International Journal Of Engineering Research & Management Technology ISSN: 2348-4039

July- 2014 Volume 1, Issue-4

Email: editor@ijermt.org www.ijermt.org

Multi-Level Authorization in Network to Enhance Security

Prof Ajit Singh
Dean and Chairperson
BPSMV, Khanpur Kalan
Sonepat, Haryana

Tanvi
BPSMV, Khanpur Kalan
Sonepat, Haryana

Abstract: In the modern era of computers everyone is using computers and networks for their day to day processing. Whether it's a small, large or medium enterprise all depends on the networks for their processing of data. So a secure network and the communication is must to run any organization securely. Authorization is an important issue that is to be considered whenever we are talking about the network and its security. In this research paper we will discuss about the basics of the authorization and a proposed design for providing multi-level authorization in the network to enhance the security.

Keywords- Authorization, Profiling.

1. Introduction

Authorization[4] is a granting an access to the user which was authenticated earlier by entering the correct details i.e. authorization is a process of allocating the resources or the data he needed but this will be done after the authentication of the user. Most computer security systems are based on a two-step process. The first step is authentication, which confirms that a user is who he or she claims to be. The second step is authorization, which allows the user access to various resources based on the user's identity. Authoring tools is used to create a final application simply by linking objects together, such as a paragraph of text, an illustration, or a poem. Most authoring systems also support a scripting language for more complex applications [5].

User Authorization is an important network security issue that has been used for providing security on networks. The premise of authorization has always been based on access that has been granted to the user on a specific network service. Traditionally the access has been a Boolean operation; it is yes or no i.e. either it will be granted or it will be denied. Single-sign-on has been a goal for many network security schemes, whereby a user's authentication determines a user's authorization on multiple systems.

Normally the devices that connect the data networks are similar in nature and these are usually computers with a processor and a large storage with some sort of display capability. But nowadays we are having mobile devices that changes its position after a short span of time so these devices has weakened the overall security structure in the network and the problem arises whether such mobile devices should be given access or not. In order to solve this problem the devices are profiled. Profiling a device to categories its function is a

solution that can be considered to solve the problem. If a device is capable of a better encryption scheme than the other, then a higher order of access will be granted to that device. The idea of profiling the devices has been discussed in java 2 platform Micro edition (J2ME) design. The connected limited device configuration (CDLC) [2] implementation gets a subset of functions from connected device configuration (CDC) [3] profile. The CDC uses the java virtual machine interpreter, whereas the CDLC utilizes the K virtual machine (KVM). The idea of cutting down a full set of access to a sub-set of access is not a difficult concept but there is a need of deciding how the sub-set of access is determined. One way of tackling this is to use the availability of authentication mechanisms to make its decision. It means that the device is identifiable by the way it interacts with the authentication server. Profiling and authentication based on the available schemes have been used and proposed for network technologies, with no specific use of authorization. This shows that the concept is not new but the implementation of it on an authorization scheme is not impossible.

2. Security Requirements

The security requirements for a multi-level authorization design should be the following attributes: a single set of login credential, device profiling, multi-level categorization of access control, and least impact on current secure network architectures.

2.1 Single Set of Login Credentials –

A single set of log-in credential offers a similar attribute to the SSO system. The aim of a SSO system like SESAME [1] is to offer multiple accesses to services on a single network, while authenticating the user only once. Users can access or utilize different systems on a single network, based on a single set of credential. This idea is used here, the user is allowed to have multiple accesses using same set of login credential but at the same time, is limited to access, and is based on the device the user logged in from.

2.2 Profiling Techniques-

This involves the step of categorizing the different attribute and abilities that advice can handle. This will pertains other level of trust advice has on the network. It is through the use of profile, which allow for a clear review on how much "trust" advice might be imparted with. It also provides for the identification of devices that may connect to a network. This is an important task, since the identity of the device William pact the overall design no faint work. The end result of profiling will include a set of devices that fall into different categories. This allows for the convenience of handling a group of devices as one, thereby reducing complexity .This method also allows for future additions, and offers legibility. There is a disadvantage ,that some devices may fallen- between profiles .This is happening very often, with he emergence of one –device –does –all philosophy from vendors .This can be solved by either make a default in the device to a lower order of security, orto the profile of the high eror derof security ,depending on the policy of the network .Profiling devices is further discussed, where methods of automatic and manual devised entification is explored. This is first preceded with a discussion on how devices can be profiled.

2.3 Multi-level categorization of Access Control-

Categorization of the access control list relating to asterism necessary to maintain a standard list of access control across the organization. This allows for access control entries to be placed in different categories,

foreaseofadministration.Forexample,accesstoaadministrativetoolslikepasswordchanginganduserprofileupdateoldfalleneronecategoryandwebaccesswithproxyrightscouldfallunderanothercategory.Thisallowsforeaseofadministration,withtheabilitytofinetunetheaccesscontrolofeachsystem, still being an option.

2.4 Access Granting-

Whenadevicehasbeenprofiled,itisuptotheauthorizationservertodecideonhowmuchaccessthedeviceistobegranted.Therearetwoapproachestothisproblem;allowingfullaccess,andthenlimitingit,orgivingonlytherightamountofaccess.

Bothmethodsareconsideredtobeequallysecure;however,emphasisisplacedontheamountofprocessingrequired.Forthefirstmethod,thenetworkwillhavetodependonanothersystemtoreducetheaccesscontrollistdowntosize,whereasforthelattermethod,dependenceisplacedontheauthorizationservertoprocessthecorrectamountofaccesstograntandnotgiveany more than it should. This approach works well in an environment that offers Access control lists (ACL)to user during authorization. However, this does not apply to systems that depend on role-names or Role-

Based Access Control(RBAC) systems.

Rolescallforadifferentapproachtothisrequirement.TheACLsinthesesystemsarenotstoredinacentralrepositoryforretrieval,butrather,everynetworkservicecontainsrulesonwhichrolesareauthorizedforconnection.Inthiscase,eitherthesystemhastobeabletodiscernthedifferencebetweendevicesautomatically,oranintermediarysystemcouldchangeauser'sprofile,tosuitth edevicetheuserisloggininfrom.

2.5 Least impact on current secure Network Architectures-

Theaimfortheproposedsystemistohavetheleastimpactoncurrentsecurenetworkarchitectures.Thisistoensureawideracceptanceofthetechnology,whilststillpreservingthecurrentrolloutofthenetworkarchitecturethatanadministratorhas.Considerationhastobeplacedintotheintegrationofthesystem.Onecommonwayistohaveanintermediaryproxyinplace.

3. Proposed Design for Multi-level Authorization

Theproposeddesignconsists oftheusualcomponentsthatarefoundontypicalsecurityarchitecture;theUser,alogindevice,anauthenticationserver,anauthorizationserver,andthenetwork.

3.1 Operations and Implementation of Proposed Design

TheUserisanypersonwithalegitimateaccountonthenetwork.TheypossesstheLoginDevicethatwillallow themtoaccessnetworkresources.Assumptions aremadethattheuser,referredtointhissection,havelegitimaterightstothenetworkresourcesandposesnothreattothenetwork.Theusercanonlyproducetheircredentialsforaccesstothenetwork,throughtheaidoftheLoginDevices.Thesedevicesrefertoalargenumberofnetworkeddevices,rangingfromsimplePersonalDigitalAssistants(PDAs)tofullfledgeworkstations,makingthisportionofthenetworkheterogeneous.Althoughthedevicesareassumednottobetrustedbythenetwork,anassumptionhastobemadethatthemodulethatconnectstothenetworksecurityframework,istrusted.Thismoduleresidesinthelogindeviceandwillhavethetaskofprovingitsidentity.Therearesevealwaysinwichthiscanbedone.Thelogindevicewillnowactonbehalfoftheuser,tocommunicatetothesecurityserverviatheNetworkThefirstpointofcontactforthelog-

indevicewillbetheDeviceIdentificationandAuthorizationFilteringProxy.Thisproxyisputinplacetohandlethecommunicationbetweentheuserandthesecurityserver.Thiswillimpactthleastonexistingsecurityarchitectures. Atthisstage,theproxywillhandletheauthenticationofthedevice.Thisallowstheproxytotagthemessagefromtheloginde vicetotheAuthenticationServer.Placingtheproxyatthispointallowsforanadditionalfeaturetosecurity.Withthedeviceauthenticationinthemessage,theauthenticationservercannowdecideifauserhasaccessonthenetwork,andalsoiftheuserhasrightstoauthenticatethroughcertaindevices.Whentheauthenticationserverisdone,itwillcontacttheAuthorizationServernext.Thisisdoneviatheproxyagain,butthistime,theproxyjustforwardsthemessage,andwillnotmanipulateit.

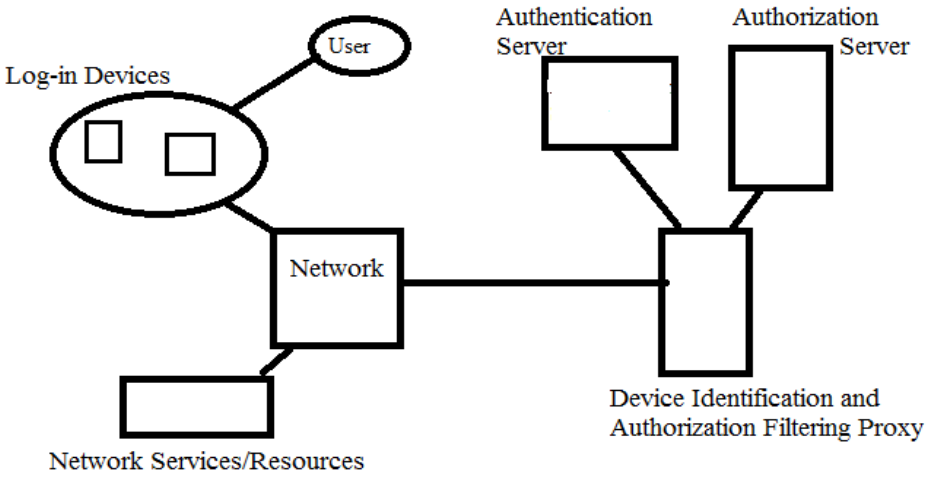

Figure1 – Proposed Design

Theauthorizationservershouldfunctionasnormal,andthenextmessageshouldbesentfromtheauthorizationserver tothelogindevice.Thismessagewillcontaintheuser'sACL.Butbeforeitgetsreceivedbythelogindevi ce,itwillhavetopassthroughtheproxyagain.Thistime,theproxywillactasafilteranddecideonthelevelofaccessausershouldhave,basedonthedevicetheyhaveloggedinfrom.ThissubsetoftheACListhenreturnedfromtheproxy,totheuser.

3.2 Device Profiling in Proposed Design

InthisproposedTechniquewewillalsoprofilethedevicestoenhancethesecurity.Developingalevelof trustbasedonthecapabilitiesofadeviceisoneofthewaystoidentifyadevice.Manydeviceshavedifferingprocessingandstoragecapabilities.Thisrangesfromsimple16MHzprocessorsfoundcommonlyinPalmPilotPDAstomulti-Gigahertzprocessorsondesktopcomputers,andstoragethatrangesfromafewhundredkilobytestogigabytesoreventerabytesofstorage.Theaimofthisistobeabletoprofileadevicebasedonitscapabilitiestohandlecryptographic calculations.Handlingtheidentificationofdevicesbyprofilingthecryptographicabilitieshasadirectrelationtotheabilityofthedevice tobesecure.

However certaindevicesdoofferbetterimpliedsecurity,withouttheneedtohaveapowerfulprocessororlargestorage.Instead,thesedevicesaretamperresistantinnature,likeasmartcard.Thismeansthattheprofilingwillstartfromthetop,betweentamperresistantdevicesandnontamperresistantdevices.Thislistwillbefurtherbrokendownintodifferentcapabilitiesofthedevices.

Theprocessofdeterminingtheprofileofadevicecanbedoneintwoways;amanualoranautomatedprocess.Bothtechniquesoffermeritsanddrawbacksatthesametime.Thebiggestconsiderationhastobetheimplicationtocommunicatingprotocolsandalsocomplexityofdesign.

Theautomaticdeviceprofilingtechniqueoffersthemostflexibility,intermsofidentificationofcurrentlyavailable devicesandfutureofferings.Anovelapproachistomeasureacryptographiccalculationintermsofthedevice'sresponsetime.Thismeasurementisthencomparedagainstasetofknownresponsetimes,therebydepriving thedevice's identification.Thisconceptissimple,butaco mplexsetofprotocolsisneededtohandleit.Otherunknownfactorslike processorbottleneckandeventransmissionmediumcongestionhavetobetakenintoconsideration.Thisisanimmensetaskforderivinganonguaranteedvalue,measuredinmilliseconds.Theothermethodforprofilinghappens manually.Alldeviceswantingtobeusedtoaccessnetworkresourceswillhavetobeidentified.Allresultsareplacedinacentralrepository,withproperidentificationtagsplacedinamoduleofthedevice.Thisapproachallowsformuch betteruseofthenetwork,andalsorequiresalesscomplexprotocol.However,profilingeverysingledeviceonanetworkwillprovetobeatediousjob.Withbothprofilingtechniquesinmind,choosingthemanualtechniqueseemsto beam ore efficient way of designing the protocol.

4. References

1. TomParkerandDenisPinkas.SESAMEV4–Overview,December1995.
2. SunMicrosystems,Inc.,901SanAntonioRoad,PaloAlto,CA94303USA.TheCLDCHotSpot^{tm}ImplementationVirtualMachine,Java2PlatformMicroEdition,2002.
3. SunMicrosystems,Inc.,901SanAntonioRoad,PaloAlto,CA94303USA.ConnectedDeviceConfiguration(CDC)andtheFoundationProfile,2001.
4. ComitteeonNationalSecuritySystems,CNSSSecretariat(101C)-NationalSecurityAgency-9800SavageRoad-STE6716-FtMeadeMD20755-6716.NationalInformationAssurance(IA)Glossary,June2006.CNNSInstructionNo.4009
5. .WilliamStallings.CryptographyandNetworkSecurity:PrinciplesandPractice.PrenticeHall,secondedition,July1998.