University of Dhaka

Department of Computer Science & Engineering

Research Paper Review
CSE-3112:Software Engineering Lab
3rd Year 1st Semester

Serial no.	Roll	Name
1	46	Arka Bhuiyan
2	48	Maksudul Hasan
3	52	Arafat Hossen

Report 1 & 2 prepared by: Arka Bhuiyan
Report 3 & 4 prepared by: Maksudul Hasan
Report 5 & 6 prepared by : Arafat Hossen

Date of Submission : 22nd february, 2018
Submitted to : Md. Mofijul Islam

Reviews By Arka Bhuiyan

Paperwork 1: Permission-Aware GUI Testing of Android

Abstract:

The dynamic permission system has been introduced recently. Although it allows users to control the access of resources and other tools by the applications, it has a mentionable lacking. It has made quite harder to test applications. We all know that the behavior and functions of softwares changes after each versions but they are tested on some granted versions. To test an application up to the mark, it needs to be tested under an wide range of permissions. Like what effects it has on built in applications, how it use resources and the rest. Well, some permissions are just additional, they can be easily skipped. The paper highlights on this topic. It gave a indication on how to determine the tests and app permissions. It developed a better to approach to adjust the time to test application and grant permissions.

Proposed Solution :

Earlier the static permission system forced a user to agree with all the permissions required by the app even he had objection with it. So in order to allow the user to control the permission access of apps dynamic permission system was introduced. But still a trade-off happened to be unsorted out. Properly testing an android app with respect to its permission-protected behavior may happen to re-execute of each test on all possible combination of permissions requested by an app.

So to make app testing time efficient " Permission-Aware GUI Testing of Android" is introduced. It highlights that a test may not interact with all permissions requested by the app. So if we revoke those permissions, it will not affect the app's behavior under that particular test. In a nutshell, the system automatically exclude those permissions which do not interact with the tests. This results in a significant reduction in testing effort. And yet it achieves a great coverage and great fault detection capability.

Limitations:

No doubt on that this method of testing is time efficient and reduces testing effort but there might be cases that result in system failure or crash. Some permissions at the beginning might not be interacted with test but later in some phases they might have a sudden interaction with testing and if they are skipped app might not function on that

particular phase. To solve this we need to know all the permissions it will interact with testing in any running phases. That might solve the problem.

Findings

- The problems of static permission system
- The reason to introduce dynamic permission system
- The lacks of it
- ways to improve the system

Link:

http://www.ics.uci.edu/~seal/publications/2017_FSE_PATDroid.pdf

Paper work-2

An Approach for Energy-Based Ranking of Android Apps

Abstract:

Mobile apps are getting much more complexed day by day which enables them to consume more energy. This high energy function results in lower battery life for Android phones.

There are wide range of apps of same category which include same features and are rated on the app respiratory systems by review or number of downloads. But the user does not get to know which app is battery efficient or which app is not. So it is mandatory to include the ranking on the basis of energy consumption for the similar categorized apps. However most systems run lack of information for battery usage or energy consumption. As a result this forces users to choose an app blindly without its energy consumption or optimization ability. So this paper introduce a better approach to provide ranking for apps on the basis of energy consumption. The authors named this approach EcoDroid.

Proposed Solution:

Undoubtedly Android is the most talked and used mobile platform. Its most used app respiratory Google Play Store comes up with a wide collection of apps. The users are at their liberty to choose app according to their demands. But the thing to be mentioned is users are blinded by only ratings or customer views. They dont get to know whether the app is battery-efficient or not. In some reviews they might get to know about it but they had to scroll down all the reviews. So it is wise for respiratory systems to include ranking on the basis of battery usage or consumption or energy consumption. It will help the user to choose the battery optimized app to use.

The talked approach EcoDroid provides an accurate ranking. But one question may arise how we will get an accurate ranking. Energy of ranking of two apps A and B will be proper if suppose A is lower on the ranking then its energy consumption should be lower than app B.

But providing an accurate ranking based on energy consumption is challenging. One need to keep account of all functions and features that consume energy more and less. There is no scope for skipping any functions. Apps which include API consume 80% more energy when API function is launched. Without addressing these functions there is a huge possibility of underestimating energy consumption.

And if we skip parts of app that general test cases dont execute that often we are to get an error. So to address these issues EcoDroid was introduced. It take account of the parts that are executed by
general test cases along with the parts that are not executed. In a sentence, it combines the static and dynamic analysis for an app which makes a proper estimation of energy consumption. Thats how it provides an accurate ranking.

Limitations

Taking account of energy consumption is quite imporatnt. However to highlight this point respiratory might ignore other points such as GUI, speed and the rest. The app with a poor GUI obviously consumes less energy and it might come top at the ranking. So before making a ranking based on energy consumption other features should get priority otherwise user will be disappointed.

Findings

- why account of energy consumption is imporatnt
- How to estimate app’s energy consumption level
- How to provide accurate ranking

Link:

http://www.ics.uci.edu/~seal/publications/2015GREENS.pdf

Paper 1:E-Police System - FIR Registration and Tracking through Android Application.
Authors: Archana Iyer, Prachi Kathale, Sagar Gathoo, Nikhil Surpam.
Paper link:https://www.irjet.net/archives/V3/i4/IRJET-V3I4235.pdf
Reviewer:Maksudul Hasan.

Abstract: The main purpose behind the E-police system was to improve the effectiveness of policy performance; to backup and recovery processes). None of this will be effective, though, unless a proper regime of incentives and disincentives in put in place to ensure stakeholders are motivated to uphold data quality.E-police system is an e-government related service and it makes the communication process a possibility, a great success for modern era which increases the professional efficiency for the government police administration. In this paper the author focused on the infrastructure of an e-police system as well as its steps, challenges of implementation and its necessity.E-police **i**s intended to provide total computerized information system support for the work of the Police. This system registers the complaints from people through online and is helpful to the police department for further process. The aim of this project is to develop an E-police reporting and management system which is easily accessible to the public, police department and the administrative department.E-police would also help provide division heads and senior officers with management information about crime control,and about administration and support services such as accounting and personnel management. This helps to higher authorities of police to have an overview about the progress of the investigation; feature is made available to public for interaction with police indirectly.

Proposed Solution:

1.FIR registration:A First Information Report (FIR) is a written document prepared by police organizations in countries like Bangladesh,india when they receive information about the commission of a cognisable offence, or in Singapore when the police receives information about any criminal offence. It is generally a complaint lodged with the police by the victim of a cognizable offense or by someone on his or her behalf, but anyone can make such a report either orally or in writing to the police.For a non cognizable offense a Community Service Register is created & registered.FIR is an important document because it sets the process of criminal justice in motion. It is only after the FIR is registered in the police station that the police take up investigation of the case.

Anyone who knows about the commission of a cognizable offence, including police officers can file an FIR.(ref-wiki).

2.E-Police System over Present System:There are several advantages of e-police system for and these are given below:

1)Establishment of E-government: Since the ratio of police-people of India is1: 728,that is not sufficient for public security and safety, that means on the perspective of People the police personnel is too much less, that is why the police cannot handle everything always and the general citizen feel in secure always. So the ratio problem may be decease if the government follows the e-police system.

2)Public Accessibility: Since e-police system is the world standards that follow the e-technology as well as technology the citizen of the country has the free accessibility, They could make a diary about any criminal as well send any information about any matter by email.

3)Secured Data Communication: Since the whole police topology and this not connected to internet anyone can not hack or access illegally.

4) Crime Reduction: It is possible to reduce any types of crime in any section of the country where police personnel could be able to interfere the police administration can and handle this but in normal police system is seemingly impossible.

5)Safety and Security incretion : For incretion of the country and country citizens' safety and security any kinds of the section our system plays an important role but if the system is the normal police system than that is not absolutely possible.

6)Standardization: In order to making the countries police administration world standard the e-police system must be essential but that is completely quite impossible by follow the normal police system.

Limitations:

1.By this system the uneducated poor people will not get any help because about 75% people of bangladesh are out of the facilities of internet.So the facilities should bring to the people with phone calling system.There are some police help line exists in bangladesh.Like any people of bangladesh can get police help through calling in the number 999.

2.In order to use IT sector of police effectively, a specialized and technical persons is needed. Therefore, to operate their information systems, police agencies choose to either train their staff or hire technical person from outside. Like British Police Organization, huge police members have their training buildings and special computer courses,their clothing matter their food habit to train their officers. Since Information

Technology world is dynamic and more complex, that is, new IT products, new version of softwares appears each day, yesterday's knowledge sometimes is not enough to operate today's systems. However, this requires endless training which means extra expenses and loss of work force temporarily for managers.so it is a big challenge for the police department to ensure skilled poeple to this sector.

3.There are also a big challenge for police managers is to ensure the security of their information systems. Therefore, they must consider the threats from the Internet. Since police records are mostly relevant to criminals, they should be kept secured and should maintain safely. Information Technology Security requires certain precautions based on both hardware and software . This issue requires both extra budget and trained-person and also cost a lot of money and time.

Findings:

1. A new solution to make the action of police easier and faster to the public.
2.Giving effective and efficient service to the community has become the main goal in modern police agencies.
3.Making the policing system more acceptable to the community.
4.Ensuring quick help during the emergency times.
5.Giving on spot help to the victim during emergency times.

Paper 2: Risk Assessment of Computer Network Security in Banks.
Authors: Tan Juan.

Paper link: http://www.sersc.org/journals/IJSIA/vol10_no4_2016/1.pdf
Reviewer: Maksudul Hasan.

Abstract:This study is devoted to the problems of improving the banking risk assessment, taking into account the new regulatory and technological requirements based on the use of modern technology and combining the latest achievements in artificial intelligence, numerical mathematics, statistics and information technology.Conducting risk assessment of computer system security of banks can increase safety management and ensure normal operation and can also make the banking system more secure and faithful to the people.This paper firstly finding out risk assessment indexes for computer system security of banks through literature review and survey. the computer network is easy to be attacked by viruses and Hackers. A damaged network will cause dire consequences and hit the bank greatly.Therefore,risk assessment of computer system security of banks can detect loop-holes in advance and warn the bank to increase the security level of computer network, ensuring that the bank is operated in a normal state. So the banking system is recommended to be highly secured.

Proposed Solution:

1.Evaluation Indicator System for Computer System Security of Banks**:**According to this paper, there are four layers of evaluation indexes for the computer system security of banks, namely they are the the network layer, data layer the physical layer, and the emergency layer. Each layer contains several second level evaluation indexes.

2.Index Weight of Computer System Security of Banks:The author suggested to use AHP to confirm the index weight of computer system security of banks. Firstly, the layer structure of computer system security of banks is established to do the assessment and secondly Secondly, the 9 scales are used to construct the comparative judgment of all indexes. The comparative judgment is established by comparing the influence of indexes of the sub layer on that of the dominant layer.The influence is confirmed according to experts judgment.

3.Risk Assessment Model for Computer System Security of Banks:

Risks of computer system security of banks are categorized into five levels : very safe, relatively safe, neutral, relatively dangerous and very dangerous . Establish risk assessment model for computer system security of banks.

4.Again the author proposed geometric process to calculate the indexes.Compute the product of elements in each line in the comparative judgment and get Vector @ and Subject vector @ to extraction and get vector $.Then Normalize vector $ and get the corresponding weight vector ỳ.

Limitations: In order to use information technology effectively, a specialized and technical persons is needed. Therefore, to operate their information systems, police agencies choose to either train their staff or hire technical person from outside. Like Turkish Police Organization, large police agencies have their training buildings and special computer courses to train their officers. Since IT world is dynamic, that is, new IT products, new version of softwares and hardwares appears each day, yesterday's knowledge sometimes is not enough to operate today's systems. However, this requires endless training which means extra expenses and loss of work force temporarily for managers.

.

Findings:

1.Making the banking system more secure and faithful to the users.
2.Making the banking system more easier and secure too and user friendly.
3.Ensuring 24 hours facility to the users.

Paper 1: A Survey on Network Security Attacks and Prevention Mechanism
Authors: Blessy Rajra M B, A J Deepa ME
Paper link: http://innovativejournal.in/jccst/index.php/jccst/article/download/35/44
Reviewer: Arafat Hossen

Abstract

Network security is an significant thing in every field like government offices, military educational institute and any business organization. Due to rapid need of computers in business and other organizations many networks have been established. Network security is a challenging problem due to the complexity of underlying hardware, software, and network interdependencies as well as human and social factors. It involves decision making in multiple levels and multiple time scales, given the limited resources available to both malicious attackers and administrators defending networked systems. The resources vary from bandwidth, computing, and energy at the machine level to manpower and scheduling at the organizational level. Data security is the extreme critical factor in ensuring the transmission of information via the network. Threats to data privacy are powerful tools in the hands of hackers that could use the vulnerabilities of a network to corrupt, destroy and steal the sensitive information. There are many types of attacks which can be penetrated in our networks or edge devices. In this paper we study about various types of attacks on network security and how to handle or prevent this attack.

TYPES OF NETWORK THREATS AND ATTACKS

Eavesdropping :

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference or fax transmission. The term **eavesdrop** derives from the practice of actually standing under the eaves of a house, listening to conversations inside.

Viruses :

Computer **virus** A computer **virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

Worms:

A worm is similar to a virus because they both are self- replicating, but the worm does not require a file to allow it to propagate [8]. There are two main types of worms, mass-mailing worms and network aware worms. Mass mailing worms use email as a means to infect other computers.

Trojans:

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus.

Phishing:

Phishing is an attempt to obtain confidential information from an individual, group, or Organization [9]. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

Proposed Solution

Prevention Mechanisms are two types : high level and low level.

High level prevention mechanism :

1. Secure group management
2. Instruction detection
3. Secure data aggregation.

Low level prevention mechanism :

1.Key establishment and trust setup

2. Secrecy and authentication
3. Privacy
4. Robustness to communication denial of service
5. Secure routing
6. Resilience to node capture.

Limitations

In this paper many limitations can be found out. Some common network security preventives like Firewalls or Antivirus method is not explained in this paper.

Now we will see how these method can prevent network security attacks.

1. Firewall:

Firewalls impose restrictions on incoming and outgoing Network packets to and from private networks. Incoming or outgoing traffic must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as choke points(borrowed from the identical military term of a combat limiting geographical feature). Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet. Firewall software may require each individual user to make decisions about allowing or denying a program's requested access to the Internet (which helps prevent malware from sending proprietary information from your computer over the Internet, among other things). Users without much computer or security experience may be uncomfortable handling the requests and alerts that small business firewall software presents to them. Alternative solution is Network firewalls and Hardware Firewalls.

a. Network firewalls: It prevents unknown programs and processes from accessing the system. However, they are not antivirus systems and make no attempt to identify or remove anything. They may protect against infection from outside the protected computer or network, and limit the activity of any malicious software which is present by blocking incoming or outgoing requests on certain TCP/IP ports. A firewall is designed to deal with broader systems.

b. Hardware Firewalls: Hardware-based firewalls protect all the computers on your network. A hardware-based firewall is easier to maintain and administer than individual software firewalls. Hardware firewall integrated into a comprehensive security solution. In addition to a firewall, the solution should include virtual private network (VPN) support, antivirus, antispam, antispyware, content filtering, and other security technologies.

2. Antivirus:

Antivirus and Internet security programs can protect a programmable device from malware by detecting and eliminating viruses; Antivirus software was mainly shareware in the early years of the Internet, but there are now several free security applications on the Internet to choose from for all platforms .Antivirus software was originally developed to detect and remove computer viruses hence the name. Some Antivirus software also include protection from other computer thread, such as infected and malicious URL, spam, scan and pishing attacks, online identity (privacy), online banking attacks, social techniques, Advance Persistent Thread (APT),botnets DDoS attacks. Anti-virus programs are not always effective against new viruses because when antivirus scan the system and new virus are found then it take a time to update the virus database during this time virus get control over the system and hide themselves . The reason for this is that the virus designers test their new viruses on the major anti-virus applications to make sure that they are not detected before releasing them into the wild also one more reason is virus has used the Graphics Processing Unit (GPU) to avoid detection from anti-virus software. Some new viruses, particularly ransomware, use polymorphic code to avoid detection by virus scanners. This type of [ransomware virus] comes from sites that use a polymorphism. Even people having antivirus software running and it's not detecting anything. In this case usually people should reinstall the operating system or reinstall backups.

Findings

Network security is an important field that is increasingly gaining attention as the internet expands.Preventing and detecting attacks that are launched over networks, and particularly over the Internet, is probably the most newsworthy aspect of security engineering. The problem is unlikely to be solved any time soon, as many different kinds of vulnerability contribute to the attacker's toolkit. Ideally,people would run carefully written code on trustworthy platforms.

In real life, this won't happen always, or even often. In the corporate world, there are grounds for hope that firewalls can keep out the worst of the attacks, careful configuration management can block most of the rest, and intrusion detection can catch most of the residue that make it through. Home users are less well placed, and most of the machines being recruited to the vast botnets we see in action today are home machines attached to DSL or cable modems.

Antivirus works on a very basic principle; they can scan a file and then matches, its digital signature against the known malwares. If the signature is match in the database is reports, delete it or even disinfect it depending on the clients setting. This system however easy has a huge drawback, whenever a new malware found ;it takes time before the antivirus database can be updated and during this period the malware can already take complete control of the system, disables the antivirus or even hides itself from the antivirus.

Paper 1: Web Application Development Using UML
Authors: Dilip Kothamasu, Zhen Jiang

Paper link: http://innovativejournal.in/jccst/index.php/jccst/article/download/35/44
Reviewer: Arafat Hossen

Abstract

The goal of the Independent study is to develop a Student Grading System, a web based application in Java using Object Oriented Design in Unified Modeling Language (UML). Web sites are progressively evolving from browsable, read-only information repositories to web-based distributed applications. Compared to traditional web sites, these web applications do not only support navigation and browsing, but also operations that have affects their contents and navigation states. The goal of the Independent study is to develop a Student Grading System, a web based application in Java using Object Oriented Design in Unified Modeling Language (UML). UML is used for developing projects in Object Oriented Design and helps in specifying, visualizing, designing the structure software applications meeting all the requirements of a project. There are some systematic designs method for Web applications which take into account the navigation space and the presentational aspects of the application. The method is based on a UML profile for the Web domain. The different models of the design process are represented by using a Web extension of UML. This thesis presents a comprehensive approach for the model-based development of Web services. The approach is based on a Web service profile for the Unified Modeling Language (UML), which allows an efficient definition of complete Web service models. Such Web service models allow the generation of the complete source code and the corresponding platform-specific configuration files necessary in order to run the modelled Web applications.

Proposed Solution

1. Requirement Specifications in Use Cases:
Use cases are a part of UML, are a way of representing requirements of a project in a effective way. Following are the use cases that are depicted from the requirements of Project: Students, Instructors, Followers.

2. Find different kinds of objects and describe their types in classes.

3. Find relationships of objects and describe then in class relationship:

a. Class Diagram: In software engineering, a **class diagram** in the Unified Modeling Language (UML) is a type of static structure **diagram** that describes the structure of a system by showing the system's **classes**, their attributes, operations (or methods), and the relationships among objects.
b. Use case diagram : A **use case diagram** at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different **use** cases in which the user is involved.
c. Sequence diagram: Sequence diagram displays the sequence of interaction between objects participating in an action, which consists of the objects and the time at which they are interacting with each other. The time sequence diagram shows a clear picture of which object should be involved while developing a particular action. The picture in Figure 2 shows the time sequence diagram for the various actions of instructor and a student while interacting with the system.

4. Implementation:
a. Constraints Security: • Each user of the system is given username and passwords. • The sessions for each logged in user is maintained and on expiration/logout, relogin is required. • Database level security is also maintained by securing with username and password. • Using “role” and “service” concept only user who has a valid service can access that particular service. Features: • Each user is given a role and to that role various services are offered. For example a student is assigned a “student” role for which the service that is available is only to check his grades. • Javascript menu is used for navigation after logging in. • Chart Director is used for graphical reports.

b. Multi-layer system using UML.
c. Implementation of UML Class diagram & Development
d. Environment setup System Requirements:
1. An operating system as Windows or Linux.
2. Java 1.4.2 or later installed [4].
3. Tomcat 4.0 or later [5].

4. MySQL 4.1 [6].

Limitations

In this paper, limitations I've come up against trying to use the UML :

Time

One disadvantage some developers might find when using UML is the time it takes to manage and maintain UML diagrams. To work properly, UML diagrams must be synchronized with the software code, which requires time to set up and maintain, and adds work to a software development project. Small companies and independent developers might not be able to handle the added amount of work required to synchronize the code.

Unclear Who Benefits

It is not always clear who benefits from a UML diagram. According to an article published on the Eiffel Software website, UML is not advantageous to software developers, mainly because software developers work with code, not pictures or diagrams. UML diagrams may be beneficial to project managers or executives to illustrate how a software tool will work, but it might be easier to draw the diagram out on a whiteboard or piece of paper, rather than take the time to learn the UML language.

Diagrams Can Get Overwhelming

When creating a UML diagram in conjunction with software development, the diagram might become overwhelming or overcomplicated, which can be confusing and frustrating for developers. Developers cannot possibly map out every single scenario for

a software tool in the diagram, and even if they try to, the diagram gets messy. One way developers can combat this issue is to only include basic facts and high-level information in UML diagrams, according to a post on Stack Overflow by Stefano Borini, a quantum chemist and UML developer.

Too Much Emphasis on Design

UML places much emphasis on design, which can be problematic for some developers and companies. Looking at a software scope in a UML diagram can lead to software project stakeholders over-analyzing problems, as well as cause people to lose focus by spending too much time and attention on software features. Companies cannot solve every problem with a software tool using a UML diagram -- eventually, they just have to start coding and testing. Brody Gooch, a co-creator of UML, said that the original vision for UML was a "graphical language to help reason about the design of a system as it unfolds." If people get hung up using a diagram to identify and solve issues, it can delay the actual work that needs to be done to fix the issues.

Findings

In this paper, we see presentation a methodology for the design of Web applications that uses a UML profile for the Web domain. Some of the modeling elements occurring in such diagrams are defined by stereotypes using the UML extension mechanism. The definition of many new stereotypes causes extra effort to read the diagrams, but once one gets use to them the diagrams are more meaningful in terms of Web design. The advantages of the methodology are the use of the UML, the consideration of specific Web aspects in design of Web applications through the definition of specialized modeling elements and the creation of the tailored models to express navigation and presentation.