INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,
Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],
Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.
Circulated all over the world & Google has verified that scholars of more than 4255 Cities in 176 countries/territories are visiting our journal on regular basis.
Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____________

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF** ____.

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Education/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the authors have seen and agreed to the submitted version of the manuscript and their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR :
Designation :
Institution/College/University with full address & Pin Code :
Residential address with Pin Code :
Mobile Number (s) with country ISD code :
WhatsApp or Viber is active on your above noted Mobile Number (Yes/No) :
Landline Number (s) with country ISD code :
E-mail Address :
Alternate E-mail Address :
Nationality :

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.
g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE**: The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS**: The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ACKNOWLEDGMENTS**: Acknowledgements can be given to reviewers, funding institutions, etc., if any.

5. **ABSTRACT**: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

6. **JEL CODE**: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at **www.aeaweb.org/econlit/jelCodes.php**

7. **KEYWORDS**: JEL Code must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

8. **MANUSCRIPT**: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. *It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited*.

9. **HEADINGS**: All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS**: All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**: The main text should follow the following sequence:

INTRODUCTION
REVIEW OF LITERATURE
NEED/IMPORTANCE OF THE STUDY
STATEMENT OF THE PROBLEM
OBJECTIVES
HYPOTHESES
RESEARCH METHODOLOGY
RESULTS & DISCUSSION
FINDINGS
RECOMMENDATIONS/SUGGESTIONS
CONCLUSIONS
LIMITATIONS
SCOPE FOR FURTHER RESEARCH
REFERENCES
APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

12. **FIGURES & TABLES**: These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

13. **EQUATIONS/FORMULAE**: These should be consecutively numbered in parentheses, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilized. If any other equation editor is utilized, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that do not have the editor.

14. **ACRONYMS**: These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES**: The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. Also check to make sure that everything that you are including in the reference section is cited in the paper. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- Headers, footers, endnotes and footnotes may not be used in the document, but in short succinct notes making a specific point, may be placed in number orders following the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

ANDROID SECURITY

T RAMATHULASI
ASST. PROFESSOR
DEPARTMENT OF MCA
SRI VENKATESWARA COLLEGE OF ENGINEERING & TECHNOLOGY
CHITTOOR

M. ARCHANA
STUDENT
DEPARTMENT OF MCA
SRI VENKATESWARA COLLEGE OF ENGINEERING & TECHNOLOGY
CHITTOOR

M.RAMA
STUDENT
DEPARTMENT OF MCA
SRI VENKATESWARA COLLEGE OF ENGINEERING & TECHNOLOGY
CHITTOOR

ABSTRACT

Android Security has been burning spot recently in both intellectual search and public concern due to numerous instances of security attacks and privacy leakage on android platform. The marketing for smart phones has been developing in the past few years. There are now more than 400,000 applications on the Android market. Over that 10 billion Android applications have been downloaded from the Android market. Due to the popularity of Android, there are now a huge number of malicious vendors targeting the android platform. Many of the honest end users are being successfully hacked on a regular basis. Based on this work Android security has been built upon a permission based on the mechanism which restricts accesses of third-party android applications to critical resources on an Android device which greatly mitigates the malicious attacks targeting the Android market. Our security solution has advantage of the fact that each application in the android platform is assigned a unique user id (UID). Our explanation stores the reputation of Android applications in an anti-malware providers' cloud (AM Cloud). The experimentalresults witness that the proposed model could well identify the reputation index of a given application and hence it's potential of being risky or not. Finally we propose several methods to further mitigate the risk of Android Security.

KEYWORDS

Smart phones, Android OS, Reputation based security, Inter Process Communication.

1. INTRODUCTION

As the development of technology, the world's mobile phone also has developed quite rapidly. Mobile phone previously could only use to phone and send SMS but now can be used for various purposed in accordance with the needs of the users Rapid advances in mobile and wireless technologies have led to the development of smart, user preference oriented and context-aware devices. In the near expectations, wireless sensors will be fully included in clothing, appliances, and vehicles and in every place we can imagine. Permission-Based and Access control lists (ACLs) security models allow administrators and operating systems to restrict actions on specific resources. In put into practice, designing and configuring Access control lists (ACLs) particularly those with a huge number of configuration parameters is a complicated task. More specifically, reaching a balance between the detailed lucidity of permissions and the usability of the system is not trivial, especially when a system will be used by experts and novices alike. One of the main problems with Permission models and Access control lists in general is that they are classically not designed by the users who will ultimately use the system, but rather by administrators or developers who may not always for see all possible use cases. While some dispute that the problem with these permission- based systems is that they are not designed with usability in mind , we believe that in addition to the usability concerns, there do not have a clear understanding of how these systems are used in practice, leading security experts to blindly attempt to make them better without knowing where to start. While there are many broadly deployed systems which use permissions, we focus on the pragmatic analysis of the permission model included in Android Operating System. Android is a new comer to the smart phone industry and in just a few years of survival has manage to obtain significant media attention, market share, and developer base. Android uses ACLs extensively to mediate inter-process communication (IPC) and to control access to special functionality on the device (e.g., GPS receiver, text messages, vibrator, etc.). Android developers have to request permission to use these special features in a standard format which is parsed at install time. The OS is then responsible for allowing or denying use of specific resources at run time. The permission model used in Android has many advantages and can be effective in preventing malware while also informing users what kind of applications are capable of doing once installed. The main objectives of our experimental analysis are: (1) To investigate how the permission-based system in Android is used in practice (e.g., whether the design expectations meet the real-world usage characteristics and (2) To identify the strengths and limitations of the current implementation. We believe such analysis can reveal interesting usage patterns, particularly when the permission-based system is being used by a wide spectrum of users with varying degrees of expertise.

SYSTEM ANALYSIS

Today, the mobile phone has been developed inconceivable. The mobile phone is sophisticated enough at this time, users can easily tenacity some of the things that is used to only be done through a computer such as email or check to see stock prices. Although not all things can be done via mobile phone, mobile phone seemed to be the major needs and become a trend among the general public things like this that affects current mobility. With the high mobility that exists today, the lose case is something very usual case of lose often occurs due to user negligence in place their mobile phone or also occurs due to user will fell confused when their mobile phone is lost because some important data such as contact or even personal photos stored on it. Such data can be misused by irresponsible parties. Therefore it takes a security application that prevents data access time in case of loss. In addition to that preventing data access by an unauthorized person and find the location of current mobile phone will lost the application must also be able to perform the deletion of data on a lost mobile phone. These data deletion facility should be added to the application of safeguards intended to provide additional security to the owner of the mobile phone during a loss.

2. CONDITIONS

In this basic form ,Access control systems have existed for a long time and security system is based on access control lists which allows the subject to perform an action (e.g., read, write, run) on an object (e.g., file) only if the subject has been assign to the available permissions. Permissions are usually defined in front of time by an administrator or the owner. Basic file system permissions on POSIX-compliant systems are the traditional example of ACL-based security since objects. In this case, files can be read, written or executed either by the owner of the file, users in the same group as the owner, and/or everyone else. High sophisticated ACL-based systems allow the specification of a complex policy to control more parameters of how an object can be access. Permission-based security term can be used to refer the subset of ACL-based systems in which the action cannot change there exist only one possible action to accept or deny an object). This will be similar to multiple ACLs, where each ACL can access to one action. We noticed that dropping the allowable actions to one does not necessarily make the system easier to understand or configure. For example, In most of the Android permission model, developers can implement finer level granularity by defining separate access for read and write actions.

2.1 *PERMISSION-BASED PROTECTION EXAMPLES*

Google's Android OS is an example of a Permission-based security model which is used for mobile devices. Android requires that developers need to have permissions in a manifest list of permissions which allows the user and must accept former to installing an application.

To restrict access to advanced or dangerous situations Android uses this permission model on the device. Based on the list of permissions added by the developer, the user can decides whether to allow an application to be installed or not.

Similar to Android OS, the Google Chrome web browser uses a permission-based architecture in its extension system. Extension developers create a manifest where specific functionality (e.g., reading bookmarks, opening tabs, contacting specific domains) required by the extension can be requested. The manifest is read at extension install time to better inform the user of what the extension is capable of doing, and reduce the privileges that extensions are given [10]. In contrast, Firefox extensions, which do not have this permission architecture, run all extension code with the same OS-level privileges as the browser itself. A third example of a currently deployed permission- based architecture is the Blackberry platform from Research in Motion (RIM). Blackberry applications written in Java must be cryptographically signed in order to gain access to advanced functionality (known as Blackberry APIs with controlled access) such as reading phone logs, making phone calls or modifying system settings [3].

2.2 *ASSOCIATED EFFORT*

The design and implementation of a framework is to detect potentially malicious applications based on permissions requested by Android applications. The framework reads the declared permissions of an application at install time and compares it against a set of rules deemed to represent dangerous behavior. For example, an application that requests access to reading phone state, record audio from the microphone, and access to the Internet could send recorded phone conversations to a remote location. The framework enables applications that don't declare (known) dangerous permission combinations to be installed automatically, and the authorization to install applications that do to the user. Present a fine-grained access control policy infrastructure for protecting applications. Their proposal extends the current Android permission model by allowing permission statements to express more detail. For example, rather than simply allowing an application to send IPC messages to another based on permission labels, context can be added to specify requirements for configurations or software versions. The authors highlight that there are real-world use cases for a more complex policy language, particularly because untrusted third-party applications frequently interact on Android.

3. PROPOSED RESOLUTION

As part of a solution to the above identified pitfalls in the android security model, we propose a reputation based security trust model to evaluate and validate the applications prior to installation. We have also analyzed the consequences of a malicious application that has managed to get installed with the full consent of the end user. The Internet is full of genuine and malicious applications. An Android mobile owner can download different applications with varying reputation ratings. In this model, it is proposed that after downloading and before installing, the mobile device asks the AM Cloud for the reputation of the downloaded application.

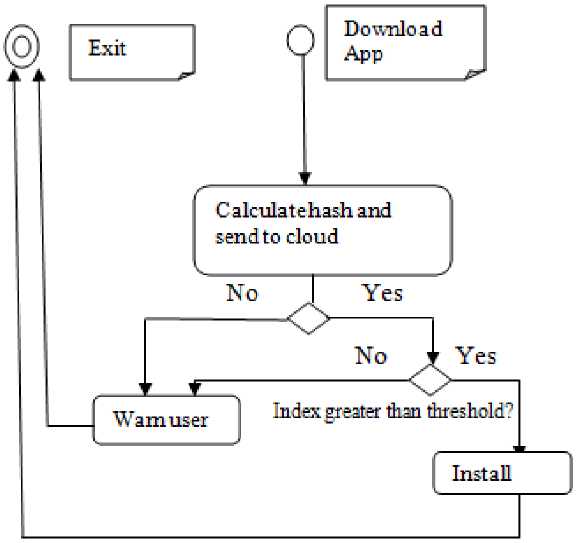
Exit
Download App
Calculate hash and send to cloud
No
Yes
No
Yes
Warn user
Index greater than threshold?
Install

Figure-1: overview of the proposed protocol

4. EXPERIMENTS

Regarding just the applications which have not yet developed a strong reputation, we need to analyse those applications. To analyse the behaviour of an Android application, it is easiest way to start with analysing the set of permissions that the application has set in the Android application package file which includes all of the application's code, resources, assets, and manifest file. To do this, we have experimented with a reputation based security model for Android applications. A second experiment was also done to analyze how a malicious application could track a mobile owner's location and report it to a third party. The results were achieved using two experiments.

4.1. *EXPERIMENT-1*

One solution can be achieved by anti-malware vendors which is used to perform analysis of the application on the Android platform. However the Android is low on resources, such as performance, battery life and main memory. So it makes more intellect to perform the analysis in the AM Cloud. To overcome these issues, another solution which has been used by anti-malware providers is to upload the entire application for analysis (for each user). For our solution, we will minimize the uploading of applications to the AM Cloud. I.e., we do not want two users, with the same exact application, to both upload the same application. Our approach to minimize the uploading of applications now follows.

4.2. *EXPERIMENT-2*

In this second experiment, we have developed two applications namely Location Tracker, The Location Tracker application has ACCESS_FINE_LOCATION, ACCESS_MOCK_ LOCATION, and ACCESS_COARSE_LOCATION permissions in the user permission manifest file of the application. The manifest file declares which permissions the application must have in order to access protected parts of the API and interact with other applications [18]. It also declares the permissions that others are required to have in order to interact with the application's components [18]. The Location Tracker application implements a location. Listener class that returns the latitude and longitude of the present location by consulting the Location Manager, which provides access to the system location services. We can use the latitude and longitude to locate the associated geographic place such as the street address, hotel, and zip codes.

5. FURTHER ARGUMENT

Designing a permission-based system is a challenging task because system designers must anticipate what usage will be given to the permissions defined in their system. The analysis in this paper has helped to identify developer usage patterns in a real-world dataset of top Android applications. Additionally, there is a constant struggle to make the system highly configurable under different use-cases while maintaining a low level of complexity. Understanding how the permission model is used in practice can help in making modifications to improve currently deployed permission systems. Furthermore, our analysis shows correlations between several of the infrequently used permissions. We note that having finer-grained permissions in a permission- based system enables users to have detailed control over what actions are allowed to take place. Whether it is beneficial to provide finer granularity will depend on many factors within a particular environment, as it increases complexity and thus may have, for example, usability impacts on designers and end-users. In the case of Android, having _too many‘ permissions impacts both developers and endusers. Developers must understand which permissions are needed to perform certain actions; determining this is often non- trivial, even for _experts‘. While some enthusiastic developers might take the time to learn what each of the 110 or more permissions do and request them appropriately when needed, other developers might choose to simply over-request functionality to make sure their application works.

5.1. *FEASIBLE ENHANCEMENTS TO ANDROID*

The Android permission model does not currently make use of the implied hierarchy in its namespace. For example, SEND_SMS and WRITE_SMS are two independent permission labels, instead of being grouped, for instance, under SMS. Android includes an optional logical permission grouping that is used for displaying permissions with more understandable names (e.g., one of the groupings reads —Services that cost you money in- stead of CALL_PHONE).

5.2. *APPLICABILITY TO OTHER PERMISSION-BASED SYSTEMS*

The attitude presented in this work has allowed us to understand how developers use the permission-based security model in Android. We believe that our methodology is applicable to explore usage trends in other permission based-based systems. A basic requirement for the methodology to work is being able to display applications and associated permissions for this representation to be possible, the set of permissions are requested by an application must be reachable. In the case of Android, the set is statically readable in a manifest file, but other systems might have different kind of implementations. Google‘s Chrome OS extension system uses an Android-like manifest and permissions to access functionality of advanced, which makes this system a major candidate for applying our methodology. An experimental study of a large set of third- party extensions using our SOM-based methodology could help us to identify what correlations are present in requesting permissions for opening tabs, read bookmarks, etc. This may also be useful in addressing the other security concerns highly raised in recent work.

6. CONCLUSION

We have introduced a different kinds of methodology to the security community for developing experimental analysis of permission- based security models. In particular, the Android permission model has been analysed to investigate how it is used in practice and to determine its advantages and disadvantages. The Self-Organizing Map (SOM) algorithm is engaged, which allows for a two- dimensional visualization of highly dimensional data. SOM also supports component planes analysis which can reveal interesting usage patterns. We have analysed the use of Android permissions in a real-world dataset of 1,100 applications, focusing on the top 50 application from 22 categories in the Android market. The results show that a small subset of the permissions is used very frequently where large subsets of permissions were used by very few applications. We suggest that the frequently used permissions, specifically INTERNET, do not provide sufficient expressiveness and hence may benefit from being divided into sub-categories, perhaps in a hierarchical manner. Equally, rare permissions such as the self-defined and the complementary permissions (e.g., install/ uninstall) could be distorted into a general category. Providing finer granularity for frequent permissions and combining the infrequent permissions can enhance the expressiveness of the permission model without increasing the complexity (i.e., maintaining a constant over all permission count) as a result of the additional permissions. We hope that our SOM-based methodology, including visualization, is of use to others exploring independent permission-based models.

REFERENCES

1. A.Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glaser. Google Android: A Comprehensive Security Assessment. In IEEE Security & Privacy, Volume 8, Issue 2, pp. 35–44, March–April 2010.
2. Tssssss.Bläsing, L.Batyuk, A.-D. Schmidt,S.A. Camtepe and S. Albayrak.An Android Application Sandbox system for suspicious software detection. In Proceedings of 5th International Conference on Malicious and Unwanted Software (MALWARE 2010), Nancy, France, Oct. 19–20, 2010.
3. M.Ongtang, S. McLaughlin, W. Enck, and P. McDaniel. Semantically Rich Application-Centric Security in Android. In Proceedings of the Annual Computer Security Applications Conference (ACSAC '09), Austin, TX, USA, December 6–10, 2009.
4. W. ShinS. Kiyomoto, K.Fukushima, and T.anaka. TowardsFormalAnalysis of the Permission-Based Security Model for Android.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, nor its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal is exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals

ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, ECONOMICS & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF
ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF
ISSN : 0976-2183
INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE & MANAGEMENT
IJRCM
IJRCM
A JOURNAL OF