CS4236 Group Project Specification

30 August 2022

Due Wednesday November 9th at 17:00

1 The task

The group project is to explore a scenario/topic/issue in computer security and formulate an in-depth approach to it, using the terminology, notation and ideas from this class. To this end I am expecting to see the use of systems/schemes, games/experiments, system properties, constructions, adversaries, definitions, oracles, theorems, perhaps diagrams, perhaps even proofs! It will not be considered enough to just repeat the information from the course; rather you are expected to apply what you have learnt to some new scenario. I will be especially looking out for original ideas.

An initial set of topics is presented in Section 2 below, for you to look at and choose a topic that appeals to your group. If you do not see a topic that appeals to you, please come up with a topic that does, and get approval from Hugh before proceeding.

The project will be worth 25% of your mark, and there are four deliverables:

1. A progress report due on the 5th of October, worth 1%.
2. A formal paper, in a prescribed LNCS format, of between 6 and (say) 12 pages describing your development. This is due on 9th of November at 17:00, and is worth 15%.
3. A presentation video (suitable for a conference) of less than 10 minutes, describing your development. This is due on 9th of November at 17:00, and is worth 5%.
4. A peer review, which will be conducted on the last week of the semester, and will be explained then. This is worth 4%

My advice is that you should meet up as a group, and try to find out the strengths and interests of each of your (pseudo-randomly chosen) group members, as soon as possible.

2 The topic list

The topic specifications given below are deliberately under-specified, and of course you can vary any of these topics. If you wish further clarification, please discuss your topic with your lecturer.

Whatever your topic, try to borrow the ideas introduced in this course: distinguishability, games, adversaries, oracles, definitions and so on. Contrived or unreasonable formulations are discouraged. The goal of formulation is to clearly identify what's being protected, and to provide a convenient way to interpret and analyze the systems.

The initial proposed topics for the groups in CS4236 in 2022 are as follows:

1. **Security formulation for contact tracing:** A main component is how you choose to formulate "security". For example: what does "privacy-preserving" mean when we talk about privacy-preserving TraceTogether? Note that TraceTogether is just one example. What would a game and an adversary look like, and what oracles would it plausibly have?

2. **Security formulation for anonymity:** Your security formulation might focus on how (say) a health database could be searched while still preserving the anonymity of the data inside. Researchers (such as epidemiologists) want to search these databases, but we would want to ensure that the search results cannot identify people. If you are interested in this topic, a good start would be to look at approaches like k-anonymity or ℓ-diversity. What would a game and an adversary look like, and what oracles would it plausibly have?

3. **Security formulation for digital media:** This project would involve formulating what "security" is in this context, exploring the techniques used in protecting media, digital watermarking and so on. What would a game and an adversary look like, and what oracles would it plausibly have?

4. **Security formulation for web based systems:** This project would involve formulating one or more views of what "security" is in this context. This could include techniques for ensuring that systems cannot leak information, or participate in injections, or something else. What would a game and an adversary look like, and what oracles would it plausibly have?

5. **Security formulation for IoT devices and systems:** This project would involve formulating one or more views of what "security" is in this context. It could include discussion on the security architecture of the systems, and/or attack techniques from malicious applications, or via the networks. What would a game and an adversary look like, and what oracles would it plausibly have? What is on the horizon? Where are we going to be in 10 or 20 years time?

6. **Security formulation for new threat landscapes:** This project would involve formulating one or more views of what "security" is in the context of weaknesses and possible attacks on blockchain/NFTs. Perhaps a good place to start would be
   `https://securityintelligence.com/articles/new-threat-landscape-nfts/`
   What would a game and an adversary look like, and what oracles would it plausibly have? What is on the horizon? Where are we going to be in 10 or 20 years time?

7. **Security formulation for multi-stage attacks:** This project would involve formulating one or more views of what "security" is in the context of multi-stage attacks (perhaps involving some mix of web app, spreadsheets or Word docs, phone, BT, BLE...). In a way this scenario involves trying to compose multiple different formalisms into one. What would a game and an adversary look like, and what oracles would it plausibly have?

8. **Security formulation for self-driving cars:** This project would involve formulating one or more views of what "security" is in the context of the unusual requirements and challenges posed by the growing use of self driving cars. It may be an opportunity for you to imagine a future where cars communicate with each other continuously to evaluate road or traffic conditions, and then to hypothesize what might happen in this scenario. What would a game and an adversary look like, and what oracles would it plausibly have?

Note that this is not an exhaustive list. You might perhaps consider topics related to BlockChain technology (not necessarily related to BitCoin), anomoly detection, medical devices, quantum effects, uncopyable keys, Trusted Platform Modules...

3 Presentation

The project is to be presented in two forms, firstly as a short paper, and secondly as a video presentation.

3.1 Your paper - 15 marks

Present the paper as a formal paper with the main body of the paper in 6-12 pages in LNCS format. You can use appendices over and above the 12 pages if needed, but the main body of your paper is what will be assessed. You can assert overall results in the main part of the paper, and just reference the detail in an appendix. Use a professional tone in your paper, avoiding informal speech and contractions. The paper should be readable by students on this course, or professional people with an interest in formal security formulations. You can use LaTeX/LyX (miktex/latex2e), with the class files in this directory:
`https://www.comp.nus.edu.sg/~hugh/cs4236/PaperFormat/Latex/`

Or, if you wish, you can use Word - with these files:
`https://www.comp.nus.edu.sg/~hugh/cs4236/PaperFormat/Word/`

There are zipped up copies of these folders here:
`https://www.comp.nus.edu.sg/~hugh/cs4236/PaperFormat/`

This link shows a sample formal paper:
`https://www.comp.nus.edu.sg/~hugh/cs4236/PaperFormat/Latex/samplepaper.pdf`

The *format* of the paper must follow exactly the specified style (including fonts, font sizes, layouts etc). In general, the *structure* of a formal paper should follow that in the sample:

- Catchy title, authors, abstract
- Body of the work - possibly something like this:
  - Introduction to the background/context for your formulation,
  - Related work, if you can find any, and
  - Overview of the specific formulations,
  - Some detail; a proof, or at least an argument of correctness, perhaps a construction, and
  - summary/conclusion
- References (and then any appendices)

Appendices can exceed the page limit, if you really cannot reduce your paper. Note: Document (reference) your sources - any *unreferenced* copied text will result in an extraordinarily low mark.

Your papers will be put together and form a “course proceedings:”, which you can download.

3.2 Your video - 5 marks

A presentation video of less than 10 minutes, describing your development. This can be delivered by all team members, or just one, or even a virtual presenter. The video should be suitable for a conference: you should make a serious attempt to explain your chosen topic/issue, outline your (mathematical) treatment, and perhaps argue for why your formulation is interesting/useful. If you decide to use presentation materials (for example PowerPoint), then you will submit your PPT as well.

4 Assessment

4.1 Project - expected level?

Your work should comprise a reasonable amount of what you present. Not at the level of original research, but more than just regurgitation.

The assessment below indicates how I expect to initially assess the projects. However, the assessment for individual projects may deviate from this in some ways, dependant on the form of the delivered project.

- On **Wednesday 5th October 17:00**, the progress report is due. You should email your lecturer 2 or 3 paragraphs, detailing what you have done so far. You should briefly describe your system, the proposed title for your paper, and the areas that you propose to formalise, perhaps with an outline of one or two of the formalisms. If you have run into problems, I want to know on that date. You will get 1 mark for this email, one email per group.
- On **Wednesday 9th November 17:00**, the paper and video are due. They will be assessed with the following assessment:
  - (10) Depth of content: An assessment of the depth of content, and level of effort you have put into the project. The marking schedule will range from 0/10 (if there is almost no evidence of understanding or development of the content; mainly the use of cut-and-paste, and the impression given is: “idle thoughts of idle minds”), through to 10/10 (where there is evidence of excellent understanding or development of the content, ideas are successfully substantiated through sound argument, good use of references, impact and significance is high, clear understanding of solution limits/domains/boundaries and so on).
  - (5) Clarity of content: An assessment of the paper clarity. The marking schedule will range from 0/5 (if there is almost no evidence of organization of the project idea, the presentation of ideas is poor or not formulated), through to 5/5 (where there is evidence of excellent organization in the presentation of the project idea, ideas are beautifully and effectively presented and sustained throughout).
  - (5) Video: An assessment of the video presentation Did you explain your context well? Did you explain the main mathematical formulations well? You could use PPT/Slides/Poster or just talk about your project, and it can be anyone you choose, or all your group members. The marking schedule will range from 0/5 (if there is almost no evidence of work put into the presentation), through to 5/5 (where there is evidence of a beautifully and effectively presented project).
- In addition, on **the last week**, there will be a peer assessment exercise worth 4 marks. More details will be provided later.

5 The groups

You should meet up with your team members as soon as possible. If you are having troubles with the course, you might also consider forming a discussion group in your project group. Each group can arrange with Hugh a discussion time for your project - given the large number of groups, perhaps only fortnightly. Here are the groups, 1-16:

1. Nitiyashree Ananthakumar e0954687, CHOO XING YU e0417539, LIM BOON KEE e0406820, LEE JING YU, JONATHAN e0544201, CHOO YI KAI e0001597

2. Baterisna Dan Alden Varsobia e0550572, Zhang Zhexiang e1061912, Tan Hua Kun e0543527, Song Zhicheng e0744007, LAM ZHI YUAN e0406104

3. XIA FUXI e0426189, Sean Ng Shan Sheng e0543670, Guo Yuhua e0966139, Saifaldeen M K Harbia e0989357, MUHAMMAD IQBAL B IMRAN e0309521
4. Ang Yong Ming e0540547, Lai Mei Tin e0550504, ONG GUAN HONG MALCOLM e0425139, JERRELL EZRALEMUEL e0302116, Chin Xing Yi Rebecca e0559622
5. Lai Chok Hoe e0543543, Ng U-Yin Rebecca e0560032, CHUA SENG YONG, EUGENE e0324752, Ma Cong e0924668, Ma Zhongnan e0724292
6. Srinivasa Ramanujan Sriram e0945771, Ria Khaitan e0556761, LIM JUN CHENG e0426083, Nyayapati Srinivasa Nikhil e0652522, WU QIRUI e0424750
7. DAVID LIMANTARA e0533995, ONG WEI XIANG e0319124, Li Hao e0540762, Reham Y. R. Rezeq e1011202, AMBROSE LIEW CHENG YUAN e0424673
8. Li Bailin e0543607, AUGUSTINE KAU ZHI CONG e0415650, Lee Xiong Jie, Isaac e0544517, RYAN KWOK e0523375, HE SONGCHI e0322951
9. KENNETH NG JIAN HAO e0310329, KOH RUI WEN TAMMY e0418023, LIAO XING PENG e0412883, Tan Weiu Cheng e0550462, Filipp Mikoian e0989364
10. Bhaiyat Aadil Mohammed Aslam e1054327, Chua Kai Jun e0543800, PANG KIM JIN e0310263, LU ZIYI e0396953, Chong Wen Hao e0540874
11. LEE WEI MIN e0412871, Jessica Jacelyn e0556245, TEO JUN HONG, KENNETH e0424979, Hu Wangyang e0724298, Ong Kim Lai e0544360
12. Koh Su En e0556272, Shivang Gupta e0638904, LIM FENG YUE e0478238, HOGAN TAN SHAO HAN e0415534, DAVID LIU KANGXUN e0543787
13. MENG AN e0492480, Andy Lam Wei Jie e0544345, TAY YI HSUEN e0534486, KOH HUI HUI ELIZABETH e0316007, Ott Kai Robin e0977852
14. MELANIE NG PEI SEE e0425256, WAN SHI JIE, BRENDAN e0406450, Liu Yiming e0945794, HOANG NGOC TRAM e0188347, Wang Shanmu e0978376
15. Hung Dejian, Daryl e0540684, Lu Xufan e1007373, ZHU YUXUAN e0424709, JIANG JIAHUI e0316063
16. Nguyen Quang Vinh e0550382, Ng Jong Ray, Edward e0540252, CHAN WEIZHONG e0260222, THAM JIN LIN e0527265

Perhaps you should meet up soon, and discuss your topic. You should be able to contact each other using the given `e0XXXXXX@u.nus.edu`. If you need any assistance, contact Hugh at `hugh@comp.nus.edu.sg` at any time. I am happy to discuss your projects with you, and suggest ideas, approaches to take and so on.

6 Final notes...

Upload your final completed videos and papers (sources, word doc, PPT, latex, PDF...), as a single zipped file to the submission folder on or before the due date.

COOPERATING AND COLLABORATION

You may discuss the problems with your friends, and study any background material with them, but the project *comprises your own group's work*. **Copying** and **cheating** will result in *failing* the project.

In addition, an Internet plagiarism checker will check the project submissions, looking for copying. If you do directly use material from other authors, you should always reference this clearly.