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 [20]. 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 [19, 17].

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. 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 quantify the limitations in the scientific community's understanding of the cybersecurity implications of mapping the IoT.
2. We conduct a comprehensive threat analysis categorising vulnerabilities according to the "three pillars" model of cybersecurity [15] where a vulnerability represents an identified weakness of a 'resource' (i.e. technology, people and processes) involved in the activity of supporting and maintaining maps of the IoT.
3. We illustrate potential threats using two example use cases of IoT deployments.

We not seek to discourage the production of IoT maps, rather we hope to help researchers understand 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* [11] 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.

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 [23, 2, 9, 12, 14]. 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 [18, 5] 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 [10] 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.

3 Evidencing a Lack of Prior Research

3.1 Methodology

To gain insights into the extent of prior research in the field we conducted a systematic literature review – adopting a similar methodology to that employed in [21] for the highways maintenance domain.

Data Sources

We recognise that security concerns specifically relating to maps of the IoT is a relatively niche area of research at the time of writing, but does sit within 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, Scopus).

Keywords

Our search queries were generated from three keyword categories: Mapping, IoT, and Security. The keywords for mapping were manually selected from common words. For the IoT and Security category, we used a subset of the keywords used by a prior literature review in IoT security [21]. The keywords are generally made up of synonyms and abbreviations of the category name, with a total count of 28 words that created 720 unique queries containing one word from each category.

Search Keywords	
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, vulnerable, vulnerability

Fig. 1: Search categories and synonyms

Automated retrieval

The number of keyword combinations required an automated approach to complete in a realistic time frame. A Python script was used to created and execute each query on each data source. This resulted in a total of $2,399$ requests across all digital libraries. Articles that contained the keywords in their abstract had their meta data saved into a spreadsheet. Details included: name of source, DOI, author list, title, abstract, publication name, and keywords.

Inclusion and exclusion criteria

Articles chosen for inclusion in the review from our three data sources and were required to be written in English, peer-reviewed, and contain a combination of keywords from our three categories. Duplicates were removed, along with any articles only weakly related. Instances where a keyword was used for a different meaning/context were also excluded. For example, keywords related to 'mapping' saw frequent use as a generic term for associating differing groups or sets of items, rather than the definition we were seeking (creation of maps). 'Survey' also saw more use as its more common definition for examining something, instead of the more geographic context in which the term can be used.

Review Process

A large set of papers were returned from the automated script and it was not feasible to review all papers. Instead we conducted an initial filtering phase for relevance based on the titles of each paper. Selections from this stage were then read and reviewed for their discussion of security concerns when dealing with maps or the IoT. Any papers that did not fit this criteria were also considered for inclusion as related works and any papers not relevant were ignored.

3.2 Results

The automated search for combinations of our three keyword categories returned $2,399$ articles (IEEE-660, Scopus-1643, ACM-96). After manual review of paper titles, removal of duplicates, and incorrect result types (e.g. entire conference proceedings), 31 papers were selected for full review.

The initial filtering process removed a large number of papers that were related to IoT systems and security (e.g [24], but very few included mapping as a core topic of the paper, and even fewer then addressed security concerns of geo-spatially mapping their IoT deployments. Those selected for full review were perceived to potentially include all these areas. However, only one paper was found to address vulnerabilities of a modern travel/navigation service [22] in which the authors explored security vulnerabilities of the Waze app. They were able to spoof vehicles to manipulate congestion predictions and affect routing and were also able to track individual users through unique identifiers used by Waze. IoT maps that rely on crowdsourced reporting and location based data and decision making are vulnerable to the same exploits if not handled correctly. e.g. fake users reporting, manipulating crowd validation to try hide/remove devices from the map, non-existent devices spoofing sensor data to manipulate systems.

Our literature survey presented in section 2 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 [13]. 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 is of the deployment of Bluetooth Low Energy (BLE) beacons around the Lancaster University campus. The beacons are used 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 [7] to fetch scheduling details and content to display – commonly a mixture of news items, event advertisements and promotional material, with different content created for combinations of students, staff, and visitors.

Over 50 of the displays are also fitted with iBeacons to enable personalisation through the use of the mobile app *Tacita* [8]. When users walk past a display their phone detects proximity to the display (using the iBeacons) and requests personalised content to be shown. To identify the display, the iBeacons attached to the display broadcast a unique identifier that is mapped to a display in the display infrastructure backend.

Attendance monitoring

Students are required to record their attendance to timetabled sessions of their course and have recently been given the option to do this via the mobile companion app of the University. BLE beacons (similar to those on the displays) are deployed into lecture theatres and seminar rooms. During timetabled sessions the mobile application reports a user as present if a beacon is detected in the background, or if the student manually triggers the scan for beacons. The goal of this service ix to automate the previously laborious and manual task of attendance capture, reducing the time spent by students and staff.

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 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 considerations 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, edit or remove fake data to disrupt a system, or provide the attacker 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. Similar 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 [25].

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 serves, accidental disclosure may occur through the lack of knowledge of use. One example of accidental data disclosure is an 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 instal-

lations across the world.

5.3 Process

Lack of standards. Standards or attempts at creating standards for describing IoT devices and their communication interfaces have previously been published (e.g. HyperCat [13]). Equally, systems for the description of location information have also been developed such as GIS. However, such standards are not specific to the mapping of IoT devices, particularly around supporting a description of device capabilities, additional eta 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 developoing intergration mechanisms that allow the use of heterogenous maps in a common system are likely to increase with the number of maps deployed. Utilising a comkmon standard for IoT maps can address these challenges and ensure compatibility.

Responsibility. Previous research has 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) [19]. However, currently no process or definition exists that clearly states which approach may be appropriate for certain contexts. For example, when is it appropriate or required for space owners or engineers to report on devices installed and populate a map? 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 longs.

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 [19].

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] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

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

[14] 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.

[15] COMMERCIAL LOGICAL. "Information technology–Security techniques–Information security management systems–Requirements". In: (2005).

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

[19] 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`.

[20] 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.

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

[22] 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.

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

[24] 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.

[25] 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`.