MACQUARIE
University

Faculty of Science & Engineering

COMP3300 Data Privacy and Information Security

Assignment – Part (b)

Expectation and Marking Guide

Learning Outcomes

On successful completion of the second part of the assignment, you will be able to

- Explain the concepts of data privacy and information security.
- Perform privacy risk assessment on digital information and datasets.
- Embed privacy in the design and architecture of IT systems and business practices.
- Apply adapted privacy and security technologies and tools to enhance the security properties of data.
- Analyse the trends for managing data security and privacy.

Assignment Description

For the second part of the assignment, you will conduct a research on a topic from the list below. Projects are allocated based on the final digit of your student ID. For example, if your student ID ends with Digit 2, you will do a research on "Privacy Protection in Transportation Systems", and if your student ID ends with Digit 6, you will work on "Drones and Citizen Privacy".

(0) **Privacy in Social Networks**
Participation in online communities is becoming ubiquitous. Not only do people keep personal content such as their journals, photos, bookmarks and contacts online, they also increasingly interact online, both socially and professionally. In online communities whose primary goal is social networking, such as Facebook and LinkedIn, each user's set of trusted users is of paramount importance to their activity on the site. Korolova et al. formalise a typical social network interface and the information about links that it provides to its users in terms of lookahead. They show a particular attack where an attacker subverts user accounts to get information about local neighborhoods in the network and pieces them together in order to get a global picture.

Ref. Korolova, Aleksandra, Rajeev Motwani, Shubha U. Nabar, and Ying Xu. "Link privacy in social networks." In Proceedings of the 17th ACM conference on Information and knowledge management, pp. 289-298. 2008.

doi:https:10.1145/1458082.1458123

(1) **Privacy in Photo Sharing**

With increasing use of mobile devices, photo sharing services are experiencing greater popularity. Aside from providing storage, photo sharing services enable bandwidth-efficient downloads to mobile devices by performing server-side image transformations (resizing, cropping). On the flip side, photo sharing services have raised privacy concerns such as leakage of photos to unauthorised viewers and the use of algorithmic recognition technologies by providers. To address these concerns, Ra et al. suggest a privacy-preserving photo encoding algorithm that extracts and encrypts a small, but significant, component of the photo, while preserving the remainder in a public, standards-compatible, part.

Ref. Ra, Moo-Ryong, Ramesh Govindan, and Antonio Ortega. "P3: Toward privacy-preserving photo sharing." In 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13), pp. 515-528. 2013.

(2) **Privacy in Transportation Systems**

An important feature of future transportation systems is that vehicles can form groups, communicate with one another, and share events' information (hazard, speed, location, etc) with road side units. Despite the benefits of such new capabilities, private information could be leaked by untrusted road side units at the edge of the network. Although the past works on differential privacy provide a strong privacy guarantee, they are limited to applications where communication parties are trusted. To address the privacy issue when the edge controller is untrusted, Ghane et al. and Jolfaei et al. suggest mechanisms to protect data privacy.

Refs. Ghane, Soheila, Alireza Jolfaei, Lars Kulik, Kotagiri Ramamohanarao, and Deepak Puthal. "Preserving privacy in the internet of connected vehicles." IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5018-5027, Aug. 2021, doi: 10.1109/TITS.2020.2964410.

Jolfaei, Alireza, Krishna Kant, and Hassan Shafei. "Secure data streaming to untrusted road side units in intelligent transportation system." In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom), pp. 793-798. IEEE, 2019.

(3) **Privacy in Healthcare**

Using patients' health data, healthcare providers offer reliable data services for better medical treatment. For example, the clinical pathway provides optimal detailed guidance for the clinical treatment. However, healthcare providers usually outsource the medical data to powerful cloud servers, which could be untrusted, and therefore, an execution of clinical pathway query service will inevitably bring huge privacy risks to patients' data. To address this problem, Zhang et al. suggest a clinical pathway query scheme which reveals neither the private information of patients, such as name, gender, age, and physical index, nor the sensitive information of hospitals, such as treatment, medication, and expense.

Ref. Zhang, Mingwu, Yu Chen, and Willy Susilo. "PPO-CPQ: a privacy-preserving optimization of clinical pathway query for e-healthcare systems." IEEE Internet of Things Journal 7, no. 10 (2020): 10660-10672.

(4) **Privacy in Smart Grids**

While intensive research efforts have been focused on ensuring data correctness in the Advanced Metering Infrastructure (AMI) data collection and protecting data confidentiality in smart grid communications, less effort has been devoted to privacy protection in smart grid data management and sharing. In smart grid data management, the AMI collects high-frequency energy consumption data, which often contains rich inhabitant and lifestyle information about the end consumers. The data is often shared with various stakeholders, such as the generators, distributors and marketers. However, the utility may not have consent of the users to share potentially sensitive data. To this end, Yang et al. suggest a solution based on data sanitisation, which eliminates sensitive/identifiable information before sharing usage data with external peers.

Ref. Yang, Lei, Hao Xue, and Fengjun Li. "Privacy-preserving data sharing in smart grid systems." In 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 878-883, 2014.

(5) **Privacy Leakage and Side Channels**

Device tracking is a serious threat to the privacy of users, as it enables spying on their habits and activities. A recent practice embeds ultrasonic beacons in audio and tracks them using the microphone of mobile devices. This side channel allows an adversary to identify a user's current location, spy on her TV viewing habits or link together her different mobile devices. Arp et al. demonstrated such vulnerabilities.

Ref. Arp, Daniel, Erwin Quiring, Christian Wressnegger, and Konrad Rieck. "Privacy threats through ultrasonic side channels on mobile devices." In 2017 IEEE European Symposium on Security and Privacy (EuroSP), pp. 35-47, 2017.

(6) **Privacy in Multi-User Augmented Reality**

Immersive Augmented Reality (AR) technologies are becoming a reality. Prior works have identified security and privacy risks raised by these technologies, primarily considering individual users or AR devices. However, users will not always use AR in isolation, but also in ecosystems of other users, and since immersive AR devices have only recently become available, the risks of AR have been largely hypothetical to date. To provide a foundation for understanding and addressing the security and privacy challenges of emerging AR technologies, grounded in the experiences of real users, Lebeck et al. conduct a qualitative lab study with an immersive AR headset, the Microsoft HoloLens, and show some of the challenging privacy problems.

Ref. Lebeck, Kiron, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. "Towards security and privacy for multi-user augmented reality: Foundations with end users." In 2018 IEEE Symposium on Security and Privacy (SP), pp. 392-408, 2018.

(7) **Privacy-Preserving Ridesharing**

Location-based services have seen tremendous developments over the recent years. These services have revolutionised transportation business, as witnessed by the success of Uber and the like. Yet from the privacy point of view, the state of the art leaves much to be desired. The location of the user is typically shared with the service, opening up for privacy abuse, as in some recently publicised cases. To this end, Hallgren et al. suggest a model for privacy-preserving ridesharing.

Ref. Hallgren, Per, Claudio Orlandi, and Andrei Sabelfeld. "PrivatePool: Privacy-preserving ridesharing." In 2017 IEEE 30th Computer Security Foundations Symposium (CSF), pp. 276-291, 2017.

(8) **Drones and Citizen Privacy**

Although drones are receiving a lot of attention, the protection of citizen privacy is still an open issue. For example, Blank et al. demonstrate how basic principles of information privacy could be integrated with existing infrastructure to build up a framework for privacy-aware Unmanned Aerial System (UAS) dispatch considering restricted areas. The software framework proposed enables UAS operators to determine whether a selected UAS flight path intersects with a restricted area, by considering privacy preferences that can be configured by citizens themselves.

Ref. Blank, Peter, Sabrina Kirrane, and Sarah Spiekermann. "Privacy-aware restricted areas for unmanned aerial systems." IEEE Security & Privacy 16, no. 2 (2018): 70-79.

(9) **Privacy in Video Surveillance Systems**

Video surveillance systems are omnipresent nowadays, with large systems in use in strategic places such as public transportation, airports, city centers, or residential areas. The prevailing sense of insecurity at the beginning of this century, with terrorist threats and high criminality, renders the intensive use of video surveillance tolerable despite its Orwellian big brother nature. However, people have a legitimate fear of this invasion of their personal privacy, with this objection slowing down a wider acceptance of video surveillance systems. To address the problem of privacy protection in video surveillance, Dufaux and Ebrahimi introduce efficient approaches to conceal regions of interest based on transform-domain or codestream-domain scrambling.

Ref. Dufaux, Frederic, and Touradj Ebrahimi. "Scrambling for privacy protection in video surveillance systems." IEEE Transactions on Circuits and Systems for Video Technology 18, no. 8 (2008): 1168-1174.

You will work on your research topic individually and will prepare a 3 to 6 minute demo video. For this, you can make a PowerPoint presentation with an audio narration and then save it as MP4.

The length of the video should not exceed 6 minutes (360 seconds) and it should not be less than 3 minutes (180 seconds). There is a 10% penalty for videos longer or shorter than the specified length.

Your video should include the following information:

- The presentation should start with a brief overview of who you are and what your research topic is.
- What privacy problem are you investigating and why is it so important?
- Has plausible deniability been implemented to some amount?
- Is the information shared somewhat useful?
- How is privacy leaked (theory and practice)?
- What could be a solution to prevent/mitigate the privacy leakage?
- What could be the legal or social issues in the privacy breaches?

The submitted video must be authored by the student submitting the work or where material from other sources is included it must be referenced.
Students found to have plagiarised will be dealt with according to university regulations.
Manage your time to successfully complete your assignment.

Marking Guide

- Marks will be released in iLearn by two weeks after Week 12.
- The marks are distributed as follows:

Content	
Introduction to the presenter, the research topic, and the importance	1 mark
Does the presentation explain the background and literature on the topic area?	1 mark
Is there a discussion on plausible deniability and the usability of shared information?	1 mark
Does the presentation explain the ways private information could be leaked?	1 mark
Are prevention/mitigation strategies explained?	1 mark
Does the presentation address the legal or social issues in the privacy breaches?	1 mark
Presentation	
Structure (logically organised, clear argument with relevant points, appropriate use of text and visual aids)	1 mark
Content (coverage of the subject material, evidence of research)	1 mark
Analysis and evaluation (balanced evaluation of information/evidence, detailed analysis of material/tools used)	1 mark
Comprehension (demonstrate an understanding of the material in presentation)	1 mark
Approach and creativity in presentation	1 mark
Oral delivery (clear and audible, appropriate timing, engaged with audience)	1 mark
Total	**12 marks**