Towards a Secure and Resilient IoT Architecture for Smart Home Energy Management

Hugh Boyes[1*], Tim Watson[1]

[1]WMG Cyber Security Centre, University of Warwick, Coventry, UK.
** hb@warwick.ac.uk*

Keywords: smart home, architecture, security, energy demand, systems integration

Abstract

This paper examines the development of consumer IoT solutions for the control of electrical energy in the home. Use of smart appliances is at the centre of the UK Government's strategy for managing CO_2 emissions and domestic electricity demand. The current market for IoT-enabled products that control domestic lighting and heating is rapidly evolving with a range of devices already available. Development of demand side response solutions will see these devices and smart appliances being integrated into consumer energy management solutions. The paper examines the architecture and security implications of these developments, explores some of the security risks and identifies a number of mitigation measures. It concludes by identifying future work that is required to address the security threats, both in the home and to the electricity supply system.

1 Introduction

From a consumer perspective the concept of living in the Internet of Things is probably best conceptualised in terms of the creation and delivery of "Smart Homes". Whereas, from a governmental perspective, a key driver for promoting smart homes and smart appliances is to address the socio-economic challenge of managing domestic energy demand, thus reducing CO_2 emissions and making best use of infrastructure and renewable energy sources. The UK Government's Industrial and Clean Growth Strategy [1] seeks to encourage consumers to become more directly involved in managing demand in the electricity system using smart appliances that react to the availability of electricity on the grid in determining their operational cycle. It is estimated that heating in buildings and industry currently accounts for around 32% of the total UK CO_2 emissions [2].

A smart appliance can be characterised as one that is communications-enabled and responsive to price and/or other signals by moderating its electricity consumption. The degree to which the energy responsive functionality, referred to as demand side response (DSR), is automatic will be determined by the appliance's smart functionality and the degree to which the consumer chooses to enable responses to price or other signals. The smart appliances are likely to include: cold and wet goods typically found in a domestic kitchen or utility room, electric vehicle (eV) charge points, electric heating controllers and future smart electrical devices used in the domestic environment.

The increasing distributed control of the UK electricity power network using consumer smart technologies exposes it to cyber security risks [3]. This paper considers the cyber security risks that may impact grid security, the security of the smart appliances, device interoperability and data privacy.

The structure of the papers is as follows, section 2 examines the likely future connections to a "Smart Home" and their relationships in respect of electricity supply and consumption. Section 3 explores the potential interactions between organisations involved in the production, transmission, distribution and use of electricity. Section 4 examines the security risks, section 5 discussed potential mitigation measures, whilst section 6 contains conclusions and recommendations for future work.

2 The future smart home

2.1. Current smart home solutions and appliances

Many potential first generation components of a future smart home are already on sale to the public, for example:

- smart heating solutions offered by HIVE™, Lightwave™, MiHome™, nest™ and Wiser™ - typically comprise a proprietary hub with Wi-Fi connected replacement heating controllers, thermostats, and thermostatic radiator valves (TRVs);
- smart lighting systems HIVE™ and PHILIPS™ - delivering wireless control of smart light bulbs using a Zigbee™ network form a Wi-Fi enable proprietary hub; and
- 'smart' power via plug-in RF controlled adaptors (all of the above manufacturers);
- smart energy storage, for example the Tesla Powerwall™, a battery and inverter system that stores electricity from the homes solar panels nd using it to reduce the amount of electricity drawn from the public supply.

These smart devices are generally provided with manufacturer specific applications (apps) that can be downloaded from the Apple™ and/or Google™ app stores. A number of them work with integration products such as Amazon's alexa™.

A range of 'smart' appliances are now being offered for sale and generally rely upon a Wi-Fi connection to a home hub or router to enable user access to the smart functionality. Appliance types that offer remote control or programming include:

schematic in Figure 2 illustrates a potential future smart home.

The smart home draws electricity from the public supply and supplements it with energy generated through a solar panel and which stored in a local battery system. The distribution of

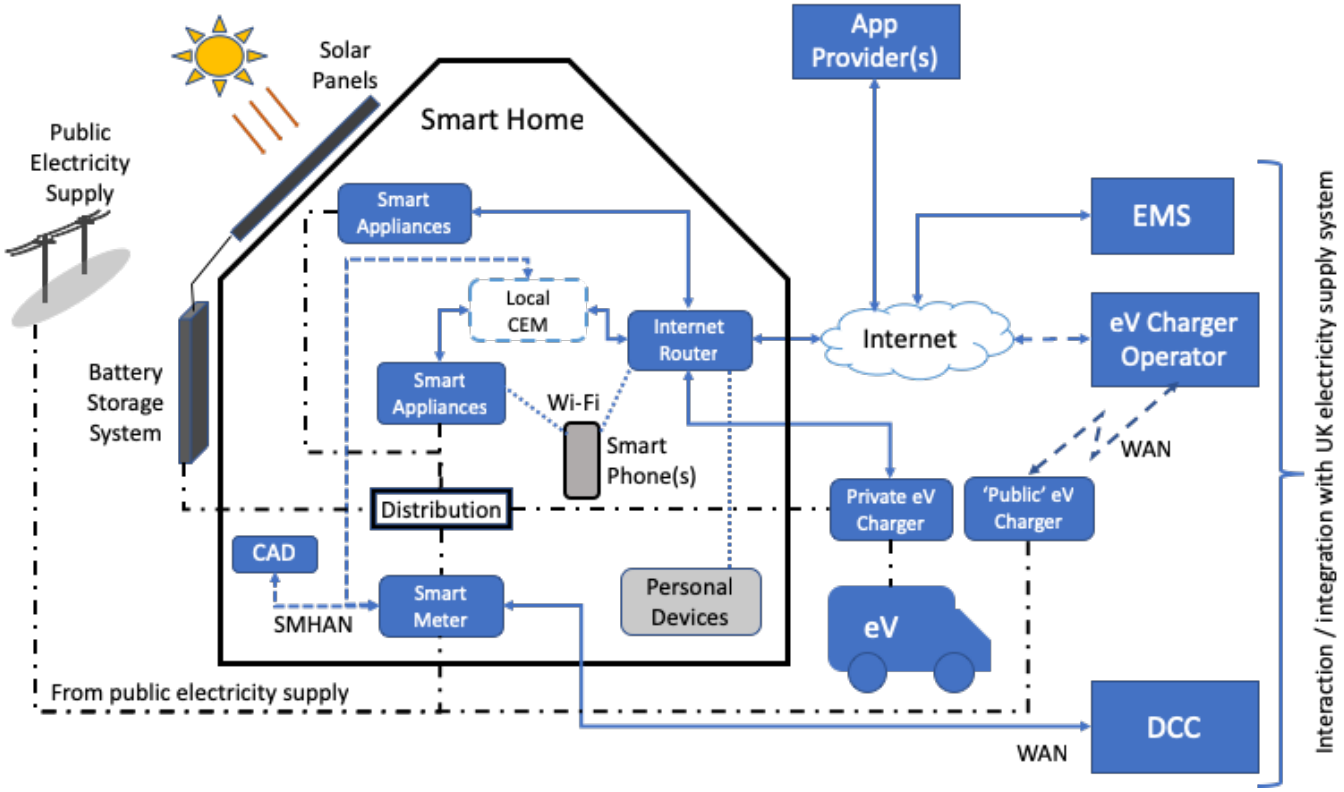

Figure 1 - Potential energy related systems in and connectivity to future Smart Home. Adapted from [5]

- Smart cooking appliance, e.g. microwave, oven, hobs, kettles and coffee makers;
- Smart cleaning appliance, e.g. dishwashers, washing machines, and robotic floor cleaners;
- Smart fridges.

Typically, the above appliances employ a manufacturer's app that permits a user to schedule their use and to remotely vary that schedule where the home router or hub has Internet connectivity.

The functionality outlined above is primarily low-level automation, partially replacing a person's physical interaction with the device or appliance by remote control via an app. A number of the smart solutions offer the capability for the user to programme 'recipes' using IFTTT (If This Then That), a web-based service that allows users or developers to create chains of simple conditional statements, called applets [4]. IFTTT is the IoT equivalent to the ladder logic found in an industrial programmable logic controller (PLC).

2.2. Anatomy of a future smart homes

To deliver the UK Government's vision of reduced domestic CO_2 emissions and managing electricity demand using DSR the future smart home will become a significantly more complex electrical and electronic environment. The

the energy is though type approved wiring, outlets and control components that comply with the electrical safety regulations, currently BS 7671 [6].

The external electricity supply passes through a smart meter that provides meter readings to the data communications centre (DCC) and receives time- and demand-based tariff information from the consumer's energy supplier. The smart meter communicates via a home area network (SMHAN) with a consumer access devices (CAD) to display electricity consumption and tariff information.

The smart home occupier has a number of smart appliances, e.g. a smart lighting system operated through a standalone local hub via a smart phone app, both of which are periodically updated via the Internet. The major appliances, i.e. cooking and wet goods are connected to a local customer energy manager (CEM) hub, which in conjunction with a cloud-based energy management service (EMS) provide DSR functionality.

The occupier's fossil-fuelled car has been replaced by an eV which is charged using a private charger. The occupier has agreed to host a public eV charger which is accessible on the road-side perimeter of the property.

The above vision of the future smart home assumes that an external supplier will have direct control over home devices, as part of a DSR contract with the occupiers. An alternative approach may be to use tariff variations as signals to an in-home CEM, with the occupier determining the relative price sensitivity of different appliances.

2.3. Demand side response (DSR)

The UK electricity transmission and distribution network is managed by a Electricity System Operator (ESO) who is responsible for balancing the network, i.e. maintaining the supply in line with demand, and managing a safe, resilient, and cost-effective electricity system [7].

DSR is a tool that can enable the ESO to manage short-term capacity issues, both in terms of generation and constraints in the transmission and distribution of the electricity to end users. Through the use of temporal changes in wholesale tariffs the ESO can signal system capacity. For example, when the generated electricity is likely to exceed demand, particularly from renewable sources, the tariff could be reduced to encourage consumption, by appliances or for storage in domestic batteries and eVs. At times where demand is likely to exceed supply the tariffs can be raised to discourage consumption, e.g. through reduced use of appliances or by drawing upon stored energy held in domestic batteries systems and parked eVs.

The tariff price signalling to domestic consumers is likely to be handled by energy management companies – these market players may be energy supply companies performing an arbitrage role or service companies offering tariff (price) comparison services to allow consumers to choose the optimum time to use electricity. The consumer may decide to automatically reduce consumption for some appliances based on specific tariff changes, time of day and weather conditions.

A second element of DSR is the ability to force reductions in consumption, which provides a short-term protective measure for the transmission and distribution networks in periods of excessive demand. This type of signal may, for example, temporarily suppress the use of a compressor in a domestic freezer. Response to these signals is likely to be automatic for any DSR enabled appliances. In this scenario the appliance may resuming normal operation after a pre-set time or if specific conditions are fulfilled, e.g. the temperature in the freezer rises to a specified but still safe level.

2.4. DSR components in the smart home

To implement DSR is a domestic environment the following components will be required:

- DSR-enabled smart appliances, these may be connected directly to the internet via a home router or via a local CEM;
- a CEM, which may be a local physical device, e.g. a local hub, or a virtual cloud-based device;
- a consumer/user interface, that may be provided via a smart phone app or a web-based portal;
- tariff information, which may be provided via the smart meter over the SMHAN or via the EMS.
- connectivity to an EMS that receives capacity and tariff information (wholesale and/or consumer) from the ESO and energy suppliers.

Use of a CEM potentially allows a consumer to predetermine how to respond to tariff changes through use of semi-autonomous control functions, i.e. responding in a pre-set manner to specific demand or tariff signals, or it may only provide a gateway function with all control actions determined by a cloud-based service [8] based on individual customer decisions and their electricity supply contractual obligations. A CEM may integrate aspects of both control methods to ensure emergency signals and additional flexibility services are implemented in accordance with the supply contract, e.g. during times of severe network stress. The semi-autonomous nature of the CEM represents a potential security risk that is discussed in section 4.

3 Future electricity market participants

The UK electricity market is governed by a complex regulatory framework comprising licences issued by Ofgem for generation, transmission and distribution of electricity and industry rules and codes that dictate how different parties interact. As noted in Government and industry consultations [9, 10] the nature of the UK electricity supply system is changing with increased demand, from eVs and decarbonisation, and increased generation and storage within the distribution network. The safe and secure operation of the electricity supply system has to date been primarily the responsibility of a small number of organisations, namely the ESO and the transmission and distribution system operators.

Introduction of smart functionality will introduce new participants:

- suppliers of smart appliances and smart add-ons to existing systems – their role is fundamental to the overall security of real-time implementation of DSR, through their implementation of trustworthy and secure and DSR functions;
- EMS – these services could be provided by the consumer's energy supplier, but it is likely that this role will be attractive to existing internet service providers, for example Amazon linking their online retail capability with their apps and voice control functionality offered by alexa™;
- eV charge operators – increasing use of eVs will lead to consumer demand for faster charging and this require installation of charge points that employ high current (>13A) or 3-phase connections. Supply and operation of these charging points, whether public or private, may be handled by specialist operators that provide the charge points, aggregate demand and arrange supply and billing of the electricity consumed.

Presence, or absence, of appropriate legislation, regulations, standards and codes of practice may determine the extent to

which the activities, products and services of these new participants impact the security, safety and stability of the electricity supply system.

4 Security risks

From a security perspective the UK Government has identified four policy principles [9] that it considers critical for energy demand to be managed using smart appliances:

- Grid Security: the prevention of outages on the grid caused by erroneous operation of smart appliances;
- Cyber-Security: the prevention of unauthorized access to smart appliances by third-parties;
- Data Privacy: the secure storing of data on the device or with any controlling party; and
- Interoperability: the ability of smart appliances to work seamlessly across any DSR services operated by any electricity system participant.

Threats that affect grid, security, cyber security and data privacy are likely to emanate in the main from parties with hostile, malicious or criminal intent, whereas interoperability issues may arise as the unintended or unforeseen consequences arising from changes to the system and/or its components.

4.1. Potential security threats

From an attacker's perspective the electricity supply system is a critical part of a nation's infrastructure. Attacks on Ukrainian electricity distribution companies [11-14] are indicative of how the electricity supply system can be a target for hostile nations. Hostile actions against the DSR system and smart home may result in:

- damage to or destruction of electricity supply equipment, assets connected to the network or homes;
- disruption of the DSR system by denying, degrading or delaying tariff or other signals aimed at managing consumption, these may have significant financial and regulatory consequences for suppliers, system operators and consumers;
- detection, discover or disclosure of data and/or information about the electricity supply systems and their operation, about customer premises and the consumers themselves. This information may be company sensitive/confidential, or personal information as defined by GDPR [15], the loss or misuse of which may result in prosecution and significant fines.

In addition to GDPR considerations the electricity supply network is covered by the NIS Regulations [16] which imposes strict security breach reporting requirements on operators of essential services (OES). As DSR becomes an integral part of network operations, EMS operators will be required to achieve the security and reporting standards required of other OES.

4.2. Impact of an IoT approach to DSR

The use of smart appliances to implement DSR exposes the system to threats that have been evident in other consumer IoT devices. For example, poor security engineering and default configuration of home routers and CCTV cameras enabled malware developers to create the Mirai botnet [17,18]. In practice the smart home architecture illustrated in Figure 1 is likely to be a composition of consumer IoT devices from various manufacturers or service providers, employing common software platforms and libraries. Jerkins [19] notes that "*Most owners of these [IoT] devices are neither security aware or motivated to secure their IoT devices. Manufacturers of these devices are not currently motivated by market forces or regulatory requirements to improve the security of their products.*"

The security of the domestic IoT environment in which DSR components will be installed is potentially further compromised by the presence of other personal devices connected to the home router. For example, homes will contain a range of personal IT devices, often running unpatched or insecure software and IoT toys, games that are not secure-by-design.

4.3. Privacy and Trust

The introduction of smart energy solutions will potentially bring an unprecedented level of collection of electricity consumption data from domestic premises. The UK smart meters provide limited granularity by recording energy use against in half hour bands [20], whereas smart energy solution of CEM could in principle collect data every second or few seconds, thus allowing very detailed consumption patterns to be gather and fine-grained control over energy demand. Collection of data at this granularity would be a significant privacy issue as it would allow detailed profiling of consumer and/or household behaviour. This becomes particularly intrusive when linked to smart phone location data used in geo-fencing, where consumers programme actions based on their proximity to home, and the collection of charging information for any eVs used by the household.

In setting out its requirements for the implementation of the smart metering programme the UK Government published a specification for the meters and the security of their communications and operation [21]. The specification seeks to protect Personal Data and ensure the confidentiality and integrity of data held in, processed by and/or communicated to the DCC by the meter. Similar government requirements do not currently exist for the smart energy devices that will deliver the DSR functionality discussed in this paper.

Given the emergent nature of the DSR market and recent behaviour by a number of web-based organisations, e.g. Facebook's collection and use of personal data, there may be legitimate concerns about the potential for EMS providers and suppliers of smart appliances/solutions to collect pattern of life data which may be resold for advertising or other commercial activities.

Use of cloud-based delivery of the CEM component may cause concerns about GDPR compliance, particularly where the service is delivered by large US corporations. Schneier [22] identifies four general systems that people use to incentivize trustworthy behaviour:

- Morals – the behaviour of social media companies and the prevalence of web site tracking suggests that the relying upon moral behaviour of organisations is unlikely to achieve an acceptable level of trustworthiness – consumers can choose whether to use social media, but in the era of the smart home they are unlikely to be able to choose not to subscribe to DSR services;
- Reputation – anecdotal evidence about the impact of data breaches on corporate reputations suggest that reputational harm following a serious data breach is generally short lived, so the threat of loss of reputation is unlikely to be an effective means of maintaining security of the domestic energy supply system;
- Institutions – organizations are generally governed by rules and laws that induce managers and boards to behave according to the group norm. The electricity supply industry has to date operated within strict licence conditions and codes relating to data security and privacy. The move to smart energy solutions and smart appliances risks eroding these protections in favour of increased data collection and sharing;
- Security systems – as noted in the previous section the UK smart metering programme was designed with security in mind. The current relative lack of smart energy security standards and obligations to demonstrate adherence to and maintenance of compliance with them is a serious weakness.

5 Potential mitigations

Potential mitigation measures applicable to development and use of IoT-based smart solutions as a mechanism for managing domestic energy demand can be grouped into the four categories described in the sub-sections below.

5.1. System architecture

System architectural measures can be separated into two components: the IoT-based energy control architecture and the physical energy distribution system within the smart home. From a safety and security perspective both are important and inter-dependent.

5.1.1 IoT-based energy control architecture

The control architectures currently on offer within the home are flat networks with shared access to an internet router. This is a weak architecture from a security perspective, lacking any separation between personal devices and the components that control mains electricity consumption and storage. Good practice in control and automation system design is to adopt an architecture based on the IEC 63443-1-1 standard [23] with protected functional zones separated by secured conduits. The current lack of separation and security increases the risk of a Mirai-style attack, providing an attractive target for malware developers to develop attacks that disrupt both the control of domestic appliances and the implementation of the DSR system. The use of apps and web-based portals to control smart appliances is a seriously vulnerability if the software is not developed in line with good engineering practices and the principles set out in the recently published guidance on Secure-by-Design [24, 25]. The design of both the in-home and network-based elements of the DSR system should be based on architectural patterns that explicitly address safety and security.

Another significant issue is the location of the CEM, if this is remotely delivered as a cloud service there may be significant safety security issues in the event of any service outage or denial service attacks affecting the service provider. Requiring a functional local CEM to be installed would enable a minimum operating capacity to be maintained in the home in the event of disruption or loss of connection to any cloud-based service.

5.1.2 Physical energy distribution system

Currently, most domestic electricity systems are relatively simple, comprising: a single-phase supply via an isolator and fuse denoting the boundary between the connection from the distribution system operator (DSO) and the home wiring; a meter; one or more distribution boards connected to lighting, mains sockets, fixed appliances; and where fitted electric heating systems. The system illustrated in Figure 1 is significantly more complex with two/three source of supply (the public supply from the DSO, the solar panels and the energy stored in the battery). Fast charging of one or more eVs is likely to exceed the 80-100A capacity of a domestic single-phase supply and some DSOs are already offering 3-phase supply to new developments. Although not discussed earlier in this paper, the future domestic energy system is likely to have the capability to export energy to the electricity supply system from both solar cells, any battery system and from eVs. This further complicates the interconnections and metering required between the different energy sources.

These developments will require a significantly more complex distribution system within the home and a potential need to integrate the switching and isolation elements with control signals provided by the IoT-based energy control architecture. For electrical safety reasons this integration will need to fail safe and secure. The necessary architecture and interlocks are more akin to an industrial control solution than the relatively simple systems found in a domestic environment today. The requirements for electrical installations [6] should in future address this architecture and any integral computer-based control functionality to ensure existing safety standards are maintained, thus reducing potential risks to the consumer and their home.

5.2. Product and system assurance

A report on security and interoperability of smart appliances [5] identified a lack of appropriate security standards. In developing these standards there is a need to go beyond the prevalent security goals of IT systems, i.e. confidentiality, integrity and availability. Instead the new standards should address the four security domains (people, process, physical and technology) and the eight goals identified in Figure 2, supported by an appropriate and effective governance regime.

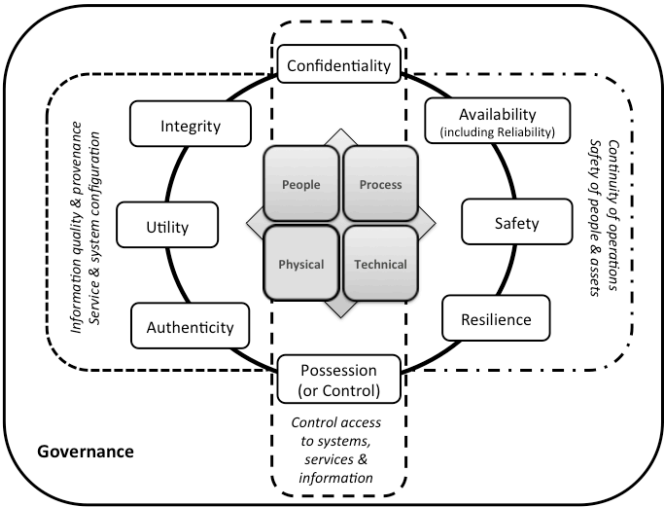

Figure 2 - Security domains and goals [26]

Enforcement of compliance with security standards for domestic energy-related IoT devices and DSR enabled appliances should be based on testing and certification schemes that have traditionally applied to electrical goods. This is good engineering practice and will provide a degree of assurance to consumers that the products they are using will not undermine their safety or security or their home's.

5.3. Legislation and regulation

The UK electricity supply market is underpinned by legislation and a complex regulatory regime. Appropriate provision will be necessary in both the legislation and regulations, so as to establish standards and codes of practice that manufacturers/suppliers of smart appliance and new DSR participants are required to adopt. In light of the behaviour of some internet-based corporations, reliance upon voluntary codes of practice is likely to provide little incentive for them to achieve the levels of safety, security and resilience needed to protect consumers, their homes and the UK electricity supply system.

The regulatory regime will also need to address how the interactions between different EMS will be managed in multi-occupancy buildings (e.g. flats), at street and substation level. This will be necessary to ensure that tariff or other signals given to one home are consistent and complimentary with those given to other homes sharing the same infrastructure, i.e. a home's energy supply and the related distribution infrastructure are not jeopardised due to competition between EMS providers.

5.3. Consumer education and awareness

The market for smart domestic energy solutions is rapidly expanding with new entrants facing few barriers to the creation and sale of IoT devices that can control mains powered objects. There is relatively little information available to consumers about the security and safety risks associated with remote control of electrical devices and appliances. This needs to be rectified if we are to reduce the risk of death, injury and damage caused by naïve or malicious use of these smart solutions.

Consumers need to understand the limitations, security and safety issues associated with smart products, including the potential for devices failing to respond to commands for technical reasons, e.g. the unpairing of devices from their controller. Consumer awareness and education should be addressed as part of the set up or configuration of smart solutions and appliances.

6 Conclusions and future work

This paper has identified a number of architectural and security issues that affect the development and use of IoT devices to control domestic electricity use. The impact of poor security may be felt not only in the smart home, it may result in disruption or damage to the UK's electricity supply network. Further work is required to develop appropriate security standards for the roll-out of DSR, addressing security at component, home and system levels. This work should include the development of IoT architectural patterns that allow the separation of control functions and commands/signalling from other domestic Internet traffic so as to maintain system integrity, resilience and responsiveness.

A broad attack surface will be presented by the future smart home. The potential mitigation measures discussed in this paper should be applied in a holistic fashion, adopting a system engineering approach rather than focussing solely on securing individual boxes IoT devices or appliances.

Work is also required to consider how interactions of DSR signals from competing EMS providers may affect the operation and integrity of the electricity supply network within the DSOs networks. This work will need to address:

a) Mixed-mode DSR, i.e. combined use of direct appliance control and tariff signals via the smart meter;

b) operation when cyber security threats impair or prevent the responses to demand signals from one or more EMS; and

c) effects of competition between EMS providers on substation and premises level energy supply.

Acknowledgements

This work was supported by Cyber Security of the Internet of Things [UK EPSRC Grant EP/N02298X/1].

6 References

[1] UK Government's Industrial and Clean Growth Strategy, https://www.gov.uk/government/publications/clean-growth-strategy/clean-growth-strategy-executive-summary, accessed: 22 February 2019

[2] BEIS (2017) UK Greenhouse Gas Inventory Statistics (1990 to 2015).

http://www.gov.uk/government/collections/final-uk-greenhouse-gas-emissions-nationalstatistics. accessed: 22 February 2019
[3] HM Government / Ofgem (2017) “Upgrading Our Energy Systems - Smart Systems and Flexibility Plan”, p16. Available: https://www.ofgem.gov.uk/system/files/docs/2017/07/upgrading_our_energy_system_-_smart_systems_and_flexibility_plan.pdf
[4] IFTTT, https://ifttt.com, accessed: 22 February 2019
[5] British Standards Institution (2018) “Secure and interoperable use of smart appliances and electric vehicle smart charge points through standards”, BSI, London. Available: https://www.bsigroup.com/en-GB/smart-appliances-flexible-energy/
[6] BS7671: “Requirements for Electrical Installations, IET Wiring Regulations 18th Edition”, 2018
[7] BEIS/Ofgem/National Grid plc (2018) “Statement on the future of Electricity System Operation”. Available: https://www.ofgem.gov.uk/system/files/docs/2018/01/joint_statement_on_the_future_of_electricity_system_operation.pdf
[8] British Standards Institution (2018) “Secure and interoperable use of smart appliances and electric vehicle smart charge points through standards”, BSI, London. p.6.
[9] Department for Business, Energy and Industrial Strategy (2018) “Consultation on Proposals regarding Smart Appliances”. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/690805/Consultation_on_Proposals_regarding_Smart_Appliances-.pdf
[10] Ofgem (2017) “Future Arrangements for the Electricity System Operator: Response to Consultation on SO Separation”, Available: https://www.ofgem.gov.uk/system/files/docs/2017/08/future_arrangements_for_the_electricity_system_operator_-_response_to_consultation_on_so_separation.pdf
[11] “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks”, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/, accessed 22 February 2019
[12] “'Crash Override': The Malware That Took Down a Power Grid”, https://www.wired.com/story/crash-override-malware/, accessed 22 February 2019
[13] “Industroyer: Biggest threat to industrial control systems since Stuxnet”, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/, accessed 22 February 2019
[14] “CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids”, https://dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/, accessed 22 February 2019
[15] General Data Protection Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN , accessed 22 February 2019
[16] The Network and Information Systems Regulations 2018, http://www.legislation.gov.uk/uksi/2018/506/contents/made , accessed 22 February 2019
[17] Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J., 2017. DDoS in the IoT: Mirai and other botnets. Computer, 50(7), pp.80-84.
[18] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M. and Kumar, D., 2017. Understanding the mirai botnet. In 26th {USENIX} Security Symposium ({USENIX} Security 17) (pp. 1093-1110).
[19] Jerkins, J.A., 2017, January. Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. In 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1-5). IEEE.
[20] Department of Energy and Climate Change (2013) “Smart Metering Implementation Programme - Smart Metering Equipment Technical Specifications, Version 2”, p.47. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/68898/smart_meters_equipment_technical_spec_version_2.pdf
[21] ibid., p37
[22] Schneier, B. (2012) “Liars and Outliers - Enabling the Trust that Society Needs to Thrive”, John Wiley & Sons, London. ISBN: 978-1118143308
[23] IEC/TS 62443-1-1 “Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models”, 2009
[24] DCMS (2018) “Secure by Design: Improving the cyber security of consumer Internet of Things Report”, London. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
[25] Day, J., Shepherd, R., Kearney, P., and Storer, R. (2018) “Secure Design: Best Practice Guide”. Release 1.2.1, December 2018, IoTSF. Available: https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/Best-Practice-Guides-Release-1.2.1-December-2018_final.pdf
[26] Boyes, H. (2015) "Cybersecurity and Cyber-Resilient Supply Chains". Technology Innovation Management Review, 5(4): 28-34