DOTA Group project specification

June 28, 2024

Due Friday July 19 at 22:00

1 The task

The group project allows you to explore a topic in some area of computer and information security, in some depth. Your group will present at the showcase on Saturday 20th July, which will be attended not only by your classmates, but also invited guests. This presentation, along with any supporting documentation/evidence is due for submission on Friday 19th July 10pm.

In addition, your group will submit a *short, formal* paper, explaining your topic/area, for assessment. Previous years papers can be found at `https://hugh.comp.nus.edu.sg/DOTA/Proceedings`. Your papers are also due for submission on Friday 19th July 10pm, and will become a course "proceedings". Your group will become the class experts on your topic. As much as possible, assuming that it appears that you have learnt a lot, and put a lot of effort into your project, you will achieve a good mark.

2 The topic list

The topic specifications given below are deliberately under-specified, and in most cases you can vary your particular topic. You could, for example, choose to demonstrate an attack, or a defence, on exactly the same topic. You could also choose a completely different topic, but this must be agreed to (with Hugh) by Thursday 4th.

The brief descriptions given below may require further clarification, so please discuss your topic with your lecturer, or Jiamin. I have pre-allocated to each group a possible project. If you are group 1, you have been allocated project 1, group 2, project 2 and so on. However, you do not have to choose this topic. If your group, after discussion, wishes to change your topic to another one (even one allocated to another group), then discuss this with Hugh as soon as possible. My advice is that you should meet up as a group, and try to find out the strengths and interests of each of your group members, as soon as possible. You might perhaps consider topics related to BlockChain technology (not necessarily related to BitCoin), forensics, anomoly detection, medical devices,

pentesting, quantum effects, uncopyable keys, NFC man-in-the-middle, hardening phones, false trigger removal from video, malware analysis, APK examiner, Trusted Platform Module (TPM) integration, SIM card sniffing. You might even want to do a more practical project (one with hardware and programming). In any case, your topic selection should be confirmed (by Hugh) on Thursday. The initial proposed topics for each group (1..7) in DOTA in July 2024 are as follows:

1. **Demo of hardware and/or side-channel attacks:** This project would involve exploring hardware related attacks, and developing a demonstration or educational website of the attacks - perhaps (for example) Spectre/Meltdown or Apple GoFetch.

2. **Security in new applications:** This project would involve exploring unusual requirements and challenges posed by newer applications, for example pay systems or the growing use of self driving cars (or some other tool/app you dream up). For example - with cars, it might 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 if there were malicious participants? How can the system protect against this? This might involve software development, or maybe design development.

3. **Looking to the future - crypto:** This project would involve exploring emerging crypto technologies. What is on the horizon? Where are we going to be in 10, 20 or 100 years time assuming the current trends in technology? You could go wide, or you could focus on a particular aspect of crypto that interests you (federated learning or the like).

4. **Testing web based systems for vulnerabilities:** Explore how to analyze and/or test (say) PHP for vulnerabilities. This could include techniques for ensuring that systems cannot leak information, or participate in injections, or something else. I am expecting that in this project you would be investigating source code analysis, develop or use some tool, and then reflect on it.

5. **Testing *programs* for vulnerabilities:** Explore various techniques used for automatically/formally analyzing programs for vulnerabilities. For example, fuzzing, static analysis. One possibility is you might develop a simulation or visualization of this kind of analysis for teaching purposes. Or perhaps an interface (front end) to an existing tool that demonstrates some aspect of its behaviour.

6. **Looking to the future - authentication:** This project would involve exploring the use of biometric and other methods for authentication. What is on the horizon? Where are we going to be in 10 or 20 years time assuming the current trends in technology? How will you manage your passwords and tokens? What human characteristics can be exploited?

7. **Testing *systems* for vulnerabilities:** Explore various techniques used for automatically/formally analyzing systems for vulnerabilities. For example, the web servers, or the DNS system, or Android or other operating systems, or the GSM/LTE phone system. All of these, or just one.

Other possible topics might include:

1. **Attacking and defending IoT devices and systems:** An overview of the techniques used to attack and defend IoT devices. It could include discussion on the security architecture of the systems, and/or attack techniques from malicious applications, or via the networks. What is on the horizon? Where are we going to be in 10 or 20 years time?

2. **Media protection and steganography:** This project would involve exploring the (technical) techniques used in protecting media, digital watermarking and other techniques. One possibility is that you could develop your own digital watermark for (say) images, and then evaluate it's performance against image manipulation (blurring, rotation, resizing, cropping and so on).

3. **Trusted Password Manager built on Intel SGX:** Have you ever wondered why you should trust an online password manager to properly safeguard your credentials? What if a staff member stole your valuable password and misused it? In this project, you will design and develop your own password manager service using Intel SGX, and show off the trustworthiness of your service to users.

4. **AccessPoint/DNS/Wifi spoofing, and/or detector:** This project would involve exploring malicious Access Points, and techniques to defeat them. Hardware to help this may be provided if needed.

5. **State-sponsored Tools and Infrastructure:** This project would involve exploring state sponsored systems (for example Grizzly Steppe and the like).

6. **AccessPoint/DNS/Wifi spoofing, and/or detector:** This project would involve exploring malicious Access Points, and techniques to defeat them.

7. **Multi-stage attacks:** This project would involve exploring multi-stage attacks, perhaps involving some mix of web app, spreadsheets or Word docs, phone, BT, BLE...

8. **BEAST (or similar) attack:** This project is primarily to assist in educating people about attacks like the BEAST attack (or similar M-i-M/encryption attacks). You can develop a simulation, animation, or a visualization of the attack for the purpose of teaching others the import and technique(s) used in the attack(s). Alternatively, perhaps you could develop a test tool for checking if a web site is susceptible to such attacks. Or both.

9. **Ransomware:** This project would involve exploring the (technical) techniques used in ransomware, and the results, with case studies.

10. **BLE/NFC attacks:** This project would involve exploring attacks on BLE or NFC in (for example) Android phones. An example might be DoS, sniffing, or drive-by attack.

11. **New threat landscapes:** Security weakness and possible attacks on blockchain/NFTs. Perhaps a good place to start would be

    `https://securityintelligence.com/articless/new-threat-landscape-nfts/`

3 Presentation

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

Present the project as a formal short paper of 4 to 6 pages in ACM conference format. This link shows a sample formal paper:

`https://hugh.comp.nus.edu.sg/DOTA/Proceedings/ACM/sigproc-sp.pdf`

If you wish, you can use Word - with this sample template file:

`https://hugh.comp.nus.edu.sg/DOTA/Proceedings/ACM/pubform.doc`

You can also use LaTeX/LyX (miktex/latex2e), with this class file:

`https://hugh.comp.nus.edu.sg/DOTA/Proceedings/ACM/acm_proc_article-sp.cls`

You can see some documentation at

`https://www.acm.org/publications/proceedings-template`

You can see some other files for the latex sample at

`https://hugh.comp.nus.edu.sg/DOTA/Proceedings/ACM/`

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:

- Title, authors, abstract
- Body of the work - possibly something like this:
  - Introduction,
  - background knowledge,
  - what you did,
  - related work, and
  - summary/conclusion
- References (and then any appendices)

Appendices can exceed the page limit, if you really cannot reduce your paper to 6 pages. Note: Document (reference) your sources - any *unreferenced* copied text will result in an extraordinarily low mark.

4 Assessment

4.1 Project - expected level?

Your project could end up in various forms, but it should at least have an interesting intuition, topic, or demonstration of something at it's core. YOUR work should comprise a reasonable amount of what you present. Not at the level of original research, but more than just regurgitation. Depending on your project, you may include a demo or github, and perhaps readme.txt files showing how to duplicate your work.

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. Three parts make up the assessment:

- On **Friday 19 July 22:00**, the video and paper are due. They will be assessed by teaching staff with the following (approximate) assessment, which contributes a maximum of **45** marks out of the final (60) project mark.

  - (20) 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 0/20 (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 20/20 (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).

  - (20) Clarity of content: An assessment of the clarity. The marking schedule will range from 0/20 (if there is almost no evidence of organization of the project idea, the presentation of ideas is poor or not formulated), through to 20/20 (where there is evidence of excellent organization in presentation of project idea, ideas are beautifully and effectively presented and sustained throughout).

  - (5) Related work/references: An assessment of the related work, and references.

- On **Saturday 20th July**, each group will present their topic with a poster. This can be augmented with a short video, and/or you could use PPT/Slides or just talk about your project. Your presentation will be assessed both by teaching staff (10 marks), and via a peer assessment exercise (5 marks). This contributes a maximum of **15** marks out of the final (60) project mark. The assessment will be looking for evidence that you have captured the most important "hard" idea in your topic, and that you have presented this idea clearly.

5 The groups

You should meet up with your team members as soon as possible. Here are the groups, your topic, and your consultation times:

- Group 1: Your (initial proposed) topic is topic 1, and your group members are HUANG NINGYUAN 黄宁远, JIN XUANYU 金轩宇, ZHU ZIYI 朱子奕, CAO YUHAN 曹雨晗, and LU ZIJUN 卢梓君. Your consultation time with Hugh is from 1:00 to 1:30, every consultation day.
- Group 2: Your (initial proposed) topic is topic 2, and your group members are CAO YUAN 曹源, HU HAOJUN 胡皓钧, YANG JINQI 杨金淇, HOU BEIJIE 侯蓓洁, and CAO LI 曹栗. Your consultation time with Hugh is from 1:30 to 2:00, every consultation day.
- Group 3: Your (initial proposed) topic is topic 3, and your group members are LIU YILEI LIU 刘伊蕾, RADHIKA RAINA, WANG JIAMIN 王稼民, WANG SHIRUI 王施睿, and XU JINGBO 许景波. Your consultation time with Hugh is from 2:00 to 2:30, every consultation day.
- Group 4: Your (initial proposed) topic is topic 4, and your group members are FANG LEYAN 方玏彦, JU XIYA 琚熙雅, MENG DANLING 蒙丹铃, WANG JINGYAN 王静妍, and ZHOU SHUHAN 周姝涵. Your consultation time with Hugh is from 2:30 to 3:00, every consultation day.
- Group 5: Your (initial proposed) topic is topic 5, and your group members are ZHANG QINGYANG 张清扬, CHEN BEN 陈贲, ZHU JIARUN 朱家润, CHEN ZHONGWEN 陈仲文, and FEI ZEBANG 费泽邦. Your consultation time with Hugh is from 3:00 to 3:30, every consultation day.
- Group 6: Your (initial proposed) topic is topic 6, and your group members are LENG YUTONG 冷雨桐, WU KEFEI 吴柯菲, YI KAIWEI 易楷为, ZHANG ZHIYU 张志宇, and HOU YIFU 侯一夫. Your consultation time with Hugh is from 3:30 to 4:00, every consultation day.
- Group 7: Your (initial proposed) topic is topic 7, and your group members are HOU YIFU 侯一夫, HU YIJING 胡一璟, ZHANG SHUWEI 张书玮, ZHENG CHANGQIAN 郑昌乾, ZHANG YIJUN 张怡君, and ZHAO ZEWEN 赵泽文. Your consultation time with Hugh is from 4:00 to 4:30, every consultation day.

You will meet Hugh on Tuesday to discuss your initial ideas, and you should perhaps be discussing your topic immediately, to see if it is going to work with your group members. You can of course change this topic if it is not interesting to your group. If you need any assistance, feel free to 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.

Please note that the topics are deliberately under-specified, to give you more freedom in choosing particular areas to look at.

6 Final notes...

Email the lecturer **hugh@comp.nus.edu.sg** with your final completed posters and papers (sources, word doc, PPT, latex, PDF...) on or before the due dates.

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.

Finally - whatever tools you use, you should provide all the sources you use for these tools - all the scripts and so on. This includes C/python/whatever sources, but also if you use (say) ChatGPT for some reason. Note that I would prefer if you do not use ChatGPT for any reason, but if you do, you MUST provide me with all your interactions - the scripts you use and the raw results you got.