CS6290 Privacy-enhancing Technologies
Tutorial 1

1 Logistics About Tutorial Sessions

(Feel free to skip this section if youd like to dive directly into the technical content.)

Goals of tutorial sessions: to

- deepen **our** understanding of key concepts covered in lectures
- help you better prepare for the final exam 🤨
- equip you with skills that will be useful for the course project
- and, of course, address any additional learning objectives you may have (feel free to share them!)

Formats of the tutorial sessions: The sessions will adopt a variety of formats, including

- discussions: e.g., case studies, FAQs, and open-ended questions
- hands-on programming: lightweight programming examples to gain practical experience
- theoretical analysis: proofs and analytical exercises to strengthen conceptual understanding

Have questions/suggestions? Or have anything to share?:

- Feel free to email us at yufeichen8@cityu.edu.hk. (Please use your CityU-DG email address.)
- Post your thoughts or questions in the "Discussions" panel on Canvas.

We Need Heroes 🦸/Heroines 🦸!

Would you like to contribute to our tutorial materials? Contributions may include:

- Suggested readings.
- Thought-provoking questions.
- Insights or reflections related to the topics covered.

Lets collaborate to make these sessions even more engaging and helpful!

2 Threat Modeling

In this tutorial, we focus on **threat modeling**, which serves as the foundation for designing secure and privacy-aware systems.

- What is Threat Modeling?

Before diving in, we recommend reviewing the OWASP Threat Modeling Project page[1]. It provides a comprehensive overview of threat modeling principles.

- Security and Privacy Failures to Reflect On

Consider the following real-world cases:

- Clipper Chip Vulnerabilities[2]
- Re-identification of Netflix Customers[3]

Can you identify any shortcomings in the threat modeling approaches that may have contributed to these failures? Next, read Sections 1.1 to 1.3 of the book by Dionysis Zindros [Zin16][4] and analyze the threat model considered in the design of blockchain protocols.

- Next Steps

After reflecting on these cases, proceed to Section 3 to explore the motivation for studying privacy-enhancing technologies. This section contains numerous real-world examples to help you understand the broader context of privacy challenges and their implications.

3 Why Care About Privacy-enhancing Technologies?

(Credit: This section is adapted from the lecture notes of *Privacy Enhancing Technologies* by Dr. Florian Tramèr. [5])

What would the world look like if we couldn't expect any privacy for some of our communications or interactions? The world (probably) wouldn't end, but it would not be a very nice place either. As beautifully put by Philip Rogaway [Rog15]:

"Cryptography rearranges power: it configures who can do what, from what."

And yet, our privacy is under constant threat. Many governments are not happy with the idea of encryption they cannot break, and push for legislation to ban (or backdoor) end-to-end encryption.

[1] https://owasp.org/www-project-threat-model/
[2] https://en.wikipedia.org/wiki/Clipper_chip
[3] https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/
[4] https://ee374.stanford.edu/blockchain-foundations.pdf
[5] Dr. Florian Tramèr's course focuses more on formalizing the notions of privacy. If you are comfortable with cryptography and statistics (which we hope you are!), consider carefully reading the lecture notes to learn more.

You might say "but I have nothing to hide!", and sure, you're not a terrorist or criminal. But the government may one day criminalize your decision to have an abortion[6], or to protest that government[7]. And encryption is just the tip of the iceberg. Even if your communications are encrypted, your online activity and communication patterns are still tracked wherever you go. Social media apps might know so much about you that they inadvertently (or on purpose) leak your health status[8], your sexual relationships[9], or the location of your army base[10]. Such metadata has been used by governments and companies to target people when they cannot read their (encrypted) messages, sometimes to fight terrorism[11], but also to target people based on their sexual orientation[12], or (again...) for their health choices[13].

The rapid progress of AI doesn't help either. The data you post online now powers large-scale facial recognition systems[14] and fuels deepfake crimes ranging from non-consensual pornography[15] to phone or video scams targeting your friends and family[16]. When companies "try" to protect data, they also often get it wrong. The field of data "anonymization" is littered with examples of data releases that were not. E.g., data of taxi cab rides in New York City which leaked drivers' incomes and home addresses[17], or the re-identification of Netflix customers from released movie ratings[18].

References

[Rog15] Phillip Rogaway. The moral character of cryptographic work. *IACR Cryptol. ePrint Arch.*, page 1162, 2015.

[Zin16] Dionysis Zindros. *Blockchain Foundations*. 2016.

[6] https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/
[7] https://cybernews.com/news/how-encrypted-messaging-changed-the-way-we-protest/
[8] https://splinternews.com/facebook-recommended-that-this-psychiatrists-patients-f1793861472
[9] https://www.cbsnews.com/sanfrancisco/news/uber-crunches-user-data-to-determine-where-the-most-one-night-stands-come-from/
[10] https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
[11] https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata
[12] https://www.politico.com/news/2024/02/13/planned-parenthood-location-track-abortion-ads-00141172
[13] https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting
[14] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
[15] https://www.techtimes.com/articles/301757/20240218/deepfake-dangers-rise-ai-generated-pornography-sparks-global-concerns.htm
[16] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[17] https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn
[18] https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/