The Quarterly Magazine for **Digital Forensics Practitioners**

Issue 35 • May 2018

DIGITAL FORENSICS Magazine

REPORT

Forensics Europe Expo

Intelligence & Investigations for the Internet of Things

DFM Sponsored Seminar

Seeing What Isn't There

Flash Memory Amnesia & Digital Forensics

PLUS

- IoT 4n6
- Standardising IoT Security
- Mitigating the Nightmare of APTs
- **From the Lab:** Data Hiding in Slack Space

35
9 772042 061004
Issue 35 / £14.99
TR Media

Standardising IoT Security: Implications for Digital Forensics

Irina Brass investigates the latest trends in standardising IoT security for complex cyber-physical systems and its challenges for Digital Forensics.

The Internet of Things (IoT) is receiving growing attention from businesses, policy-makers, the media and consumers [1], [2]. Now, it is also in the spotlight for the challenges it raises to digital forensic investigators.

Digital forensics is faced with a difficult balancing act. On the one hand, the IoT is becoming a rich source of evidence, used across a wide range of activities, from criminal investigations [3] to liability claims. On the other hand, the IoT itself adds new security vulnerabilities to existing digital and physical infrastructures, which may challenge data integrity and recovery, as well as the safety of individuals and the wider public. These are only some of the reasons why establishing a baseline for IoT cyber security has become a pressing issue for governments, industry, regulatory agencies and standards development organisations [4]-[7]. But what exactly is so disruptive about the IoT, given that the technologies and processes that make up an end-to-end IoT system have been around for a while (e.g. RFID, LANs, cloud computing etc.)?

The IoT as Disruptive Innovation

At a basic level, the IoT is a process that embeds sensing, communication, data processing and actuation techniques into physical objects and infrastructures. Thus, an IoT system is characterised by "a proliferation of visible and hidden sensors that collect and transmit data; processes that interpret and make use of the aggregated information; and actuators that, on the basis of this information, take action without direct human intervention" [8].

According to a recent report commissioned by OFCOM (the communications regulator in the UK), the number of IoT connections in the country is estimated to reach 155.7 million by the end of 2024, at an expected compound average growth rate of approximately 36%. The report also identifies three market segments of rapid growth: consumer electronics (and fast-moving consumer goods), automotive, and utilities [9].

The combined effects of rapid IoT uptake, and the increased 'embeddedness' and connectivity of physical objects and infrastructures, are triggering three main disruptions relevant to digital forensics. First,

Internet Connected People and Things

Guess what? The International Telecommunications Union estimates that the total number of Internet users in the world has reached 3.2 billion in 2015. Gartner, Inc. forecasts that over 20 billion connected "things" will be in use by 2020.

Insecure IoT is not only threatening the resilience of the Internet infrastructure, but is also exposing blind spots and misalignments between regulatory frameworks that have been dealing with data protection, cyber security, safety and product liability in a siloed manner.

they are leading to increased pervasiveness, invisibility and variability of IoT systems across several application domains, from consumer goods to critical infrastructures. Each of these systems can vary in terms of their topology, the device type, security specifications, data formats and storage across multiple locations [10]–[12]. This is further complicated by the use of proprietary standards for various processes, such as data formats, protocols, and interfaces. This complexity requires new tools and techniques that integrate mobility and cloud forensics into established digital investigation practices, while requiring enough flexibility to understand use typologies for different devices and services, as well as different data flows and trails.

Secondly, as the IoT adds data gathering, communication and automation layers to physical objects and infrastructures, it also creates new cyber-physical interactions and interdependencies that are not fully understood from a technical and regulatory perspective [13], [14]. This brings new challenges to digital forensic investigators, who need awareness of new types of cyber-physical vulnerabilities that may emerge from the application of IoT in physical processes and infrastructures, ▷

EXPERT TIP

The standards world can be quite daunting. A useful way to navigate it is to think of standards as falling into three broad categories:

1. *Technical specifications that address the general design of a component or system.*
2. *Performance standards, which generally address organisational or procedural requirements, such as risk assessment procedures.*
3. *Outcome standards, which focus on the achievement of a desired outcome, such as safety.*

Standards are also divided into two broad categories: de facto or market-driven standards, developed by industry players or consortia, and de jure standards, developed by formal standardisation organisations such as the BSI in the UK or ISO internationally.

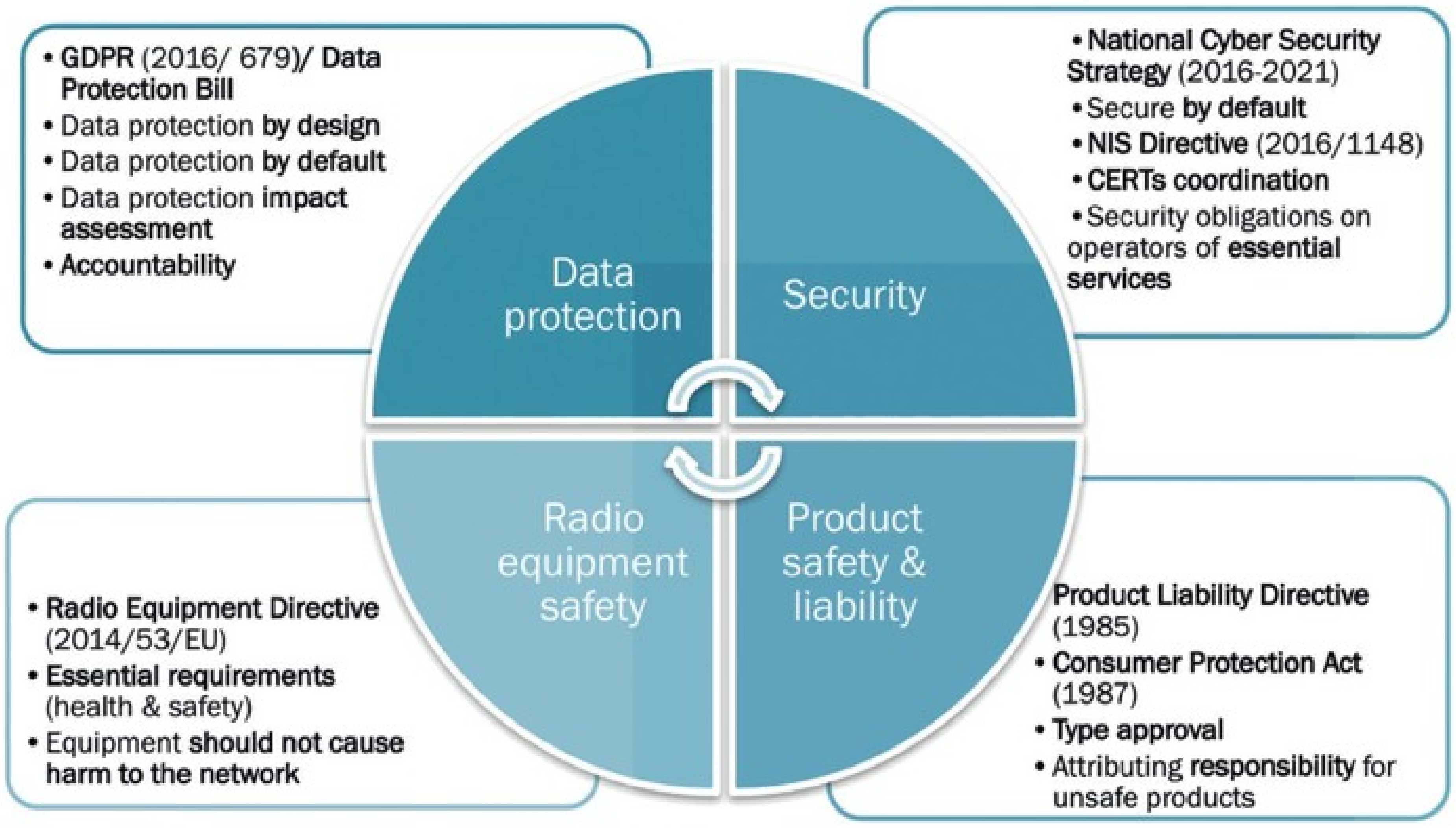

Figure 1. Regulatory Frameworks

> ***Manufacturers of smart products have struggled to internalise the costs of cyber security into their business models, and coupled with highly competitive global supply chains, they are under pressure to place smart but insecure devices on the market.***

which otherwise require high levels of safety, reliability and resilience. The growth of Industrial IoT in manufacturing, transport, utilities and health provides useful examples of these complexities [15]. This also raises a scaling-up problem, whereby forensic investigations are put under pressure to understand system behaviours that includes human factors, physical and digital processes, all coupled in complex ways [16].

Lastly, the IoT is known for contributing to the security threat landscape, by connecting endpoints with low hanging security vulnerabilities [17], as well as raising several data protection concerns [18]. Given the rapid IoT uptake, manufacturers of smart products have struggled to internalise the costs of cyber security into their business models, and coupled with highly competitive global supply chains, they are under pressure to place smart but insecure devices on the market. This behaviour is not only threatening the resilience of the Internet infrastructure, as seen with the Mirai-based botnet, but is also exposing blind spots and misalignments between regulatory frameworks that have been dealing with data protection, cyber security, safety and product liability in a siloed manner (Figure 1) [19], [20]. This is not only a challenge for regulators, but also for digital forensic investigators, who need to understand the wide range of security vulnerabilities and associated risks that IoT devices, services and systems pose to individual consumers and the public at large.

Connected and Autonomous Vehicles (CAVs) are a very good example of complex cyber-physical systems that expose the disruptive effects discussed above.

The investment that has been channelled into CAVs and other IoT systems over the past years has also prompted policy-makers, regulators and industry players to consider ways of standardising IoT security, as a means of establishing a baseline of good practice that could reduce security vulnerabilities derived from the IoT. Beyond an interest in consumer safety and security, as well as business continuity, this baseline could benefit digital forensic investigators by supporting the development of standardised tools, processes and guidance for identifying, preserving and analysing data in complex cyber-physical systems.

Connected & Autonomous Vehicles (CAVs)

CAVs are sometimes portrayed as a thing of the future. However, they are very much an 'IoT thing' of the present. Since 2016, the UK Government has established a £15 million 'connected corridor' from London to Dover (A2/M2), as a public-private partnership to trial the advancement of in-vehicle, vehicle-to-vehicle (V-2-V), and vehicle-to-infrastructure (V-2-I) technologies. Brass et al. [21] argue that the rapid increase in automation and connectivity in motor vehicles "raises important questions about our readiness to understand and regulate interdependencies in cyber-physical systems that integrate computation, communication processes and physical systems in smart environments". These have several implications for how we currently regulate defective product liability, supply chain management, safety assurance processes, and cyber security. And they also raise crucial issues for digital forensics.

As our cars become more connected and communicate with the objects and physical infrastructures around them, they can also become more vulnerable to attacks. In such dynamic environments, an attacker "may exploit a number of minor vulnerabilities that emerge as a the result of component updates by different entities, each of little significance on their own, but with damaging interactive consequences for system integrity and vehicle safety within the connected environment" [21]. For digital forensics, identifying these vulnerabilities in a highly mobile environment, where data travels across several objects and stakeholders, and is communicated via several local and wide areas networks, can be highly problematic.

In addition, CAVs raise important questions about establishing liability in defective products. In current legislation, motor vehicles are treated as products, and liability for product defects is placed with the producer and or importer of the vehicle. However, this liability framework speaks to physical rather than software 'defects' [22]. In this context, it is likely that digital forensic investigators will be asked to identify, collect and analyse evidence about the cyber security and integrity of the entire system, as it could have consequences for the physical processes of the vehicle and, more so, for the physical safety and security of human beings.

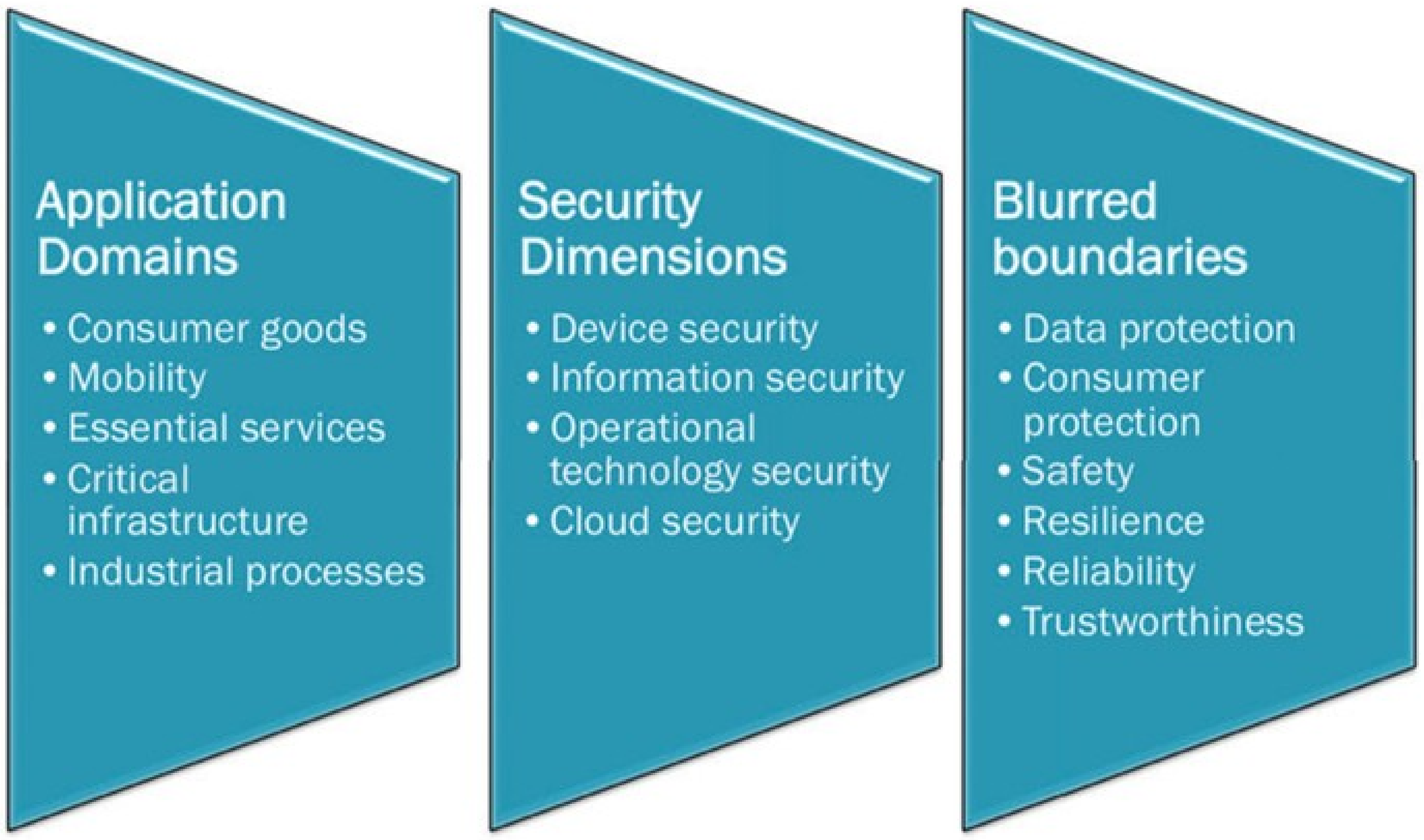

Figure 2. IoT Security Domains

Can a Baseline for IoT Security be Achieved?

Several approaches to standardising IoT security are currently emerging. They follow from increased awareness that IoT security vulnerabilities impact consumers, businesses, operators and managers of critical infrastructures, as well as governments who have a duty of care to balance the opportunities and risks associated with emerging technologies.

A first approach is the proposal of legislation and regulations to adopt minimum cyber security standards for the IoT. Such proposals have been introduced in the US, through the IoT Cybersecurity Improvement Bill, requiring written proof of third-party security certification in public acquisition contracts and procurement of IoT systems; and in the EU, though the proposal of a Cybersecurity Act, which aims to establish an initial voluntary cybersecurity certification scheme based on three assurance levels. Whereas these legislative proposals aim to ensure compliance with cyber security good practices through certification schemes, they do not and cannot specify what these principles and good practices should be.

In addition, achieving a baseline of IoT security across several application domains is proving problematic. IoT security in a smart home environment is different from IoT security in healthcare or critical infrastructure (Figure 2). Whereas the focus on IoT security in the smart home is at the device, hub, or cloud level, with implications for data protection; in industrial processes and systems the focus is on interdependencies between established control systems, operational technologies (OT) and information technologies (IT), with implications for safety, reliability and resilience of these complex systems. In addition, conducting good practice safety and security in highly critical cyber-physical systems may sometimes be contradictory, as increasing the real-time safety of the system may actually decrease its overall security.

In order to respond to these challenges, several governments and industry consortia have developed Codes of Practice that set high-level guidelines for IoT security. In the UK, the government has already proposed high-level principles in several IoT application domains, such as CAVs and smart consumer goods (Box 2).

Similarly, industry consortia have developed codes of practice, guidelines and technical specifications for establishing a baseline of IoT security. Increasingly, these guidelines are supplemented by compliance testing procedures and certification schemes. But the development of these de facto standards and guidelines are also contributing to the fragmentation of the IoT security standards landscape, leading to parallel certification schemes that can place high compliance costs on businesses. Equally, this fragmentation can complicate digital forensic investigations as data could be encrypted or stored in various formats, depending on the adopted specifications.

In addition, the development of formal standards pertaining to IoT security is also fragmented and relatively slow moving. This is in part due to the consensus-based, highly institutionalised approval and review processes of formal standardisation. ▷

Promoting Codes of Practice in CAVs and Consumer IoT

The UK Government has published several Codes of Practice for IoT Security. These set basic security design principles for IoT as well as organisational best practices. However, at the moment, these Codes of Practice remain voluntary and are not enforced through mandatory requirements.

Examples of Key Principles of Cyber Security for Connected and Automated Vehicles, DfT: [25]

- ***Principle 2.4:** Security risks, specific to, and/or encompassing, supply chains, sub-contractors and service providers are identified and managed through design, specification and procurement practices.*
- ***Principle 3.3:** There is an active programme in place to identify critical vulnerabilities and appropriate systems in place to mitigate them in a proportionate manner.*
- ***Principle 3.4:** Organisations ensure their systems are able to support data forensics and the recovery of forensically robust, uniquely identifiable data. This may be used to identify the cause of any cyber, or other, incident.*

Examples of Key Principles for Security in Consumer IoT Products and Associated Services, DCMS: [4]

- ***Principle 1:** No default passwords. All IoT device passwords must be unique and not resettable to any universal factory default value.*
- ***Principle 3:** Keep software updated. All software components in internet-connected devices should be securely updateable. Updates must be timely and not impact on the functioning of the device. An end-of-life policy must be published for end-point devices, which explicitly states the minimum length of time for which a device will receive software updates and the reasons why. [...] For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.*

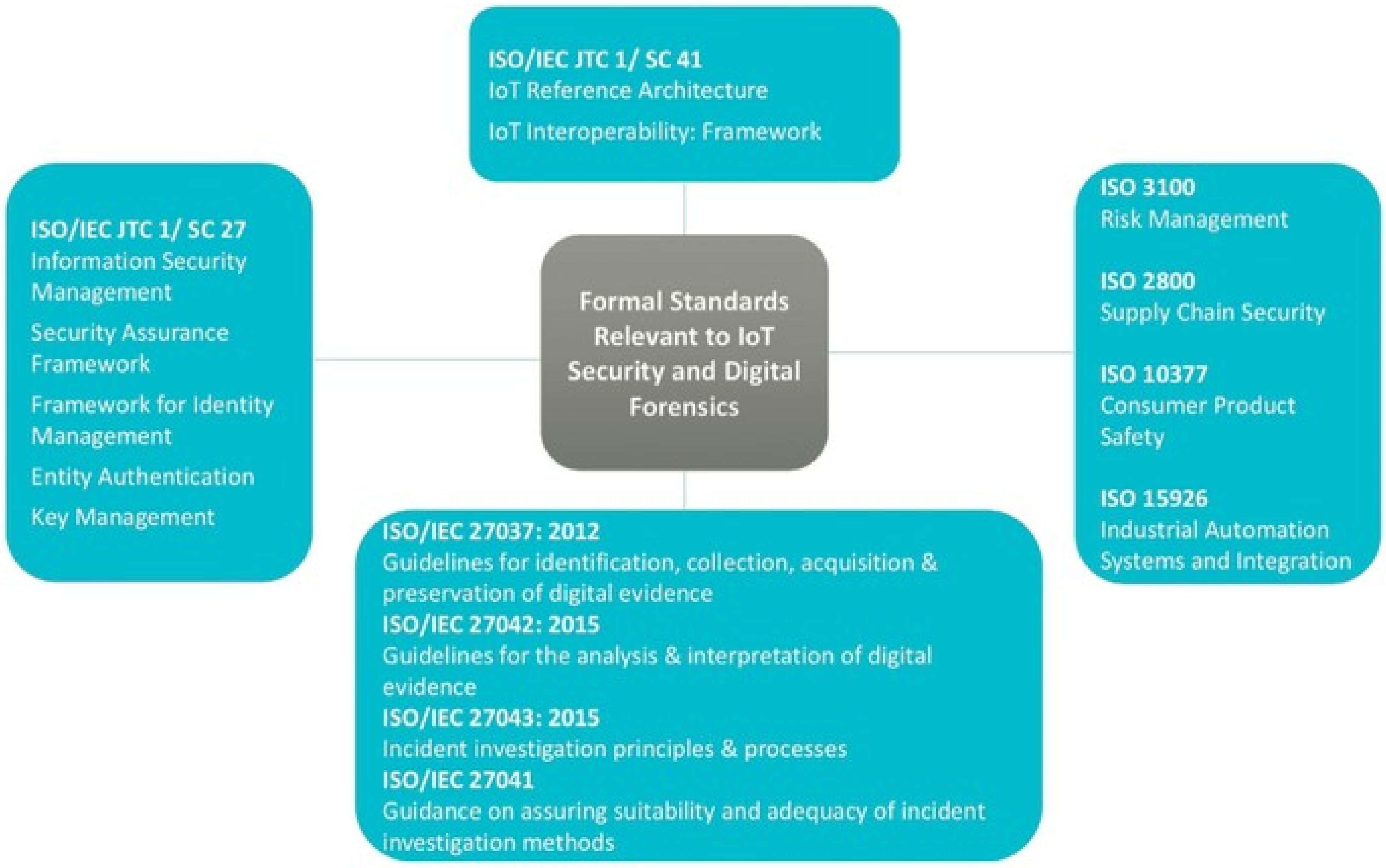

Figure 3. ISO Standards

MORE INFO

Interested in other Codes of Practice relevant to IoT security and data integrity? Here are a few examples from the US.

1. *Strategic Principles for Securing the Internet of Things, 2016 [26] Outlines core principles of cyber security for IoT; it is one of the first codes of practice to have been published by a government department.*
2. *Postmarket Management of Cybersecurity in Medical Devices. Guidance for Industry and Food and Drug Administration Staff, 2016 [27] Outlines connected medical device cybersecurity risk management.*
3. *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety, 2016 [28] Proposes a framework for CAVs performance guidance that integrates safety and cyber security.*

Standardising such complex processes, with different topologies and use typologies across different IoT application domains is challenging for formal standardisation organisations, which have traditionally dealt with each of these issues in separate technical jurisdictions.

But, when it comes to IoT security, it is also a consequence of the blurring of boundaries between information security, physical security & safety that characterise complex cyber-physical systems. Standardising such complex processes, with different topologies and use typologies across different IoT application domains is challenging for formal standardisation organisations, which have traditionally dealt with each of these issues in separate technical jurisdictions. An example of this challenge is the diversity of ISO standards that can apply to aspects of IoT security and digital forensic investigation (Figure 3).

Achieving alignment across these standards is a difficult, if not impossible, task. However, at a minimum level, more can be done to develop and harmonise standards that map and model vulnerabilities at the intersection of security and safety, and that develop classifications of risk in cyber-physical systems. This also offers an opportunity to inform, review and update established guidelines for the identification, collection and analysis of digital evidence in complex cyber-physical systems.

Where Next for IoT Security and Forensics?

Developing a baseline of IoT security is proving difficult at the moment. This is not only due to the blurring of boundaries between physical security, cyber security, safety, reliability and resilience that complex cyber-physical systems bring. It is also challenging because cyber security is inherently a dynamic process of vulnerability discovery and correction, with different requirements across IoT application domains and verticals.

However, if we are slowly moving in the direction of standardising and even regulating IoT cyber security as safety, using outcome-based standards and risk-based regulatory frameworks, then we should also consider the implications for digital forensics. The complex interdependencies inherent in cyber-physical systems, such as Connected and Autonomous Vehicles (CAVs), could imply that, increasingly, digital forensic investigators work alongside safety forensic investigators. Training and the development of standardised tools for identifying, collecting, analysing and preserving evidence in such dynamic and interdependent environments is a must. •

Dr Irina Brass *is Lecturer in Regulation, Innovation and Public Policy at UCL Department for Science, Technology, Engineering and Public Policy (UCL STEaPP). She is also Co-Investigator in the Standards, Governance and Policy Stream of the EPSRC-funded PETRAS IoT Research Hub. Her research focuses on the economic and social regulation of disruptive technologies, especially digital technologies, and she is currently working closely with policy makers and the standards development community on governance frameworks for managing cybersecurity and data protection in the Internet of Things (IoT). In 2017, Dr Brass was appointed Chair of the IoT-1 Technical Committee of the BSI - the UK National Standards Body. Dr Brass is also the Deputy Programme Lead of the MPA in Digital Technology and Public Policy at UCL STEaPP.*

REFERENCES

1. OECD, The Next Production Revolution: Implications for Governments and Business. OECD Publishing, 2017 [Online]. Available: http://www.oecd-ilibrary.org/science-and-technology/the-next-production-revolution_9789264271036-en. [Accessed: 18-Jan-2018]
2. CIGI, 'Global Commission on Internet Governance. One Internet', 2016 [Online]. Available: https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf. [Accessed: 22-Jan-2018]
3. H. Edwards, 'Alexa Takes the Stand: Listening Devices Raise Privacy Issues', Time, 05-Apr-2017 [Online]. Available: http://time.com/4766611/alexa-takes-the-stand-listening-devices-raise-privacy-issues/. [Accessed: 18-Apr-2018]
4. UK Department for Digital, Culture, Media and Sport, Secure By Design: Improving the Cyber Security of Consumer Internet of Things Report. 2018 [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf. [Accessed: 08-Mar-2018]
5. US Senate, 'Internet of Things Cybersecurity Improvement Act'. Jul-2017 [Online]. Available: https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt
6. ENISA, 'Baseline Security Recommendations for IoT in the context of Critical Information Infrastructure', Nov. 2017 [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
7. BSI Group, 'IoT Assurance Services'. [Online]. Available: https://www.bsigroup.com/en-GB/industries-and-sectors/Internet-of-Things/IoT-Assurance-Services/. [Accessed: 03-Jan-2018]
8. L. Tanczer, I. Brass, M. Elsden, M. Carr, and J. Blackstock, 'The United Kingdom's Emerging Internet of Things (IoT) Policy and Legislative Landscape', in Rewired: Cybersecurity Governance, Wiley, forthcoming.
9. Cambridge Consultants, 'Review of Latest Developments in the Internet of Things.pdf', OFCOM, May 2017 [Online]. Available: https://www.ofcom.org.uk/__data/assets/pdf_file/0007/102004/Review-of-latest-developments-in-the-Internet-of-Things.pdf. [Accessed: 03-Jan-2018]
10. R. C. Hegarty, D. J. Lamb, and A. Attwood, 'Digital Evidence Challenges in the Internet of Things', p. 10.
11. Scar, 'Internet Of Things Mobility Forensics', Forensic Focus, 17-May-2017 [Online]. Available: https://articles.forensicfocus.com/2017/05/17/internet-of-things-mobility-forensics/. [Accessed: 15-Apr-2018]
12. S. Watson and A. Dehghantanha, 'Digital forensics: the missing piece of the Internet of Things promise', Computer Fraud & Security, vol. 2016, no. 6, pp. 5–8, 2016.
13. A. S. Elmaghraby and M. M. Losavio, 'Cyber security challenges in Smart Cities: Safety, security and privacy', Journal of Advanced Research, vol. 5, no. 4, pp. 491–497, Jul. 2014 [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S2090123214000290. [Accessed: 02-Mar-2018]
14. Z. A. Baig et al., 'Future challenges for smart cities: Cyber-security and digital forensics', Digital Investigation, vol. 22, pp. 3–13, Sep. 2017 [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1742287617300579. [Accessed: 02-Mar-2018]
15. Industrial Internet Consortium, 'Testbeds'. [Online]. Available: http://www.iiconsortium.org/test-beds.htm. [Accessed: 18-Apr-2018]
16. C. Maple, 'Security and privacy in the internet of things', Journal of Cyber Policy, vol. 2, no. 2, pp. 155–184, May 2017 [Online]. Available: https://doi.org/10.1080/23738871.2017.1366536
17. Krebs on Security, 'Hacked Cameras, DVRs Powered Today's Massive Internet Outage'. 21-Oct-2016 [Online]. Available: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/. [Accessed: 18-Apr-2018]
18. P. Oltermann, 'German parents told to destroy doll that can spy on children', the Guardian, 17-Feb-2017. [Online]. Available: http://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children. [Accessed: 18-Apr-2018]
19. I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock, 'IoT Security: A Review of the Regulatory and Standards Landscape. Presentation at the Royal Society (RS) Conference "Internet of Things: Opportunities and Threats".', 11-Mar-2017 [Online]. Available: http://www.youtube.com/playlist?list=PLg7f-TkW11iWmGIFJ9-IkIfflcwRt9s74. [Accessed: 11-Jan-2018]
20. P. Taylor et al., 'Internet of Things: Realising the Potential of a Trusted Smart World', Royal Academy of Engineering, PETRAS IoT Research Hub, Mar. 2018 [Online]. Available: https://www.raeng.org.uk/publications/reports/internet-of-things-realising-the-potential-of-a-tr. [Accessed: 18-Apr-2018]
21. I. Brass, M. Carr, L. Tanczer, C. Maple, and J. Blackstock, 'Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles', Connected and Autonomous Vehicles: The Emerging Legal Challenges, vol. Pinsent Masons, pp. 08–10, May-2017 [Online]. Available: https://www.pinsentmasons.com/PDF/2017/Freedom-to-Succeed-AMT/Connected-autonomous-vehicles-report-2017.pdf. [Accessed: 18-Apr-2018]
22. Guardtime, 'Connected Vehicle. Real-time Situational Awareness for On-Board Systems'. [Online]. Available: https://guardtime.com/solutions/connected-car. [Accessed: 15-Apr-2018]
23. European Commission, COM(2017) 477 Final Proposal for a Regulation of The European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''). 2017 [Online]. Available: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en
24. G. Sabaliauskaite and A. P. Mathur, 'Aligning Cyber-Physical System Safety and Security', in Complex Systems Design & Management Asia, Springer, Cham, 2015, pp. 41–53 [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-12544-2_4. [Accessed: 18-Apr-2018]
25. UK Department for Transport, The Key Principles of Cyber Security for Connected and Automated Vehicles. 2017 [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf. [Accessed: 11-Jan-2018]
26. US Department for Homeland Security, Strategic Principles for Securing the Internet of Things. 2016 [Online]. Available: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf. [Accessed: 27-Dec-2016]
27. US Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. 2016 [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. [Accessed: 11-Jan-2018]
28. US National Highway Traffic Safety Administration (NHTSA), Federal Automated Vehicles Policy: Accelerating the Next Revolution In Roadway Safety. 2016 [Online]. Available: http://www.safetyresearch.net/Library/Federal_Automated_Vehicles_Policy.pdf. [Accessed: 11-Jan-2018]
29. I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock, 'Standardising a Moving Target: The Development and Evolution of IoT Security Standards', in IET Conference Proceedings, forthcoming [Online]. Available: https://events.theiet.org/petras/programme.cfm