Research Proposal Transcript

Course: MSc Computer Science

Module: Research Methods and Professional Practice

Assignment: Research Proposal Presentation

Date: Saturday 14th May 2022

Student ID: 126853

Table of Contents

Slide 1 – Title/Overview:

Good Afternoon and welcome to my Research Proposal Presentation. The content of this presentation will be based upon my proposed dissertation project, which is currently titled **Crowdsourced Device Tracking: Security and Privacy Concerns**. This project aims to highlight the hidden risks behind recently released solutions, such as the Apple ‘Find My’ network, demonstrating how privacy concerns can affect their day-to-day use.

Apple has been chosen as the basis for this research due to the vast number of devices which they have available at their disposal. A Verge (2022) article stated that Tim Cook, Apple CEO, reported that there were over 1.8 billion active Apple devices.

Slide 2 – Significance to the discipline:

At present, the Information of Things (IoT) is an ever-changing topic that involves the development of internet-connected solutions to make our lives easier, such as portable tracking devices & smart doorbells. Within this sector, consumer trust in such devices is massively impacted by the lack of security in place (AlHogil, 2018).

Throughout this presentation, I aim to highlight the ways in which I will identify the security risks within the crowdsourced tracking aspect of the IoT ecosystem. These risks will be linked with potential remedial action, which could be as simple as providing information to consumers on how to protect themselves against the risks.

All research and findings produced as part of this project will be done with the intention of increasing public trust in IoT devices, allowing innovation to continue.

Slide 3 – Research Question:

My research question is **“What action can be taken by IoT device manufacturers to ensure that security and privacy of their users can be sustained?”**.

As part of my research, I will aim to analyse the ways in which IoT manufacturers can modify their systems in order to maintain public trust and prevent privacy issues. For example, building in the ability to reduce the overall effectiveness of trackers by showing the values in a less accurate manner (For example, randomising the location within a 20m radius).

A 2019 study (Internet Society, 2019) showed that across Australia; Canada; France; Japan;The UK and the US, 63% of surveyed consumers found IoT devices ‘creepy’ based upon the volume of data collected about individuals. Whilst 88% thought that security standards for IoT devices should be enforced and guided by regulator bodies as opposed to the manufacturers.

Slide 4 – Aims and Objectives:

Within this project, there is a broad aim and a series of objectives that will be undertaken in order to produce a comprehensive research document.

The aim for this project is: **To investigate the effectiveness of crowdsourced tracking and related privacy concerns**. This will be supported by a series of objectives, including the following:

- Production of datasets demonstrating the accuracy of crowdsourced tracking in an urbanised environment.
- Development of a tool to explain the data and risks behind IoT tracking devices in a jargon-free manner for consumers.

Slide 5 – Key Literature (Secure Mobile Networking Lab):

As this is a relatively new innovation, there is a limited amount of peer-reviewed academic material to identify both the positives and negatives of such technology.

At present, the most significant section of research has been undertaken by a team of researchers at the Secure Mobile Networking lab at Technische Universität Darmstadt in Germany (Heinrich et al., 2021). Within their research, they have highlighted the technological limitations and fundamental flaws behind the Apple Find My network, whilst also demonstrating how such exploits can be leveraged to avoid detection by the “Tracker Nearby” notifications embedded within the iOS Operating System.

In order to demonstrate the accuracy of such technologies, I have included a map produced as part of their research. The red points are crowdsourced location reports, which have been smoothed out to produce a line of best fit, which is shown as a solid red line. The blue line shows the real GPS path that the experiment participant

had taken. Based on a walking scenario, this shows on average, there was 25.9m difference between the crowdsourced path and the GPS path. Although, this research does not highlight external factors that may have affected the accuracy of this experiment, such as population density, time of day and weather, all of which can affect the number of devices within range at any one time.

Slide 6 – Key Literature (Secure Mobile Networking Lab - Conference):

The second piece of Key literature for my topic has also been produced by representatives of the Secure Mobile Networking Lab, but was presented as part of a virtual conference held in Austria. Their research focuses on producing a protocol that is less prone to abuse, as continual tracking was not enabled by default, but instead, only when a device was marked as lost (Wellet et al., 2020).

Their research also focuses on the existing solutions available within the global marketplace, in particular, those produced by manufacturer, Tile. They found that the Tile app was reporting the currently used WiFi name and MAC address (On the devices reporting the locations of nearby tags), which, if compromised, could actually allow Tile to track the locations of all of their app users using publicly available maps of WiFi networks comprised of data gathered during wardriving exercises.

Slide 7 – Key Literature (University College London):

The third piece of Key Literature relating to my topic has been produced and presented by a series of researchers at the University College London. Their publications detail how features of IoT devices can be exploited in a manner that can

be used maliciously in cases involving Domestic Abuse and Intimate Partner Violence (Parkin et al., 2019). In particular, they focus on the fact that IoT abuse cannot necessarily be mitigated as a matter of lawmaking/policy or manufacturers, but, all involved parties should be made aware of the risks of such technology and provide victims with a way out of the abuse.

Slide 8 – Methodology/Research Design:

In order to conduct my research, I will be producing a questionnaire in order to gain the public pre-conceptions and use-cases for crowdsourced tracking devices. All questions produced will be of Quantitative nature, allowing me to easily distinguish the actual uses of such technology, such as those that have used it for theft-prevention, identify location of lost devices & those that have maybe used it to track other individuals. It is worth bearing in mind that some survey participants may have preconceived negative opinions on the technology based on prior first hand experience.

I will also be undertaking a significant amount of literature review, utilising the research and statistics which have been produced and published by other academic institutions. This will form a key part of my research, guiding me to areas which require more research in order to come up with a concrete conclusion.

This slide contains a sample of the questions which I propose to use as part of this project, which will be subject to Ethical approval in the dissertation module.

Slide 9 – Ethical Considerations:

Portable ‘trackers’, such as the Apple AirTag and Tile Mate are commonly used for locating stolen/lost items, but in more nefarious cases, can be used to track high end vehicles (Taylor, 2021) or stalk individuals. As my project will be focusing on potentially vulnerable participants, I will need to be incredibly mindful of the ethical aspects when designing any survey materials, such as questionnaires. At this stage, I would plan to ask a series of closed questions, with any personally identifiable information being omitted from the data collection process in order to prevent any legal and ethical issues arising from information disclosure.

Slide 10 – Risk Assessment:

As part of my initial ethical considerations, I have produced a basic research risk assessment. Key risks have been categorised into both Safeguarding risks, as well as Legal risks, as discussed in documentation published by the University of Essex (n.d.).

Firstly, we risk a survey participant disclosing that they have been undertaking potential criminal activity, such as stalking others, or placing trackers on their possessions in order to steal or vandalise them. This would require disclosure to relevant authorities, such as the Police. I will be preventing the disclosure of such information in my questionnaires by only asking closed questions to gain quantitative data, which can be analysed to establish specific trends.

Secondly, the safeguarding risks that may be associated with our collection of data is that a survey participant may inadvertently disclose that they have been a victim of an unreported crime. This also, would need to be reported to relevant authorities, such as Safeguarding teams and/or the police. This will also be prevented by the question formatting previously discussed, as well as the inclusion of contact details for relevant authorities on the front page of the questionnaire.

Slide 11 – Description of Artefacts:

For the artefacts section of my research, I currently plan to produce a series of datasets which can identify the accuracy and effectiveness of device tracking using crowdsourced data. For example, I aim to produce datasets that will demonstrate the number of devices which are actively responding to location tracking requests, as well as testing the accuracy of the data reported by those devices compared to a near-perfect GPS log. When conducting this piece of research, I will need to be mindful of the location, time of day and how busy a particular location is, as all of these factors are likely to affect the reliability of the data produced.

In addition, an educational tool will be produced to demonstrate the risks and uses of such technologies to consumers, in a jargon-free manner. This should help consumers understand the technology better, as well as the volume of data that can be collected without their awareness.

Slide 12 – Timeline of activities:

I have identified a series of tasks which will need to be undertaken in order for the research to be completed, which have been included in the table in the slide. Based upon an overall module length of 30 weeks (UoEo, n.d.), I have created a Gantt chart showing the tasks, as well as the time I have provisionally allocated to each (Based upon the time I anticipate them requiring).

As shown in the Gantt Chart, I have split the timescales into 3 distinct sections; Approval and Initial Discussions, Research and Write-Up, all of which contain a series of sub-tasks that will need to be completed in order to produce my research document.

Within the Approval and Initial Discussions section of the chart, I have allocated a small amount of time to both, Project Concept Discussions as well as Ethical Approval. Both of which will be discussed in depth with my chosen supervisor prior to beginning the research or write-up elements of the module.

During the research element, I will be conducting some initial research to gather a selection of academic material related to my chosen topic. This will be followed by an in-depth literature review, which will be included as part of my final write-up. At the same time as both of these, my public survey will be running for a total of 4 weeks in order to gather enough information from the public participants.

Finally, I have included the Write-up section, which has been allocated the majority of the time that is available within the 30 week window. A series of approximately 5 weeks have been allocated towards the first draft, followed by 2 weeks for tutor review and feedback, followed by up to 10 weeks to make changes and review with the tutor, prior to submission.

Slide 13 – Ending:

Finally, I'd like to thank you for spending the time to watch my presentation. I hope this has given you an in-depth understanding of my proposed research topic as well as highlighting the fundamental risks of using Crowdsourced data for tracking individuals and objects.

Albeit brief, I have aimed to cover the techniques and methods which will be used within the data gathering phase of this research project, highlighting how this data can be expected to be used and analysed. The tasks shown in the previous slide have been based upon full usage of the available 30 weeks in the dissertation module I will be starting in the near future, although, these dates may change based upon availability of both myself and allocated tutors.

References:

AlHogail, A. (2018) Improving IoT Technology Adoption through Improving Consumer Trust. *Technologies* 6(3). DOI: https://doi.org/10.3390/technologies6030064

Heinrich, A., Stute, M., Kornhuber, T., Hollick, M. (2021) Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System: *Proceedings on Privacy Enhancing Technologies*. 1-19. DOI: https://doi.org/10.48550/arXiv.2103.02282

Internet Society. (2019) The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things. Available from: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/ [Accessed 15th May 2022].

Parkin, S., Patel, T., Lopez-Neira, I., Tanczer, L. 'Usability Analysis of Shared Device Ecosystem Security:Informing Support for Survivors of IoT-Facilitated Tech-Abuse', NPSW. Costa Rica, 2019. San Carlos: Association for Computing Machinery. 1-15.

Taylor, T. (2021) Thieves are now hiding Apple AirTags to track and steal high-end vehicles. Available from: https://www.dailymail.co.uk/news/article-10284303/Thieves-hiding-Apple-AirTags-track-steal-high-end-vehicles.html [Accessed 14th May 2022].

UoEo. (n.d.) MSc Computing Project. Available from: https://online.essex.ac.uk/wp-content/uploads/One-page-module-guides/Computing/CSPROJ.pdf [Accessed 15th May 2022].

University of Essex. (n.d.) Research risk assessment. Available from: https://www.essex.ac.uk/student/postgraduate-research/research-risk-assessment [Accessed 16th May 2022].

Warren, T. (2022) Apple now has 1.8 billion active devices. Available from: https://www.theverge.com/2022/1/28/22906071/apple-1-8-billion-active-devices-stats [Accessed 14th May 2022].

Weller, M., Classen, J., Ullrich, F., Waßmann, D., Tews, E. (2020) 'Lost and Found: Stopping Bluetooth Finders from Leaking Private Information', WiSec. Austria, 2020. Linz: Association for Computing Machinery. 184-194.