Towards an Understanding of Emerging Cyber Security Threats in Mapping the IoT

Peter Shaw, Mateusz Mikusz, Ludwig Trotter, Mike Harding, Nigel Davies

Lancaster University, UK
{p.shaw, m.mikusz l.k.trotter, m.harding, n.a.davies}@lancaster.ac.uk

Abstract

The increase in IoT sensing and actuating devices that are seamlessly integrated into the environment is often leading to a mistrust of users as it becomes impossible to spot deployed IoT devices and understand their purposes and capabilities. One approach is to provide an appropriate mechanism of mapping the IoT and address stakeholder requirements. However, providing comprehensive maps of the IoT may expose a number of vulnerabilities that need to be addressed. We conducted a comprehensive literature survey outlining the limitations of the existing body of work regarding the mapping of the IoT and conducting an appropriate threat analysis. We subsequently applied the STRIDE model to two case studies (smart campus and urban environment) to identify a set of potential vulnerabilities and approaches at addressing these issues in the context of IoT maps.

Keywords: internet-of-things, cybersecurity

1 Introduction

The Internet of Things (IoT) is growing rapidly with an estimated 23 billion connected devices deployed worldwide in 2018 [23]. These devices range from expensive infrastructure components, such as actuators in smart cities, through to low-cost commodity devices such as radio frequency beacons (e.g. iBeacons). While the number of devices, and the degree of connectivity is growing, researchers have noted that we are increasingly unaware of the locations and purposes of such devices with consequences for the types of applications that can be supported and for user trust in the IoT [17, 22].

In order to address these issues, researchers have begun to consider the notion of "mapping the IoT" by developing mechanisms, to create comprehensive catalogues of IoT devices deployed in an environments such as smart buildings and, at larger scales, urban environments [21]. While there are clear advantages for the creation of maps of the IoT, we believe *the security implications of the creation, storage, and distribution of IoT maps, and the subsequent use of these maps by client devices or critical infrastructure have not been considered previously*. In this paper, we make three contributions:

1. We present the results of a systematic literature review designed to help provide an initial understanding of cybersecurity-related implications from mapping the IoT.
2. We conduct a comprehensive threat analysis by categorising potential vulnerabilities based on the "three pillars" model of cybersecurity [1].
3. We illustrate potential threats in the context of two real-world use cases of IoT deployments.

We note that in the context of this work we primarily aim at providing a better understanding of the potential threats and vulnerabilities associated with mapping IoT-based systems and highlight the need for further research in this area.

2 Related work

2.1 Digital maps

It has been claimed we are currently in the midst of an era of web mapping termed by some as the *GeoWeb* or *Web mapping 2.0* [12] and it's hard to dispute these systems and services have become ubiquitous in our modern lives. Web map providers like Google Maps, TomTom and OpenStreetMaps have enabled a wide variety of services and applications (including satellite, street level image snapshots and indoor floor plans; transport planning and routing services; and turn-by-turn navigation for mobile device versions of the maps). Many of the common mapping services are for human use, although we have seen a recent rise in the use of maps by machines (more specifically autonomous robots) for navigation [3].

2.2 Mapping the IoT

Recent years have seen a drastic increase in research and commercial interest in the Internet of Things, with many ventures producing management platforms, frameworks, and novel systems for the IoT [20].

The breadth of IoT devices that exist today with varied capabilities and details has made it difficult to reach a widely adopted standard for representing and interacting with the various devices and services. While one solution might be for some standard to emerge for devices themselves, others have opted to instead create frameworks and systems to support the cataloguing and interactions for IoT devices with the goal of maximising interoperability between heterogeneous IoT devices and services [2, 10, 13, 15, 26]. Work done in [6] has also explored localised and directional queries of geo-tagged sensor data-sets in the hopes to not overwhelm users with potentially cluttered maps.

Some previous attempts have also been made at creating open data sets of IoT devices deployed around the world [5, 19] and although these particular examples appear to have stopped receiving regular updates or upkeep, it does show a growing desire to generate repositories and geo-spatial maps of IoT devices.

2.3 Security risks from location traces

Despite efforts at anonymising location traces (e.g. by using anonymous identifiers), access to historic anonymised location traces can yet reveal comprehensive insights into individuals and their identities [16]. Even the application of more sophisticated approaches to protect user privacy, e.g. by adding noise using face location information, cannot provide sufficient security – and insights into activities and individuals can still be revealed [4]. Gassen and Fhom [11] describe the risks of "Mobile Location Analytics" that emerge from using location tracking (and additional sensors) in commercial contexts such as retail and airports and specifically raise concerns regarding the sensitive nature of data captured, processed and stored about analytics. The authors suggest that location tracking is always transparently and clearly communicated to individuals to improve privacy [11].

3 Evidencing a Lack of Prior Research

3.1 Methodology

In order to gain insights into the extent of prior research in the field of security threats from mapping the IoT we conducted a systematic literature review adopting a methodology developed by Trotter et al. [24] consisting of five core steps: the identification of relevant *data sources*, generation of *keywords*, development of an *automated search process*, the application of appropriate *inclusion and exclusion criteria*, and a *review process*.

Data Sources

We recognise that security concerns specifically relating to maps of the IoT are a niche area of research at the time of writing, yet still relevant for established areas of computer science. We selected three of the most well known digital libraries in the space to try cover the majority of existing material: ACM Digital Library, IEEE Xplore Digital Library, and Scopus.

Table 1: Keyword search terms.

Category	Search terms
Mapping	mapping, map, charting, cartography, atlas, survey, catalogue, cataloguing
Internet of Things	iot, internet-of-things, sensor networks, web of things, internet of everything, smart infrastructure, connected devices, connected things, connected objects, networked devices, networked things, networked objects, smart devices, smart things, smart objects
Security	security, safety, privacy, risk, threat, vulnerability

Keywords

Our search queries were generated from three relevant keyword categories: *Mapping*, *IoT*, and *Security*. For each category, we manually selected a set of keywords based on common words. Additionally, for the *IoT* and *Security* categories, we used a subset of the keywords provided in prior work [24]. The keywords have been generally created from synonyms and abbreviations of the category name. The total number of 28 keywords yielded 720 unique search queries created from all permutation of one word from each category.

Automated Retrieval

The large number of keyword combinations required an automated approach to allow us to retrieve and analyse relevant papers based on the keywords provided. We utilised a Python-based script that executed all 720 search queries on each of the identified data sources resulting in a total of 2399 requests across all digital libraries. Publications which contained the keywords as part of their abstract have been saved in a spreadsheet for further analysis with the following details: name of source, digital object identifier, author list, title, abstract, publication name, and keywords.

Inclusion and Exclusion Criteria

We applied a set of inclusion and exclusion criteria to the initial set of publications that have been retrieved. Publications were required to be written in English language, peer-reviewed, and contain a combination of keywords from our three categories. We removed duplicates, publications unrelated to the research topic and instances in which keywords were used in a different meaning and context. For example, keywords related to "mapping" were used in the context of links or assosiations instead. The keyword "survey" has also been used more frequently in its more common context of examining, whilst in our context "survey" refers to surveying geographical areas and maps.

Review Process

Due to the large number of publications returned as part of the automated retrieval process, we initially filtered out publications based on the relevance of their titles. The remaining publications have then been manually reviewed by researchers in order to identify potential discussions regarding security concerns with relation to the mapping of the IoT. Any publications that have not included relevant discussions have been considered for the related work.

3.2 Results

The automated search for combinations of our three keyword categories returned 2399 articles (ACM Digital Library: 96; IEEE Xplore Digital Library: 660; Scopus: 1643). After applying the previously described filtering and reviewing stages, 31 papers remained for full review .

Our initial filtering process removed a large number of papers that were related to IoT systems and security only (e.g. [27]), 27 publications included some relation to geo-spatial/location topics, and from those, two were found that addressed security concerns of geo-spatially mapping their IoT deployments. We found only a single relevant publication that addresses vulnerabilities of a modern travel and navigation service in which the authors explored security vulnerabilities of the Waze application [25]. The authors were able to spoof vehicles in order to manipulate congestion predictions and, as a result, affect the routing for other users. Additionally, the authors were able to track individuals through unique identifiers used by Waze [25]. IoT maps that rely on crowd-sourced reporting and location based data and decision making are vulnerable to the same exploits if not handled correctly, e.g. reporting from fake users, manipulating crowd validation to try hide/remove devices from the map, non-existent devices spoofing sensor data to manipulate systems.

As part of the related work presented in section 2, we identified a set of attempts at mapping the IoT, e.g. by providing spatial maps of IoT sensors deployed in urban environments [5], repositories of data captured through a subset of IoT sensors deployed [6] and providing security and interoperability standards such as HyperCat [14]. We identified a set of techniques for the creation and maintenance of mapping the IoT. However, these existing mapping services are primarily targeted at supporting the administration and management of IoT devices, at a similar level as inventory and deployment management platforms. For example, Microsoft Azure provides a mapping service that administrators can use to maintain a database of IoT devices, their spatial locations, captured data and supported interfaces. However, the result of our systematic literature review highlighted that while much research is being conducted to secure IoT data and location privacy, some using geo-spatial maps as use cases, there is an almost total lack of research into the security risks once malicious 3rd parties could gain access to or manipulate the map data.

4 Case Studies

To help scope our analysis of security threats when designing, generating, and maintaining maps of the IoT we present two example case studies of IoT deployments. The use cases differ in context of deployment and the types of devices in use.

4.1 Case Study 1: A Smart Campus Environment

Our first case study considers the wide deployment of Bluetooth Low Energy (BLE) beacons at the Lancaster University campus. The BLE beacons are utilised for two distinct purposes: to support a pervasive display personalisation research test-bed, and to enable automatic student attendance check-ins.

The e-Campus Display Testbed

The e-Campus display network consists of over 80 displays and is the world's largest research test-bed for digital signage, with displays placed in commonly visited areas around campus (including student learning zones, department building, college porters lodges, and outside lecture theatres). The displays use the *Yarely* signage player [8] to handle scheduling details and content to display. The content shown typically consists of a mixture of news items, event advertisements and promotional material, with different content created for combinations of students, staff, and visitors.

Over 50 displays part of the testbed have been equipped with BLE beacons to enable display content personalisation utilising a dedicated mobile phone application *Tacita* [9]. When users approach a display, their mobile phone detects the proximity to the display based on the BLE beacons deployed and requests the personalised content to be shown. To identify the display nearby, the BLE beacons broadcast a unique identifier that is mapped to an individual display through the display infrastructure backend.

Attendance Monitoring

The university is required to record student attendance to timetabled sessions and seminars. Recently, the attendance monitoring has been achieved by using a dedicated mobile phone application in conjunction with BLE beacons deployed in all lecture theatres, seminar rooms and laboratories. During timetabled sessions the mobile application reports the student's location based on BLE beacons detected in their proximity. The goal of this service is to automate the previously laborious and manual task of attendance capture and tracking in order to reduce time and efforts spent by staff and students.

While the attendance monitoring and digital signage applications both use BLE beacons they are operated as entirely separate systems and beacons are only used for a single purpose.

4.2 Case Study 2: Smart Urban Environment

Our second case study focuses on the deployment of a novel cyber-physical drainage management system (SmartWater) developed to support managing transport authorities in undertaking more proactive maintenance planning to mitigate the impact of flooding across the network and reduce cost.

At present the system, that comprising remote drainage condition sensing (i.e. silt-level), predictive analytics and data visualisation capabilities is the first of its kind to be deployed in the

UK across four urban environments (including Worcester, Plymouth & Bristol City Centres) with 36 gully probes deployed in both road-side gullies and rail-side catch pits.

The system provides a step-change in inefficient "corrective" maintenance practices through a next-generation IoT sensor probe, empowering maintainers with a deeper understanding of drainage silt, water and light level conditions. In particular, these new forms of drainage data address limitations of manual asset inspection information that is often relied upon to coordinate work but is collected infrequently, highly subjective and generally perceived as unreliable by maintainers themselves.

Data transmission in-field is supported through a multi-band wireless communications network that relays condition information to a cloud-based data processing platform where online training of new statistical models to predict asset conditions (e.g. future risk of flooding) is performed. The broad needs of maintainers in strategic, tactical and operational roles has resulted in a diverse range of end-user decision-support tools as part of the system that support explicit data exploration of historic, real-time and future asset conditions, 'at-a-glance' map-based overlays of probes deployed in drainage assets and SMS/Email notifications to draw attention to emerging flood risks on the network.

While the drainage system described above currently has a limited number of sensors deployed in the field this is expected to increase significantly as the technology gains acceptance.

5 Threat Analysis

To identify and address the potential threats of mapping the IoT, we categorise threats according to the three pillars of cyber-security set out by the international standard ISO27001 [1]: *Technology*, *People*, *Process*. These pillars enable us to assess the existence of specific threats for the integrity of the data and, additionally, issues that can arise if malicious parties get possession of the map datasets.

5.1 Technology

Data tampering. While not a unique security concern to IoT maps, data tempering still presents an important set of threats. Attackers could inject fake data, edit existing data or remove legitimate data to disrupt a system. Additionally, data tempering could provide attackers with control over a system based on insights gained through the data encoded. In the context of the display personalisation system in our first case study ("a smart campus environment"), the mobile client application relies on beacon details to detect the user's proximity to a particular display. Manipulating beacon identifiers stored as part of the map would effectively disable the core functionality of the system. Furthermore, man-in-the-middle attacks could be executed if certain callback URIs for personaliseable display applications were manipulated.

Physical tampering. Public spaces are likely to consist of a large number of IoT devices that are left open to physical tampering such as damaging, re-location or manipulations. Storing IoT devices in a common map may allow attackers to retrieve the physical locations of potentially hidden IoT devices that have been installed in public areas. Related to data tampering, physical tampering can lead to the map description of a space not representing the situation in the real world. Our smart urban environment use case is particularly sensitive to physical tampering: incorrect sensor readings or physically damaged sensors can incur heavy costs and asset loss if not managed properly.

Access control. IoT maps are likely to contain sensitive information, especially in high security areas where access to these maps also becomes important (e.g. map of a bank vaults CCTV cameras and other sensors). IoT maps containing auxiliary information (e.g. beacon details and IP addresses) can further provide the necessary basis for attackers to use the information encoded to fake, spoof and exploit system functionality. In the context of the attendance monitoring system part of the smart campus environment, fake beacons can be created based on the beacon identifiers encoded in a map in order to fake and spoof attendance from any location. Furthermore, knowing network details can reveal potential targets for DDoS attacks or entry points for hacking into devices which is of particular concern in the IoT space where many sensors or devices have been found to have weak security [28].

Broadcasting. If IoT maps are designed and populated on the basis that IoT devices broadcast their locations and capabilities, potential attackers are not required to gain access to an IoT map. Instead, broadcasting features of IoT devices may be used by malicious parties to create their own maps of the IoT simply by 'visiting' places or accessing network points (depending on the broadcasting technology used).

5.2 People

Accurate data entry. The entry of data into an IoT map will likely not originate from a single entity but will be relying on third parties that are required to enter correct data. This is especially the case in which third parties installing a device are not necessarily the space owners or map providers. As a result, the accuracy and integrity of the resulting map may be negatively impacted.

Data disclosure. A large portion of map data is open to disclosure (either deliberately or accidentally) suggesting a need for new trust relationships to develop at all stages ranging form the installation of IoT devices through to giving third parties access to the data. With the growth of location tracking services, accidental disclosure may occur through the lack of knowledge of use. One example of accidental data disclosure is the exercise application Strava that tracked user routes through location services and released anonymised location traces. However, the correlation of (anonymised) location traces from multiple users allowed attackers to identify secret military installations across the world [18].

5.3 Process

Lack of standards. Standards or attempts at creating standards for describing IoT devices and their communication interfaces have been published previously (e.g. HyperCat [14]). Equally, systems for the description of location information have also been developed such as GIS [7]. However, such standards are not specific to the mapping of IoT devices, particularly around supporting a description of device capabilities, additional meta data and various location description types. The lack of such standards can lead to a high amount of heterogenous and incompatible maps for the IoT – increasing the burden for maintaining and using such maps. As a direct consequence, the costs for maintaining maps of varying standards and developing integration mechanisms that allow the use of heterogenous maps in a common system are likely to increase with the number of maps deployed. Utilising a common standard for IoT maps can address these challenges and ensure compatibility.

Responsibility. Previous research identified a number of different approaches to creating and populating IoT maps, e.g. authoritative (space owners or administrators provide details of devices) and crowd-souring (individuals report locations and capabilities of devices) [21]. However, currently no process or definition exists that clearly states which of these approaches are optimal or which contexts suit them best. For example, when is it recommended or required for space owners or engineers to report on devices installed and populate a map instead of crows sourcing form user? Such a lack of processes defining responsibilities may lead to confusion and consequently to missing, incomplete or inaccurate maps. In the context of a smart campus, for example, an incomplete map directly impacts on the system reliability and availability, leading to a poor user experience or missing attendance logs.

6 Closing remarks

The vision of the IoT is becoming a reality with a wide range of sensors and actuators being deployed and used in a multitude of different settings. We now rely on the IoT to deliver safe, secure critical infrastructure such as transport, power and communications networks while IoT devices are also widely used in domestic and entertainment settings. The increasing proliferation of devices in the wild has led researchers to call for the development of IoT maps that show the location and purpose of IoT devices – primarily to help ease concerns regarding privacy and trust [21].

However, our research suggests that little attention has been paid to the potential cybersecurity risks that such maps might incur. In this paper we have provided evidence of the lack of research focus in this area and provided examples of potential threats based on two case studies – a smart campus and a component of an IoT enabled transport infrastructure.

Acknowledgments

This work is part funded by the UK EPSRC under grants EP/N023234/1 (PETRAS IoT Research Hub – Cybersecurity of the Internet of Things) and EP/N028228/1 (PACTMAN).

References

[1] ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*. Standard. Geneva, CH: International Organization for Standardization (ISO), 2013.

[2] Gianluca Aloi et al. “Enabling IoT interoperability through opportunistic smartphone-based mobile gateways”. In: *Journal of Network and Computer Applications* 81 (2017), pp. 74–84.

[3] Tim Bailey and Hugh Durrant-Whyte. “Simultaneous localization and mapping (SLAM): Part II”. In: *IEEE Robotics & Automation Magazine* 13.3 (2006), pp. 108–117.

[4] Vincent Bindschaedler and Reza Shokri. “Synthesizing plausible privacy-preserving location traces”. In: *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2016, pp. 546–563.

[5] Jonathan Brandon. *Thingful aims to be the Google of the Internet of Things*. `http://telecoms.com/206211/thingul-aims-to-be-the-google-of-the-internet-of-things/`. Accessed: 2018-10-17. 2018.

[6] James D Carswell and Junjun Yin. “Mobile spatial interaction in the Future Internet of Things”. In: *2012 20th International Conference on Geoinformatics*. IEEE. 2012, pp. 1–6.

[7] Keith C Clarke. “Advances in geographic information systems”. In: *Computers, environment and urban systems* 10.3-4 (1986), pp. 175–184.

[8] Sarah Clinch et al. “Yarely: a software player for open pervasive display networks”. In: *Proceedings of the 2nd ACM International Symposium on Pervasive Displays*. ACM. 2013, pp. 25–30.

[9] Nigel Davies et al. “Personalisation and privacy in future pervasive display networks”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2014, pp. 2357–2366.

[10] Suparna De et al. “An internet of things platform for real-world and digital objects”. In: *Scalable Computing: Practice and Experience* 13.1 (2012), pp. 45–58.

[11] Marius Gassen and Hervais Simo Fhom. “Towards Privacy-preserving Mobile Location Analytics.” In: *EDBT/ICDT Workshops*. 2016.

[12] Muki Haklay, Alex Singleton, and Chris Parker. “Web mapping 2.0: The neogeography of the GeoWeb”. In: *Geography Compass* 2.6 (2008), pp. 2011–2039.

[13] Sehyeon Heo et al. “IoT-MAP: IoT mashup application platform for the flexible IoT ecosystem”. In: *Internet of Things (IOT), 2015 5th International Conference on the*. IEEE. 2015, pp. 163–170.

[14] IoT Ecosystem Demonstrator Interoperability Working Group and Rodger Lea. *HyperCat: an IoT interoperability specification*. English. IoT ecosystem demonstrator interoperability working group, Sept. 2013.

[15] Fei Li et al. “Efficient and scalable IoT service delivery on cloud”. In: *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*. IEEE. 2013, pp. 740–747.

[16] Chris YT Ma et al. “Privacy vulnerability of published anonymous mobility traces”. In: *IEEE/ACM transactions on networking (TON)* 21.3 (2013), pp. 720–733.

[17] Mateusz Mikusz et al. “Raising awareness of IoT sensor deployments”. In: (2018).

[18] Richard Pérez-Peña and Matthew Rosenberg. “Strava Fitness App Can Reveal Military Sites, Analysts Say”. In: *The New York Times* (2018). URL: `https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html`.

[19] Radius Networks. *WikiBeacon by Radius Networks*. `http://www.wikibeacon.org/`. Accessed: 2018-10-18. 2018.

[20] Partha Pratim Ray. “A survey of IoT cloud platforms”. In: *Future Computing and Informatics Journal* 1.1-2 (2016), pp. 35–46.

[21] Peter Shaw et al. “IoT Maps: Charting the Internet of Things”. In: *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications*. HotMobile ’19. Santa Cruz, CA, USA: ACM, 2019, pp. 105–110. ISBN: 978-1-4503-6273-3. DOI: `10.1145/3301293.3302375`. URL: `http://doi.acm.org/10.1145/3301293.3302375`.

[22] Peter Shaw et al. “Using Smartwatches for Privacy Awareness in Pervasive Environments”. In: *HotMobile 2017* (2017).

[23] statista. *Internet of Things - number of connected devices worldwide 2015-2025)*. `https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/`. Accessed: 2018-10-18. 2018.

[24] Ludwig Trotter et al. “IoT-Enabled Highway Maintenance: Understanding Emerging Cybersecurity Threats”. In: *IEEE Pervasive Computing* 17.3 (2018), pp. 23–34.

[25] Gang Wang et al. “Ghost Riders: Sybil Attacks on Crowdsourced Mobile Mapping Services”. In: *IEEE/ACM transactions on networking* 26.3 (2018), pp. 1123–1136.

[26] Guangyi Xiao et al. “User interoperability with heterogeneous IoT devices through transformation”. In: *IEEE Transactions on Industrial Informatics* 10.2 (2014), pp. 1486–1496.

[27] Zhang Yanqun and Wang Qianping. “Security model for distributed GIS spatial data”. In: *2008 International Symposium on Information Science and Engineering*. Vol. 2. IEEE. 2008, pp. 641–645.

[28] Z. Zhang et al. “IoT Security: Ongoing Challenges and Research Opportunities”. In: *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. 2014, pp. 230–234. DOI: `10.1109/SOCA.2014.58`.