GROUP PROJECT
Lecture 3a

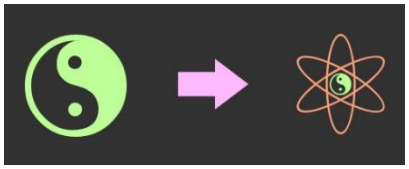
COMPSCI 702
Security for Smart-Devices

Muhammad **Rizwan** Asghar

March 4, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

CODE OBFUSCATION



- Code obfuscation aims at hardening the process of reverse engineering

- Code obfuscation can be broadly classified into four main categories [Balachandran TIFS13]
  - Layout obfuscation
  - Design obfuscation
  - Data obfuscation
  - Control obfuscation

LAYOUT OBFUSCATION

- Layout obfuscation refers to obscuring the layout of the program

- Examples
  - Deleting comments
  - Removing debugging information
  - Renaming variables
  - Changing formatting of source code
  - …

DESIGN OBFUSCATION

- Design obfuscation refers to obscuring the design of the software system

- Examples
  - Splitting classes
  - Merging classes
  - …

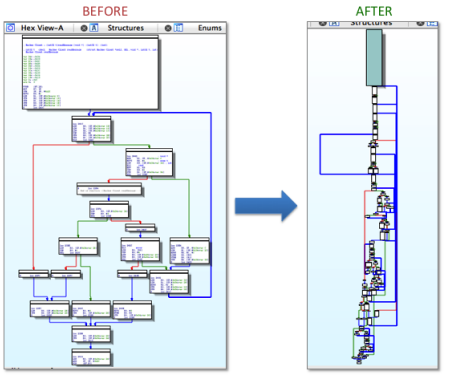
DATA OBFUSCATION

```
public static void main(String[] args) {

    String first_name = "William";
    String family_name= "Shakespeare";

    System.out.println( first_name + " " + family_name);
}
```

- Data obfuscation aims at preventing the adversary from extracting information from the data used in the program

- Examples
  - Data to procedure conversion
    - Encoding (or encryption)
  - Variable splitting
  - Changing lifetime of variables
  - …

CONTROL OBFUSCATION



- Control obfuscation obscures the control flow information of the program

- Examples
  - Opaque predicates
    - E.g., “if (1 > 0)”
  - Control flow flattening
  - …

PROJECT ARTEFACTS

- An obfuscated app
  - Must cover data obfuscation and control obfuscation
- An obfuscation tool
  - You can build on existing obfuscation tools
  - You have to state your contributions in the report
    - Your proposal
    - What has been automated using this tool?
    - Do you perform any task manually?
- Final report
- Project presentation

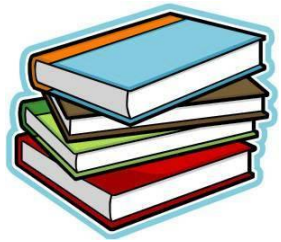
APP REQUIREMENTS

- Easy to install
- App should run smoothly
- Bug free
- A clear separation between GUI and core logic
- 400-1000 lines of code
  - Almost 50% code should be part of the service component
- Somewhat novel/interesting
  - What are consequences of toy or really simple apps?

PROJECT EVALUATION

- 30 marks in total
  - 4 marks for your app
  - 15 marks for obfuscation
  - 10 marks for reverse engineering
  - 1 mark for group presentation
- Grading
  - Percentage contribution of each member!
  - A list of tasks each member was involved in
  - It is responsibility of each member to actively contribute to the project

RESOURCES



- [Balachandran TIFS13] Balachandran, Vivek, and Sabu Emmanuel. "Potent and stealthy control flow obfuscation by stack based self-modifying code." IEEE Transactions on Information Forensics and Security (TIFS) 8, no. 4 (2013): 669-681.

- Some tools: https://mobilesecuritywiki.com

- For more information, visit: https://www.cs.auckland.ac.nz/courses/compsci702s1c/assignments

Questions?

Thanks for your attention!