Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2018 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2018

AppAware: A Model for Privacy Policy Visualization for Mobile Applications

Ioannis Paspatis
Ionian University Corfu, ipaspatis@ionio.gr

Aggeliki Tsohou
Ionian University, atsohou@ionio.gr

Spyros Kokolakis
University of the Aegean, sak@aegean.gr

Follow this and additional works at: https://aisel.aisnet.org/mcis2018

Recommended Citation
Paspatis, Ioannis; Tsohou, Aggeliki; and Kokolakis, Spyros, "AppAware: A Model for Privacy Policy Visualization for Mobile Applications" (2018). *MCIS 2018 Proceedings*. 3.
https://aisel.aisnet.org/mcis2018/3

This material is brought to you by the Mediterranean Conference on Information Systems (MCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MCIS 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

APPAWARE: A MODEL FOR PRIVACY POLICY VISUALIZATION FOR MOBILE APPLICATIONS

Research full-length paper

Track No 12- General Track

Paspatis, Ioannis, Ionian University, Corfu, GR, ipaspatis@ionio.gr

Tsohou, Aggeliki, Ionian University, Corfu, GR, atsohou@ionio.gr

Kokolakis, Spyros, University of Aegean, Samos, GR, sak@aegean.gr

Abstract

Privacy policies emerge as the main mechanism to inform users on the way their information is managed by online service providers, and still remain the dominant approach for this purpose. Literature notes that users find difficulties in understanding privacy policies because they are usually written in technical or legal language even, although most users are unfamiliar with them. These difficulties have led most users to skip reading privacy policies and blindly accept them. In an effort to address this challenge this paper presents AppWare, a multiplatform tool that intends to improve the visualization of privacy policies for mobile applications. AppWare formulates a visualized report with the permission set of an application, which is easily understandable by a common user. AppWare aims to bridge the difficulty to read privacy policies and android's obscure permission set with a new privacy policy visualization model. To validate AppAware we conducted a survey through questionnaire aiming to evaluate AppAware in terms of installability, usability, and viability-purpose. The results demonstrate that AppAware is assessed above average by the users in all categories.

Keywords: Awareness, Privacy policies, Mobile application permissions, Android.

1 Introduction

The great increase of smartphone users' in just 10 years from 85.000 users in 2010 to 2.5 billion in 2017 (Statista, 2017a) has led many computer program developers to turn to mobile application (apps) developers. In March 2017, Google Play Android Store had available for downloading nearly 3 billion mobile applications (apps) (Statista, 2017b) and the Apple store had more than 2.2 billion (Statista, 2017c) while just a decade ago these two webstores had almost 65.000 apps in total (Statista, 2018). A user who wants to install an app from the application store markets needs to read and accept its relevant privacy policy, commonly presented in a textual form. Cranor et al. (2008) concluded that it is unrealistic to believe that users would ever be capable to read every single privacy policy because of the length of such documents, the time that a user needs to spend and the legal language these policies are written in.

Our research objective is to demonstrate an alternate approach to represent a privacy policy, compared to the traditional textual approach. We introduce AppAware, a new visualization model for representing privacy policies for mobile apps. We show that AppAware can create a representative visualized privacy policy for a mobile app which is easy to read for the common user, enhances their privacy awareness and informs them for the threats they may encounter.

Many researchers have suggested alternate models of privacy policies representation by transforming them to more readable policies such as PPVM (Albalawi and Ghazinour, 2009) and RSLingo4Privacy (Da Silva et al., 2016). The main disadvantage of these models is that they transform a given policy, making it simpler and easier to understand, but they do not make more understandable the privacy threats deriving from a particular mobile application. Another disadvantage is that the above models didn't present any automation in transforming the privacy policies but it was necessary a human interaction for the transformation to get complete and validated. Contrary to the above models our approach does not focus on transforming a given privacy policy, but instead on creating a visualized privacy-threating report regarding the specific permission set of a given mobile app. Our approach has many advantages over the traditional privacy policies and the existing privacy models, such as PPVM, in terms of efficiency and privacy accuracy. Moreover, the application of AppAware does not require any additional actions from mobile app developers. To the best of our knowledge, this is the first paper to propose a privacy threat visualization report deriving from the permission set of given mobile app. AppAware works both proactively and reactively by helping mobile app users to understand the threats they may encounter by accepting the terms and conditions of a given mobile app.

The paper is structured as follows. In section two we present the related work. Section three presents the methodology we followed and the preparation we made in order to develop AppAware. In section four, we demonstrate the steps we followed to evaluate AppAware through survey and we present our empirical questionnaire results (see Appendix). Finally, in section five presents the contribution of the paper and future work.

2 Privacy risks, awareness and policy visualization

In order to examine scholar disquisition associated to our research objective, we reviewed the literature on privacy policies as well as the available literature and resources on mobile apps' features and vulnerabilities. Our literature review analysis consists of three parts: potential risks/threats that mobile app users encounter, user privacy awareness, privacy policies' reading cost, and new visualization approaches. We narrow our efforts on Androids OS's and exclude IOS from our research because only Android's security and privacy settings can be changed by the user without any special expertise (Benenson & Reinfelder, 2013). In IOS users have limited capabilities of changing the security and privacy settings of an app. Apple (the Company providing IOS) claims that any app that

is available through the official App store is reviewed by Apple's review process system for security and privacy issues. This feature does not allow users to change apps' settings.

2.1 Users' privacy concerns

Bandyopadhyay (2009) investigated the antecedents and consequences of consumer's online privacy concerns. He identified the main factors that influence consumers' privacy concerns such as vulnerability to information misuse, perceived ability to control the disclosure and use of private information, and characteristics of the consumer's cultural background. He also found that consumer's privacy concerns lead to limited willingness to disclose personal data online, to abandonment of e-commerce services or even to the total unwillingness to use the internet. Several studies had come to the same conclusions, that privacy concerns are determined by factors as awareness of information collection, perceived vulnerability to information misuse, experience with Internet use and cultural background of consumers (Sheehan and Hoy, 2000; Dinev and Hart, 2004; Bellman et al., 2004).

Buchenscheit et al. (2014) investigated if the use of the WhatsApp app could reveal users' behavior patterns and activities. Through an experiment they collected information on intended and actual behaviors (e.g., typical activities, typical sleeping hours), which they correlated with automatically obtained information from the usage of WhatsApp app. The participants, who didn't have significant privacy concerns for using the app, were surprised by the results highlighting that users do not fully realize the privacy implications of their online behaviors. Paspatis et al. (2017) used a pseudorandom dataset of 2000 telephone numbers and try to de-anonymize Viber users'. They found 682 users who had Viber installed and de-anonymized the 75% of them, revealing their full name, address and in about half of the cases their profile picture and occupation. After the de-anonymization process, authors conducted an empirical questionnaire and habits monitoring with 20 participants of the de-anonymization set. Most participants didn't have significant privacy concerns as they did not know that their data can be exposed and considered as public data or that someone can monitor their habits.

2.2 Users' privacy awareness and the cost of reading privacy policies

McDonald and Cranor (2008) tried to calculate the time and cost of users reading the privacy policies of each online service they visit. Through their empirical study they found out that every website user visit at least 1354 unique websites and that the average cost for the time they spend is 4.48 dollars per hour (if a Privacy Policy is read at home) or 35.86 dollars per hour (if the Privacy Policy should be read in office). They calculated that every website user would need 40 minutes per day for reading Privacy Polices when the average time of web surfing is 72 minutes per day. The total financial cost for all website users would be almost 781 billion dollars per year.

Kritzinger and von Solms (2010) state that the most important factor for home users being vulnerable to security threats is their lack of awareness about risks of using the Internet. Karavaras et al. (2016) conducted an empirical survey with 190 participants to explore Facebook users' awareness regarding malicious link threats, revealing that their low awareness can make them vulnerable to such attacks. Church and Oliveira (2013) researched what users are concerned at most when they are using mobile apps such as WhatsApp. They found that most users were more concerned about the "last seen feature" wherewith someone can see at what exact time a user was read a message. Using this feature a user is capable to understand someone's habits such sleep routine. Almuhimedi et al. (2014) demonstrated that users low awareness regarding location data -among others by mobile apps and suggest a permission manager to protect their privacy. Graeef and Harmon (2002) found that privacy concerns vary by age, income and gender. In addition, they saw that younger users are more aware of their information leak while older users are concerned more about their financial privacy. To raise web

users' awareness, Malandrino et al. (2013) produces NoTrace, a mozilla firefox add-on that monitor users' browsing activity and inform them what personal and sensitive information they leak towards third-party such as advertising companies. NoTrace is also capable to block or or alter the browser fingerprint information. Hazari and Brown (2013) conducted a questionnaire-based survey with 157 business students enrolling regarding privacy behavior, trust policies and technology and correlate their results with others researchers' previous studies. His results showed that individuals are concerned about their privacy and would like to control their digital reputation as it can directly impact their business relationships and/or employment prospects. He also suggested the importance of awareness training providing by institutions to make students aware of privacy issues.

2.3 Privacy policy visualization approaches

Barker et al. (2009) described purpose, visibility, granularity, retention and constraints as the key elements that form a privacy policy and categorized their research around a conceptual framework for data privacy. Ghazinour et al. (2009) presented a framework for visualizing privacy policies called Privacy Policy Visualization Model (PPVM). They suggested a graphical tool that combines Entity Relationship Modeling, Entity Relationship diagramming and the elements described by Barker et al. (2009) to show the association between the data provider, the collector and the data they collected. Albalawi and Ghazinour (2009) have evaluated PPVM using Jensen's (2014) Structured Analysis of Privacy (STARP) heuristics evaluation framework to inspect privacy usability and vulnerabilities and suggested solutions to improve usability issues encountered during evaluation. Domiongo-Ferrer (2009) suggested a three-dimensional conceptual framework for privacy policies. His proposal identifies privacy issues in a privacy policy that relate to the data provider, house and third-parties with every issue is grouped to one these categories. Anwar et al (2009) described an access control model of assessing privacy policies through visualization. Da Silva et al (2016) suggested a multi-language framework tool based on Lingo programming language called RSLingo4Privacy which intends to improve the specification and analysis of a privacy policy. Their tool automatically classifies extracted text statements and text snippets from a policy into five classes: Collection -which data are collected; Disclosure -which data is disclosed and to whom; Retention -how long data will be available; Usage -why are they collecting users' data; and Informative -which is a general purposes class and after the conversion provides an improved version of the policy in a natural language. Kelley et al (2009) conducted a survey testing the readability, accuracy and comprehension of five different format privacy policies: full text policy in natural language, standardized table format, short standardized table, short natural language and layered notices. They concluded that the best results in all categories were provided by the two table-type policies. Micallef et al. (2017) conducted an empirical study to investigate users' preferences on multiple types of privacy policies such as combinations of visual nudges, vibration, audio and speech on mobile apps. They revealed that users are annoyed when low priority notification nudges use audio or speech to alert them and developers should prefer non – salient privacy nudges to inform them. Keith et al (2018) examined an approach to improve privacy policies through the design and usage of mediated content, such as video instead of textual privacy policies. They aimed to explore if design factors such as gender, animation style, music tone or color scheme affect users' perceived risk, perceived benefits and disclosure decisions. Their results indicate that the most effective video privacy policies are those that use female narrators with vibrant color palettes and light musical tones.

Research shows that users have low privacy awareness and privacy concerns which are raised when understanding the actual privacy threats. Studies also show that users facedifficulties on reading privacy policies, such as the difficult legal language they are written in. All the above, do not create the appropriate conditions for conscious consent for the disclosure of personal information. Additionally, the users are confronted with a fragmented approach, since they need to read and understand the different privacy policies of the million mobile apps that are available. Therefore, there is a challenge on creating a single approach that can assist users and resolve the problem of the million

privacy policies the users need to read. AppAware target to address this issue by using as a foundation for user awareness the permission set of the mobile apps (which is what they do and not what they state they do) and not the privacy policy. This gives the opportunity to automatically transform a privacy policy to a visualized privacy report, with representative pictures and easy to read for the common user.

3 Methodology

In this section, we analyze our methodology for developing AppAware and for validating its effect on users' privacy awareness.

3.1 Technical Methodology

We developed AppAware with Java JDK. We chose to use java instead of other programming languages because of its compatibility with different operating systems such as Windows, Linux, IOS and because it is easily modified to be used for android mobile devices (Android OS and its applications are written in a version of Java). To store our data, AppAware's global database is based on MySQL while there is a standalone version of AppAware that is using SQLite DB. We chose MySQL because its freeware, supports more than 10 million records per table while it supports and performs fast enough with many users simultaneously. The local version of AppAware is using SQLite db to store data. We chose SQLite to release users of the requirement of a local database installation such as MySQL or SQL Server. AppAware is following a different approach than the new models we referred in the related work section. Instead of trying to transform a given mobile app privacy policy into more comprehensive forms, AppAware creates a visualized report with images and privacy descriptions in natural language of the permissions that are obtained from an App during installation or use. In particular, we have matched every permission from the Android's permission set with a representative image, a permission description and a possible threat. We obtained permissions' descriptions from Pew Research (Olmstead and Atkinson, 2015) and we chose the associated images and possible threats based on google's image matching. We believe that the descriptive images of the visualized report will catch the eye of users and increase their privacy awareness. In this way, users may read the description of the permission they are giving access as well as the possible threat(s) they may encounter. Our module is consisted of four java classes: a) Dataset, b) AppData, c) AppHandling and d) AppPerms which cooperate as follows:

Dataset Class. This class includes all Android's Permissions. It is consisted of 3 fields: android's permission name, permission privacy description and potential theat. As we mentioned before permission privacy descriptions obtained from Pew Research (Olmstead and Atkinson, 2015) previous work. We chose these descriptions because of the natural language they used which is easy understandable for the common user.

AppData. This is AppAware's main class. From this class users can see which android applications are stored in the database as well as which permissions can be obtained during installation. Also, they can export the visualized report (figure 2, 3). For the purposes of our experiment we include to AppAware the twenty most famous applications for the 2017 (Hartmans, 2017).

AppHandling. From this class a user can add a new app that does not included to AppAware's database and send it for evaluation and permission matching. In order to add a new app, user must update AppAware's database to it latest version. Thus, users can also see stored apps with minimum details. After the app's evaluation and permission matching, AppAware's user is ready to create the new visualized report.

Figure 1 below shows AppAware's Schema:

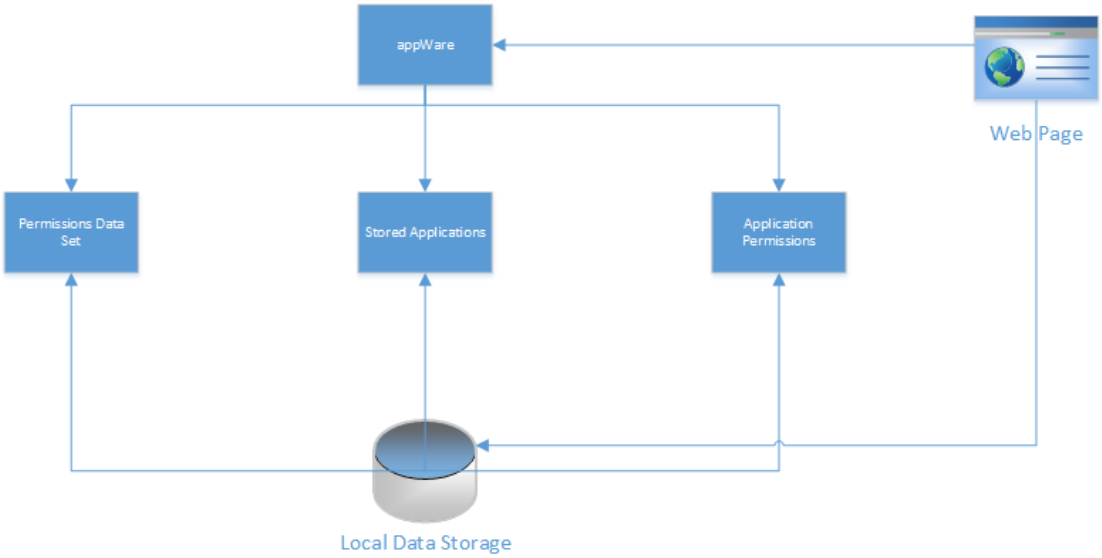

Figure 1. AppAware Schema

AppPerms. This is the class where more advanced users and administration team can match a new application with the permissions it gains upon install/use. After the matching, app's permissions are uploading to AppAware's web database in order to update AppAware's users. To avoid spam or false permissions matching, AppAware's Server will wait for a non-specified number of users to send permissions matching for the same app. After this step server will correlate the results and if there is a specific number of permissions matching will send an updated data set to AppAware's clients.

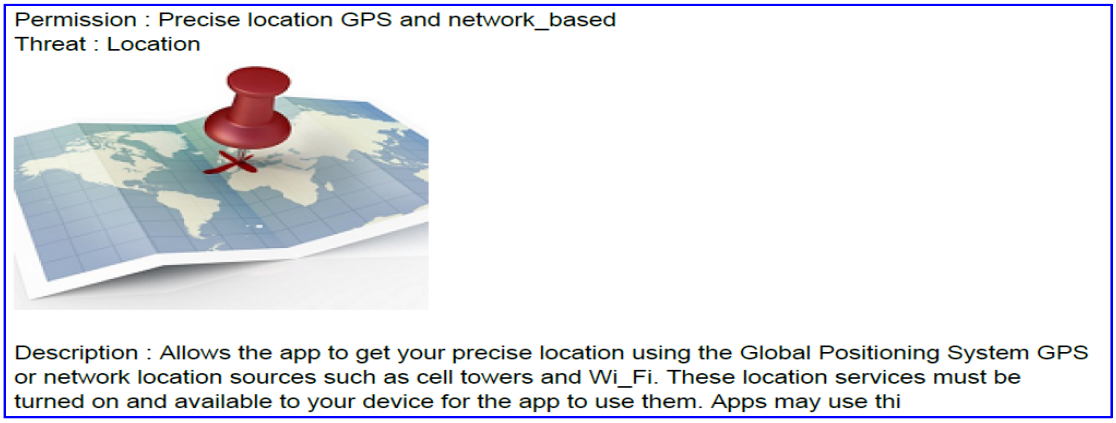

Figure 2. Representative picture and description and threat from the visualized report

Permission : Directly call phone numbers
Threat : Overcharge

Description : Allows the app to call any phone number including emergency numbers without your intervention. Malicious apps may place unnecessary and illegal calls to emergency services

Figure 3. Representative picture and description and threat from the visualized report

All AppAware classes are been showed to the Figures 4, 5, 6, 7 below.

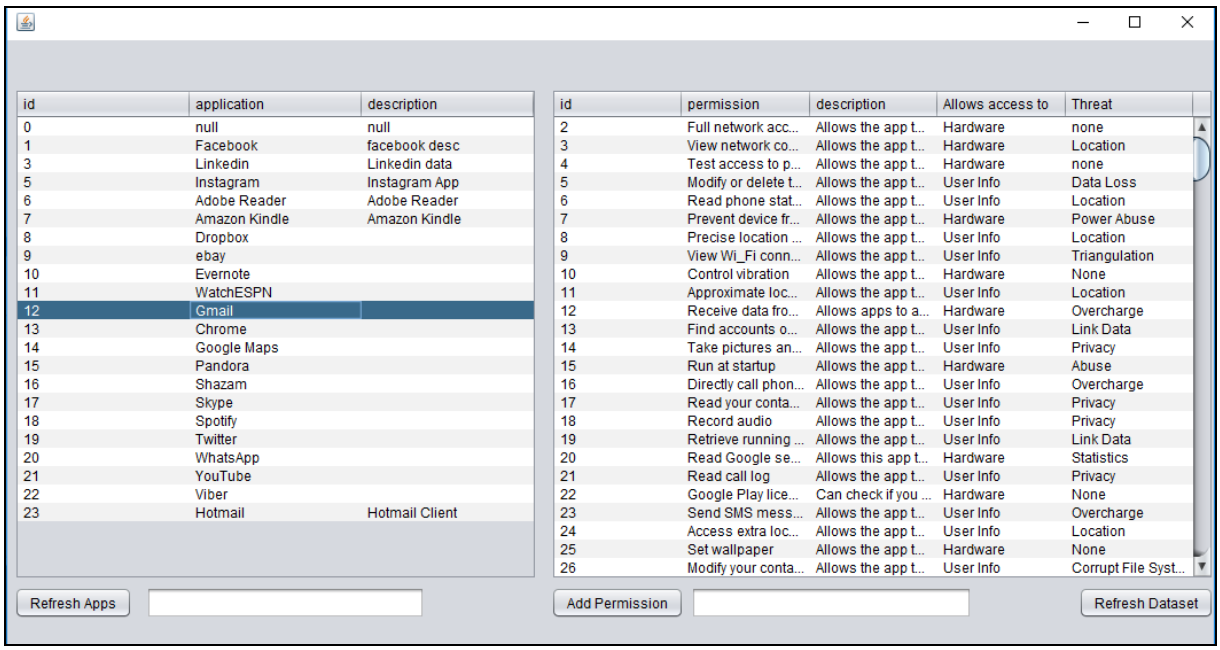

Figure 4. Class AppPerms

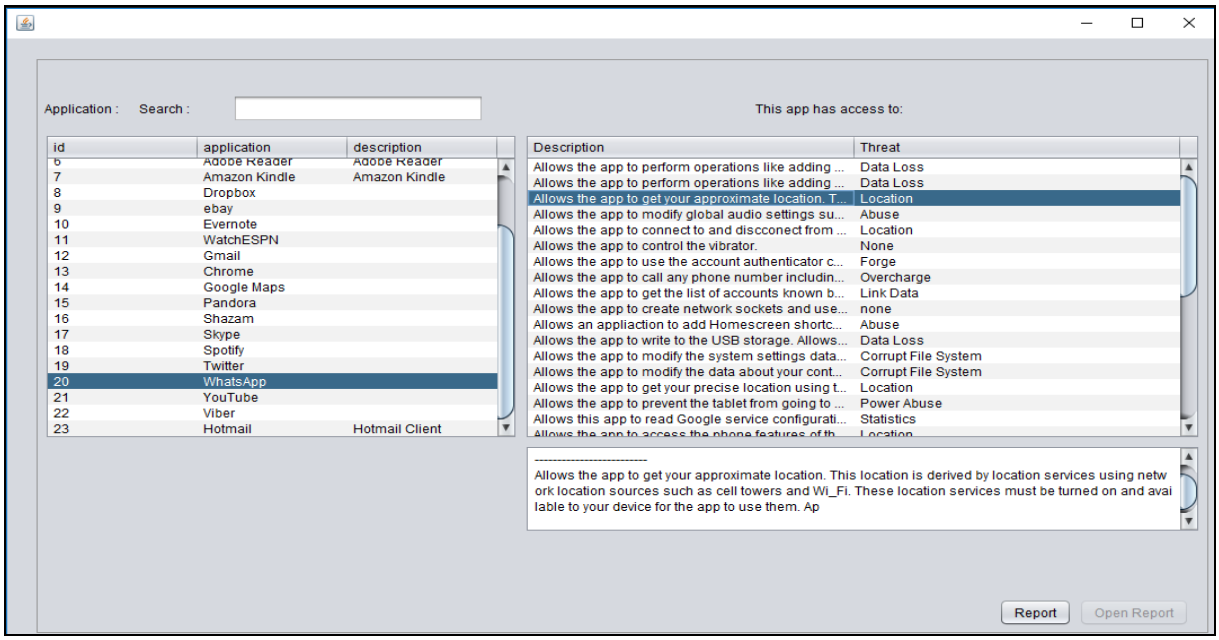

Figure 5. Class AppData

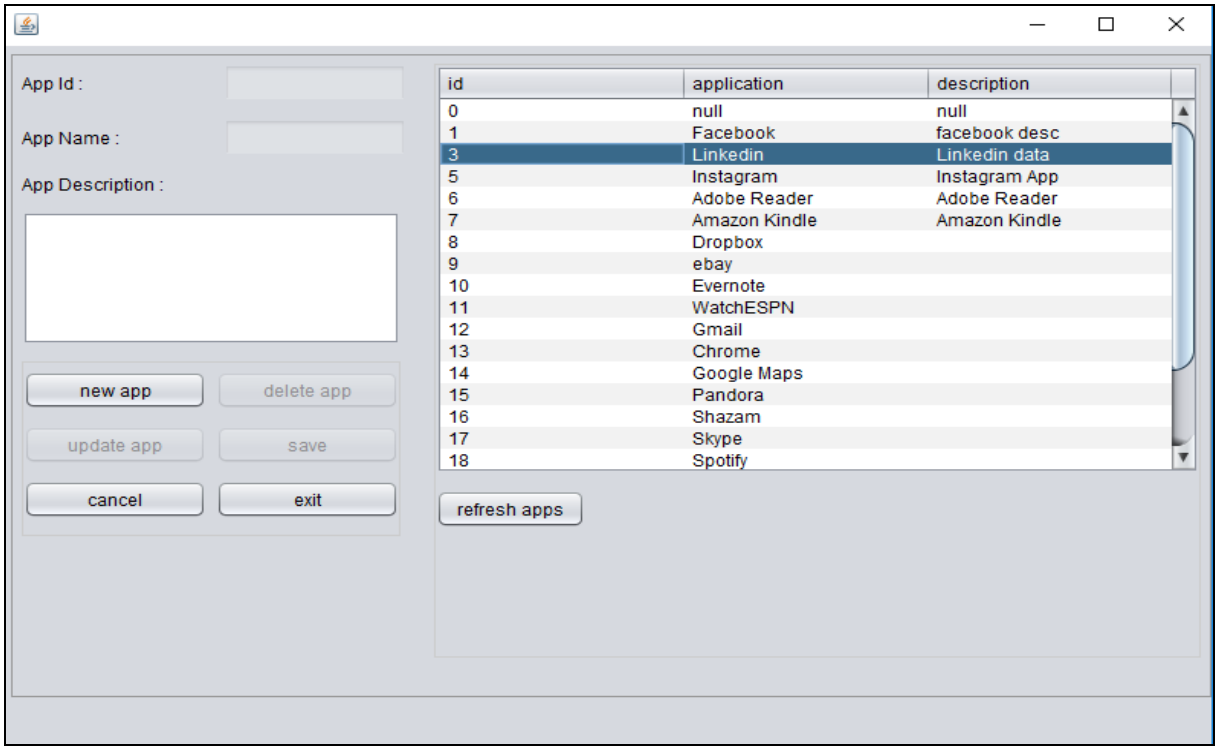

Figure 6. Class AppHandling

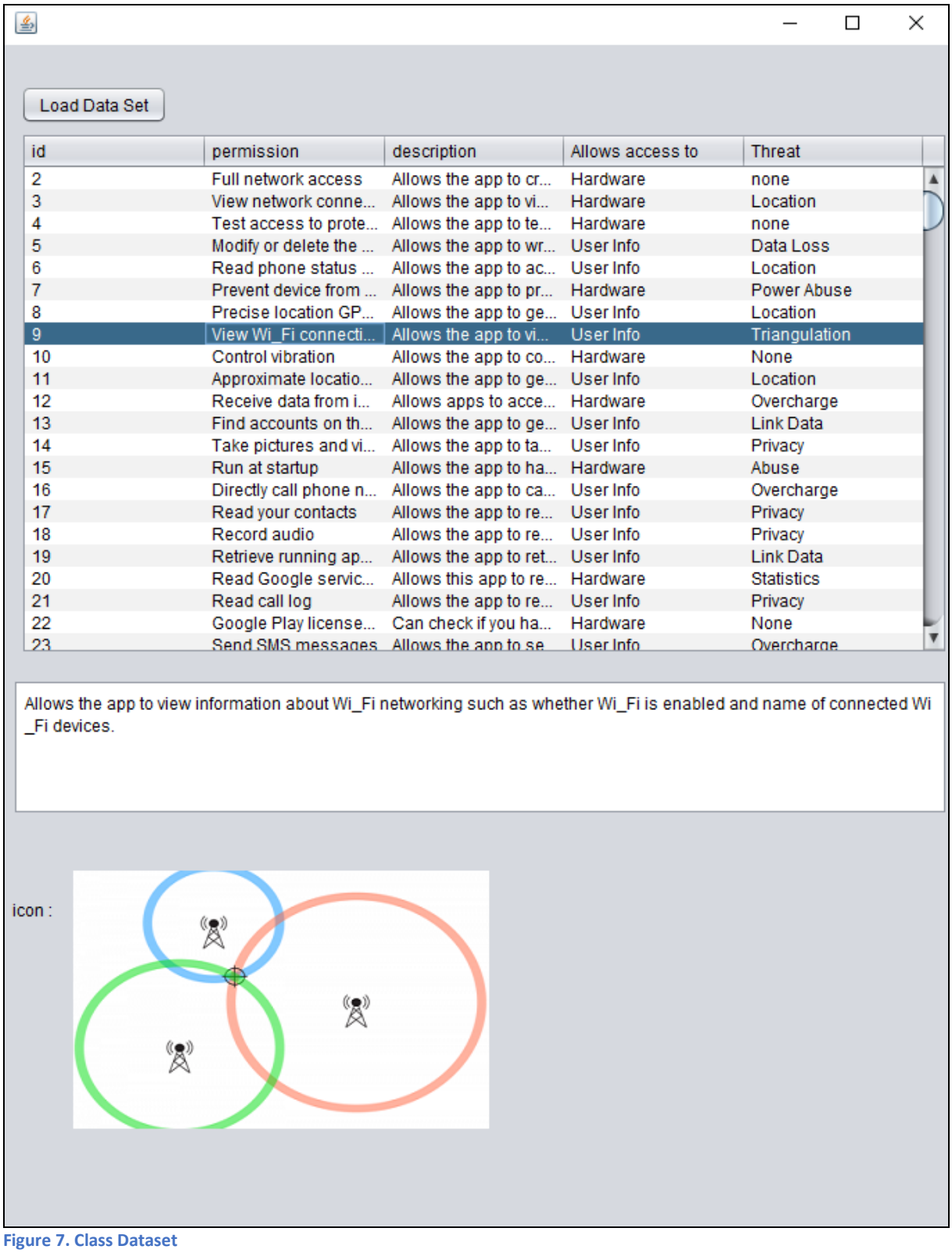

Figure 7. Class Dataset

AppAware is support database update function for future implementation. In case of a ready Apps-permission dataset be available in public, it will be capable to support as many apps there are in the dataset. Thus, AppAware users can create and export their dataset that created with AppData class and

send it to AppAware's team for evaluation and import to the web database. Until now, Playstore does not giving public and massive access to their apps database and their permission set. In case of Playstore give in public an app-permission set in public, AppAware will automatically update its global database.

3.2 Evaluation methodology

In order to evaluate AppAware, we conducted a survey using a questionnaire. The purpose of the survey was to investigate how mobile app users evaluate AppAware's Visualized Report in terms of installability, usability, and viability-purpose compared to the traditional privacy policy of WhatsApp. The criteria and questions -except demographics- derived from ISO/IEC 9126-1 Software engineering — Product quality. All questions were Likert type and mandatory. To design and distribute the questionnaire (Appendix) we used Google Forms due to its popularity and characteristics, such as provision of real-time statistical results, the security and anonymity protection that it offers.

A requirement for participation to our survey was to install AppAware and use it for a trial period before answering the questionnaire. For this purpose, we did not target the general population, but instead we distributed the designed questionnaire to colleagues and undergraduate students of various disciplines. In order to test the effect of computer science knowledge on the AppAware evaluation we included a question about the profession or studies of the participants to maintain control over this characteristic of the sample. To complete the questionnaire, participants should first read WhatsApp's privacy policy and then install AppAware and export the WhatsApp's Visualized Report using it. The survey was running for 40 consecutive days and we received 73 answers. We consider that this number of responses is sufficient, especially given the obstacles caused by the requirement to install an unknown application or the refusal to participate because of installation problems. The 73 participants were equally distributed in terms of gender (36 Males, 35 Females, 2 unknown), were mainly aged between 18 – 34 years and most of them had at least bachelor degree. The demographics of the questionnaire are analyzed in detail in Table 1.

Demographics (n=73)		
Gender	Male	36 (49.3%)
	Female	35 (47.9)
	Other/Unknown	2 (2.7%)
Age	18-	1 (1.4%)
	18-34	54 (74%)
	35-44	10 (13.7%)
	44+	8 (11%)
Level of education	High School	4 (5.5%)
	Associate Degree	4 (5.5%)
	Bachelor Degree	32 (43.8%)
	Master's Degree	28 (38.4%)
	PhD Graduate Degree	5 (6.8%)
Profession	Economics	14 (19.2%)
	Political Science	7 (9.6%)
	Social Science	9 (12.4%)
	Computer Science	31 (42.5%)
	Educational Science	4 (5.5%)
	Other	8 (11%)

Table 1: Sample Demographics

4 AppAware users' evaluation

The questionnaire intended to collect users' opinion regarding aspects of AppAware installability, usability, and viability/purpose.

AppAware scored in all categories above average with mean values varying from 3.07 to 4.01 (scale 1 – 5). Our results in the category Viability and Purpose reveal that participants would prefer to use AppAware's Visualized Report than read the traditional privacy policy. In terms of installabilty, participants didn't confront any difficulties to install or understand how to use AppAware since the mean values in this aspect range from 3.48 to 4.04. Regarding usability and purpose, AppAware scored lower mean values ranging from 3.07 to 3.75.

The results are analyzed in Table 2, that includes three columns with column one demonstrating total mean values with all professions calculated, in column 2 we exclude participants with computer related degree and finally in column three we demonstrate the mean values only of participants with computer related degree.

Question	**Total mean values**	**Mean values of participants**
I believe It was easy to install AppAware to my system	3,81	4,02
I believe that I understand what the software does and its purpose	4,01	4,29
I believe that It was easy to learn how to use AppAware's basic functions	3,93	4,21
I believe that It was easy to learn how to use AppAware's advanced characteristics/functions/features	3,48	3,69
I believe that AppAware's Visualized report helped me to understand better the WhatsApp's privacy policy.	3,64	4,05
I believe AppAware's Visualized Report helped me to find the potential threats I may be confronted with using WhatsApp	3,68	4,05
I believe AppAware's Visualized Report was easy to read	3,47	3,83
I believe that AppAware's Visualized Report was easy to understand	3,38	3,74
I believe that the descriptions of AppAware's permission set are accurate.	3,75	4,10
I believe that the actual threat of AppAware's permission set is accurate.	3,74	4,10
I believe that AppAware is a stable Application	3,64	4,10
I believe that AppAware is a useful Application	3,53	3,88
I believe that AppAware is appropriate for its purpose	3,63	4,00

It was faster to read AppAware's Visualized Report than WhatsApp's privacy policy.	3,71	4,07
I prefer to use AppAware than to read the privacy policy of an App.	3,53	3,81
I believe that AppAware is a unique software tool	3,30	3,48
I believe that AppAware will be helpful to me	3,07	3,19

Table 2. Questionnaire results

5 Conclusions and future work

In this paper, we suggested a visualized model for representing privacy policies for mobile apps and the permissions they obtain upon installation. We processed android's permission set and we matched all permissions with a potential threat and a representative picture. We included in AppAware the 20 most popular applications for 2017 and then we evaluated AppAware using a survey with 73 participants. We focused our evaluation on installability, usability, and viability/purpose of AppAware. AppAware was evaluated above average in all categories especially in the usability category.

To the best of our knowledge, there is no other approach like AppAware. There are several approaches to visualize the text of a privacy policy, but there is no approach that enhances user understanding by creating a permission visualization model. The advantage of our approach is that a user does not need necessary to read all privacy policies of all mobile apps to visualize them but only to import the mobile apps and their permission set to AppAware's database. At the time of this paper we have included the 20 most popular mobile apps for the 2017. Unfortunately, we can't automatically import all available applications because Google Play store does not allow the use of crawlers or parsers.

AppAware provides significant implications for mobile app developers as well as marketplaces. Our findings show that app users would prefer to use a visualized report instead of the privacy policy of an app. App developers could provide the permission dataset they use in their apps. Researchers could use instantly and with ease their dataset to update public databases such as AppAware's. In this way, applications that target to mitigate users' privacy concerns and raise users' awareness could be up to date and help users to understand privacy threats and protect their data equally. For the same reason, we recommend app marketplaces to provide publicly the permission dataset for the apps they are hosting to assist transparency and give control to the users over their data. At the moment, AppAware is only a client-server application created in java due to its multiplatform capabilities. In the future, we envision to develop AppAware into a web-accessible database as well as a web browser add-on.

6 Appendix

A. Demographics

1.What is your gender?
Male\Female

2. What is your age?

18-\18-34\35-44\30-39\40-49\50-59\60+

3. What is the highest level of school you have completed or the highest degree you have received?

Less than high school degree\High school degree or equivalent (e.g., GED) \Some college but no degree\Associate degree\Bachelor degree\Master's degree\P.H.D. Graduate degree

4. What is your profession?

Economics/Political Science/Social Science/Computer Science/Educational Science/Other

B. AppAware Evaluation (Likert Scale 1-5)

Installability
1. I believe It was easy to install AppAware to my system

Learnability

1. I believe that I understand what the software does and its purpose

2. I believe that it was easy to learn how to use AppAware's basic functions

3. I believe that it was easy to learn how to use AppAware's advanced characteristics/functions/features

4. I believe that AppAware's Visualized report helped me to understand better the WhatsApp's privacy policy.

Usability

1. I believe AppAware's Visualized Report helped me to find the potential threats I may be confronted with using WhatsApp.

2. I believe AppAware's Visualized Report was easy to read.

3. I believe that AppAware's Visualized Report was easy to understand.

4. I believe that the descriptions of AppAware's permission set are accurate.

5. I believe that the actual threat of AppAware's permission set is accurate.

Viability-Purpose

1. I believe that AppAware is a stable Application.

2. I believe that AppAware is a useful Application.

3. I believe that AppAware is appropriate for its purpose.

4. It was faster to read AppAware's Visualized Report than WhatsApp's privacy policy.

5. I prefer to use AppAware than to read the privacy policy of an App.

6. I believe that AppAware is a unique software tool.

7. I believe that AppAware will be helpful to me.

References

Amran, A., Zaaba, Z., Singh, M. and Marashdih, A. (2017). Usable Security: Revealing End-Users Comprehensions on Security Warnings. Procedia Computer Science, 124, pp.624-631.

Anwar, M., Fong, P., Yang, X. and Hamilton, H. (2010). Visualizing Privacy Implications of Access Control Policies in Social Network Systems. Data Privacy Management and Autonomous Spontaneous Security, pp.106-120.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. Computers in Human Behavior, 706-714.

Bandyopadhyay, S. (2011). Antecedents and Consequences of Consumers Online Privacy Concerns. Journal of Business & Economics Research (JBER)

Barker K, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun, and A. Williams. "A data privacy taxonomy." (in press) BNCOD '09: The 26th British National Conference on Databases. 12 pages, Birmingham, UK, 2009.

Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. The Information Society, 20, 313-324

Benenson Z, Reinfelder L. (2013). Should the users be informed? On differences in risk perception between Android and iPhone users. In Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK.

Buchenscheit, A., Könings, B., Neubert, A., Schaub, F., Schneider, M. and Kargl, F. (2014). Privacy implications of presence sharing in mobile messaging applications. Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia - MUM '14.

Budnitz, M. (1998). Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate. South Carolina Law Review, 49 (1), 847-886.

Church, K., & de Oliveira, R. (2013) What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS. 15th international conference on Human-computer interaction with mobile devices and services, Munich, August 30th, 2013, (pp. 352-361). ACM, Munich.

Da Silva, A., Caramujo, J., Monfared, S., Calado, P. and Breaux, T. (2016). Improving the Specification and Analysis of Privacy Policies - The RSLingo4Privacy Approach. Proceedings of the 18th International Conference on Enterprise Information Systems.

Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model. Behavior and Information Technology, 23 (6), 413-422.

Domiongo-Ferrer (2009). "A three-dimensional conceptual framework for database privacy". In Secure Data Management 2007, volume 4721/2007, pages 193–202, Vienna, Austria, 2007.

Ghazinour, K. and Albalawi, T. (2016). A Usability Study on the Privacy Policy Visualization Model. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech).

Graeff, T. and Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. Journal of Consumer Marketing, 19(4), pp.302-318.

Hartmans A. (2017). The 20 most popular iPhone apps of 2017. Business Insider. Available at: http://www.businessinsider.com/top-apple-iphone-apps-2017-12

Hazari, S. and Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. Journal of Information Privacy and Security, 9(4), pp.31-51.

Jensen, C. (2004), ''Toward a method for privacy vulnerability Analysis'', CHI 2004, extended abstracts on Human factors in computing systems, Publisher: ACM

Kambiz Ghazinour, Maryam Majedi, Ken Barker, A Model for Privacy Policy Visualization in 2009 33rd Annual IEEE International Computer Software and Applications Conference, 2009.

Karavaras E, Magkos E, Tsohou A (2016) Low User Awareness Against social malware: An Empirical Study and Design of a Security Awareness Application.

Kelley, P., Cesca, L., Bresee, J. and Cranor, L. (2010). Standardizing privacy notices. Proceedings of the 28th international conference on Human factors in computing systems - CHI '10.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security, 840-847.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R. and Krishnamurthy, B. (2013). Privacy awareness about information leakage. Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society - WPES '13.

McDonald A., Cranor L.F., (2008). The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society 2008. Privacy Year in Review issue. [online] Available at: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.[Accessed 25 Jun 2017].

Micallef, N., Just, M., Baillie, L. and Alharby, M. (2017). Stop annoying me! Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17.

Olmstead, K. and Atkinson, M. (2015). APPS PERMISSIONS IN THE GOOGLE PLAY. [online] Pew Research Center. Available at: http://www.pewinternet.org/2015/11/10/the-majority-of-smartphone-owners-download-apps/ [Accessed 20 Jan. 2017].

Paspatis Ioannis, Tsohou Aggeliki and Kokolakis Spyros, "Mobile Application Privacy Risks : Viber Users' De-Anonymization Using Public Data" (2017). MCIS 2017 Proceedings. 32. Available at : http://aisel.aisnet.org/mcis2017/32

Raab, C.D. & Bennet, C.J. (1998). The Distribution of Privacy Risks: Who Needs Protection? The Information Society, 14 (4), 253-262.

Rindfleish, T.C. (1997). Privacy, Information Technology, and Healthcare. Communications of the ACM, 40, 92-100.

Saunders, K. & Zucker, B. (1999). Contracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. International Review of Law, Computers, and Technology, 13 (2), 183-192.

Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. Journal of Public Policy and Marketing, 19 (1), 62-73.

Statista (2017a). Global cumulative shipments of smartphones using the Android operating system from 2007 to 2016. https://www.statista.com/statistics/241943/forecast-of-global-cumulative-shipments-of-smartphones-using-android-os/

Statista (2017b). Number of apps available in leading app stores as of March 2017. https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Statista_(2017c). Number of available apps in the Apple App Store from July 2008 to January 2017. https://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/

Statista (2018). Number of available applications in the Google Play Store from December 2009 to December 2017. https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

Tsohou, Aggeliki & Kosta, Eleni. (2017). Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. Computer Law & Security Review. 10.1016/j.clsr.2017.03.027.

Wilson, S., Schaub, F., Dara, A., Liu, F., Cherivirala, S., Giovanni Leon, P., Schaarup Andersen, M., Zimmeck, S., Sathyendra, K., Russell, N., B. Norton, T., Hovy, E., Reidenberg, J. and Sadeh, N. (2016). The Creation and Analysis of a Website Privacy Policy Corpus. Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers).