Mobility as a service: MAnaging Cyber Security Risks across Consumers, Organisations and Sectors (MACRO)

Mobility as a service and cyber security workshop report

February 2024

By Pegah Mirzania, Nazmiye Ozkan, Weisi Guo, Shujun Li, Ali Alderete Peralta, Kai-Fung Chu

Executive summary

The purpose of this workshop was to present the project findings and discuss on their implications for governing and developing Mobility as a Service (MaaS) in the UK. The primary aim was to present the following key results:

- Identification of the factors influencing users' and organizations' comprehension of cyber security risks.

- Examination of the influence of incentives on users' MaaS preferences and the emergence of travel patterns in light of alternative cyber security risks, utilizing an innovative agent-based model.

- Exploration of public perceptions and attitudes regarding data sharing for MaaS services, and how these perceptions vary based on geographical factors and types of journeys.

- Discussion on the management of risks associated with the use of deep learning algorithms within the broader MaaS ecosystem.

This report provides an overview of the presentations and discussions held during the workshop. The workshop obeyed the Chatham House rules, ensuring that none of the viewpoints expressed are attributed to any individuals or organizations. For more information about the project, please feel free to reach out to Prof Nazmiye Ozkan at n.ozkan@cranfield.ac.uk or Dr Pegah Mirzania at P.Mirzania@cranfield.ac.uk

Key findings:

- The Agent-Based Modeling (ABM) approach can help characterize more comprehensive scenarios of MaaS ecosystems beyond simple pricing strategies.
- In an economy undergoing digital transformation, the emergence of cyber-physical systems like the MaaS ecosystem will inevitably bring about cyber security risk.
- Federated Deep Deterministic Policy Gradient (FDDPG) could enhance MaaS utility and foster passenger trust and participation in data-driven transportation systems.
- Transparency, trust, and clear communication emerged as significant contributors to user confidence and acceptance of MaaS services.
- Awareness of phishing attacks was notably high, with the public acknowledging cyber security as an inherent aspect of modern life.
- The results of an online survey indicate that some cyber security and privacy-related factors do have an effect on travellers' adoption of MaaS services, but their effect is outweighed by costs and benefit-related factors when all factors are considered together.

Introduction

The event commenced with a presentation by Prof Nazmiye Ozkan, outlining the project's aims, objectives, and progress to date.

Prof Ozkan articulated the primary aim of the project: MACRO's goal is to identify and manage cross-organizational and cross-sectoral cybersecurity risks within the broader Mobility as a Service (MaaS) ecosystem. This is achieved through socio-technical solutions, empirically developed via a set of tools, models, and datasets.

MACRO comprises four work packages (WPs), each serving a distinct purpose:

WP1: Consumer-Centric MaaS Modelling, which investigates and defines the overall MaaS framework and implements it using Agent-Based Modelling (ABM).

WP2: Modelling Cyber Security Risks, focusing on generating suitable modelling components for cyber security risks affecting individuals and organizations within the MaaS ecosystem.

WP3: Adversarial Machine Learning, aimed at addressing risks from adversarial attacks on deep learning (DL) and examining risk and trust propagation across the wider MaaS ecosystem.

WP4: Implications for Governance, Policy, and Regulation, conducting four focus groups to assess public acceptance of MaaS scenarios and explore their social and behavioural dimensions in greater detail.

The day's layout was structured to provide a multidisciplinary perspective on Mobility as a Service (MaaS). In the morning, we had two presentations focusing on different aspects of the MaaS ecosystem. The first presentations, led by Dr Ali Alderete Peralta and Dr Kai-Fung Chu, delved into the modelling aspects of MaaS. Following that, Dr Pegah Mirzania presented on the social and public acceptance of MaaS learned from four focus groups, and Prof Shujun Li presented WP2 work on two online surveys, some interviews, a systematic literature review and MaaS related business-to-business relationship discovery.

Keynote Presentation:

Our keynote speaker, Dr Patrizia Franco from Connected Places Catapult, delivered a fascinating presentation on modelling MaaS and the evolving attitudes toward data sharing.

In the presentation, Patrizia highlighted the challenges and strategies for governance in distributed architectures. She also discussed the future plans and improvement strategies, which focus on climate, manufacturing, and health, utilizing LSOA-level aggregated data.

In terms of governance and data sharing, she highlighted the following points:

- Identified the challenge of identifying Heavy Goods Vehicle (HGV) drivers within a dataset comprising 664K agents across 550 areas.
- Advocated for the implementation of common Application Programming Interfaces (APIs) among local authorities, following a standardized approach. She stressed the significance of data ownership by local authorities to ensure the accessibility, inclusivity, and equity of services.

During the presentation, we explored ways to enhance the transportation model. Here are the top three suggestions:

- Integrating a mix of active travel into the model to address the current lack of monitoring caused by data limitations.
- Exploring the potential of utilising satellite data, as many researchers currently rely on Strava data.
- Harnessing Artificial Intelligence (AI) to predict travel behaviour more accurately.

Morning Session:

Bounding the risk: modelling cyber security risk perceptions for the adoption of MaaS

Dr Ali Alderete Peralta from Cranfield University (MACRO project team member) presented his findings on modelling cyber security risk perceptions for the adoption of MaaS.

Ali highlighted the following in his presentation:

- The perception of cyber security aspects within MaaS ecosystems will significantly influence the adoption and development of MaaS.
- Incorporating perceived cyber security risks' cost/benefits into the analysis can yield robust results that may inform MaaS providers' cyber security strategies.
- Understanding of malicious gamification algorithms among the public was assessed, the results indicated that contacting regulators or seeking compensation in response to attacks did not yield significant outcomes.
- A 5% probability of customer data compromise resulted in a 10-12% reduction in bus usage over a three-month period, with 100 agents per mode across four modes (walking, car, cycle, bus).
- In cases of multiple attacks within public MaaS systems, individuals tended to switch to walking from using the bus, while car users remained loyal to their vehicles. The model assumes petrol cars (EVs not included), but future work could explore environmental benefits. It's worth considering the potential trade-offs between security and environmental benefits, as EVs could attract different types of attacks.
- In the scenario of daily attacks, only 50% of subscribers cancelled their subscriptions.
- This model could be beneficial for policymakers, local authorities, and MaaS service providers. Procurement notices could specify resilience levels and customer service requirements. With the increasing cyber-attack frequency in the UK, there's a potential for multiple service providers to switch to alternative options. There's a balance between being a first mover and the economics of scale, and policies and regulations play a crucial role in ensuring quality.
- The Agent-Based Modeling (ABM) approach can help characterize more comprehensive scenarios of MaaS ecosystems beyond simple pricing strategies.
- The research findings suggests that in an economy undergoing digital transformation, the emergence of cyber-physical systems like the MaaS ecosystem will inevitably bring about cybersecurity risk.

Ali presented a 7-dimensional matrix, which serves not only to assess the maturity level of current systems but also to aid in designing more robust models and scenarios.

For instance, existing models with relatively simple scenarios found in the literature could integrate the missing dimensions, providing policymakers with more realistic insights into potential pathways for MaaS development.

During his presentation, there was a discussion emphasising the importance of customer service levels in planning and business modelling for MaaS. Additionally, it was argued that governance structures can influence the adaptation of MaaS. Furthermore, pay as you go option was discussed as an alternative to MaaS.

Further questions were raised during the presentation, highlighting areas for future research, particularly regarding the incentive model and the desired format of incentives in the future. Additionally, based on the presented data, the question of who will be the main user of MaaS has been raised. This also demands further research.

Deep Learning in Mobility-as-a-Service and its Privacy Risks

Dr Kai-Fung Chu, formerly affiliated with Cranfield University and currently with the University of Cambridge, and a member of the MACRO project team, presented his work, emphasising the following points.

- Deep reinforcement learning (DRL) offers potential to enhance passenger satisfaction by tailoring transport services to individual preferences.
- However, centralized DRL methods introduce privacy risks to MaaS platforms.
- A proposed solution is Federated Deep Deterministic Policy Gradient (FDDPG), aimed at maximizing passenger satisfaction and MaaS profit while safeguarding privacy.
- An equally weighted experience sampling mechanism is enforced to prevent sampling bias, ensuring FDDPG's solution quality matches centralized algorithms.
- Information processing is conducted locally during model training and inference, with only gradients shared to prevent information leakage.
- Secure aggregation protocols are employed during gradient sharing to mitigate inference attacks.
- Experiments conducted on real-world and synthetic scenarios in New York City demonstrate FDDPG's ability to improve MaaS profit by approximately 90% and passenger satisfaction by 15%, while maintaining stable training

against agent dropout.

- These findings suggest that FDDPG could enhance MaaS utility and foster passenger trust and participation in data-driven transportation systems.

After Kai presentation the following points have been raised:

- If a transport authority prioritises routes optimal for the system rather than for individual passengers, it is feasible. This approach can integrate benefits for both the customer and the entire transport system. However, from a public acceptability standpoint, this raises concerns about perceived surveillance or oversight, akin to "Big Brother" dictating societal norms. The concept of inertia, as highlighted by one of the attendees, plays a significant role in public acceptance.
- New approaches and black box methodologies in decision-making prompt questions regarding transparency, equity, and fairness. Stakeholders are increasingly focusing on the ability of AI systems to ensure trustworthiness, transparency, and fairness.
- When considering data utilization within and between models, inquiries arise regarding data movement, anonymization, and aggregation rationales. Additionally, the issue of digital exclusion is pertinent, especially for individuals without access to smartphones or data, resulting in disparities in data availability and usage.
- One attendee suggested that the UK could learn from Spain's approach, which involves implementing ticket machines that offer MaaS platforms in train stations. This initiative aims to provide common access to MaaS, ensuring that everyone can utilise the service.

Afternoon Session

Public perception and acceptance in the context of different cyber security risks

Dr Pegah Mirzania presented her preliminary results on public perception and acceptance of MaaS. Pegah’s findings were based on the results of four focus groups, with a total of 24 participants, averaging six participants per group. The key variables differentiating these focus groups were traveller type and location,

specifically urban versus rural settings, aimed at understanding differences in views among leisure travellers and commuters. The primary aim of the focus groups was to explore the impact of cybersecurity risks on public perceptions and acceptance of Mobility as a Service (MaaS). Additionally, the objective was to evaluate public opinion of MaaS in the context of different cybersecurity risk or data breach scenarios.

The results indicated that in terms of willingness to use MaaS, the majority of public were satisfied with using it for long and unfamiliar routes, but not on a daily basis. Some emphasized the necessity for MaaS to be operated only by trusted providers, which is crucial for uptake consideration. Additionally, some mentioned being open to adoption but found MaaS complicated and requiring too much effort compared to their current planning applications.

Pegah's findings highlighted the following points:

- Currently, the majority of people find journey planning easy with available applications.
- Some participants raised concerns about living in the suburbs, where access to certain services like City Mapper may be unavailable.
- There was an emphasis on utilising travel planning tools, especially when unfamiliar with a route.
- Transparency, trust, and clear communication emerged as significant contributors to user confidence and acceptance of MaaS services.
- Awareness of phishing attacks was notably high, with public acknowledging cybersecurity as an inherent aspect of modern life.
- The majority of public expressed concerns that older generations and less tech-savvy individuals might reject the service due to perceived cybersecurity risks.
- The study brought attention to a privacy paradox, revealing that while participants generally prioritize privacy, they are willing to disclose personal information when offered small rewards.

After Pegah's presentation, questions were raised regarding the role of regulation in the adoption of MaaS in rural areas. Additionally, there was discussion on how local authorities can contribute to the uptake and governance of MaaS, including the establishment of accessibility standards, which necessitates further investigation.

Another point highlighted by participants that requires further investigation is the impact of making driving more challenging, such as through fees or taxes, on the willingness to accept MaaS. Additionally, there is a need to explore how an increase in the cost of other forms of transport would affect the acceptance of MaaS.

Work in WP2

Prof Shujun Li, who leads the sub-team of the MACRO project at the University of Kent, highlighted their results, which were based on two surveys. The main aim of the surveys was to understand how different factors can affect travellers' adoption of MaaS systems, focusing on how cyber security and privacy-related factors interact with other factors, especially costs and benefits.

In addition to the surveys, the University of Kent researchers are also conducting interviews with MaaS experts to identify and investigate the cross-organisational and cross-sectoral cyber security and privacy risks of MaaS systems. They aim to achieve a better understanding of the policy frameworks and governance mechanisms regarding cyber security and privacy in the MaaS ecosystem. The interviews are still ongoing, and the results will be released later.

Prof Li also introduced an ongoing systematic literature review on cyber security and privacy aspects of MaaS systems, which is close to be completed. Finally, he briefly explained another ongoing work on using public data to explore business-to-business relationships, which can help study how different stakeholders in the MaaS ecosystem interact with each other.

The following points have been highlighted in Prof Li’s presentation:

- The results of the surveys indicate that some cyber security and privacy related factors do have an effect on travellers’ adoption of MaaS system, but their affect is overweighed by costs and benefit related factors when all factors are considered together.

During Prof Li's presentation, a couple of points were raised by participants that merit further investigation:

- Cyber security affects various aspects of service delivery, including trust, relationships with local authorities (LAs), individual cyber security, and how services are designed and delivered by LAs. It is important to explore how cyber security is affected by factors such as costs and service quality.
- Location and the origin of MaaS-related organisations and cultural background of travellers can impact people's trust and adoption of MaaS services. Further investigation is needed to understand the extent of this influence since the surveys are based on UK participants only.

If you wish to learn more or engage with the project team, please feel free to contact the principal investigator of the project, Prof Nazmiye Ozkan, at n.ozkan@cranfield.ac.uk