Towards Development of Secure Mobile Software

A Tutorial Proposal for IEEE ISSRE 2018

By

Dr. Hossain Shahriar
Associate Professor of Information Technology
College of Computing and Software Engineering
Kennesaw State University
Marietta, GA 30066, USA

Email: hshahria@kennesaw.edu

1. Title: Towards Development of Secure Mobile Software

2. Duration: Half day, 3 hours

3. Abstract

An increasing number of mobile software (applications) are being developed to meet various needs of end users including SMS messaging, social networking, and game playing. Android is currently the leading smartphone Operating System in the world and currently occupying more than 70% of the global market share of smartphone. Unfortunately, many Android applications have been reported suffering from security and reliability issues. More than 50% of mobile devices have unpatched vulnerabilities, opening to malicious applications (malware) and attacks.

Malware on a smartphone can make a phone partially or fully unusable, cause unwanted billing, or steal contact information stored in a phonebook. Further, benign applications may contain vulnerabilities due to the lack of developer knowledge and malware applications can exploit the known vulnerabilities by providing malicious inputs. Android applications may also suffer from resource leakage. Particularly, memory leak can occur when users navigate applications in devices though screen rotation and pressing of built-in buttons leading to the crash of applications.

This tutorial is intended to provide an overview of Android applications, malware engineering, classification of malware, and mitigation approaches. In particular, we plan to demonstrate examples of static analysis and dynamic analysis techniques. We then explore some recent hands on labware developed as part of NSF Secure Mobile Software Development (SMSD, see https://sites.google.com/site/smsdproject/home) project, intended to promote secure mobile software development among practitioners. Finally, we also discuss content provider leakage and memory leak vulnerabilities, and mitigation approaches.

4. Target audience and interest for the ISSRE community

The tutorial is intended for mobile *software designers and developers*, *software security testers*, *cyber security researchers*, *scientists*, and *graduate students*. As the tutorial is addressing one of the most emerging and crucial issues in software security and quality assurance, it demonstrates an extremely high degree of relevance and addresses a broad spectrum of potential attendees of IEEE ISSRE 2018. The tutorial will benefit related stakeholders to understand the most common mobile application security vulnerabilities. Moreover, it helps relevant professionals to apply appropriate vulnerability mitigation techniques.

5. Outline of the tutorial

The tutorial consists of three major parts. In the first part, we provide an overview of built in security features of Android followed by a set of common malware types. We show an example of various malware, reverse engineering tools, permission analysis, and some common mitigation approaches including static and dynamic analysis. In the second part, we introduce a set of hands on labaware example to demonstrate common vulnerabilities such as inter process communication, lack of input validation, data leakage, and access control. We show examples of mitigation techniques.

In the third part, we discuss content provider leakage vulnerabilities and memory leak issues. We demonstrate common memory leak patterns followed by some practices of preventing them.

For each of the part, we provide estimated duration, subtopics as below in structure of contents followed by a list of the most relevant literatures.

Structure of Contents

- **Introduction (10 min)**
  - Mobile application and background
- **Mobile malware (Part 1: 75 min)**
  - Android malware classification
  - Repackaging and permission analysis
  - Common Mitigation approaches
  - Static and dynamic analysis (demo)
- **Secure mobile software development (Part 3: 45 min)**
  - Secure inter process communication
  - Data sanitization for input validation
  - Data protection
  - Unintended data leakage
  - Access control
- **Other vulnerability (Part 2: 35 min)**
  - Content provider leakage and demo
  - Example of leakage types
  - Android memory manager
  - Memory leak patterns
  - Mitigation approaches and best practices
- **Summary (15 min)**

References

1. Secure Mobile Software Development Learning (SMSD), https://sites.google.com/site/smsdproject/home
2. Xianyong Meng, Kai Qian, Dan Lo, Hossain Shahriar, Md Arabin Islam Talukder, Prabir Bhattacharya, "Secure Mobile IPC Software Development with Vulnerability Detectors in Android Studio," *Proc. of 42nd IEEE Annual Computer Software and Applications Conference (COMPSAC)*, July 2018, pp. 829-830.
3. Maryam Farhadi, Hisham Haddad, Hossain Shahriar, "Static Analysis of HIPPA Security Requirements in Electronic Health Record Applications," *Proc. of 42nd IEEE Annual Computer Software and Applications Conference (COMPSAC)*, July 2018, pp. 474-479.
4. Reza M Parizi, Kai Qian, Hossain Shahriar, Fan Wu, Lixin Tao, Benchmark Requirements for Assessing Software Security Vulnerability Testing Tools, *Proc. of 42nd IEEE Annual Computer Software and Applications Conference (COMPSAC)*, July 2018, pp. 825-826.
5. Kai Qian, Dan Lo, Hossain Shahriar, Lei Li, Fan Wu, Prabir Bhattacharya, Learning database security with hands-on mobile labs, *Proc. of IEEE Frontiers in Education Conference (FIE)*, Indianapolis, USA, March 2017, pp. 1-6.
6. Kai Qian, Hossain Shahriar, Fan Wu, Lixin Tao, Prabir Bhattacharya, Labware for Secure Mobile Software Development (SMSD) Education, *Proceedings of the 2017 ACM Conference on Innovation and Technology in Computer Science Education*, pp. 375-375
7. Vanessa N. Cooper, Hossain Shahriar, and Hisham M. Haddad. Development and Mitigation of Android Malware, *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, Editors: Maria Manuela Cruz-Cunha and Irene Maria Portela, IGI Global, pp. 51-66, January 2015.

8. Vanessa N. Cooper, Hisham M. Haddad, Hossain Shahriar, "Android Malware Detection Using Kullback-Leibler Divergence," *ADCAIJ: Advances In Distributed Computing and Artificial Intelligence Journal, Vol. 3, Issue 9,* pp. 1-9, December 2014.
9. Hossain Shahriar, Hisham M Haddad, "Content Provider Leakage Vulnerability Detection in Android Applications," *Proc. of the 7th International Conference on Security of Information and Networks*, Glasgow, Scotland, pp. 359-366, September 2014.
10. Hossain Shahriar, Victor Clincy, "Detection of repackaged Android Malware," *Proc. of 9th International Conference for Internet Technology and Secured Transactions*, IEEE, London, UK, Dec 2014, pp. 349-354.
11. Hossain Shahriar, Steve North, Edward Mawangi, "Testing of Memory Leak in Android Applications," *Proc. of 15th IEEE International Symposium on High-Assurance Systems Engineering (HASE)*, Miami, FL, USA, pp. 176-183, January 2014.

6. Specific goals and learning objectives

After completing the tutorial, the participants are expected to do the followings:

- Describe various types of android malware applications, analyze permissions
- Identify malware, spyware, adware using static and dynamic analysis
- Apply best practices to build secure mobile software, particularly, android
- Identify memory leak patterns, content provider leakage and avoiding them

7. Expected background of the audience

Participants are expected to have some familiarity with Java languages and mobile application development platform preferably Android Development Studio. Some knowledge of XML and access to mobile device or emulator would be helpful for demo.

8. Presenter bios

Dr. Hossain Shahriar is an Associate Professor of Information Technology at Kennesaw State University, Georgia, USA. His research interests include software security, secure mobile and web application development, software testing, malware analysis, health informatics, and cybersecurity. Dr. Shahriar is an expert on software security testing, secured software development with extensive publications and research experience. He has published over 75 peer reviewed articles in IEEE/ACM conferences, journals and book chapters. His research has attracted a number of awards including *IEEE DASC 2011 Best Paper Award*, *Outstanding PhD Research Achievement Award 2011*, and *IEEE Kingston Section Research Excellence Award 2008*. His research projects have been supported by various agencies including National Science Foundation (USA), Affordable Learning Georgia (USA), and NSERC (Canada). Dr. Shahriar presented many tutorials on software security areas including in IEEE ISSRE (2012 and 2009) and ACM SAC (2016, 2015, 2014, and 2011). He served as Program Chair (SIN 2016), Fast Abstract Chair (IEEE COMPSAC 2015-current, Publication Chair (ACM SAC 2017-current), Student Research Competition Chair (SAC 2016), Workshop Chair (IEEE STPSA workshop 2017 - current). He is also an associate editor of the International Journal of Secure Software Engineering. Dr. Shahriar is currently a professional member of IEEE and ACM.

9. Audio Visual equipment needed for the presentation

Projector for power point slide show would be sufficient.

10. Related experience by the presenter

a. Tutorial in International Conference

1. Secure and Reliable Mobile Applications: Challenges and Approaches, In ACM SAC 2016, Pisa, Italy. Attendees: 28 (see https://www.sigapp.org/sac/sac2016/tutorials.html)
2. Security of Web Applications and Browsers: Challenges and Solutions, In ACM SAC 2015, Salamanca, Spain. Attendees: 24 (see https://www.sigapp.org/sac/sac2015/)
3. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In ACM SAC 2014, Gyeongju, South Korea. Attendees: 30 (see https://www.sigapp.org/sac/sac2014/)
4. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In IEEE ISSRE 2012, Dallas, TX, USA. Attendees: 25
5. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In ACM SAC 2011, Taichung, Taiwan, March 2011. Attendees: 22. See http://www.sigapp.org/sac/sac2011/
6. Testing Program Security Vulnerabilities, In IEEE ISSRE 2009, Mysuru, India, November 2009. Attendees: 20+, See http://www.issre2009.org/content/tutorials/index.html

b) Academic course teaching

1. Ethical Hacking (IT 6843), Kennesaw State University, USA.
2. Health Information Security and Privacy (IT6533), Kennesaw State University, USA.
3. Information Security Concepts and Administration (IT6823), Kennesaw State University, USA.