Context Based Access Control System for Mobile Devices

Divya Nautiyal
Department of Computer Science, SRM Institute of Science and Technology, Ramapuram Campus, Tamil Nadu, India

Dhikhi T.
Assistant Professor, Department of Computer Science, SRM Institute of Science and Technology, Ramapuram Campus, Tamil Nadu, India

Abstract – Many devices nowadays are intact with powerful resources, some of these resources can sometimes be harmful and can spy on our systems. Hence there emerges a need for a system which can enable users to restrict the privileges given to any external application according to the user's comfort. So this actually gives the user control over their device functioning by restricting certain application privileges while being in certain places like e.g. in confidential meetings .These restrictions are based on certain factors called as contexts. The contexts provided here are basically Location and Time. The user has to provide the specific location where it wants the application to be restricted.

Index Terms - Context-based access control, privacy and security, wifi, smartphone devices, restriction policies, firewall, device management.

1. INTRODUCTION

In these days, with advancement in technology, there is increasing need of a secure system which can protect and secure our data. On the time of installing apps, we generally pay no attention to the permissions we are granting them. Some of those apps can be malicious and can harm our mobile and steal very critical information. The need for restriction increases for people working in certain areas as high profile employees. They are not allowed to carry devices at all the places, such as government officials have restricted their employees from bringing any camera-enabled device to the work, this includes smart phones, even if their devices may contain important data and services they might need. Another problem arises when a person needs their mobile information to be safe and not accessible by anyone.

They can restrict the application and at that particular location, no one can access that restricted application. In these cases, CBAC mechanism plays an important role. By restricting; for example: camera on the mobile, the employees can still bring the mobile device to the work place and this will help them prevent using camera while still giving access to other important applications and documents on the mobile phone.

To overcome this, Cisco IOS developed a Firewall Feature Set which actively inspects the activity behind a firewall. This feature of CISCO was called CBAC (Context Based Access Control) specifies what traffic needs to be let in and what traffic needs to be let out by using access lists. IP access control lists (ACLs) are used to :

- Filter network traffic and also contains brief descriptions of the IP ACL types, feature availability, and an example of use in a network.
- Define traffic to Network Address Translate (NAT) or encrypt, or filtering non-IP protocols such as AppleTalk or IPX
- Control traffic flow using TCP session information
- Allow IP traffic only after authentication
- Debug traffic

Now there are some limitations for ACLs also which include space constraints which makes it somewhat not possible to address every use for ACLs in the Cisco IOS.

The major problem faced by system was Denial Of Service attack. DOS is a cyber attack in which the attacker aims at making a machine or network resource unavailable to the particular user by varying the services of a host connected via a network. Due to this problem, the required requests were never fulfilled .Ordinary firewalls were prone to this problem of DOS attack. So CISCO came up with the concept of CBAC. CBAC is a feature of firewall software, which basically filters TCP (Transfer Control Protocols) and UDP (User Datagram Protocol).

This application has been developed using android application development platform eclipse (IDE) , and coded using java.

2. RELATED WORK

This section describes the similar firewall management solutions that have been discussed.

In [1], the accuracy of location detection algorithm used in CBAC was tested. The number of success and failures were detected. A modified version of the android OS supporting context-based access control policies was proposed which restricted application from accessing specific data based on user context. But in this case the Permission management and setting up the required control policies were difficult .

In [2],the SDM wizard was used to help with firewalls and security. The SDM method user interface represents an intermediate to the CDI and SDM. The SDM also has the ability to monitor both the devices status and firewall operations in real-time. The problem with this system was the lack of prevention of DOS.

In [3], the system provides a method, apparatus and machine-readable medium for preventing Denial Of Service attack on a networking device. This system provides a way to eliminate the attacking group from the network. It further provides a method for accomplishing the removal of the attacking group. The main problem in this system was the time delay . The algorithms included for the completion of the process took unexpectedly long time and hence time delay was there.

In System [4], FWS was used to verify the guidelines of a firewall policy with needed functionality and security of a network in the case study. Several iptables policies were tested on by real-world scenarios. The major drawback of this system was the lack of prevention of DOS attacks on the system.

In System[5], an android application was implemented which supports context based access control policies. This will help the application to restrict the malicious data and allow the system to access only specific data based on context given by user. But the only failure was difficulty in Re-gaining of original privileges in the application.

3. PORPOSED MODELLING

The proposed system has a separate login for the user and it has different set of privileges. The app has option to select from different policy – set and the user will be able to restrict that app.

The physical parameters such as longitude and latitude has to be provided. The proposed system has an access control mechanism that deals with access, collection, storage, processing, and usage of context information and device policies.

CBAC policies are enforced as a set of restrictions applied to the smartphone applications when the device is located within a specified location . As soon as the device gets in the context, the policy executer enforces device restrictions by comparing the device's context with the configured policies.

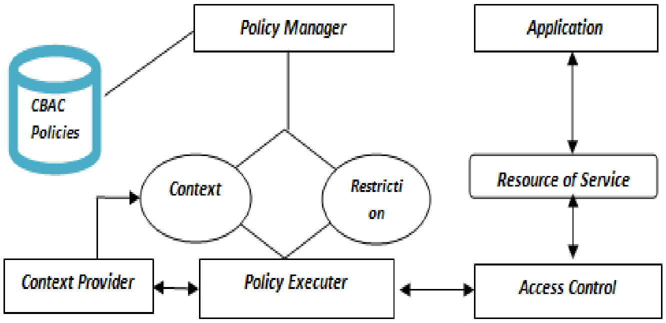

Figure 1.SYSTEM ARCHITECTURE

The different modules used in the architecture are:

1.The Context Provider (CP)

It collects the physical location parameters (GPS, Wi-Fi parameters, Cell IDs,) through the device sensors and stores them. Storing is done in its own database, linking each physical location to a location pre-defined by the user. The parameters are also updated and verified by the Context Provider , each time the device is re-located.

2. The Access Controller (AC)

It controls the authorizations of applications and prevents unauthorized usage of device resources or services. The access controller supports the android operating system with the permission control system with more control methods, inspite of android OS having its own system. The permission control system checks if an application has privileges to request resources or services, the and specific finely arranged control permissions that reflect the application capabilities and narrow down its accessibility to resources.

The Access Provider also increases the security of the system. Contrary to the native android devices which have some permissions that if they are once allowed to or granted to the applications can give the applications unrequired accessibility which they may or may not need.

3.The Policy Manager (PM)

It represents the interface used to create policies. It basically works by assigning application restrictions to contexts. It mainly gives control to the user to configure which resources and services are accessible by applications at the given context provided by the CP. It lets user choose the set of policies and contexts accordingly.

It is also used by the Policy Executer to check for granting or denying the access to application requests. The user can create their own set of policies for restricting the applications by configuring application's restrictions and linking them to contexts.

4.The Policy Executor (PE)

The PE enforces device restrictions by comparing the device's context with the configured policies. As soon as the application requests to access a given resource in the device, the PE checks the restrictions set which were earlier configured by the user at the Policy Manager to either grant or deny access to the request made by the application.

The PE also acts as a policy enforcement by sending the authorization information to the Access Controller to handle application requests. It is also responsible to simplify the policy conflicts and apply the most restrictions and rules.

4. RESULTS AND DISCUSSIONS

The CBAC is implemented as an android application that runs on mobile devices. It has a login page for the user .

Then it leads to the page in which the user can set privileges or view the existing and previously set privileges as well. The longitude and the latitudes has to be entered correctly by the user.

There is a grid view in app which shows different options of about the app, set privileges, view privileges and delete privileges too

Figure 2 App's logo

The application home screen is displayed in Fig 3.

5. CONCLUSION

The CBAC is a powerful tool to help secure the firewall and user's important information. Previous work on security for mobile operating systems focuses on restricting applications from accessing sensitive data and resources, but mostly lacks efficient techniques for enforcing those restrictions according to fine-grained contexts that differentiate between closely located subareas. CBAC overcomes the drawback and allows smartphone users to set configuration policies over their applications' usage of device resources and services at different contexts.

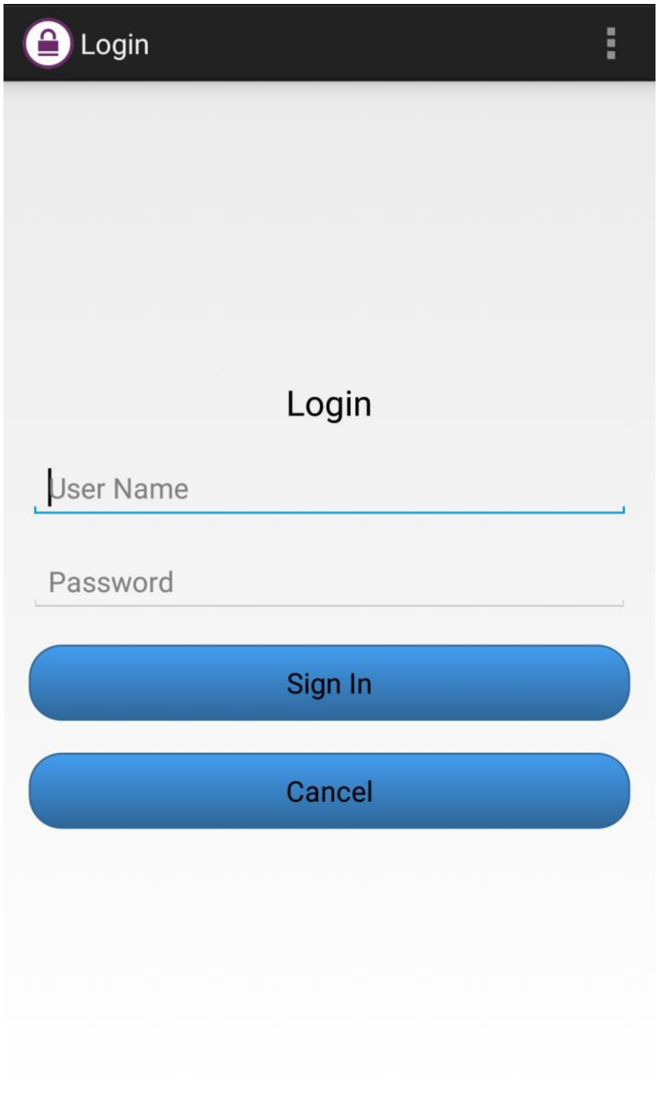

Figure 3 Mobile Home Screen

The context based relevance evaluation mechanism can be applied to expand the query. The contextual senses integrated with some other features can be applied to query words to increase the query length in the selected context to improve the search.

The proposed context based mechanism is applied to handle only the textual data, the work can be carried out to include the functionality to handle video and images data.

The proposed context based mechanism if integrated with other existing focused techniques will help the search engine to display more relevant as well as popular web documents to the user at top position in the result list. Thus, it can improve the precision to some extent.

REFERENCES

[1] Bilal Shebaro, Oyindamola Oluwatimi, Elisa Bertino Computer Science, Cyber Center and CERIAS, Purdue University," CBAC for mobile devices", IEEE Transactions on dependable and secure computing,2013.

[2] S P Maj, W Makasiranondh, D Veal, Edith Cowan University, Perth, Western Australia," An evaluation of firewall configuration method, IJCSNS International Journal of Computer Science and Network Security, vol.10,No.8,August 2010.

[3] Jai Balasubramaniyan,Kanata(CA),Kunal Daftary, Milpitas,CA(US)," Method and System for preventing DOS Attack", United States Patent Aug 2010.

[4] Chiara Bodei1, Pierpaolo Degano, Riccardo Focardi, Letterio Galletta, Mauro Tempesta, and Lorenzo Veronese, Department, of Information Technology," Firewall Management with Firewall Synthesizer ",University of ITALY, Vol.2058,2016.

[5] D.Geetharani, K.Saravanan ,"Provision of Access Control for Mobile Devices Based on Situation using CBAC Mechanism", International Journal on Applications in Information and Communication Engineering , Volume 2:Issue 6: June 2016, pp 39-42.