Third countries may not always have been deemed adequate for EU citizens data to be stored there, and thus once data travels abroad, it can be harder to control who has access to it and where this data actually is located (in this context, access by foreign law enforcement to sensitive data from other countries which is now located on its territory raises important concerns). In this situation, adequate protection of data is difficult to be achieved.[93] Local storage seems a better answer for companies (less issues with compliance), consumers (safer and more secure treatment of their personal data) and the smart home IoT sector in general (increased consumers' trust that their data is protected).

If data processing takes place on the edge of the network instead of centralized processing taking place in the cloud, this could not only diminish but also completely discard the need to distribute personal data and the privacy dangers that are linked to this distribution.[94] Edge computing can reduce to the minimum the amount of data that is distributed (only the necessary data to respond to a certain issue or query is being sent to external actors). Advances in federated learning mean it can be possible to do distributed data analytics in more privacy preserving ways.[95] As opposed to more common machine learning that uses centralized approaches, "federated learning is a decentralized training approach", that enables devices "located at different geographical locations to collaboratively learn a machine learning model while keeping all the personal data that may contain private information on the device" .[96] This is more consistent with the data minimisation principle (article 5 GDPR). Moreover, there are other advantages when data processing takes place at the edge such as reduced latency issues (there is no necessity for the data to travel between the home and remote data centres), improved resilience related to actuation (actuation is not dependent upon uninterrupted connectivity) and diminished costs of data processing.[97] As we can see, if the computation of data takes place at the network's edge, this can have potentially many advantages over the currently predominant cloud architectures, including more oversight for security and privacy of data.

The Databox is an example of an edge computing approach, a personal information management system (PIMS). It has been developed with smart homes in mind, where the objective is to "transform the current provider centric system into a human centric system where individuals are protected against unlawful processing of their data and against intrusive tracking and profiling techniques that aim at circumventing key data protection principles" .[98] Databox stores data locally and keeps information close to the owners of IoT smart home devices which allows the end user to have more control over data, and for the creation of a more user centric and ethical architecture for future IoT products.[99] Databox wants to give people back control over their information. It collects data from smart home devices, "either directly or via APIs, and makes them available to apps that enable data processing and actuation" .[100] In the Databox model, smart home devices all feed into the box and raw data never leaves the latter. All the externals actors can receive is the result of the analysis performed to answer particular queries.[101] Moreover, Databox can enable new and more effective types of threat management. It spots security threats on the home network and once it spots them, it informs users that devices are being used in ways that are not expected (by drawing on Manufacturer Usage Description profiles of expected behaviour) .[102] This way, Databox allows for potentially faster and more effective threat management.

3.4. *The thirteen principles derived from current standards*

As we have seen, data from IoT devices is usually distributed to the cloud and standards are being written based on those cloud-based architectures. Even though they have mapped and analysed standards created by different organisations, ENISA and the DCMS have arrived at the exact same thirteen principles derived from those standards. This shows that there is a trend related to how standards are being written at the moment. This is not negative in itself as the standards developed for cloud-based architectures are often quite obvious requirements of what should have been done from the beginning and should exist (for example, ensuring that the software is regularly updated or that there are no default passwords). Many of them would be also relevant and important for edge computing architectures. Furthermore, as a lot of IoT devices currently do rely on cloud, these standards are not wrong to focus on this design. However, as standards, they can set direction of travel for best practice, and thus should be more aspirational in trying to change industry practice (which is in conjunction with legal requirements to do so anyway).

The DCMS and ETSI described the following thirteen guidelines as necessary to protect citizens' safety and privacy:

1 Lack of a default password,

[93] Ibid

[94] A. Crabtree and others, 'Building Accountability into the Internet of Things: the IoT Databox Model' (2018) 4 Journal of Reliable Intelligent Environments 39

[95] C. Troncoso and others, 'Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments' (2017) 4 Proceedings on Privacy Enhancing Technologies

[96] Z. Li, V. Sharma and S. P. Mohanty, 'Preserving Data Privacy via Federated Learning: Challenges and Solutions' (2020) 9 Ieee Consum Electr M 8

[97] Crabtree and others

[98] EDPS, 'Opinion 9/2016 on Personal Information Management Systems'

[99] Urquhart, Crabtree and Lodge

[100] Crabtree and others

[101] Urquhart, Crabtree and Lodge

[102] A. Hamza and others, 'Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles' (Publication: IoT S&P '18: Proceedings of the 2018 Workshop on IoT Security and Privacy, Budapest, August 2018)

2 Vulnerability disclosures,
3 Support for the whole lifecycle of IoT products,
4 Secure storage of sensitive data,
5 Secure communications,
6 The application of the least privilege principle (minimising exposed attack surfaces, for example, by closing all unused software and network ports),
7 Maintenance of the integrity of the software,
8 Protection of personal data,
9 Resilience of systems to outages,
10 Monitoring telemetry data (examining data automatically transferred by users' devices to an IT system in a separate location for security evaluation and quick mitigation of potential issues),
11 Facilitating the removal of personal data,
12 Easy configuration of the devices and
13 Validating the data input.

How do different stakeholders perceive those principles? We will take the lack of a default password requirement as an example. The Internet Society's Online Trust Alliance (an American NGO) considers that companies should "include strong authentication by default, including providing unique, system-generated or single use passwords; or alternatively use secure certificate credentials" .[103] A formal standardization body, the ISO, demands in its standard 27002 to "ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed" .[104] In its standard ISO/IEC 19,790 it states that "authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates" .[105] Similarly, the multinational conglomerate AT&T considers that "rather than permitting an easy-to-hack default password, each device should require the user to define a unique and reasonably secure password for access from a network interface" and according to the GSMA trade body "it is imperative that all authentication systems enforce strong passwords where passwords are required for user authentication"[106] .[107] As we can see, NGOs, governmental actors and companies share a similar view and this is not surprising as a standard requiring to set unique passwords seems to be an obvious recommendation, beneficial to all stakeholders. Similarly, principles such as the one stating that personal data needs to be protected or that support should be given during the whole lifecycle of products (and all of the others principles actually) would help, if effectively implemented, in protecting users of smart home devices and in ensuring that organisations comply with regulations.

However, those principles will be more easily applied in practice using the Databox architecture (please see Section 3.3 for arguments in favour of edge computing). We can take the example of the principle that calls for making systems resilient to outages. Provision 5.9–1 of the ETSI standard states that "resilience should be built into IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power" .[108] As we have seen in a previous section, this is clearly easier in the Databox scenario where actuation is not dependent on uninterrupted connectivity. This could prevent situations such as the Google Nest outage from May 2018 when smart security cameras, smart thermostats and smart locks were all affected.[109] Because edge computing solutions such as Databox are safer methods of storing and processing users' data, this means that such architectures could be more efficient in successfully implementing the thirteen principles derived from current cybersecurity standards presented above. Moreover, if new standards based specifically on this edge computing approach would be written, this could potentially add additional safety layers to this already safer architectural model.

3.5. *Addressing the standards gap for human threats using rat*

In addition to the above, cybersecurity standards also assume that homes are safe spaces and that the network manager is a good person. They do not consider the problems of in-home human threats (which do exist as we have seen in the introduction and Section 2). We can take domestic abuse as example. This problem has been recently discussed in an interesting article. In June 2018, the New York Times warned about the rising number of smart home devices in cases of domestic abuse.[110] The author shows that IoT products can lead to an imbalance of power within homes. She describes how people called hotlines extremely worried about what was happening. A woman called informing that the code numbers of the lock at her house door changed each day and that she did not know why. Another person complained that she continued to hear the sound of the doorbell ringing, however there was no one at the door. These are examples of new forms of domestic abuse

[103] OTA, 'IoT Trust by Framework' (2017) <https://www.internetsociety.org/iot/trust-framework/> accessed 6 May 2020
[104] ISO, 'ISO/IEC 27002:2013 Information Technology - Security Techniques - Code of Practice for Information Security Controls' (2013) <https://www.iso.org/standard/54533.html> accessed 12 May 2020
[105] ISO, 'ISO/IEC 19790:2012 Information Technology - Security Techniques - Security Requirements for Cryptographic Modules' (2012) <https://www.iso.org/standard/52906.html> accessed 12 May 2020
[106] GSMA, 'IoT Security Guidelines for IoT Service Ecosystem' (2017) <https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.12-v2.0.pdf> accessed 5 April 2020
[107] AT&T, 'Exploring IoT Security' (AT&T, 2016) <https://www.business.att.com/content/dam/attbusiness/reports/exploringiotsecurity.pdf> accessed 25 March 2020
[108] ETSI, 'TS 103 645 Cyber Security for Consumer Internet of Things' (2019) <https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf> accessed 12 May 2020
[109] The Register, 'Three-Hour Outage Renders Nest-Equipped Smart Homes Very Dumb' (2018) <https://www.theregister.co.uk/2018/05/17/nest_outage/> accessed 12 May 2020
[110] N. Bowles, 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' (*The New York Times*, 2018) <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> accessed 12 May 2020

Type of threat	Examples
Technical threats	denial of service attacks, information leakage or sharing, unintentional modifications of data in information systems, inadequately designed smart homes, outages etc.
Human threats	social engineering, domestic abuse, eavesdropping, hijacking, interception, only one person knowing how to manage the smart home, abuse of personal data etc.

Fig. 1 – Classification of smart home threats.

through harassment, monitoring etc. Bad actors remotely control connected devices to abuse their victims. Problems are worsened when other members of the household know little about the workings of smart homes and how to make the abuser legally and practically stop his criminal behaviour. Most often, only one person in the house installs the technology, understands how it works and possesses all the passwords. This gives this person the power to use the technology for domestic abuse. The opportunities to go to court and legal recourse in general can be quite limited.[111] Technologies such as IoT devices give perpetrators new tools to harass and control people. Women and girls continue to be the most affected by domestic abuse.[112] Smart devices create a distinct group of challenges in the field of domestic violence that are still not fully understood and acknowledged, and which require specific responses.[113] There are also other human threats related to smart homes, such as social surveillance, which should be analysed and resolved as well[114 115 116].[117] Social surveillance can be defined as the "ongoing eavesdropping, investigation, gossip and inquiry that constitutes information gathering by people about their peers, made salient by the social digitization", which could be done for malicious purposes using IoT products (just as it has been the case for many years with social media)[118].

As we have mentioned previously, this paper's objective is not to find concrete solutions to the lack of standards (please see Fig. 1 and Fig. 2 below) related to human threats inside people's homes. In this additional section, we would simply like to raise awareness about the fact that there seems to be a lack of capable guardians as human threats within smart homes keep materialising. The RAT theory could be effective in analysing how the insecurity of smart devices can be exploited internally by motivated offenders against suitable targets as well as in finding potential capable guardians. It has already been applied to analyse domestic and intimate violence in the past.[119]

In this context and concerning the relationship between in-home human threats, standards and architectures, the Databox architecture would probably not be able to act as a capable guardian here as it deals with problems related to data leaving the home, not to data used by its inhabitants in their interactions with each other. Standards also do not provide any solution at the moment. However, maybe they could become capable guardians and prevent in-home human threats by limiting what the devices can or cannot do through technical guidance developed with the help of sociological research. They could shape design to remove affordances ("affordances define what actions are possible"[120]) for human threats and to reduce vectors for influence and manipulation. For example, in the context of intimate partner violence, some authors advocate in favour of refining "authentication mechanisms to better distinguish between legitimate users and UI-bound adversaries" and developing new frameworks "to consider adversarial users while designing and evaluating UIs in order to limit systems' abusability" .[121] Further research in this area is needed in terms of how standards could offer guidance. Moreover, this approach has its limitations as it focuses on the situation instead of the actual cause of crimes so it would need to be accompanied by other strategies to target human threats inside the home. This is a broad area of research in policing, victimology and criminology more generally and there is also a need to engage with wider societal aspects that lead to domestic violence and other human crimes in the first place.

To really understand in-home threats and identify capable guardians, ethnographic studies should be used to complement the RAT analysis by explaining the actions and routines of motivated offenders. A home network is a "sociological object wrapped up in the organisation of" the lives of household members.[122] Indeed, network management is indivisibly interweaved with everyday activities that form part and organize domestic life. As a consequence, "the developers of network control and management facilities need to be aware of the impact of the social and moral ordering of domestic activities and the host of relationships and situated judgments involved" .[123]

[111] Ibid
[112] L. Tanczer and others, 'Gender and IoT Research Report. The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse' (*University College London*, 2019) <https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf> accessed 12 May 2020
[113] Goulden
[114] M. Goulden and others, 'Living with Interpersonal Data: Observability and Accountability in the Age of Pervasive ICT' (2018) 20 New Media & Society 1580
[115] A. Marwick, 'The Public Domain: Surveillance in Everyday Life' (2012) 9 Surveillance & Society 378
[116] M. Flintham and others, 'Domesticating Data: Socio-Legal Perspectives on Smart Homes & Good Data Design' in A. Daly (ed), *Good Data* (SK Devitt & M Mann 2019)
[117] Freed and others
[118] Marwick
[119] Mannon
[120] D. Norman, *The Design of Everyday Things* (Perseus Books Group, 2013)
[121] Freed and others
[122] A. Crabtree and others, 'Unremarkable Networking' (Proceedings of the Designing Interactive Systems Conference on - DIS '12, Newcastle Upon Tyne, June 2012)
[123] Ibid

	Existing security principles (derived from standards) relevant to *technical threats* (see Fig 1)	**Existing security principles (derived from standards) relevant to *human threats* (see Fig 1)**
External threats (from outside of the home)	Support for the whole lifecycle of IoT products – updates should be timely, secure and easy to implement Lack of a default password – need to follow best practices on authentication procedures, possibility of enhancing security by unique and immutable identities Secure storage of sensitive data – no hard-coded credentials The application of the least privilege principle (reducing the number of attack surfaces) – closing unused software services and ports Maintenance of the integrity of the software – verifying and alerting the consumer and administrator about unauthorised modifications Monitoring telemetry data – analysing telemetry data for security threats, consumers should be informed Validating the data input –wrongly formatted data or code can be subverted for criminal purposes Vulnerability disclosures – dealing with vulnerabilities in a timely manner, immediately inform the consumer	Monitoring telemetry data – analysing telemetry data for security threats, consumers should be informed Resilience of systems to outages – smart home devices should continue to operate in the case of loss of power or data network outages Secure communications – use of appropriate encryption mechanisms Secure storage of sensitive data – no hard-coded credentials
Internal threats (in the home)	Support for the whole lifecycle of IoT products – updates should be timely, secure, easy to implement Easy configuration of the devices – configuration and maintenance should follow best practices on usability Protection of personal data – clear information and consent practices related to how consumers' data is being used Resilience of systems to outages -smart home devices should continue to operate in the case of loss of power or data network outages Facilitating removal of personal data – easy removal procedures with clear instructions	**No standards**

Fig. 2 – Gap analysis of threats against standards.

The negative consequences and trauma related to violence in a private and trusted environment such as our home can be much stronger than the effects of crimes which occur in the streets or in the "more obvious" high crime places.[124] It is important to continue doing studies on the influence of IoT devices on threats inside the home in order to identify capable guardians, prevent bad actors from being able to use those devices to commit crimes and vulnerable people from being exposed to even greater risk.[125]

In Figs. 1 and 2 below, we have used the DCMS documents, the ETSI Standard and ENISA's reports on the cyberthreat landscape to find out which types of threats are

[124] Mannon

[125] Zheng and others

tackled by principles derived from standards[126] [127] [128] [129].[130] Fig. 1 presents various technical and human smart home related threats.

In Fig. 2 we now look at the technical and human threats from Fig. 1 in more depth to explore how they have been addressed by principles derived from standards. We arrived at the conclusion that none of the 13 principles identified in the ETSI standard, the DCMS Code of Practice and in the "Mapping of IoT Security Recommendations, Guidance and Standards" document of the DCMS respond to in-home human threats. The latter includes "IoT security and privacy related" standards and recommendations developed by organisations such as the Cloud Security Alliance (CSA), the GSMA, the Alliance for Internet of Things Innovation (AIOTI) and many others.[131]

4. Applying the rat concept to external threats

A vulnerability of current smart home devices is that most of them do not have or have only a few security features reflecting the current standards. We are a long way from the latter being widely adopted.[132] It is important to consider if the application of standards based on cloud architectures could have prevented security breaches from happening as well as whether standards combined with the Databox architecture, would have been more effective. To conduct our analysis, we will use RAT. We will briefly discuss RAT's theory applicability to cybercrime (4.1), before analysing our case studies – the WIFI Hello Barbie Doll (4.2) and the Mirai Botnet affair (4.3).

4.1. *The rat theory*

There are currently debates on whether cybercrime should be regarded as a new and unique category of criminal activities, and, as a consequence, an activity that requires the creation of new criminological theories and terms. RAT "has been repeatedly nominated as a theory capable of adaptation to cyberspace" .[133] This is what we tried to achieve in our paper, adapting and using RAT to better analyse smart home related cybersecurity threats.[134] We agree cybercrime is a "range of illicit activities whose common denominator is the central role played by networks of information and communication technology (ICT) in their commission" .[135] A cybercrime can start in cyberspace and then continue in the "real world" based on the data obtained on the internet.

In Section 2, we have explained in more detail why we consider RAT as a useful tool for our analysis. According to this theory, for a criminal act to exist there needs to be convergence in time and space of three factors, namely motivated offenders, suitable targets and the lack of capable guardians.[136] The absence of one of them is enough to prevent crimes from happening. RAT does not focus on the motivations of the offender and concentrates instead on the circumstances in which the crime has been committed.[137] RAT presupposes that there will always be people inclined to commit crime for a multitude of reasons. RAT theorists analyse "the manner in which the spatio-temporal organization of social activities helps people to translate their criminal inclinations into action" .[138] Following RAT's reasoning, there will always be motivated actors seeking to exploit smart homes for various purposes. The real question is therefore how to prevent them from being successful.

There are four main properties used to analyse the suitability of specific targets: value, inertia, visibility and accessibility (VIVA) .[139] Even though they differ in terms of their applicability between "traditional" crimes and cybercrimes, they can be adapted to the latter.[140]

In terms of a capable guardian that can defend smart home dwellers against cyber threats, we will evaluate whether standards and Databox could act effectively as such a guardian. According to RAT, the presence of a capable guardian is the most likely element to diminish victimisation.[141]

Finally, it is important to remember that RAT requires the convergence in time and space of the three factors described above. We will evaluate in our case studies if this convergence happens.

4.2. *The wi-fi enabled hello barbie doll, standards and the databox*

In 2015, Mattel produced a Wi-Fi enabled Barbie doll. The Hello Barbie doll was described as the first interactive doll in the world, able to listen to children and talk with them. The doll is connected to the internet through Wi-Fi. It possesses a microphone that records children. This data is then transferred to third-parties for processing. A security researcher, Matt Jakubowski, managed to hack the doll. This permitted him to gain access to its system and account information, audio data files and the doll's microphone.[142]

If we apply RAT here, the motivated offenders would be the hackers of the Barbie doll. In terms of suitable targets and

[126] ENISA, 'Threat Landscape and Good Practice Guide for Smart Home and Converged Media' (2014) <https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence> accessed 12 May 2020
[127] ENISA, 'Threat Landscape 2018'
[128] DCMS, 'Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security'
[129] ETSI, 'EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements'
[130] DCMS, 'Code of Practice for Consumer IoT Security'
[131] DCMS, 'Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security'
[132] Lin and Bergmann
[133] Yar
[134] Leukfeldt and Yar
[135] Yar
[136] Cohen and Felson
[137] T. N. Fawn and R. Paternoster, 'Cybercrime Victimization: An Examination of Individual and Situational Level Factors' (2011) 5 International Journal of Cyber Criminology 773
[138] Cohen and Felson
[139] Ibid
[140] Yar
[141] Leukfeldt and Yar
[142] S. Gibbs, 'Hackers can Hijack Wi-Fi Hello Barbie to Spy on your Children' (*The Guardian*, 2015) <https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children> accessed 12 May 2020

the VIVA criteria, the value of the target could be acquiring personal sensitive information or using the doll to hack into other devices. This could then be used for various criminal purposes. The visibility of the target would be very high as the doll was widely marketed. M. Jakubowski showed how easily the doll could be hacked and accessed by cybercriminals. Finally, in terms of the inertia criteria, which can be interpreted in cyberspace as "files and technological specifications" offering varying levels of resistance (for example, file size or limitations of the tools used by the cybercriminal), it does not seem that there was any effective inertia resistance to prevent crimes from being successful.

There was no capable guardian as the Barbie doll simply lacked enough features to ensure its safety and security. Even if used in the presence of adults, the latter would not have been able to be capable guardians as it is difficult to consider that they would know about the doll's security flaws or if they did, that they would know how to prevent threats from materialising. Similarly, the poor security practices of the doll vendor suggest they are also not a capable guardian. With the Hello Barbie doll, it is easy to envisage the convergence in time and space of motivated offenders, suitable targets and the absence of a capable guardian. For example, the attacker could spy through the doll's microphone and use this opportunity to conduct any criminal activity he could think of at the time of his choosing, when capable guardians would not be present. He could also use information present on the doll to take over home Wi-Fi networks and hack into other devices.

The Hello Barbie doll is far from being the only smart home toy suffering from security problems. Another doll named Cayla has been denounced by German officials as enabling spying on families and gathering personal data.[143] This doll transferred the data it recorded to the United States. This not only posed threats to the family's security but was also incompatible with GDPR's requirements related to the protection of personal data, such as the ones regarding limitations of international data transfers. Moreover, in a technical analysis commissioned by the Norwegian Consumer Council, the study discovered that anyone could access the speakers and the microphone of the doll, without needing physical access to the device[144].[145] This serious security flaw resulted from the lack of any security measures concerning Cayla's Bluetooth connection. Anyone within approximately a 15-meter radius would have been able to connect to the doll and use this connection for potentially malicious purposes.

Both in the case of the Hello Barbie doll and Cayla, the implementation of relevant standards would have helped with ensuring that those devices are more secure and that users' personal data is safer. Standards might have been capable guardians against hacking the doll if implemented correctly. In particular, a requirement such as the "no universal default passwords" ETSI standard's requirement might have prevented issues.[146] This was not the case for Hello Barbie as, for example, the mobile API and ToyTalk website allowed users to use weak passwords, did not prevent brute force password attacks and allowed unlimited password guesses.[147] However, even if standards were implemented, the dangers related to storing and sending data into the cloud for processing by unknown third parties would be still present.

An effective implementation of standards and an edge led approach is the safest choice for consumers. Databox would have been able to act as a capable guardian. With Databox, the architecture places the processing of data at the edge of the network, in user's home environment and "enables the data subject to control external access to data via app manifests that provide granular choice encoded as enforceable data processing policies on-the-box, and constrains data distribution to the results of processing". Moreover, "The IoT Databox stores data in a distributed array of containers, which encrypt data at rest".[148] In this kind of environment, the hacker would have to overcome those security barriers to gain access to the doll's data. Children's conversations with the doll would not be sent to the cloud but stored locally. Finally, any unusual activity by the doll e.g. if it was attempting to export data to a remote server, parents would be informed through its easy to read interface and would be able to provide consent for any data leaving the box.[149]

4.3. *The mirai botnet, standards and the databox*

On the 20th of September 2016, the web page of a well-known journalist writing about profit seeking cyber-criminals has been taken down during one of the biggest Distributed Denial of Service (DDoS) attacks we have ever seen. This attack was caused by what has been later identified as the Mirai botnet. A botnet can be defined as "a group of malware infected computers also called "zombies" or bots that can be used remotely to carry out attacks against other computer systems."[150] Mirai has been considered by some as the "beginning of a chaotic and worrisome era of the Internet".[151] It has been seen as a

[143] A. Erickson, 'This Pretty Blond Doll Could be Spying on your Family' (2017) <https://www.washingtonpost.com/news/worldviews/wp/2017/02/23/this-pretty-blond-doll-could-be-spying-on-your-family/?noredirect=on&utm_term=.00adeafac872> accessed 12 May 2020

[144] Forbrukerradet (Norwegian Consumer Council), '#Toyfail An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys' (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf> accessed 19 July 2020

[145] Bouvet on behalf of the Norwegian Consumer Council, 'Investigation of Privacy and Security Issues with Smart Toys' (2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf> accessed 19 July 2020

[146] ETSI, 'EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements'

[147] Somerset Recon, 'Hello Barbie Initial Security Analysis' (2018) <http://static1.squarespace.com/static/543effd8e4b095fba39dfe59/t/56a66d424bf1187ad34383b2/1453747529070/HelloBarbieSecurityAnalysis.pdf> accessed 12 May 2020

[148] Urquhart, Crabtree and Lodge

[149] Crabtree and others

[150] OECD, 'Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL' (2008) <https://www.oecd.org/internet/ieconomy/40724457.pdf> accessed 19 July 2020

[151] J. Margolis and others, 'An In-Depth Analysis of the Mirai Botnet' (Proceedings 2017 International Conference on Software Security and Assurance (Icssa), Altoona, 2017)

wake-up call to include security concerns into the design and production of IoT devices.

If we applied the RAT analysis in this context, the motivated offender would be the 3 individuals who created the Mirai botnet and the botnet itself controlled by them. Those individuals wanted to use the botnet on people they held grudges against (the suitable targets) as well as to rent it to other motivated offenders (who could then use it against their own suitable targets) .[152] The reach of the botnet was therefore wide.

We will now apply RAT's VIVA properties to analyse the suitability of targets in the Mirai case. In terms of the value of the suitable targets, it is difficult to provide one answer as there were so many motivated offenders that might have used the botnet for their own specific reasons. However, the value of the targets must have been high for many offenders. The creators of the botnet assigned value to the fact that they could victimise people that they held grudges against as well as for economic reasons while those who rented Mirai might have had different ones. The variety of people the botnet could affect expanded the range and importance of value attached to suitable targets. Concerning targets' visibility, any person owning a smart home device could have been targeted by the botnet. The botnet actively scanned for vulnerable targets, making those with weak security defence mechanisms (in this case mainly default passwords) more accessible and therefore more suitable. Finally, there were no inertial properties that could make hacks more difficult.

There was no capable guardian as Mirai easily exploited the default and weak passwords of smart home devices such as IP cameras and internet routers. Users of those devices lacked knowledge and were not conscious of the security risks so they could not have been capable guardians. In the case of Mirai, there was convergence in time and (cyber)space of motivated offenders, suitable targets and the lack of a capable guardian. Companies must change their approach and be forced to ensure that no devices use default passwords. Standards would be capable guardians if they were effectively implemented. We cannot rely on consumers to know when and how to change their passwords. They should be guided through this process.

The implementation of a standard requiring to set up unique and well-protected passwords by the manufacturers and providers of IoT devices and services would have reduced the criminals' accessibility to victims, their suitability as targets and, therefore, possibly prevented the damage caused by the Mirai botnet. Questions such as how often will those passwords need to be changed, will users remember to change them and where will they store them, would need to be covered by cybersecurity standards to prevent threats from materialising. The ETSI standard asks for changing default passwords but does not provide a detailed enough answer to the previous questions. Standards should probably provide more guidance in relation to this issue.

On a side note, smart devices often talk with each other so it is important to prevent hackers from being able to gain control of all devices by only hacking one of them. We can imagine a situation where a hacker turns on a light bulb to let the system know that someone is home. The system (such as Google's Nest central app) would then turn off the smart alarm and the criminal could steal property without being detected. In this situation, there would be convergence in time and space of a motivated offender, a suitable target and the lack of a guardian. Concerning suitable targets, the value here would be property, the visibility the smart devices connected to the internet, accessibility their weak security settings and no inertial properties. The capable guardian would not be present as the hacker would be able to see, for example through smart cameras, that no one was home. One hack can lead to the whole smart home being under threat. Organisations developing and deploying IoT devices need to implement cybersecurity standards, and experts need to write the right standards, otherwise hackers will continue to have an easy job.

Going back to the Mirai case study, the features of the Databox would help as well as they would make systems resilient to outages for example. Key services would continue to work limiting the impact of the Mirai botnet. However, without implementing best practices based on standards, in particular in terms of password protection, the Databox would have difficulties in being a capable guardian in the Mirai affair. While safer than cloud architectures, the edge also has its limitations. It is essential for standards to support Databox in ensuring the security of smart homes and their owners. Architectures, standards and regulations implemented together can become a capable guardian.

5. Conclusion and future research

Today, smart homes are insecure environments. The high number of security breaches, the rising number of internal and external threats linked to smart home devices, and the many situational and informational harms they have caused prove this.

Standards influence the activities of all stakeholders in the IoT world. Current standards written to increase security in smart homes are developed on the basis of cloud architectures. They are often obvious demands setting out what should have been done from the beginning such as the "no default password" requirement. Unfortunately, IoT products often continue to ignore those requirements, standards do not contain enough guidance on how the latter should be implemented and security breaches continue to take place.

A new architecture to help mitigate harms is needed. RAT helped us see inadequacies in current standards and also helped us analyse the value of edge computing for creating a safer and more secure architecture. PIMS such as the Databox are an opportunity to foster the successful development of smart homes as they can make IoT devices and services more accountable to individuals than in a cloud archi-

[152] Engadget, 'Mirai Botnet Hackers will Serve their Time Working for the FBI' (2018) <https://www.engadget.com/2018/09/20/mirai-botnet-hackers-serve-time-fbi/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=DM2YAeitgnx0utn80b3opg> accessed 12 May 2020

tecture scenario.[153] Furthermore, by moving to the edge, we are able to remedy the absence of 'reliable guardians' which can then protect the 'suitable targets' of insecure IoT devices from 'motivated offenders'. Of course, companies have reasons to continue using the cloud-based architectures for IoT products. Mining data of consumers can contribute to increasing their revenue streams and economic benefits. However, there is no reason why companies would not switch to the Databox model if they were incentivised to do so, for example, by policy makers who could take measures that benefit those adopting the Databox. Indeed, under article 25 of the GDPR, companies should already be putting in place data protection by design and default, by employing organisational and technical safeguards to protect processing of personal data. Moreover, more research is needed to evaluate whether the benefits of gaining the trust of consumers and making smart homes more secure are higher for IoT stakeholders than the benefits currently associated with convenience of the cloud (as contrasted with concerns about mining users' data in the cloud).

There should also be more research done on the actual content of standards written for edge computing. Some of the latter would differ from the cloud-based standards as the local storage of data and how to maintain a secure environment would require guidance for vendors of such edge approaches. Moreover, current standards do not keep up with threat levels, do not provide enough detail on the best approach to take and many standards are written by various organisations on the same topic (which adds to the confusion around best practices in standards' implementation).

We also argue in favour of understanding technology use in practice. There are increasing numbers of in-home human threats linked to smart home devices, in addition to the vast external threat landscape. As we have seen, no standards dealing with these problems seem to have been developed so far. Maybe it's an omission which needs to be rectified (standards could potentially shape design of IoT products to remove affordances for in-home human threats) or maybe they are not the right instrument to do so. Nevertheless, further research in this area is needed. If standards cannot help in this context, are there other regulatory tools that could resolve human threats inside the home? Criminal law may be one, but this moves us into a separate domain, requiring focus on digital forensics for evidence collection and access to justice to prosecute cybercrimes. Securing the IoT needs us to rethink current technical architectures, question the social dimensions of attack(ers) and threats, and question assumptions underpinning emergent IoT standards.

Declaration of Competing Interest

The authors declare no conflict of interest.

Acknowledgements

This work was supported by the Economic and Social Research Council [grant numbers EP/L015463/1, EP/T022493/1, EP/R03351X/1, EP/M02315X/1, EP/S023305/1].

[153] Crabtree and others