Jarks Hack

Ance K A¹, Jiji S², Kavya S³, Rubeena T S⁴, Saritha P P⁵, Saneesh Mohammed N⁶

¹,²,³,⁴,⁵ B Tech Students, Department of Computer Science and Engineering, Ammini College of Engineering Palakkad, Kerala, INDIA

⁶Assistant Professor, Department of Computer Science and Engineering, Ammini College of Engineering Palakkad, Kerala, INDIA

ABSTRACT

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose. Most of the reported hacks occur on computers or smartphones, but they are far from the only devices that the hackers are capable of exploiting. There are many hacking techniques are involved to hack a mobile phone simply with MAC address, IP address and port number. MAC address is embedded in our hardware only during its manufacturing, hence there are many way to spoof MAC address, IP address and port number. Wireless connections are not as secure for android mobiles. Various methods for manipulating radio network traffic including mobile phones and wireless networks.

Jarks Hack is an android based application for providing protection to the mobile phones from hacking. Spam messages, calls, Email and Apk files are usually use for this purpose. This app detect the spams and block their further actions.

As in Jarks Hack, if spam Messages, Calls, Emails and Apk files are receive in application then there it will be checked. If yes then it will be sent to the user by saying that the message or access is been blocked.

II. LITERATURE SURVEY

1. Opportunities and Challenges of Software-Defined Mobile Networks in Network Security

To transform rigid and disparate legacy mobile networks into scalable and dynamic ecosystems, software defined mobile network (SDMN) architecture integrates software-defined networks, network functions virtualization, and cloud computing principles. However, because SDMN architecture separates control and data planes, it can introduce new security challenges.

- Security Mechanisms in Mobile Networks
  Securing Only the Perimeter Today’s telecommunications networks heavily rely on perimeter security mechanisms. Mobile network edges interfacing to external networks are considered the most vulnerable points in the network and are protected by intrusion prevention systems (IPSs), firewalls, customer edge switching (CES), carrier-grade network address translators (NATs), and so on.

- Vulnerability to IP-Based Attacks
  Recent IP-based mobile networks (for instance, LTE and LTE-Advanced) are vulnerable to security attacks such as distributed denial of service (DDoS), insider attacks, botnets, and other IP-based attacks. DDoS attacks are common in telecommunications networks. More than 90 percent of mobile operators experienced DDoS attacks

Keywords—Android application, Hacking detection, Hacking prevention, Notification.
in 2012. Unprotected and always-on devices, such as smartphones and tablets, are great platforms for attackers to launch DDoS. For instance, attackers can deploy a botnet on a smart phone to carry out DDoS attacks on a mobile network.
- **Granular Policy Management**
  SDMN supports more granular policy management schemes than the existing mobile networks. The controller can enforce security policies based on application, service, user, flow, device, and other levels. Such fine-grained enforcement and security policies are necessary to provide carrier-grade services while supporting millions of dynamic users in a single mobile network.

2. **Survey on E-mail Spam Detection Using NLP**

E-mail spam causes a serious problem for the internet user. It has a lot of consequences. It reduces productivity, takes extra space in mail boxes, extend viruses, Trojans, and materials that contains potentially harmful information for a certain category of users, destroy stability of mail servers, and as a result users spend a lot of time for sorting incoming mail and deleting undesirable correspondence. So it is necessary to detect the spam so that its consequences can be reduced. There are various classifiers used for e-mail spam detection like Naïve Bayes Classifier, KNN, and SVM Classifiers etc. Some of these methods are discussed in this paper.

Spam is an unwanted communication intended to be delivered to an indiscriminate target, directly or indirectly, notwithstanding measures to prevent its delivery. Spam filter is an automated technique to identify spam for the purpose of preventing its delivery. The motivation behind spam is to have information delivered to the recipient that contains a payload such as advertising for a (likely worthless, illegal, or non-existent) product, bait for a fraud scheme, promotion of a cause, or computer malware designed to hijack the recipient’s computer. Because it is so cheap to send information, only a very small fraction of targeted recipients — perhaps one in ten thousand or fewer — need to receive and respond to the payload for spam to be profitable to its sender. The main characteristics of spam are unwanted, indiscriminate, disingenuous, payload bearing. Unwanted spam means spam messages are not wanted by vast majority of people. Indiscriminate spam means Spam is transmitted outside of any reasonable relationship or prospective relationship between the sender and the receiver. In general, it is more cost effective for the spammer to send more spam than to be selective as to its target.

Disingenuous spam means because spam is unwanted and indiscriminate, it must disguise itself to optimize the chance that its payload will be delivered and acted upon. The payload of a spam message may be obvious or hidden; in either case spam abatement may be enhanced by identifying the payload and the mechanism by which actions triggered by it profit the spammer.

Obvious payloads include product names, political mantras, web links, telephone numbers, and the like. These may be in plain text, or they may be obfuscated so as to be readable by the human but appear benign to the computer. Or they may be obfuscated so as to appear benign to the human but trigger some malicious computer action. The payload might consist of an obscure word or phrase like — go urangal or — platypus race! in the hope that the recipient will be curious and perform a web search and be delivered to the spammer’s webpage or, more likely, a paid advertisement for the spammer’s webpage. Another form of indirect payload delivery is *backscatter:* The spam message is sent to a non-existent user on a real mail server, with the (forged) return address of a real user.

Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments. E-mail is a good, quick and a low cost communication approach. So spammers always opt to send spam through e-mail. Today every second user has an E-mail, and they are faced with spam problem consequently. E-mail Spam is non-requested information sent to the E-mail boxes. Spam may be a massive drawback for users and for ISPs. The causes are growth of value of electronic communications on the one hand and improvement of spam sending technology on the other hand.

3. **An Approach for SMS Spam Detection**

In the today’s world the use of mobile increase tremendously. And hence the companies start to use of SMS for their advertisement. At the beginning the companies are send their promotional messages through SMS gateways. But due to increasing number of promotional messages the companies start the service DND, the DND service restrict only the SMS send through SMS gateways. But due to increasing number of promotional messages the companies start the service DND, the DND service restrict only the SMS send through SMS gateways and hence the companies start to send their promotional advertisement messages through spammer’s mobile phones. The approach presented in this paper detects these messages sent through spammers mobile and restrict it.

Phase 1: Designing and textual communication program which allows the users to register and start messaging service. It will be a prototype model of user mobile phones.

Phase 2: Develop a server which could be a mobile service provider application server which allows the connected users to communicate. It will manage the proper transfer of messages from sender to receiver.

Phase 3: Database designing to stores the predefined spam content & all SMS log in proper indexed format to have fast and reliable access to the records at any time of instance.
Phase 4: Database analysis service which could be used to find out the direct or mutual relation between sender and receiver in order to conclude non spam entity and check for the content of message to allow the message forwarding to receiver with normal or spam tag.

In the proposed system as shown in figure above sender will first unicast, multicast a text message which will land at mobile service provider server. Once the message is received by the server then server will send the sender and the receivers address to relationships analysis module which will give the concluded result in positive or the negative format. Here the relation analysis module will look into and previous SMS log between the sender and receiver and also look for the direct or mutual relation between sender and receiver. System will also check for the message replication or the individual message to different message and check for the content of the message. After the successful result from result analyzer system will apply and normal or spam as a tag to message and forward it to receiver or system can discard the message on the basis of configuration.

4. Trust-based VoIP Spam Detection based on Call Duration and Human Relationships

Spam over Internet Telephony (SPIT) will become a serious threat in the near future because of the growing number of Voice over IP (VoIP) users. Due to the real-time processing requirements of voice communication, SPIT is more difficult to filter than email spam. We propose a trust-based mechanism that uses the duration of calls between users to distinguish legitimate callers and spammers. The trust value is adjustable according to the calling behavior. We also propose a trust inference mechanism in order to calculate a trust value for an unknown caller to a callee. Realistic simulation results show that our approaches are effective at discriminating spam calls from legitimate calls.

To deal with VoIP spam, we have presented an approach combining trust ratings and characteristics of callers. A trust value based on call duration is calculated for each friend in the buddy list. This technique provides a simple way to use call duration as an automatically assigned trust value based on human behavior. Due to the reliability of this value, it is difficult for a spammer to subvert the system. The proposed technique is also implemented according to call behavior and human reasoning. The trust values of long-time-no-call friends and spammers are decreased by default. However, the trust value of a legitimate user can be increased with calls lasting long enough. This supports the bidirectional communication characteristic of a legitimate user call. To extend the detection scalability, we further proposed a trust propagation method in case a caller and a callee do not have a direct relationship. Based on realistic simulation results, we found that the proposed technique can detect all SPIT completely after a few periods (learning period) while keeping a low false positive rate. We also demonstrated that even when the number of spammers was increased, the accuracy of spam and legitimate call detection were still higher than 98% and 95% respectively.

The size and the relationship characteristics among nodes in the network did not affect the detection efficiency.

5. Spyware Detection in Android Using Hybridization of Description Analysis, Permission Mapping and Interface Analysis

Among all available Mobile OS, Android is an ideal target for attackers due to its huge popularity. Android provides open-source OS and also provides ability to install third party applications that poses threat of user’s privacy breach. In this paper, we have a close look at permissions that are granted during installation period. We have proposed a hybrid approach for detection of malicious applications by scanning with different antivirus software and comparing all. This hybrid approach depends upon three parameters- Description Mapping, Interface Analysis and Source Code Analysis that defines an application’s behavior i.e. either it behaves malicious or normal.. In this methodology following steps have been followed which is shown in Fig.
III. SYSTEM ANALYSIS

3.1 FEASIBILITY STUDY

A feasibility study is an evaluation of a proposal designed to determine the difficulty in carrying out a designated task. Generally, a feasibility study precedes technical development and project implementation. In other words, a feasibility study is an evaluation or analysis of the potential impact of a proposed project. Feasibility Study is performed to choose the system that meets the performance requirements at least cost. The most essential tasks performed by a Feasibility Study are the identification and description of candidate systems, the evaluation of the candidate systems and the selection of the best of the candidate systems. The best system means the system that meet performance requirements at the least cost. The most difficult part of a Feasibility Study is the identification of the candidate systems and the evaluation of their performances and costs. The new system has no additional expense to implement the system. The new system has advantages such as we can easily access files from any client in the Network, accurate output for accurate input and this application is more user friendly. We can use this application not only in this organization but also in other firms. So it is worth solving the problem.

3.1.1 Economic feasibility

Economic Feasibility Study is the most frequently used method for evaluating the effectiveness of a candidate system. More commonly known as cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with cost. This analysis phase determines how much cost is needed to produce the proposed system. As the organization has required machines and supporting programs for the application to execute itself.

In economic feasibility study our application provides less implementation cost and free application.

3.1.2 Operational feasibility

Operational feasibility is a measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development. The operational feasibility assessment focuses on the degree to which the proposed development projects fit in with the existing business environment and objectives with regard to development schedule, delivery date, corporate culture, and existing business processes. To ensure success, desired operational outcomes must be imparted during design and development. These include such design-dependent parameters such as reliability, maintainability, supportability, usability, reducibility, disposability, sustainability, affordability and others. These parameters are required to be considered at the early stages of design if desired operational behaviors are to be realized. A system design and development requires appropriate and timely application of engineering and management efforts to meet the previously mentioned parameters. A system may serve its intended purpose most effectively when its technical and operating characteristics are engineered into the design. Therefore, operational feasibility is a critical aspect of systems engineering that needs to be an integral part of the early design phases.

In operational feasibility study our application provides user friendly and operations are very easy.

3.1.3 Technical feasibility

Technical Feasibility study is performed to check whether the proposed system is technically feasible or not. Technical feasibility centers on the existing computer. This involves financial consideration to accommodate technical enhancement. This system is technically feasible. All the data are stored in files. The input can be done through dialog boxes which are both interactive and user friendly. Technical feasibility enters on the existing manual system of the test management process and to what extend it can support the system.

According to feasibility analysis procedure the technical feasibility of the system is analyzed and the technical requirements such as software facilities, procedure, inputs are identified. It is also one of the system developments.

In technical feasibility study our application provides updating is possible and compactable with new configuration.

3.2 EXISTING SYSTEM

- Text Secure Private Messenger
  There are vast number of secure messaging apps available in Play Store, but the trouble part is that most of them work only if both the parties use the same application for encryption to work. TextSecure breaks that barrier and works with standard SMS text messages as well, which means you can add an extra layer of security to regular texting even if the client you are messaging is not using TextSecure. It is completely open-source and supports end-to-end encryption for secure text messages, means nothing is stored on its server. Your private conversations will be even safer if both parties are chatting directly through the TextSecure app, but the ability to encrypt your standard SMS messages makes it different from other secure messaging apps.

- Red Phone: Private Calls.
  RedPhone is a free secure call app that provides end-to-end encryption for your private calls, securing your phone conversations in a way that nobody can listen in. The purpose for which I use the Red Phone app is that it’s very easy to use. Red phone uses your standard phone number to make and receive phone calls, so there is no need for any other identifier.

- K-9 Mail
  Emails contains the most sensitive data as it’s related to both our personal as well as professional life. K-9 Mail meets your expectations by providing you a secure email
encryption service. K-9 Mail is a free and open source email encryption software for Android that allows you to securely send and receive email from one or more email accounts when used with Android Privacy Guard (APG) to encrypt the contents.

- **Apk files**
  No consolidate technique have been developed to extract the English keywords used in the description of an android application.
  - API documentation has been used but it does not provide sufficient information.
  - There is need to check the objects and classes related to each permission defined in AndroidManifest.XML file.
  - Till date no technique uses the identification of Frame Layout but it is capable of hiding surface view holder inside it if another child is added after surface view which can be used in background process to click the photos of the user and record videos etc.

### 3.2.1 Drawbacks of existing system

The main drawback of existing system is there is no integration of different hacking methods. They are only dealing with specific methods of hacking. So they are not user friendly. Most of the existing system is based on the online account hacking prevention technique.

### 3.3 PROPOSED SYSTEM

We can implement this app in two ways, a graphical user interface (GUI) or utility software. Android provides a variety of pre-built UI components such as structured layout objects and UI controls that allow you to build the graphical user interface for apps. Android also provides other UI modules for special interfaces such as dialogs, notifications, and menus. So in this way we can implement our app. Another way of implementation is Utility software. Utility software is system software designed to help analyze, configure, optimize or maintain a computer.

Utility software, along with operating system software, is a type of system software used to support the computer infrastructure, distinguishing it from application software which is aimed at directly performing tasks that benefit ordinary users.

There are various applications in Android Market in which some of these applications are available free of cost and some are paid ones. The main purpose of this proposed system is to provide a combination technique to prevent various kind of hacking methods. It provide integration of Messages, Calls, Emails and Apk files. The app will check all the Messages, Calls Emails and Apk files received from our smart phone. And detect whether it is a hacking content. If the app will find any spam content then it notifies the user and immediately block the spam content.

### 3.3.1 Advantages of proposed system

- User friendly.
- Freely available.

- It provides hacking prevention from messages, calls, Emails and Apk files.
- It provides integration of different hacking methods.
- Upgradation is possible.

### 3.4 SYSTEM SPECIFICATION

#### 3.4.1 HARDWARE REQUIREMENT

- Microprocessor - Intel Dual core processor
- RAM - 2GB
- Cache - 3MB
- Hard disk - 40GB
- Keyboard - 104 Keys
- Mouse – Normal
- Smartphone
- USB Cable

#### 3.4.2 SOFTWARE REQUIREMENT

- Platform: Android
- Language: java
- Tool: SDK and JDK bundle

### IV. SYSTEM DESIGN

The Purpose of Jarks Hack Design Document is to describe the design and the architecture of JARKS HACK android app. The design is expressed in sufficient detail so as to enable all the developers to understand the underlying architecture of Jarks Hack.

#### DETAILED DESIGN

- **Use Case Diagram**

  A use case corresponds to a sequence of transactions, on which each transaction is invoked from outside the system (actors) and engages internal objects to interact with one another and will the system’s surroundings. The description of a use case defines what happens in the system when the use case is performed. Use cases represent specific flow of events in the system. The use cases are initiated by actors and describe the flow of events that these actors set off. An actor is anything that interacts with a use case: it could be a human user, external hardware, or another system. An actor represents a category of user rather than physical user. A use-case diagram is a graph of actors, a set of use cases enclosed by a system boundary, communication associations between the actors and use cases, and generalizations among the use-cases.
**Figure: Use case diagram**

- **Activity Diagram**
  
  An activity diagram visually presents a series of actions or flow of control in a system similar to a flowchart or a data flow diagram. Activity diagrams are often used in business process modeling. They can also describe the steps in a use case diagram. Activities modeled can be sequential and concurrent. In both cases an activity diagram will have a beginning and an end.

![Activity Diagram](image)

**Figure: Activity diagram**

- **Sequence Diagram**

  Sequence diagrams describe interactions among classes in terms of an exchange of messages over time. They're also called event diagrams. A sequence diagram is a good way to visualize and validate various runtime scenarios. These can help to predict how a system will behave and to discover responsibilities a class may need to have in the process of modeling a new system.

![Sequence Diagram](image)

**Figure: Sequence diagram**

**MODULE DESIGN**

- **Identification of hacking method**

  In this module we identifies the hacking method. The main methods of hacking are Messages, Calls, Emails and Apk files. In this module we choose different criteria to identify them. First we check whether it is a spam content or not. Then proceed with next module.

- **Blocking of hacking attempt**

  In this module identified spam content is blocked. It may be a number, mail or apk file. So the hacker cannot reach the smartphone in which the app is installed.

- **Notification**

  Here we make a notification to the user that his or her smartphone has tried to hack and the app block the hacker appropriately from further actions.

**V. CONCLUSION**

These Jarks Hack is an android based application for providing protection to the mobile phones from hacking. With this app we get complete protection from hacking. It is easy to hack a mobile phone simply with MAC address, IP address and port number. MAC address is embedded in our hardware only during its manufacturing, hence there are many way to spoof MAC address, IP address and port number. Wireless connections are not as secure for android mobiles. Various methods for manipulating radio network traffic including mobile phones and wireless networks. Thus in our application these types of methods are prevented. Spam is an unwanted communication intended to be delivered to an indiscriminate target, directly or indirectly. Our app will provides all type of protection from spam hacking. It provides detection and blocking of spam Messages, Calls, Emails and Apk files. We can implement this app in two methods. System utility and graphical user interface.

**REFERENCES**