Secure and Reliable Mobile Applications: Challenges and Approaches

A Tutorial Proposal for ACM SAC 2016

By

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

hshahria@kennesaw.edu

1. Title: Secure and Reliable Mobile Applications: Challenges and Approaches

2. Duration: Half day, 3 hours

3. Abstract

An increasing number of mobile applications are being developed to meet various needs of end users including SMS messaging, social networking, and game playing. It has been estimated that the revenues from mobile applications are expected to rise globally from $68Bn in 2013 to $143Bn in 2016. Android has become the leading smartphone Operating System in the world and currently occupying more than 50% of the global market share of smartphone. Unfortunately, this emerging area is not free from security and reliability issues.

Many of developed mobile applications contain vulnerabilities that may be exploited to cause unwanted actions. Reports find that 92% of Android's top 500 popular applications are vulnerable to some extent of security or privacy risk. More than 50% of mobile devices have unpatched vulnerabilities, opening to malicious applications (malware) and attacks.

4. Motivation, target audience, and interest for the SAC community

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 a basic overview of Android applications, malware engineering, classification of malware, and mitigation approaches. We also explore content leakage vulnerability that may lead to security breaches and memory leakage that may cause an application to crash.

The tutorial is intended for mobile *application designers and developers*, *security testers*, *security researchers*, *scientists*, and *graduate students*. As the tutorial is addressing one of the most emerging and crucial issues in security and quality assurance, it demonstrates an extremely high degree of relevance and addresses a broad spectrum of potential attendees of ACM SAC 2016. 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 application of reverse engineering tools that can be used to inject arbitrary code in benign Android applications. We then provide an overview of recent development to combat against malware.

In the second part, we introduce the content leakage vulnerability in android applications. We show examples of best programming practices to reduce the exposure of content leakage issue.

In the third part, we address the memory leak issue. We demonstrate a number of common memory leak patterns followed by some practices of preventing them. We discuss future research directions. The discussion would argue that existing tools can address the challenge for building reliable and secure applications partially.

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: 45 min)**
  - Android malware classification and repackaging
  - Permission analysis
  - Mitigation approaches for malware
- **Security testing (Part 2: 40 min)**
  - Content provider leakage and demo
  - Example of leakage types
  - Mitigation approaches and best practices
- **Memory leak vulnerabilities (Part 3: 45 min)**
  - Android memory manager
  - Memory leak patterns in source code
  - Best practices and mitigation approaches
- **Summary (10 min)**

References

1. 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.
2. 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.
3. Hossain Shahriar, Hisham M Haddad, "Content Provider Leakage Vulnerability Detection in Android Applications," *Proc. of the 7th ACM International Conference on Security of Information and Networks*, Glasgow, Scotland, pp. 359-366, September 2014, ACM.
4. Hossain Shahriar, Victor Clincy, "Detection of repackaged Android Malware," *Proc. of 9th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 349-354, London, UK, December 2014.
5. Vanessa N Cooper, Hossain Shahriar, Hisham M Haddad, "A Survey of Android Malware Characterisitics and Mitigation Techniques," *Proc. of 11th IEEE International Conference on Information Technology: New Generations (ITNG)*, Las Vegas, NV, IEEE CS Press, April 2014, pp. 327-332.

6. 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, pp. 176-183, January 2014.

6. Specific goals and learning objectives

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

- Explain various types of android malware applications and how they perform unwanted activities, analyze permissions and their consequences, best practices for defense
- Explain various types of content provider leakage vulnerabilities, prevention and best practices
- Recognize various types of memory leak patterns, their presence in source code, mitigation and best programming principles to prevent vulnerabilities
- Choose appropriate defense techniques to defend against malware and resource leakage issues

7. Expected background of the audience

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

8. Presenter bios

Dr. Hossain Shahriar is currently an Assistant Professor of Computer Science in the Information Technology Department at Kennesaw State University, Georgia, USA. His research interests include software security, web application security, software testing, mobile application security, and malware analysis. Dr. Shahriar is an expert on software security testing, secured software development with extensive publications and research experience. 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*. Dr. Shahriar presented tutorials in ACM SAC 2011, 2014 and 2015, IEEE ISSRE 2012, and ACM SIN 2013. He has served as Workshop Co-Chair in SIN 2015, Fast Abstract Chair in IEEE COMPSAC 2015, and PC member in various international conferences related to computer and security such as ACM SAC 2014, 2015, and 2016 (Computer Security Track), ACM/SIGSAC SIN 2013 and 2014, and IEEE ITNG 2014. He is also serving as an associate editor of the International Journal of Secure Software Engineering. Dr. Shahriar is currently a member of the ACM, ACM SIGAPP, and IEEE.

9. Audio Visual equipment needed for the presentation

Projector for power point slide show would be sufficient.

10. Teaching materials on the topic by the presenter

a. Tutorial in International Conference

1. Security of Web Applications and Browsers: Challenges and Solutions, In ACM SAC 2015, Salamanca, Spain.
2. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In ACM SAC 2014, Gyeongju, South Korea.

3. Security Vulnerabilities and Mitigation Techniques of Web Applications, In ACM/SIGSAC SIN 2013, Aksaray, Turkey.
4. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In IEEE ISSRE 2012, Dallas, TX, USA.
5. Mitigation of Program Security Vulnerabilities: Approaches and Challenges, In ACM SAC 2011, Taichung, Taiwan, March 2011.

b) Invited talk/Guest speaker seminar

1. Web Application Security Vulnerability: Mitigation Approaches and Challenges, CIISE, Concordia University, Quebec, Canada, February 2013.
2. Web Security Vulnerabilities: Challenges, Approaches, and Future, The School of Informatics, The University of Edinburgh, Scotland, UK, March 2012.
3. Web Security, School of Computing (Guest Lecture Seminar), Queen's University, Canada, November 2010.

c) Academic courses

1. Ethical Hacking (IT 6843), Kennesaw State University, GA, USA.
2. Computing Security (CS6040), Kennesaw State University, GA, USA.
3. Theory of Networking & Security (CS3550), Kennesaw State University, GA, USA.
4. Secure Software Development (CS4550), Kennesaw State University, GA, USA.