INTRODUCTION
Lecture 1

COMPSCI 702
Security for Smart-Devices

Muhammad **Rizwan** Asghar

March 06, 2017

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND
Te Whare Wānanga o Tāmaki Makaurau

TEACHING STAFF

- Course Coordinator
  - Rizwan Asghar
  - Office: Building 303S, Room 585
  - Address: 38 Princess Street, Auckland
  - Email: r.asghar@auckland.ac.nz
  - Homepage: https://www.cs.auckland.ac.nz/~asghar/

- Tutor
  - Shujie Cui
  - Office: Building 303S, Room 576
  - Address: 38 Princess Street, Auckland
  - Email: scui379@aucklanduni.ac.nz
  - Homepage: https://www.cs.auckland.ac.nz/~scui379/

ABOUT YOU

- Name
- Current degree
- Any experience related to this course
- Your expectations from this course

CLASS REPRESENTATIVE (CR)

- Who
  - Any volunteer
- Core responsibilities
  - An important link between students and the staff
  - A CR gives the department feedback on various aspects of the course
- Benefit
  - At the end of the semester, a CR can request a Class Rep certificate
- For further information, visit:
  - http://www2.ausa.auckland.ac.nz/representation/class-reps/
  - http://www3.ausa.auckland.ac.nz/representation/class-reps/class-rep-guide/

WHEN AND WHERE: LECTURES (WEEK 1 TO 12)

Day	Time	Location
Monday	17:00 – 18:00	OCH2-104G54 (Old Choral Hall, Room G54)
Tuesday	12:00 – 13:00	303-G02 (Science Centre, Room G02)
Wednesday	17:00 – 18:00	105-032 (Clock Tower, Room 032)

WHEN AND WHERE: TUTORIALS (WEEK 7 TO 12)

Day	Time	Location
Monday	14:00 – 15:00	105-012 (Clock Tower, Room 012)
Tuesday	14:00 – 15:00	206-203 (Arts 1, Room 203)
Wednesday	14:00 – 15:00	421E-619 (Architecture - East, Room 619)

- The main objective of the tutorials is to conduct some of the seminars
- The attendance of tutorials is optional

COURSE STRUCTURE

- First half [Week 1 to 6]
  - Introduction to course/project
  - Android security architecture
  - iOS security architecture

- Second half [Week 7 to 12]
  - Individual seminars
  - Project presentations and demos
  - Guest lecture (optional) – to be confirmed!
  - Course revision and exam info

EXPECTED FROM STUDENTS

- Attend lectures and presentations
- Active class participation
- Present a research article
- Work in a team on a group project
  - *Development Phase:* Develop obfuscated code
  - *Challenge Phase:* De-obfuscate (i.e., reverse engineer) code developed by other groups
  - Group size 5
  - Project report (6 to 10 pages)
  - Project presentation
- Rights and responsibilities
  - Academic integrity: http://www.auckland.ac.nz/uoa/home/about/teaching-learning/honesty
  - Inclusiveness: https://www.auckland.ac.nz/en/about/eo-equity-office/zero-tolerance-for-discrimination.html

DEADLINES

- Article selection for presentation
  - Thursday, March 9, 2017
  - By email to me CC course tutor
- Group formation
  - Friday, March 10, 2017
  - By email to me CC course tutor and your group members
- Code and app submission
  - Tuesday, May 2, 2017
  - Use Basecamp
- Project report
  - Tuesday, May 16, 2017
  - Use Basecamp

SUPPORT DURING THIS COURSE

- Discussion for selecting an article for presentation
  - Thursday, March 9, 2017
- Interim feedback on development phase
  - From Monday, April 17 to Friday, April 28, 2017
- Interim feedback on challenge phase
  - From Monday, May 8 to Friday, May 12, 2017

FUTURE POSSIBLITIES

- Extending report as a research article
- Thesis/dissertation

COURSE OBJECTIVES

- Learning mobile security fundamentals
- Understanding mobile security technologies and common defense strategies
- Learning current research approaches in this area
- Demonstrating critical understanding of research and novel ideas

LEARNING OUTCOMES

- Give basic advice on securing smart devices
- Demonstrate critical and appreciative comprehension of technical literature on mobile security
- Demonstrate technical skills to increase security of smart devices
- Prepare and deliver an oral presentation on an advanced topic in mobile security

ASSESSMENT

- 15% presentation
- 25% project
- 60% exam

INDIVIDUAL PRESENTATION

- List of recent research articles
  - https://www.cs.auckland.ac.nz/courses/compsci702s1c/seminar/
- Selected from top-notch research venues
- Compiled considering relevancy, background and interest
- A different research article that is not covered in
  - COMPSCI 725
  - COMPSCI 726

INDIVIDUAL PRESENTATION (2)

- Grading
  - 5% introduction (motivation, background and problem)
  - 5% description (idea, details and results)
  - 5% criticism (summary, issues and improvements)
- Duration
  - 3 presentations per lecture or tutorial
  - Every presenter will get 20 minutes
    - 15 minutes for presentation
    - 5 minutes for QA
- Feedback
  - Lecturer and tutor
  - Students

GROUP PROJECT

- Develop a technique/tool that should make it difficult to reverse engineer Android apps

- Develop an app that should employ your proposed technique
  - Use java for development of your app
  - Any app with reasonable logic (be innovative!)
    - E.g., input marks (90) and output is grade (A)
  - Lines of code: 400 to 1000

- Challenge phase will begin after the app submission
  - Reverse engineer Android apps developed by other groups

STRUCTURE OF REPORT

- Summary (1 page)
- Introduction (1 page)
  - Context (1 paragraph)
  - Problem (1 paragraph)
  - State-of-the-art (1 paragraph)
  - Solution (1 paragraph)
  - Novelty (1-2 sentences)
- Related work (1-2 pages)
  - Highlight how your idea is different from existing research approaches (cite 4-5 research articles)
  - Justify how your technique is different from existing tools
- Proposed idea (1-2 pages)
  - Your technique
  - Details

STRUCTURE OF REPORT (2)

- Evaluation (1-2 pages)
  - Strength of your obfuscation
    - Your app vs its obfuscated version
  - Performance overhead
    - Execution time of your app vs its obfuscated version
  - Storage overhead
    - Size of your app vs its obfuscated version
  - Status of reverse engineering
    - Explain how you reverse engineered the apps developed and obfuscated by other groups

- Discussion (1 page)
  - Limitations
  - Possible extensions
  - Debugging and updates

PROJECT REPORT

- Page limit: 6-10

- For your report (in **PDF** only), use the following format
  - Times New Roman
  - Font 12
  - Single column
  - Single line spacing
  - 1 inch margin

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

EXAM

- Lectures
- Lecture resources
- Presentations
  - Including presented research articles

- Closed book
- 8-10 questions
- 2 hours

SOME RESOURCES

- **Android Security Internals: An In-Depth Guide to Android's Security Architecture**
  Elenkov, Nikolay
  First Edition
  No Starch Press 2014
  ISBN:1593275811 9781593275815

- **iOS Hacker’s Handbook**
  Miller, Charlie, Dion Blazakis, Dino DaiZovi, Stefan Esser, Vincenzo Iozzo, and Ralf-Philip Weinmann
  John Wiley & Sons, 2012

LECTURE UPLOAD POLICY

- Presentation slides will be uploaded after the lecture

READING: HOW TO READ A RESEARCH ARTICLE

- How to Read an Engineering Research Paper
  William G. Griswold
  CSE, UC San Diego
  http://cseweb.ucsd.edu/~wgg/CSE210/howtoread.html

- How to Read a Paper
  S. Keshav
  University of Waterloo
  http://ccr.sigcomm.org/online/files/p83-keshavA.pdf

- How to Read a Technical Paper
  Jason Eisner (2009)
  http://www.cs.jhu.edu/~jason/advice/how-to-read-a-paper.html

READING: HOW TO PRESENT A RESEARCH ARTICLE

- How To Make an Oral Presentation of Your Research
  Center for Undergraduate Excellence
  University of Virginia
  http://www.virginia.edu/cue/presentationtips.html

- Notes on Presenting a Paper
  Matthew O. Jackson
  http://web.stanford.edu/~jacksonm/present.pdf

READING: HOW TO WRITE A REPORT

- How to Write a Research Paper
  Charles King
  http://faculty.georgetown.edu/kingch/How_to_Write_a_Research_Paper.htm

- How to Write a Great Research Paper
  Jon Turner
  Computer Science & Engineering
  Washington University
  http://www.arl.wustl.edu/~pcrowley/cse/591/writingResearchPapers.pdf

- Tips for Writing Technical Papers
  Jennifer Widom
  January 2006
  http://cs.stanford.edu/people/widom/paper-writing.html

CANVAS AND COURSE WEBSITE

- Canvas for announcements
- Course website for lectures and seminars
  - https://www.cs.auckland.ac.nz/courses/compsci702s1c/

Questions?

Thanks for your attention!