2018

Profile Analysis of Mobile Application Security

Adetunji A. Olunuga
University of North Florida, n00978816@ospreys.unf.edu

PROFILE ANALYSIS OF MOBILE APPLICATION SECURITY

by

Adetunji A. Olunuga

A thesis submitted to the
School of Computing
in partial fulfillment of the requirements for the degree of

Master of Science in Computer and Information Sciences

UNIVERSITY OF NORTH FLORIDA
SCHOOL OF COMPUTING

December, 2018

The thesis "Profile Analysis on Mobile Application Security" submitted by Adetunji Olunuga in partial fulfillment of the requirements for the degree of Master of Science in Computer and Information Sciences has been

Approved by the thesis committee: Date

Dr. Karthikeyan Umapathy
Thesis Advisor and Committee Chairperson

Dr. Swapnoneel Roy

Dr. Sandeep Reddivari

Accepted for the School of Computing:

Dr. Sherif Elfayoumy
Director of the School

Accepted for the College of Computing, Engineering, and Construction:

Dr. William F. Klostermeyer
Interim Dean of the College

Accepted for the University:

Dr. John Kantner
Dean of the Graduate School

CONTENTS

FIGURES

TABLES

ABSTRACT

This thesis conducts profile analysis on the mobile application security using peer-review articles that were published from 2010 to 2018. From the analysis, we will identify prolific authors, intuitions, and geographic regions as well as the topics addressed by the articles. The profile analysis will reveal most frequently used research methods, research approaches (quantitative, qualitative and mixed), and theories used to study the field. This thesis reveals that none of the researchers have made significant contributions to the field, and researches are not collaborating to solve their research problems. The profile analysis shows that surveys and experiments are the most utilized research methods, and most researchers studied the field at a higher level, i.e., security was the focus of the research but did not go deeper into various aspects of security such as privacy, security vulnerabilities, and mobile application security best practices.

Chapter 1

INTRODUCTION

Over the last decade, mobile devices have been used for both business and personal purposes. Mobile device usage increased drastically since the arrival of smartphones and the availability of mobile applications (Guo, et al., 2013). In 2011, the shipment of 400 million Apple-iOS, and Google-Android based smartphones and tablets which exceeded the 350 million units of portable computers shipped (Guo, et al., 2013). Smartphones have changed the computing landscape. Smartphones are considered as a device complementing traditional computing equipment such as desktop and laptops. However, there are cases where mobile devices supplant traditional computers such as bank ATMs, document scanners, online transactions (Chin, et al., 2012).

Regardless of the popularity of smartphones, there are justifications to believe that privacy and security concerns might be obstructing users from experiencing the full potential of their mobile devices. Based on a commercial study, it was found that 60% of smartphone users are concerned that using mobile payments could put their financial and personal security at risk (Chin, et al., 2012). The relevant security risks and concerns of a mobile application depends on the architecture utilized. For example, an online banking application that deals with sensitive financial data will have different security concerns and challenges from a mobile application that provides the front end to an organization's website (Payne, 2013). Areas of concern in regard to mobile websites are mainly data

protection, secure authentication, code vulnerability, and intellectual property protection (Chakraborti, et al., 2015). Additional concerns and challenges associated with a mobile banking application would include improper session handling, client-side injection, broken cryptography, poor authorization and authentication, and insufficient transport layer protection (New Generation Applications Pvt Ltd, 2017).

The recent years have witnessed the rapid and increased occurrence of mobile applications. Due to the flourishing mobile app industry, the functionalities of smartphones have been intensely extended to meet diversified user needs (Zhu, et al., 2014). Thereafter, the smartphone market has continued to increase dramatically (Liu, et al., 2015). There have been reviews of published literature on the challenges and best practices that can be realized during the development of mobile application (Aldayel and Alnafjan, 2017). Aldayel and Alnafjan, (2017) reviewed relevant literatures to identify the key characteristics of mobile application development that defines quality applications. In another study, based on relevant literatures, the authors developed mobile application security pattern library to assist with capturing and validating mobile application security requirements (Noorrezam, et al., 2016). The above studies conducted focused literature reviews to gain understanding of a specific aspect (quality and requirements) of mobile application security. As per our knowledge concerns, we have not found any study that conducted systematic analysis of research activities occurring in the field of mobile application security. As a result, we do not have clarity on what are the concepts related to mobile application security, what has been researched, and research gaps that exist. This thesis conducts profile analysis

(Dwivedi, et al., 2009) by reviewing peer-reviewed, published research articles to provide clarity and identify research gaps.

With reference to journal publications, profiling is considered an art of self-examination that aims to benefit specific audience and takes a journal towards the right balanced direction (Dwivedi, et al., 2009). The above article provides an overview of methodology that can be adapted to conduct extensive literature profiling research studies. The aim of this thesis research is to achieve the following objectives: 1) to identify commonly used publication avenues for a given mobile app security topic; 2) to identify the breadth and depth of the mobile app security field; 3) to determine how often the topic was investigated and analyze the trends; 4) to identify the most frequently used keywords in mobile application security; 5) to identify the breadth and depth of research methodologies used to conduct mobile application security studies; 6) to aggregate the best practices described in literature relevant to mobile application security; and 7) to determine the citation count of the published research articles.

To achieve these objectives, a comprehensive review of articles published between 2010 and 2018 in the following computing digital libraries: ACM, IEEE, AIS, Springer, and ScienceDirect was conducted. Methodological details of the review process are covered in the remainder of this document. The articles were selected based on brief review of their title and abstract which were obtained from search results of specific keywords discussed further in Chapter 3. I believe this study can help provide answers to the above inquiries which will be beneficial to students, developers, researchers and the society on improving mobile application security.

Chapter 2

BACKGROUND

2.1 Profile Analysis

Dwivedi, et al., (2009) stated that profiling is considered an art of introspection of a research domain that aims to benefit specific audience such as researchers and/or readers of a journal or a research topic. Conducting profile analysis for a specific journal might help in finding the right and balanced direction for its future issue publications. In (Dwivedi et al., 2009) research on Information Systems (IS) journals, they stated the "study is likely to stimulate researchers to profile other IS journals in order to conduct comparative/cross-journal studies which will in the end help to understand the overall evolution of the IS discipline."

Dwivedi, et al., (2009) analyzed the first ten years of research published in the Information Systems Frontiers (ISF) from 1999 to 2008. From the published material, the analysis included examining variables such as most productive authors, citation analysis, universities associated with the most publications, geographic diversity, authors' background, and research methods. The authors stated that the ISF is a high-ranking research journal and a premier journal focusing on the frontiers of IS. Their paper provided an overview of research published in the journal which was intended to help them appreciate and identify topics worthy of research and publication. The aim of their paper

was to provide a systematic review of ISF publications in order to ascertain their "current state of play" along a number of dimensions. They reviewed research articles to capture data which is also termed as "meta-study". They recorded various items for each article including the citation of selected articles, geographic regions, authors' background and research methods used by the authors. They used both Web of Science and Google Scholar citation count for assessment. Dwivedi, et al., (2009) used a knowledge domain visualization software for co-citation analysis called the CiteSpace (Chen., 2018). From the analysis presented, the main conclusions that emerged were discussed such as the most productive authors, largest number of researchers from Management Information Systems (MIS), Information Systems, and Computer science and Software Engineering, and most productive institutions amongst others. Dwivedi et al., (2009) anticipated that their paper will prove to be a useful source of information for readers who wish to learn more about various aspects pertaining to the existing body of published IS research in the ISF journal.

CiteSpace is a software used for Visualizing Patterns and Trends in Scientific Literature (Chen., 2018). The primary data source for CiteSpace is the bibliographic records retrieved from the Web of Science in the Thomson Reuters Web of Knowledge format, formerly ISI Export Format. CiteSpace was used in the co-citation analysis by Dwivedi, et al., (2009). The following steps were performed: 1) download the citation data that was pertaining to ISF journal from the ISI web of knowledge database in ISI format; 2) feed the data into CiteSpace; 3) various CiteSpace options were selected, which included the time interval of analysis (2001-2008), the unit of analysis (1 year), the citation threshold (between 2 and 3), the co-citation threshold (between 2 and 3), the pruning and merging option (Pathfinder

network scaling), and the visualization option (merged network cluster view), and 4) they performed a total of four analyses using four different node types.

Shiau, (2010) profiled research that was published on Expert Systems with Applications (ESWA) from the year 1995 to 2008. The analysis identified the most productive author and universities, research paper numbers per geographic region, and research methodologies used by the most highly published authors. Shiau, (2010) explained that the expert system is a kind of information system, a subfield of artificial intelligence; and a software that is used to reproduce the performance of one or more human experts. The objective for conducting profile analysis on articles published in ESWA was to provide a broader understanding of expert systems domain for authors, reviewers, journal editors, universities and research institutions. Shiau, (2010) described the research method followed to conduct profile analysis which involved examining each article to capture the relevant data which includes title, author, subject, affiliation, and citation. She counted and recorded various items for each article that was analyzed including the productivity of authors, geographic regions, author's background, research issues, and the impact of the research by the most productive authors. They assess the impact and contributions made by an author based on self-citation count within ESWA, ISI citation counts, and Google's scholar citation counts. She emphasized that the findings from the study should be regarded as an indicative and not an authoritative statement because such profiling was applied within ESWA. From her findings, she stated ESWA is really internationalized from the view-point of geography and were able to come to a conclusion that leading authors deal with different issues with diverse methods. Her recommendation was presented to research

programs and journal editors to continue diverse research and publish special issues in urgent problems such as financial crisis, global recession in order to meet the worldwide requirements of timely fashion.

Galliers and Whitley, (2007) stated that the field of information systems research has been developing since the first commercial application of information and communication technologies were introduced in the early 1950s. Their paper aimed to address questions and build on the limited empirical work on the topic by developing a profile of European IS research that can form the basis for international comparison. The questions in their research are "Do European researchers have different publishing and citation preferences? Are there particular characteristics that differentiate European IS research from that done elsewhere?" amongst others. In developing the European IS research, their paper reported on all publications in the proceedings of the first 10 years of European Conference on Information Systems (ECIS) conferences, two main databases were used, the Endnote library and the second database was created using Access and stored details of all ECIS papers. They analyzed each paper initially in terms of its title but also by examining the abstract and contents to locate it within the classification. From the presentation of their results, they stated that it is apparent that there are significant patterns to European IS research as evidenced through papers presented in the first 10 European conferences on IS and that some of the patterns are different from those in evidence in the North America IS research tradition (for example, European IS researchers are more business/strategy issues focused).

Palvia, et al., (2007) stated that Information and Management (I&M) has been consistently regarded as one of the top academic journals in information systems (IS). The authors explained that MIS and IS are parts of a young and unique field that is constantly experiencing rapid change and turmoil which is characterized by diversity because of the many problem it addresses. Their article profiled research published in Information and Management (I&M) journal. They used a two-pronged approach to capture the breadth and depth of the data given the need for massive data collection. They identified the most productive authors and universities associated with research publications in I&M during the past 13 years (1992-2005). They also conducted a deeper content analysis on articles published during 1998 to 2005 (which includes 435 articles) to determine the subject areas most often investigated, different types of analyses used, and the research methodologies most often employed. Their result indicated that "while information systems research is dominated by the US-based universities, international researchers are beginning to make inroads" (Palvia, et al., 2007). They explained that most researchers have focused their attention on fundamental and traditional areas of research but there is also sufficient interest in mainstay and emerging topics. They stated that the study provides upcoming researchers with a "bird's eye view" of possible role models and an understanding of their scholarly mindset. In conclusion, the authors stated that the information system field is still young and continues to show explosive growth and continual self-introspection is useful for any field as it matures and thrives.

Dwivedi, et al., (2008) stated that the development and growth of electronic commerce (EC) has experienced sudden increase since its inception for a number of reasons. Due to the early 2000 dot-com bubble crash (Wikipedia contributors, 2018), there has been

attempts by both industry and academia to understand the reasons for failure to assist with the building of successful electronic commerce ventures. Their article profiled the types of research published in the Journal of Electronic Commerce Research (JECR) from 2000 to 2007. The published materials were examined for variables such as citation analysis, universities associated with the most publications, geographic diversity, authors' backgrounds, subject areas most often investigated, and research methodologies. The author stated that their work has implication for researchers, journal editors, universities, and research institutes. The aim of the paper was to provide a systematic review of JECR publications in order to ascertain the current "state of play" of the EC field. From the analysis, authors were able to identify articles of the highest research impact, and most influential researchers amongst others. Tables 1 and 2 provide summary of literature review of profile analysis articles.

Profile analysis is similar to performing a systematic literature review, however, it is different in regards to the research purpose and how the data are collected and interpreted. In systematic literature review, the research purpose is to evaluate and interpret the articles published relevant to a set of research questions (Budgen and Brereton, 2006). Whereas, in profile analysis, the research purpose is to outline the research activities in a publication avenue or a topic. Profile analysis and systematic literature review utilizes similar research method protocol such as identifying publication sources, search and exclusion criteria, and data collection strategies. However, in systematic literature view, only data pertaining to the research questions are collected from the selected articles, whereas in profile analysis entire article is considered as the dataset. Profile analysis and systematic literature review

vary in how the data is interpreted. In systematic literature review, data is evaluated to assess the scientific progression achieved in relevance to the research question. In profile analysis, data is analyzed to identify influential researchers, publication avenues, research topics addressed, and research impacts.

Profile analysis is considered an art of introspection of a research domain that aims to benefit specific audience such as researchers and/or readers of a journal. In light of the above, the aim of this thesis is to give the audience (students, researchers, institutions, and faculty) a better understanding of the peer-reviewed publications of mobile application security. The initial objective was to develop design guidelines for securing mobile applications. Towards that, we were conducting a systematic literature search to identify peer-reviewed articles that empirically investigated mobile application security. We conducted literature search in computing digital libraries including Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), Springer, Association for Information Systems (AIS) and ScienceDirect. Our search revealed that none of articles identified relevant findings to develop design guidelines. This revelation inspired us to conduct profile analysis to discover what is going on in the field of mobile application security.

	(Dwivedi et al., 2009)	(Wen-Lung Shiau, 2010)	(Robert D. Galliers & Edgar A. Whitley, 2007)	(Palvia, Pinjani, & Sibley, 2007)	(Yogesh K. Dwivedi, Melody Y. Kiang, Michael D. Williams, & Banita Lal, 2008)
Profile Analysis Goal	Profiling publication in ISF	Experts Systems Field	IS research by Europeans	Profiling publication in I&M	Electronic commerce field
Year Range	1999 to 2008	1995 to 2008	1993 to 2002	1992 to 2005	2000 to 2007
Digital Library	ISF Journal	ESWA Journal	ECIS Conference	I&M Journal	JECR Journal
Search Criteria	All published articles in the year range	All published articles in the year range	All published articles in the year range	All published articles in the year range	All published articles in the year range
Exclusion Criteria	Systematic classification of published research	Excluded non-peer reviewed articles	Ran queries against the data and checking specific hypothesis and trends	Used two-pronged approach	Systematic classification of research (meta-studies).
Total number of articles analyzed	307	1836		768	139
Data Collected	Citations of selected articles, geographic regions, authors' backgrounds, and research methods.	Title, authors, subject terms, abstract, author affiliation, publication avenue, year, and citations.	Key characteristics of EIS conference, key references and sources used by researchers presenting papers, research areas	Most productive authors, universities with most research publications, most investigated topics, most applied research methodology, and best practices	Citation of selected articles, geographic regions, author's background, research topics and research methodology.
Analysis Performed	Most productive authors, authors' background, discipline, geographic regions, leading research universities, research methods, keyword analysis, citation analysis, mapping the evolution of IS based on ISF publications, and intellectually significant articles	Productive authors, geographic regions, author's background, research issues, and impact of the research by the productive authors.	Most cited authors, most frequently cited articles, papers by research topic, percentages of papers in each research topic by year, most popular social theory sources, number of papers per conference, and number of institutions, papers, authors per paper	Productive authors, leading research universities, research topics trends in research topics, research methodologies, leading research profiles, topics of leading researchers, and methodology used by leading researchers.	Citation analysis, co-author analysis, academic expertise, authors background, leading research universities, country, research paradigm, research methods, unit of analysis, and detailed research topics.

Table 1: Profile Analysis Literature Review

	(Dwivedi et al., 2009)	(Wen-Lung Shiau, 2010)	(Robert D. Galliers & Edgar A. Whitley, 2007)	(Palvia, Pinjani, & Sibley, 2007)	(Yogesh K. Dwivedi, Melody Y. Kiang, Michael D. Williams, & Banita Lal, 2008)
Contributions	• Provided systematic and comprehensive review to describe the current state of IS research • Authors indicated a strong level of collaboration amongst academic and industry experts	• Authors address variety of expert systems research issues using diverse set of research methods. • Productive authors either develop mathematical models or solve emerging real-world problems. • Recommend authors to consider using social science research methods • Recommend editors to create special issues on emerging topics.	• Identified particular characteristic of the European style of research compared to research done in other parts of the world.	• Authors recommend editors to encourage diversity in research to obtain an optimum balance. • The community can observe the role of leading authors easily. • Authors do not promote that all should follow the pattern of leading authors but rather the research topics and methodology.	• Provided a comparison between JECR's profile and other information systems journal. • Authors address it is likely to form the basis and motivation for profiling other journals.

Table 2: Profile Analysis Literature Review Cont'd

Chapter 3

RESEARCH METHODOLOGY

In developing the profile of mobile application security, this thesis reports on peer-reviewed publications from ACM, IEEE, Springer, AIS and ScienceDirect digital libraries between the years 2010 to 2018. We adopted (Dwivedi and Kuljis, 2008) classification scheme for capturing the data. For a detailed analysis, each article was carefully examined to capture the relevant data. Relevant data includes author details, article title, year, citation count, publication type, and publication title.

In the first step, we determined the digital libraries for the analysis. There are so many choices to use but we needed to search for digital libraries with the most comprehensive, extensive, and technical database of articles and also has positive impact on education in the computing field. Hence, it was decided to search four of the leading computing digital libraries:

- ACM Digital Library (https://dl.acm.org/)
- IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp)
- SpringerLink (https://link.springer.com/)
- AIS e-Library (http://aisel.aisnet.org/)
- ScienceDirect (https://www.sciencedirect.com/).

The second step was to determine the search phrases for the search on the digital libraries. The phrases used were “mobile apps” and “application security”, "mobile apps" and "software security", "mobile applications" and "software security" and "mobile applications" and "application security". Other research papers discuss the mobile application security but not all of them address the term in the same way. The rationale behind using above specified search phrases was to capture all possible instances of the mobile application security in publications from the digital libraries selected. This step was created as a method to determine relevant articles to mobile application security, also this step was not found in any other profile analysis research done over the years.

In the third step, searches were conducted on each digital library. Advanced search functionality was used where the search phrase that appeared either in the title or abstract of the publications between 2010 and 2018, which produced different search results from each of the search phrase. Figure 1 shows a screenshot of advanced search functionality for ACM Digital Library. During the search, fields were added to find where the phrases matches in the articles. Advance search functionality in SpringerLink could not accommodate the above search process and did not perform as expected. Thus, the regular search functionality available in the SpringerLink homepage was used to conduct the searches. The search result from each library was exported to a .csv file to the local computer for further analysis. The number of articles retrieved from each library search are shown in Table 3 below.

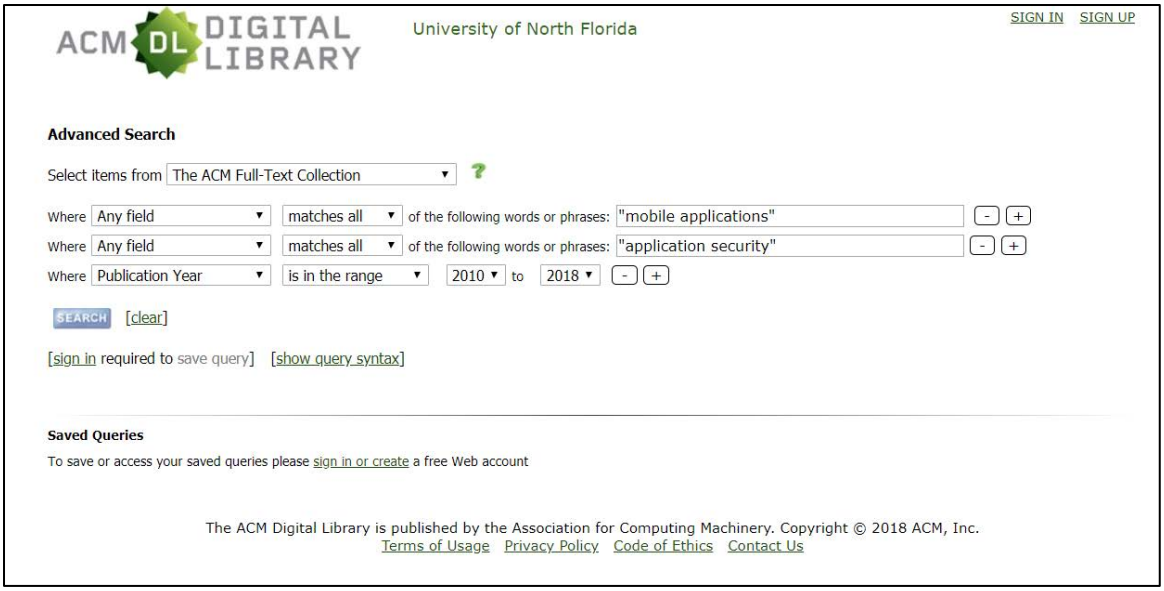

Figure 1: ACM Digital Library Search

Keywords / Search Date	IEEE	ACM	Springer	AIS	ScienceDirect
	July 19, 2018	July 19, 2018	July 19, 2018	July 19, 2018	July 19, 2018
"mobile apps" and "application security"	191	25	98	8	61
"mobile apps" and "software security"	77	11	41	5	39
"mobile applications" and "software security"	163	8	85	11	69
"mobile applications" and "application security"	340	36	235	15	128
Total	771	80	459	39	297

Table 3: Search Results

The fourth step involved reading the title and abstract of each article from the search results. The aim was to determine if the focus of the article was on mobile application security. From the review of the articles, those that were relevant to/discussed mobile application

security were selected for the second stage of review. See Table 4 for the result of the fourth step. The results had a number of articles that appeared multiple times from all 4 searches performed. A filtration process was done to eliminate the duplicates by loading the results into a database using MySQL Workbench tool and each duplicate was reviewed extensively to determine the relevance to the field before it was discarded or moved to the next stage of the analysis as shown in Figure 2.

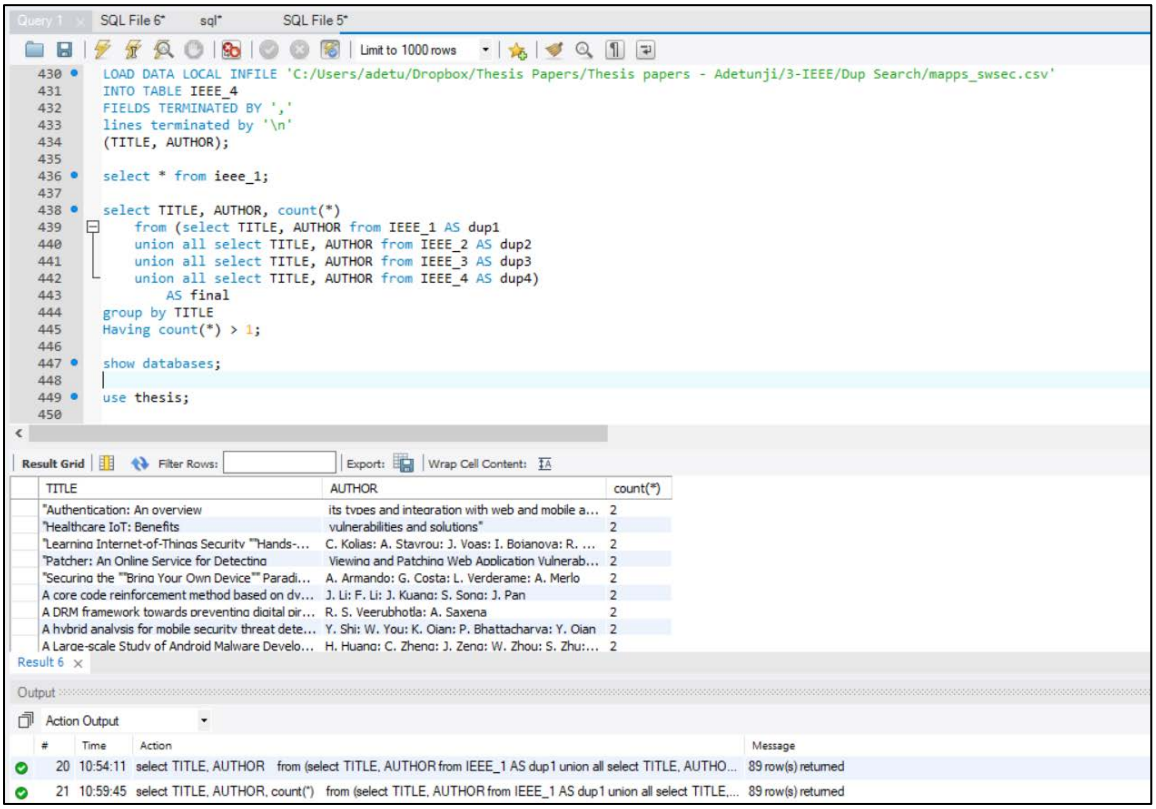

Figure 2: Preprocess Step

For the fifth step, each article selected from the previous step was examined fully to ensure the article is pertinent to mobile application security. After reading through the title and abstract of the paper in the previous step, if there was no clear understanding from the paper

if the authors discussed/studied the mobile application security topic, then this step was implemented to further review the articles to be able to select the specific articles needed for the analysis. Articles that were not relevant to mobile application security were left out from further considerations.

In the sixth step, each article selected from the previous step was read very carefully to extract information on the article title, author information, author affiliations, publication year, publication type, publication title, number of citations, and number of co-authors. Google's scholar was used to obtain the number of citations received for each article. As in previous studies, in order to report authors' productivity data, a normal count approach was used. A normal count approach means each publication counted as one for all authors which is not regarding the number of co-authors. This stage revealed that 70 articles were relevant to the research as shown in the Table 4. Appendix A provides a listing of the selected articles.

Digital Libraries	Fourth Step	Fifth Step
ACM	17	14
IEEE	25	18
Springer	20	12
AIS	13	12
ScienceDirect	20	14
Total	95	70

Table 4. Fourth and Fifth Steps Results

The seventy articles found through the systematic literature search explained in this section were the basis for conducting the profile analysis of the mobile application security field. The profile analysis started by obtaining the author's information from those articles. The

profile analysis reported on the research methods, research approach (quantitative, qualitative, and mixed), theories used, data analysis performed, and keywords reported in those research articles.

Chapter 4

FINDINGS

The profile analysis was conducted using (Dwivedi, et al., 2009) as a guide. The findings of the profile analysis on the mobile application security topic is presented in the following subsections. The first subsection presents the geographical diversity of the authors; which includes the most productive authors, top countries, geographic regions, number of co-authors, and the authors' background. The following section provides the most active universities in the field followed by the research methods used. The following subsections will discuss the most frequently used keywords in mobile application security and also results of the topic level analysis.

4.1 Productive Authors

For presenting the findings of the analysis, those authors who have published two or more articles during the analysis period (2010 to 2018) are included in the list. There was a total number of 224 authors who contributed to the articles on mobile application security. Table 5 below shows the list of the 6 most productive authors ordered according to the number of articles published during the study period and also the recent affiliation. The findings show us that only two authors have contributed to 3 publications wherein both of them are from IBM Research Center and co-authored those 3 articles. The remaining 4 authors contributed two articles each. The largest number of authors (218) contributed one

article each. This finding clearly indicates that none of the authors have published sufficient number of articles to be considered as an influential researcher of mobile application security.

NO	Author Name	Count	Recent Affiliation
1	Omer Tripp	3	IBM Thomas J. Watson Research Center
2	Marco Pistoia	3	IBM Thomas J. Watson Research Center
3	Long Lu	2	Stony Brook University
4	Paolina Centonze	2	Iona College
5	John Grundy	2	Swinburne University of Technology
6	Hui Xiong	2	Rutgers University

Table 5. The most productive authors

4.2 Country and Geographic Region

From the analysis conducted, the authors from a total of 30 countries who published between the years 2010 and 2018 on mobile application security were identified. The analysis was performed based on the author affiliation and geographic location information provided in the articles. In terms of the number of contributors from diverse/different countries, it was noticed that the largest number of authors were from the USA (81) followed by Germany (16) at a distant second followed by the third largest which was India (13) and in fourth place was Spain and Austria with 11 each. The top 11 countries are listed in Table 6 below. There was a total of 13 articles that had no countries reported and were labeled null. From Table 7, if the European countries are combined, they will rank second and will closely match the count of the North America region.

In addition to the table above, a map view was added to visualize the findings which is shown in Figure 2. Tableau was used to compose the findings visually (Tableau 2018). The top 11 countries are labeled on the map as well as other countries that did not meet the top 11 but published articles within the analysis period.

Rank	Country	Count
1	USA	81
2	Germany	16
3	India	13
4	Austria	11
5	Spain	11
6	Australia	9
7	Canada	8
8	Korea	7
9	Italy	6
10	China	5
11	Malaysia	5

Table 6. Countries

Rank	Geographic Region	Count
1	North America	92
2	Europe	66
3	Asia	40
4	South America	3
5	Africa	2

Table 7. Geographic Regions

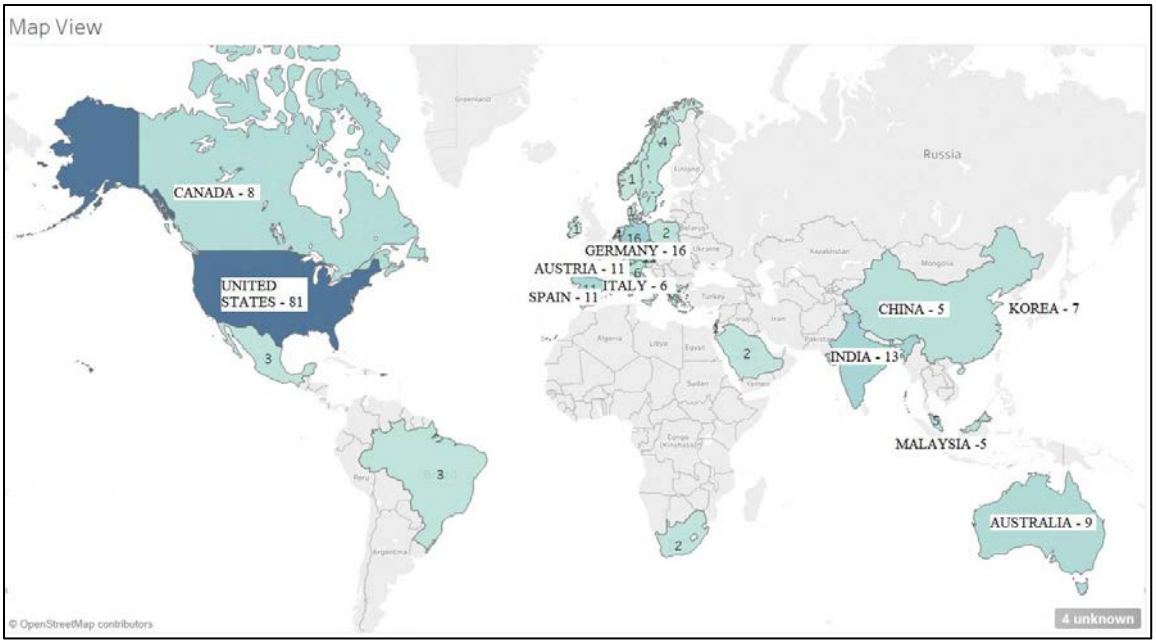

Figure 3: Top 11 Countries

4.3 Number of Authors

From the analysis, we have 70 unique articles with 224 unique authors in total which indicates that on average articles had three collaborators. This finding is corroborated by the table 8, which shows there were more articles published with three authors than two or four authors. About 91% of the published articles had more than one author which shows that researchers feel this is not an aspect that can be addressed by single researcher and collaboration is an important consideration to making knowledge contribution. Most of the articles did not provide departmental or disciplinary background information about the authors, due to which we could not perform analysis on interdisciplinary collaborations that may be occurring.

Number of Authors	Count
1	6
2	16
3	23
4	11
5	7
6	5
7	1
8	1
Total	70

Table 8. Number of Authors

4.4 Top Universities

Similar to the most productive authors, we performed another analysis in terms of the most productive institutions. To perform this analysis, we counted unique the affiliation occurrences within each article. For instance, if an article had multiple authors from same university, then that university received one count. The analysis showed that academic institutes are leading the scientific progression of mobile application security. Table 9 shows that the authors were from 58 universities, 5 colleges (that were not classified as university) and 24 research institutes in total. Table 10 shows that the University of California, Syracuse University and North Carolina Agricultural and Technical State University were on top of the list for universities with 6 articles each. It should be noted that all of the top 10 universities are within the United States which indicates researchers from other countries were not as productive in conducting research on mobile application security. When the articles related to the top ten universities were carefully examined, it was noticed there were no collaborations amongst the authors across the leading

universities. Also, it was noticed that only two authors from the top six productive authors listed in Table 5 are from one of the top universities on the list in Table 10. In regard to non-academic institutions, it was noticed that the top research entity was the IBM Thomas J. Watson Research Center with 7 articles. Table 11 shows a list of some of the research institutions and the country where they are located as stated in the published articles.

Authors' Affiliation		Count
Academic	University	58
	College	5
Research Industries		24
Total		87

Table 9. Author's Affiliation

Rank	University	Count
1	University of California	6
2	Syracuse University	6
3	North Carolina Agricultural and Technical State University	6
4	Stony Brook University	5
5	Old Dominion University	4
6	University of California, Berkeley	4
7	Dakota State University	3
8	Rutgers University	3
9	University of New Haven	3
10	University of South Carolina	3

Table 10. Top 10 Universities

NO	Name	Country
1	IBM Thomas J. Watson Research Center	USA
2	Scarfone Cybersecurity	USA
3	Tapestry Technologies	USA
4	IBM Research - Hafia Mount Carmel	Israel
5	New York Institue of Technology	Canada
6	Computer Security Lab (COSEC)	Spain
7	Shanghai Key Laboratory of Computer Software Testing and Evaluation	China
8	SBA Research	Austria

Table 11. Top Non-academic Institutions

We created a plot of articles by the year they were published to give a visualization of the number of articles and the year they were published. Figures 4 and 5 show us that majority of the research on mobile application security was done between 2014 and 2017.

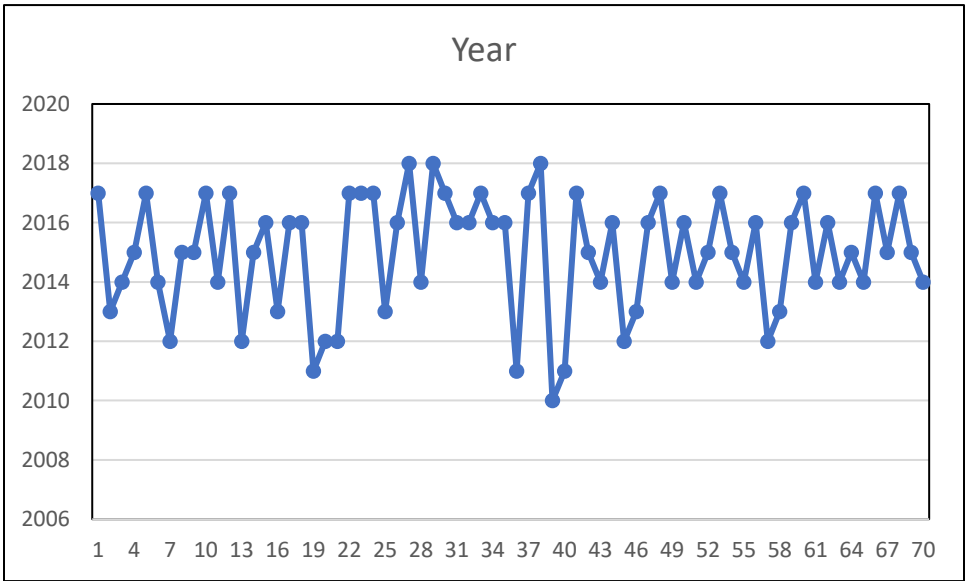

Figure 4: Articles by Year Published

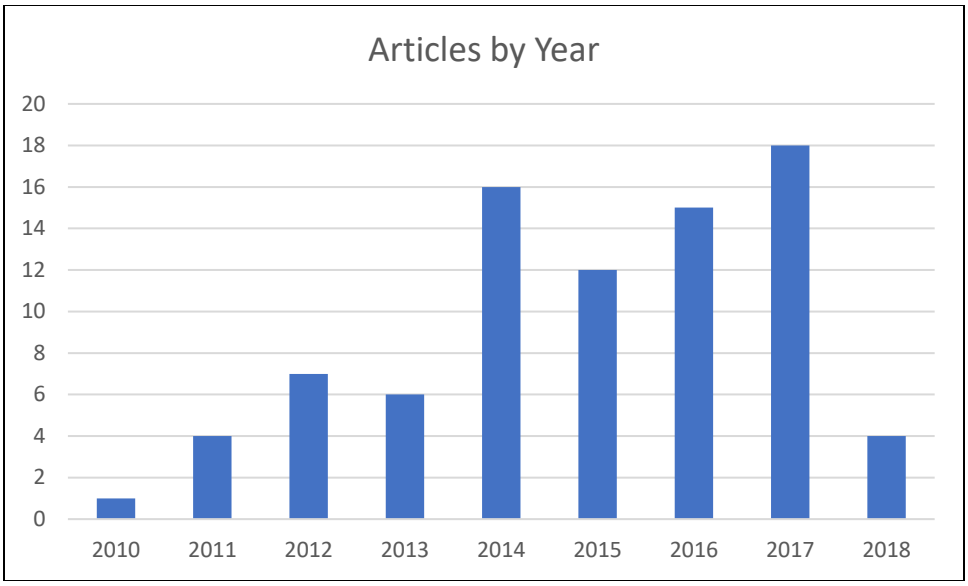

Figure 5: Distribution by Year Published

4.5 Publication Types

This section provides a tabulation of publication types of the articles included in the profile analysis. The following publication types were considered for the analysis: Book, Book Chapter, Conference Proceeding, Journal, and Workshop as shown in Table 12. Each article was categorized into one of the publication types as stated in the digital library and the article. Conference is the preferred publication type among the mobile application security researchers, which is not a surprising finding given the general publication trend within the computing discipline. ScienceDirect digital library published more journal articles than the rest of the digital libraries, which may be a reflection of concerted effort of ScienceDirect to publish journals and books to provide an in-depth analysis of topics (ScienceDirect, 2018).

	ACM	IEEE	AIS	Springer	ScienceDirect	Total
Journal	-	5	-	2	8	15
Conference	10	12	12	9	1	44
Workshop	4	1	-	-	-	5
Book	-	-	-	-	-	-
Book Chapter	-	-	-	1	5	6
Total	14	18	12	12	14	70

Table 12. Publication Types

From the analysis, it was noticed that only 7 publication venues had more than one article on mobile application security as shown in Table 13. It was also noticed that only one author (Marco Pistao) published twice within the same library (ACM) in the same publication (International Workshop on Mobile Development Lifecycle). This finding indicates that none of the researchers are not consistently pursuing their research on a topic relevant to mobile application security to build their body of work. By not going to the same conference on regular basis, researchers are missing opportunities to building community of researchers to work on the topic.

Publication Name	Publication Type	Digital Library	Count
International Workshop on Mobile Development Lifecycle	Conference	ACM	3
Journal of System and Software	Journal	ScienceDirect	3
International Conference on Mobile Web and Information Systems	Conference	Springer	2
International Conference on Information Systems	Conference	AIS	2
International Conference on Information Resource Management	Conference	AIS	2
Computers and Security	Journal	ScienceDirect	2
European Conference on Information Systems	Conference	AIS	2

Table 13. Top Publication Avenues

4.6 Research Method

In a peer-reviewed article, the research method section is expected to describe the process followed to collect the research data as well as the type of analysis performed to produce research results (Kerry, 2013). Research methods can also be said to influence the audience on how research was done which describes the step by step procedure that was used for the research. Thus, describing research methods adopted to conduct research is important. Table 14 provides the listing of reported research methods we found from the published articles. The analysis shows that only 25 articles revealed the research methods adopted for conducting their research on mobile application security.

It was expected of the authors to explicitly state the research methods used, but when an article did not explicitly state the research methods adopted, we read the article carefully to find statements that may describe data collection and analysis process of a known research method. During the process of extracting research method findings, we also found that the majority of the authors did not provide any information, even though these are peer-reviewed, scientific articles. From the articles where the research methods were stated, a process was performed to combine the similar research methods that are described differently. For example, one author stated survey was used as the research method and another author stated he used questionnaire; the results were combined as survey. The findings show that the majority of the articles published in the field of mobile application security used surveys and experiments as the primary research method. These two methods help researchers get direct feedback from users and developers.

Rank	Research Method	Count
1	Survey	8
2	Experiment	8
3	Hybrid Analysis (Static & Dynamic)	4
4	Online Experiment	3
5	Comparison	2

Table 14. Research Methods

4.7 Most Frequently Used Keywords

In order to get the most frequently used keywords by the authors, all the keywords reported in the articles were collected. There was a total of 231 keywords. Fifty-two articles reported the keywords in their research and 18 articles did not. Most frequent keywords along with the number of occurrences are listed in the Table 15. The table shows keywords that were listed in more than two articles. Given that there were 70 articles relevant to mobile application security, it was observed that majority of the keywords were on a specific security topic. When generic variant topics such as security and applications were excluded, we have privacy and trust were the most frequent keywords used by the researchers.

Keywords	Count
Security	11
Smartphones	6
Mobile Application	6
Privacy	5
Mobile Apps	5
Mobile Security	4
Mobile Application Development	4
Trust	3
Survey	3

Table 15. Keywords

4.8 Topic Level Analysis

As the keyword analysis did not reveal any major topic level directionality among the researchers, it was decided to perform a topic level analysis of the articles. Based on the reading of the articles, each article was classified using an emergent list of topics. An open coding process from the grounded theory method was followed (Flick, 2009). Each article was read and then assigned a set of topics based on the focus of the research problem addressed in the article. This process allowed for using the same topic on multiple articles if the research foci were similar, even though authors might have used different keywords to describe them. Each article was classified into different topics and then the topics were analyzed with the countries of the author affiliations to detect any interesting trend that may exist. Table 16 shows the results of topic level analysis. In comparison to keyword analysis, topic level analysis revealed that researchers are focused on documenting the challenges of securing mobile applications and addressing their privacy issues. The analysis also revealed interesting findings such as Android Security is popular among Indian researchers and Mobile Banking is popular among South African researchers.

Keyword	Country	Count
Challenges of Securing Apps	USA, Saudi Arabia, Switzerland	5
Privacy	USA, China, Brazil	4
Trust	Germany, South Africa, Australia	3
S/W Development Process	Italy, USA	3
Android security	India, Italy, London, Hong Kong	3
Security Integration	USA, South Africa	3
App Recommendation	USA	2
Mobile Malware	Korea, Singapore	2
Security Requirement	Malaysia, Australia	2
m-healthcare development	USA	2
Security Vulnerabilities	USA	2

Keyword	Country	Count
Mobile Banking	South Africa, USA	2
Agile Software Dev.	Italy	1
Testing Techniques	Malaysia	1
Detection Techniques	India	1
Identity Management	Sweden	1
Connected Device Security	USA	1
Payment Apps	Canada	1
Personal Identity	Sweden	1
User Confidence	USA	1
Real World Experiences	USA	1
Update Delivery	Germany	1
Digital Applications	Germany	1
Testing Framework	USA	1
Security Discrepancies Between Androids Apps	USA	1
E-commerce	South Africa	1
Web App Security	USA	1
Information Sensitivity	USA	1
Policy Enforcement	USA	1
Quality of Mobile Apps	Australia	1
Risk Analysis	Italy	1
Security Analysis	Australia	1
Access Control	Poland	1
Managing Mobile Security	USA	1
Android Application Repackaging	India	1
Significance of Mobile Security	Macedonia	1
Personal Information	Germany	1
Impact of Security	Germany	1
Software Security Threat	Netherlands	1
Code Injection	USA	1
Secure Passwords	Austria	1
Software Security	China	1
Capture and Validate Security Req.	Malaysia	1
S/W Engineering Process	Denmark	1
App Installation Mechanism	USA	1
Smart Device Malware	Spain	1
Smartphone App Security	USA	1
Security Breach	Mexico	1
Security Evaluation	Greece	1

Table 16. Topic Level Keyword Analysis

4.9 Citation Count

A citation analysis was performed to determine the research impact of the articles based on the number of publication citations. Google Scholar was used to obtain citation counts for the articles (Google Scholar, 2018). Table 17 summarizes the articles with the highest number of citations from each digital library that was used for the analysis. Table 18 shows the list of articles with citations more than 100. From Tables 17 and 18, it can be noted that AIS articles do not have significant impact on the field, whereas, ACM and IEEE articles are making considerable impact to the field.

Library	Title	Author	Recent Affiliation	Year	Citation Count
ACM	Measuring User Confidence in Smartphone Security and Privacy	Erika Chin, Adrienne Porter Felt, Vyas Sekar, David Wagner	University of California	2012	291
ScienceDirect	Chapter 5 - Android device, data, and app security	Andrew Hoog		2011	273
IEEE	Android Security: A Survey of Issues, Malware Penetration, and Defenses	Parvez Faruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Gaur, Mauro Conti	Government MCA College, Ahmedabad	2015	206
Springer	Defending Users against Smartphone Apps: Techniques and Future Directions	Wiliam Enck	North Carolina State University	2011	120
AIS	Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?	Mark Harris, Karen Pattern, Elizabeth Regan, Jerry Fjermestad	University of South Carolina	2012	15

Table 17. Citation Analysis

Digital Library	Title	Cited	Year
ACM	Measuring User Confidence in Smartphone Security and Privacy	291	2012
ScienceDirect	Chapter 5 - Android device, data, and app security,	273	2011
IEEE	Android Security: A Survey of Issues, Malware Penetration, and Defenses	206	2015
IEEE	Evolution, Detection and Analysis of Malware for Smart Devices	177	2014
Springer	Defending Users against Smartphone Apps: Techniques and Future Directions	120	2011
ACM	Code Injection Attacks on HTML5-based Mobile Apps: Characterization, Detection and Mitigation	108	2014

Table 18. Citation count above 100

Chapter 5

DISCUSSIONS

In this thesis, results of the profile analysis on mobile application security were provided. The initial goal for the thesis was to develop and present mobile application security best practices for application designers and developers. Towards that, systematic search was conducted to identify relevant literatures that have empirical findings on mobile application security. However, the search did not reveal sufficient number of articles to generate best practices. This finding lead us to wonder what's being studied about mobile application security as a whole. Profile analysis is the appropriate research method to answer our curiosity.

This thesis shows that some geographical regions of the world are doing more research in the area of mobile application security than the rest. America was the top productive country followed by Germany at a distance. When we analyzed from continent perspective, Europe caught up with North America. When the number of smartphone users is considered, China and India are first and second countries with highest number of users followed by the United States (Newzoo, 2018). However, there were only 13 articles from India and 5 from China. Over the years, the continent of Africa has been witnessing a rapid pole of smartphone adoption. However, only two articles from Africa were found which were from South Africa (QuartzAfrica, 2016). Thus, we highly encourage researchers from China and India as well as African countries to study mobile application security given the large and still increasing user base in their respective countries.

Our analysis on authors of the articles revealed that only two out of 224 authors have published more than 2 articles. When affiliations of authors were considered, it was found that IBM Thomas J. Watson Research Center was the leading institution with 7 articles, followed by three Universities (University of California, Syracuse University, and North Carolina Agricultural and Technical State University) with 6 articles each. Inspection of these articles did not reveal any consistent development of body of work on mobile application security, but rather a diversified research focus. Our findings also revealed the articles with affiliations to the IBM Research Center or the above-listed Universities had different sets of authors. Thus, authors from these affiliations were not collaborating with other researchers even within the same institution. Clearly, this shows the need for researchers to collaboratively work on mobile application security to build a community of researchers. Furthermore, researchers need to consistently work on the field to develop a significant and impactful body of work and influence future directions.

One of the purposes of profile analysis is to determine the leading topics researched within the mobile application security field. Our topic level analysis revealed that challenges, privacy and trust aspects of mobile application security were frequently studied. Other topics that were also studied included mobile banking and payment applications, security integration, security vulnerabilities, m-healthcare applications and identity management. In general, our findings revealed that the topics studied by researchers were extremely diversified, thus, did not reveal a significant gravitation of topics within the field. We did not find any articles on mobile application security with focus on gaming applications. Given the extensive growth of mobile gaming applications and well-published security

issues (Statista, 2018), we were surprised to not find any article on this subject. Mobile applications are the biggest drainers of mobile devices (Wilke, Gotz, & Uwe, 2013); however, we did not find any article that studied battery consumption by mobile applications from security vulnerability standpoint.

We also discovered that, only 25 out of the 70 articles reported the research methods used to conduct their research study. Thus, majority of the authors who studied the field of mobile application security did not properly report their data collection and analysis methods. When researchers do not provide detailed account of how data were gathered and analyzed, readers question the scientific rigor of the study. Also, other researchers are discouraged to replicate findings of the authors. We highly recommend editors of publishing venues on future research to ensure researchers report their research methods.

In regard to digital libraries, IEEE had the largest number of articles followed by the ACM and ScienceDirect. Our analysis on the publication venues did not reveal any article that was narrowly focused on mobile application security. Articles we found were published in venues that focused on computer security or mobile applications generically, as opposed to specifically. Thus, computing digital libraries such as ACM, IEEE, AIS, Springer, and ScienceDirect should consider creating publication venues that are specifically focused on mobile application security.

Chapter 6

CONCLUSION

From this thesis' findings, it is apparent that there are significant patterns on mobile application security from performing profile analysis on mobile application security based on the research performed in the field between the years 2010 and 2018. We reviewed articles that were published in the field to extract data and also generate our conclusion from. This thesis was able to give an understanding of the mobile application security field as a whole and the current "state of play" based on the findings. We were able to determine the most productive author that published articles on mobile application security within the research period, we determined the countries and geographic region that has done more research, the most frequently used keyword, research methods used in the mobile application security field, and the major topics being researched.

Some interesting results emerged by analyzing the data during that period. The research was done on the IEEE, ACM, AIS, Springer and ScienceDirect digital libraries. This work tells us mobile application security is a major field and with the increase in the use of mobile applications and smartphones, there is a need for more collaboration amongst researchers. As part of future work, we intend to expand on the study of mobile application security to perform research on the field more closely as we have seen topics studied by researchers were extremely diversified and to develop a holistic empirical model research on security requirements of secure mobile applications.

6.1 Contributions

This thesis introduced a profile analysis of mobile application security, based on the other profile analyses performed within the computing discipline. Findings from this thesis show that profile analysis can be used as a useful source of information for readers who wish to learn more about the different aspects of the existing body of work in the field of mobile application security. Table 19 provides a summary of profile analysis contributions.

Profile Analysis Goal	Mobile application security
Year Range	2010 to 2018
Digital Library	ACM, AIS, IEEE, Springer, ScienceDirect
Search Criteria	"mobile apps" and "application security", "mobile apps" and "software security", "mobile applications" and "software security" and "mobile applications" and "application security"
Exclusion Criteria	Reviewed articles for relevance on mobile application security
Total number of articles analyzed	70
Data Collected	article title, author information, author affiliations, publication year, publication type, publication title, number of citations, and number of co-authors.
Analysis Performed	Productive authors, country and geographic region, number of authors, top universities, publication types, research method, most frequently used keywords, topic level analysis, and citation count
Contributions	• Provide a snapshot of mobile application security and extent to which it is being researched for better understanding. • Recommend that editors should encourage diversity in research to gain the best balance. • Our findings revealed that topics studied by researchers are extremely diversified, thus, did not reveal a significant gravitation of topics within the phenomenon. • Non-of the authors have published sufficient number of articles to be considered influential. • There is need for researchers to collaboratively work on mobile app security to build a community of researchers. • A topic level analysis indicated that challenges, privacy, and trust were the most utilized keywords.

Table 19. Contributions

6.2 Future work

As future work, we recommend more research on mobile application security as a whole, but in a more focused and not so diverse way as we have seen from the findings of the profile analysis. Another direction for the future work is to generate a holistic empirical model for developing secure mobile applications.

References

Aldayel, A., & Alnafjan, K. (2017). Challenges and best practices for mobile application. *Proceedings of the International Conference on Compute and Data Analysis*, pp.: 41-48.

Budgen, D., & Brereton, P. (2006). Performing systematic literature reviews in software engineering. *Proceedings of the 28th International Conference on Software Engineering, pp.:* 1051-1052.

Chakraborti, S., Acharjya, D. P., & Sanyal, S. (2015). Application security framework for mobile app development in enterprise setup. *The Computing Research Repository (CoRR), March issue*. Retrieved from http://arxiv.org/abs/1503.05992

Chin, E., Felt, A., Sekar, V., & Wagner, D. (Jul 11, 2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security*. Article 1, pp.: 1 to 16.

Dwivedi, Y. K., Lal, B., Mustafee, N., & Williams, M. D. (2009). Profiling a decade of information systems frontiers' research. *Information Systems Frontiers,* 11 (1), pp.: 87 – 102.

Flick, U. (2009). *An introduction to qualitative research* (5th ed.). London: Sage Publications.

Guo, M., Bhattacharya, P., Yang, M., Qian, K., & Yang, L. (2013). Learning mobile security with android security labware. *Proceeding of the 44th ACM technical symposium on Computer science education, pp.:* 675-680.

Kerry, H. (2013). *An introduction to the philosophy of methodology* (1st ed.). London: Sage Publications.

Liu, B., Kong, D., Cen, L., Gong, N. Z., Jin, H., & Xiong, H. (Feb 2, 2015). Personalized mobile app recommendation. *Proceedings of the Eighth ACM International Conference on Web Search and Data Mining*, pp.: 315-324.

New Generation Applications Pvt Ltd. (2017). 10 biggest risks to mobile apps security. Retrieved from https://www.newgenapps.com/blog/10-biggest-risks-to-mobile-apps-security

newzoo. (2018). Top 50 countries/markets by smartphone users and penetration. Retrieved from https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/

Yusop, N., Kamalrudin, M., Sidek, S., & Grundy, J. (2016). *Automated support to capture and validate security requirements for mobile apps. Proceedings in the Asia Pacific Requirements Engineering Conference*, pp.: 97 – 112. Springer.

Palvia, P., Pinjani, P., & Sibley, E. H. (2007). A profile of information systems research published in information & management. *Information & Management, 44*(1), pp.: 1-11.

Payne, J. (2013). Secure mobile application development. *IT Professional, 15*(3), pp.: 6-9.

Quartzafrica (2016). Smartphone use has doubled in Africa in two years. Retrieved from https://qz.com/africa/748354/smartphone-use-has-more-than-doubled-in-africa-in-two-years/

Galliers, R. D. & Whitley, E.A. (2007). Vive les differences? Developing a profile of European information systems research as a basis for international comparisons. *European Journal of Information Systems, 16(1)*, pp.: 20–35.

ScienceDirect. (2018). Peer-reviewed scholarly literature. Retrieved from https://www.elsevier.com/solutions/sciencedirect

Statista. (2018). Mobile gaming industry - statistics & facts. Retrieved from https://www.statista.com/topics/1906/mobile-gaming/

Shiau, W.L. (2010). A profile of information systems research published in expert systems with applications from 1995 to 2008. *Expert Systems with Applications, 38(4)*, pp.: 3999-4005.

Wikipedia contributors. (2018). Retrieved from https://en.wikipedia.org/wiki/Dot-com_bubble

Wilke, C., Gotz, S., & Uwe, A. (2013). Energy consumption and efficiency in mobile applications: A user feedback study. *Proceedings in the International Conference on Green Computing and Communications,* pp.: 134-141.

Dwivedi, Y.K., & Kuljis, J. (2008). Profile of IS research published in the European journal of information systems. *European Journal of Information Systems 17(6)*, pp.: 678–693.

Dwivedi, Y.K., Kiang, M.Y., Williams, M.D., & Lal, B. (2008). Profiling research published in the journal of electronic commerce research. *Journal of Electronic Commerce Research, 9(2)*, pp.: 77 – 91.

Zhu, H., Xiong, H., Ge, Y., & Chen, E. (Aug 24, 2014). Mobile app recommendations with security and privacy awareness. *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp.: 951-960.

Chen, C., (2018). CiteSpace. Retrieved from http://cluster.cis.drexel.edu/~cchen/citespace/

Google Scholar (2018). Retrieved from http://scholar.google.com

Tableau (2018). https://www.tableau.com/

APPENDIX A – ARTICLES SELECTED FOR PROFILE ANALYSIS

Below, is the list 70 articles that fit the search criteria used for the profile analysis on mobile application security.

IEEE

Jaramillo, D., Newhook, R. Nassar, N. (2014). Techniques and real world experiences in mobile device security. *In SouthEastcon 2014*, IEEE pp.: 1-6.

Milosevic, J., Ferrante, A., Regazzoni, F. (2015). Security challenges for hardware designers of mobile systems *In Mobile Systems Technologies Workshop (MST),* 2015, pp.: 27-32.

Abernathy, A., Yuan, X., Hill, E., Xu, J., Bryant, K., & Williams, K. (2017, March). SACH: A tool for assisting Secure Android application development. *In SoutheastCon*, 2017, pp.: 1-4. IEEE.

Buhov, D., Huber, M., Merzdovnik, G., Weippl, E., & Dimitrova, V. (2015, August). Network security challenges in Android applications. *In Availability, Reliability and Security (ARES)*, 2015 10th International Conference, pp.: 327-332.

Khadiranaikar, B., Zavarsky, P., & Malik, Y. (2017, October). Improving Android application security for intent based attacks. *In Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017 8th IEEE Annual,* pp.: 62-67.

Ziegler, D., Rauter, M., Stromberger, C., Teufl, P., & Hein, D. (2014, May). Do you think your passwords are secure?. *In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference,* pp.: 1-8.

Lopes, H., & Chatterjee, M. (2014, April). Application H-Secure for mobile security. *In Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014 International Conference,* pp.: 370-374.

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android security: a survey of issues, malware penetration, and defenses. *IEEE communications surveys & tutorials*, *17(2),* pp.: 998-1022.

Benítez-Mejía, D. G. N., Sánchez-Pérez, G., & Toscano-Medina, L. K. (2016, July). Android applications and security breach. *In Digital Information Processing, Data*

Mining, and Wireless Communications (DIPDMWC), 2016 Third International Conference, pp.: 164-169.

Wang, Y., Wei, J., & Vangury, K. (2014, January). Bring your own device security issues and challenges. *In Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th,* pp.: 80-85.

Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2014). Evolution, detection and analysis of malware for smart devices. *IEEE Communications Surveys & Tutorials, 16(2),* pp.: 961-987.

Payne, J. (2013). Secure mobile application development. *IT Professional, 15(3),* pp.: 6-9.

Chandramohan, M., & Tan, H. B. K. (2012). Detection of mobile malware in the wild. Computer, 45(9), pp.: 65-71.

Eshmawi, A., & Nair, S. (2013, May). Smartphone applications security: Survey of new vectors and solutions. *In 2013 ACS International Conference on Computer Systems and Applications (AICCSA),* pp.: 1-4.

Aron, L., & Hanacek, P. (2015, March). Overview of security on mobile devices. In Web Applications and Networking (WSWAN), *2015 2nd World Symposium,* pp.: 1-11.

Liu, Z., Hu, Y., & Cai, L. (2014, August). Research on software security and compatibility test for mobile application. *In Innovative Computing Technology (INTECH), 2014 Fourth International Conference,* pp.: 140-145.

Srinivasan, S. M., & Sangwan, R. S. (2017). Web App Security: A Comparison and Categorization of Testing Frameworks. *IEEE Software, (1),* pp.: 99-102.

Harish, U., & Ganesan, R. (2012, March). Design and development of secured m-healthcare system. *In Advances in Engineering, Science and Management (ICAESM), 2012 International Conference,* pp.: 470-473.

Springer

Morera, E., de la Torre Díez, I., Garcia-Zapirain, B., López-Coronado, M., & Arambarri, J. (2016). Security recommendations for mHealth apps: Elaboration of a developer's guide. *Journal of Medical Systems, 40(6),* pp.:1-13.

Saini, J. (2017, October). Security Protocol of Social Payment Apps. *In International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments,* pp.: 139-150.

Yusop, N., Kamalrudin, M., Sidek, S., & Grundy, J. (2016, November). Automated support to capture and validate security requirements for mobile apps. *In Asia Pacific Requirements Engineering Conference,* pp.: 97-112.

Corral, L., Sillitti, A., & Succi, G. (2013, August). Agile software development processes for mobile systems: Accomplishment, evidence and evolution. *In International Conference on Mobile Web and Information Systems,* pp.: 90-106.

Cho, H., Lim, J., Kim, H., & Yi, J. H. (2016). Anti-debugging scheme for protecting mobile apps on android platform. *The Journal of Supercomputing, 72(1),* pp.: 232-246.

Alavi, A., Quach, A., Zhang, H., Marsh, B., Haq, F. U., Qian, Z., ... & Gupta, R. (2017, March). Where Is the Weakest Link? A Study on Security Discrepancies Between Android Apps and Their Website Counterparts. *In International Conference on Passive and Active Network Measurement,* pp.: 100-112.

Poniszewska-Maranda, A., & Majchrzycka, A. (2016, August). Access control approach in development of mobile applications. *In International Conference on Mobile Web and Information Systems,* pp.: 149-162.

Krupskiy, A., Blessinga, R., Scholte, J., & Jansen, S. (2017, June). Mobile Software Security Threats in the Software Ecosystem, a Call to Arms. *In International Conference of Software Business,* pp.: 161-175.

Pranata, I., Athauda, R., & Skinner, G. (2012, November). Determining trustworthiness and quality of mobile applications. *In International Conference on Mobile Wireless Middleware, Operating Systems, and Applications,* pp.: 192-206.

Enck, W. (2011, December). Defending users against smartphone apps: Techniques and future directions. *In International Conference on Information Systems Security*, pp.: 49-70.

Seo, S. H., Yim, K., & You, I. (2012, August). Mobile malware threats and defenses for homeland security. *In International Conference on Availability, Reliability, and Security*, pp.: 516-524.

Teles, A., Silva, F. J., & Batista, R. (2013). Security and privacy issues in mobile social networks. *In Security and Privacy Preserving in Social Networks,* pp.: 281-313.

ACM

Aldayel, A., & Alnafjan, K. (2017, May). Challenges and Best Practices for Mobile Application Development. *In Proceedings of the International Conference on Compute and Data Analysis,* pp.: 41-48.

Tripp, O., Pistoia, M., & Centonze, P. (2015, May). Application-and user-sensitive privacy enforcement in mobile systems. *In Proceedings of the Second ACM International Conference on Mobile Software Engineering and Systems,* pp.: 162-163.

Pistoia, M., & Tripp, O. (2014, October). Integrating security, analytics and application management into the mobile development lifecycle. *In Proceedings of the 2nd International Workshop on Mobile Development Lifecycle* pp.: 17-18.

Mitra, J., & Ranganath, V. P. (2017, November). Ghera: A Repository of Android App Vulnerability Benchmarks. *In Proceedings of the 13th International Conference on Predictive Models and Data Analytics in Software Engineerin*g, pp.: 43-52.

Davidson, D., Chen, Y., George, F., Lu, L., & Jha, S. (2017, April). Secure integration of web content and applications on commodity mobile operating systems. *In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security,* pp.: 652-665.

Liu, B., Kong, D., Cen, L., Gong, N. Z., Jin, H., & Xiong, H. (2015, February). Personalized mobile app recommendation: Reconciling app functionality and user privacy preference. *In Proceedings of the Eighth ACM International Conference on Web Search and Data Mining,* pp.: 315-324.

Guo, M., Bhattacharya, P., Yang, M., Qian, K., & Yang, L. (2013, March). Learning mobile security with android security labware. *In Proceeding of the 44th ACM technical symposium on Computer science education,* pp.: 675-680.

Zheng, X., Pan, L., & Yilmaz, E. (2017, January). Security analysis of modern mission critical android mobile applications. *In Proceedings of the Australasian Computer Science Week Multiconference,* pp.: 2.

Zhu, H., Xiong, H., Ge, Y., & Chen, E. (2014, August). Mobile app recommendations with security and privacy awareness. *In Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining,* pp.: 951-960.

Barrera, D., Clark, J., McCarney, D., & Van Oorschot, P. C. (2012, October). Understanding and improving app installation security mechanisms through empirical analysis of android. *In Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices,* pp.: 81-92.

Jin, X., Hu, X., Ying, K., Du, W., Yin, H., & Peri, G. N. (2014, November). Code injection attacks on html5-based mobile apps: Characterization, detection and mitigation. *In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* pp.: 66-77.

Abadi, A., Flynn, L., & Gray, J. (2015, October). Mobile security: challenges, tools, and techniques (panel). *In Proceedings of the 3rd International Workshop on Mobile Development Lifecycle,* pp.: 51-53.

Pistoia, M., Tripp, O., Ferrara, P., & Centonze, P. (2015, October). Automatic detection, correction, and visualization of security vulnerabilities in mobile apps. *In Proceedings of the 3rd International Workshop on Mobile Development Lifecycle,* pp.: 35-36.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. *In Proceedings of the Eighth Symposium on Usable Privacy and Security,* pp.: 1.

ScienceDirect

Jabangwe, R., Edison, H., & Duc, A. N. (2018). Software engineering process models for mobile app development: A systematic literature review. *Journal of Systems and Software, 145*, pp.: 98-111.

Xenakis, C., Ntantogian, C., & Panos, O. (2016). (U) SimMonitor: A mobile application for security evaluation of cellular networks. *Computers & Security, 60,* pp.: 62-78.

Dini, G., Martinelli, F., Matteucci, I., Petrocchi, M., Saracino, A., & Sgandurra, D. (2018). Risk analysis of Android applications: A user-centric solution. *Future Generation Computer Systems, 80*, pp.: 505-518.

Goode, A. (2010). Managing mobile security: How are we doing? *Network Security, 2010(2),* pp.:12-15.

Zhang, X., Baggili, I., & Breitinger, F. (2017). Breaking into the vault: Privacy, security and forensic analysis of Android vault applications. *Computers & Security, 70*, pp.: 516-531.

Zein, S., Salleh, N., & Grundy, J. (2016). A systematic mapping study of mobile application testing techniques. *Journal of Systems and Software, 117,* pp.: 334-356.

Cano, M. D., & Domenech-Asensi, G. (2011). A secure energy-efficient m-banking application for mobile devices. *Journal of Systems and Software, 84(11),* pp.: 1899-1909.

Rastogi, S., Bhushan, K., & Gupta, B. B. (2016). Android applications repackaging detection techniques for smartphone devices. *Procedia Computer Science, 78,* pp.: 26-32.

Dye, S. M., & Scarfone, K. (2014). A standard for developing secure mobile applications. *Computer Standards & Interfaces, 36(3),* pp.: 524-530.

Yu, X., Kywe, S. M., & Li, Y. (2017). Security issues of in-store mobile payment. *In Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2,* pp.: 115-144.

Tully, S., & Mohanraj, Y. (2016). Mobile Security: A Practitioner's Perspective. *In Mobile Security and Privacy,* pp.: 5-55.

Felderer, M., Büchler, M., Johns, M., Brucker, A. D., Breu, R., & Pretschner, A. (2016). Security testing: A survey. *In Advances in Computers Vol. 101,* pp.: 1-51.

Sturm, R., Pollard, C., & Craig, J. (2017). Application Performance Management (APM) in the Digital Enterprise: Managing Applications for Cloud, Mobile, IoT and EBusiness. Morgan Kaufmann.

Hoog, A. (2011). Android forensics: investigation, analysis and mobile security for Google Android.

AIS

He, W., Tian, X., Shen, J., & Li, Y. (2015). Understanding Mobile Banking Applications' Security risks through Blog Mining and the Workflow Technology.

Georgiadis, C. K., Stiakakis, E., & Andronoudi, A. (2014). The Significance of Mobile Security Breaches in Terms of Their Economic Impact on Users. *In ICMB,* pp.: 7.

Chehrazi, G., Heimbach, I., & Hinz, O. (2016, June). The Impact of Security by Design on the Success of Open Source Software. *In ECIS,* pp.: ResearchPaper179.

Barrett, A. A., & Matthee, M. (2016). Rethinking Trust in E-Commerce in a Context-aware, Mobile World. *In CONF-IRM,* pp.: 24.

Degirmenci, K., Guhr, N., & Breitner, M. H. (2013). Mobile applications and access to personal information: A discussion of users' privacy concerns.

Harris, M., Patten, K., Regan, E., & Fjermestad, J. (2012). Mobile and connected device security considerations: A dilemma for small and medium enterprise business mobility?.

Karegar, F., Lindegren, D., Pettersson, J. S., & Fischer-Hübner, S. (2017). Assessments of a Cloud-Based Data Wallet for Personal Identity Management.

Koohikamali, M., & Kim, D. (2015). Does information sensitivity make a difference? Mobile applications' privacy statements: a text mining approach. *In Americas Conference on Information Systems. AIS, Puerto Rico,* Vol. 170.

Janson, A., Hoffmann, A., Hoffmann, H., & Leimeister, J. M. (2013, July). How customers trust mobile marketing applications. *In Thirty Fourth International Conference on Information Systems, Milan*.

Machiridza, M. (2016). Misalignment challenges when integrating security requirements into mobile banking application development. *In CONF-IRM,* pp.: 33.

Grupp, T., & Schneider, D. (2017). Seamless Updates–How Security And Feature Update Delivery Strategies Affect Continuance Intentions With Digital Applications.

Tse, D., Liu, X., Nusaputra, C., Hu, B., Wang, Y., & Xing, M. W. (2014). Strategies in Improving Android Security. *In PACIS,* pp.: 275.

VITA

Adetunji Olunuga is originally from Nigeria and currently lives in Jacksonville, Florida. He has a Bachelor of Technology degree in Computer Science from The Bells University of Technology, Nigeria, and expects to receive a Master of Science in Computing and Information Science from the University of North Florida (UNF). He has a passion for computers and has previous experience in the computing industry as a Technical Analyst, Systems Manager and SQL developer.

Adetunji has other interests apart from Computing. He enjoys spending time with friends and family, playing piano and drums. Adetunji aspires to continue using his skills in the IT field and contribute what he can to the community.