ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

A Proposed Approach for Mobile Devices with Context Based Access Control Mechanism

[I]Savrav Prakash, [II]Suhel Ahmed, [III]Dhaval Patel, [IV]Ashok Tiwari, [V]Prof. Shubhangi Vairagar
[I,II,III,IV,V]Dept. of Computer Engineering, Siddhant College of Engineering, Pune, India

Abstract
Now-a-days, android applications have become a craze in people. Mobile applications are increasingly being deployed and used by enterprises, military and other secured industries. As mobile applications have so many advantages but every application comes with issue of data security. Mobile Android applications have access to sensitive data and resources on the user device. Misuse of this data by malicious applications may result in privacy breakage and sensitive data leakage. Protecting this sensitive data from leakage is a critical issue. In android mobile applications, the chances of such critical data leakage will be on higher side. For example, in many applications at the time of installation the application ask for system privileges. The fact is that Android users do not have control over the application capabilities once the applications have been granted the requested privileges upon installation. Mobile devices cannot be protected by physical security the same way as stationary systems can be protected. In this paper an access control mechanism is proposed which will avoid data leakages and misuse of user privileges.

Keywords
Context Awareness, Context Based Access Control, Mobile Application, Smart phone devices, Security and Privacy.

I. Introduction

Users of Smart phones and other mobile devices are found everywhere. The organizations like IT industries, government sectors, military, aviation industry and e-commerce are using mobile applications to make work simpler. But at the same time the data which is transferred or shared during application installation has become a critical issue. This means sensitive data will invariably be placed on mobile devices (see Table 1). Security will be the limiting factor for deploying mobile devices in many scenarios where they would otherwise be extremely useful.

Table 1. Sensitive Data on Mobile devices on the basis of organization under which device is used.

Device Type	Sensitive data
IT industries	Company Bonds, Tender Data
Government	Tax Files, Police Records
Aviation industry	Plane Routes, Passengers information

As smart phones are becoming more powerful in terms of computational and communication capabilities, application developers are taking advantage of these capabilities in order to provide new or enhanced services to their applications. The danger arises when a device application acts intentionally harmful and uses device resources to keep a watch on user's activities or leak the user's personal data without the user's consent. Moreover, users carrying their Smartphone in public and private places may unknowingly expose their private information and can put their personal security in danger. The smart phone user is not aware of the existence of malicious activities getting performed on their devices. To prevent such harm and leakages, users must be able to have a better control over their device capabilities by reducing certain application privileges while being in public places e.g. At work place, shopping malls. To achieve such type of security mechanism, Smartphone systems must provide device owners with configurable policies that enable users to control their device usage of system resources and application privileges according to context, mainly location and time. Since such a feature is still missing in popular Smartphone systems, such as in Android systems, it is crucial to work on such systems and make them more secure and efficient.

II. Architectural Design

We studied the some architectures and one of them we are going to implement more efficiently. Studied framework consists of an access control mechanism that deals with access, collection, storage, processing, and usage of context information and device policies. To handle all the aforementioned functions, given framework design consists of four main components. The Context Provider (CP) collects the physical location parameters (GPS, Cell IDs, Wi-Fi parameters) through the device sensors and stores them in its own database, linking each physical location to a user-defined logical location. It also verifies and updates those parameters whenever the device is re-located. The Access Controller (AC) controls the authorizations of applications and prevents unauthorized usage of device resources or services. Even though the Android OS has its own permission control system that checks if an application has privileges to request resources or services, the AC complements this system with more control methods. The AC enhances the security of the device system since the existing Android system has some permissions that, once granted to applications, may give applications more accessibility than they need, which malicious code can take advantage of. The Policy Manager (PM) represents the interface used to create policies, mainly 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.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

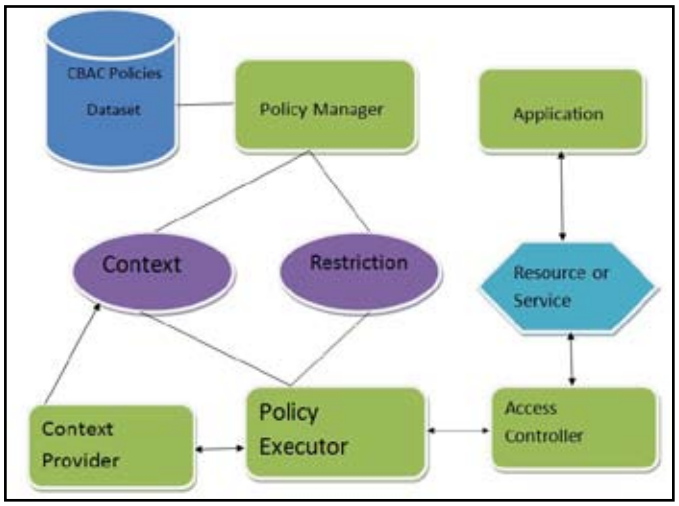

Fig. 1. Architectural Design

III. Proposed System Design

The policy decision engine keeps track of the current risk state. The state is simply a list of risk factor abstraction statements from risk assessment components.

Location_Zone(Red_Zone, active);
Location_Peer(Smith, John, Lieutenant, 45m, active);
Location_Peer(Owen, Chad, Private, 85m, detected);
Auth(PIN, know, 6, 13:45:12, 14:34:12);
Auth(Voice_Rec, 4, 13:38:23, 14:43:23);
Threat(Gun_Shot, 7, 13:38:23, 14:43:23);
Condition(Force_Protection, 5, active);

Above example shows risk state composed of risk factor statements.

Risk assessment components convert environmental, system and user inputs into abstracted risk factor statements before sending them to the policy decision engine. Most of the intelligence and complexity in the system will reside in the risk assessment components. This agent-based approach offers flexibility and supports plug-and-play for new components and configurations. Components can be developed by different venders independently and integrated in the overall framework. Risk assessment agents will continuously produce risk factor statements to update the state. New statements will replace existing statements with the same identifier. Meta-policies define the meaning of risk factor abstractions and values. For example, a Threat value of 7 can be defined by the meta-policy as "imminent danger".

That definition is used by the risk assessment agents in computing risk factor statements. The access control policy uses the same definition to specify access control conditions to resources. The policy decision engine, however, does not need to be aware of the meanings and can simply make syntactic evaluations. The policy decision engine will also implements aggregation and de-conflict functions according to the meta-policy. For example, two Authentication statements with values of 6 and 4 can yield a general authentication value of 8. These functions are simply hard coded. Access control policies are specified using risk factors statements joined by Boolean operators. Omitted risk factor fields are not taken into account by the policy decision engine. Omitting the identifier field means the policy statement should refer to the overall value for the risk factor.

Following is the example of access control policy:

AND{
Auth(value>7),
Threat(value<7),
Threat(ID=Gun_Shot, value=0),
OR{
Location_Zone(ID=green_zone, status =active),
Location_Network(ID=base, status=active),
},
NOT{Location_Peer(status=captured, distance<50m)}
}

IV. Conclusion

In this paper, an android application has been implemented which support context based access control policies. This will help the application to restrict the malicious data and allow the system to access the specific data and/or resources based on user context. The proposed CBAC mechanism for android systems allows smartphone users to set configuration policies over their applications' usage of device resources and services at different contexts. For example, set of restricted privileges for device applications can be set when using the device at public place, and device applications may re-gain their original privileges when the device is used at private place.

References

[1]. *J. Leyden, "Your phone may not be spying on you now – but it soon will be," http://www.theregister.co.uk/2013/04/24/kaspersky mobile malware infosec/, April 2013.*
[2]. *R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, "Placeraider: Virtual theft in physical spaces with smartphones," CoRR, 2012.*
[3]. *R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones," in Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS), Feb. 2011.*
[4]. *L. L. N. Laboratory, "Controlled items that are prohibited on llnl proporty," https://www.llnl.gov/about/controlleditems.html.*
[5]. *M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: context-related policy enforcement for android," in Proceedings of the 13th international conference on Information security, ser. ISC'10. Berlin, Heidelberg: Springer-Verlag, 2011.*
[6]. *A. Kushwaha and V. Kushwaha, "Location based services using android mobile operating system," International Journal of Advances in Engineering and Technology, 2011.*
[7]. *S. M. Furnellb, N. L. Clarkeb R. A. Bothaa, "From desktop to mobile: Examining the security experience," Computers & Security, vol. 28, no. 3-4, pp. 130-137.*
[8]. *M. Kang J. Luo, "Application Lockbox for Mobile Device Security," in 8th International Conference on Information Technology : New Generations, 2011.*
[9]. *R. Choudhary, "A Policy Based Architecture for NSA RAdAC Model," in Proceedings of the 2005 IEEE Workshop on Information Assurance and Security, West Point, NY, 2005.*