AUTOMATED SECURITY ASSESSMENT FRAMEWORK DESIGN FOR MOBILE APPLICATIONS

[1]Tapas Ku. Nayak[2]AdarashRoul[3] Malla Reddy Meka
Gandhi Institute for Technology, Bhubaneswar

Abstract—**With the rapid development of mobile Internet, mobileapplications are explosive growing. Due to the lack of securitysupervision of mobile applications in the mobile marketing, manysecurity issues continue to emerge. Aiming at the single functionof existing mobile application security assessment tools, which isunable to implement full range of security supervision to mobileapplications,thispaperdesignsanautomatedsecurityassessment framework for mobile applications. Based on the ideaofstaticanddynamicanalysis,theproposedframeworkcanperform security assessment respectively on mobile applications,data communication and the back-end server, and can realize theefficient and accurate security assessment on both Android andIOS platform.**

Keywords-MobileApplications;SecurityAssessment;ServerSide;Android;iOS

I. INTRODUCTION

With the continuous popularization of smart phones, thenumber of various mobile applications is also growing rapidly.At the same time, the security problems of various mobileapplications are also emerging. 360 Internet Security Centerrecentlyreleasedthe"2016Chinesemobile phonesecuritysituation report" data show that, the annual Android of 2016mobile phone users a total of 253 million people infected withmaliciousprograms,andtheaveragedailynumberofmaliciousprogram infections reached 70 thousand people[1]. With thecontinuesemergingofmobilemalware,notonlythedeveloper'sknowledgeandcopyrightcannotbeguaranteed,but also lead to the disclosure of information or even economiclosses. The security requirements of mobile applications havebecomeamajorprobleminthedevelopmentof theentireapplicationmarket.

Thebiggestreasonformobileapplicationsecurityproblemsisthatmostdevelopersintheapplicationdevelopment, only pay attention to application developmentspeed, while ignoring the safety of the application, resulting inall kinds of vulnerability are not found and repaired in time.Because of the open source characteristic of Android system,the application of Android platform has become the key targetof malicious virus attack. According to relevant data shows,Androidplatformhasnearly97%applicationsexistvulnerabilities, and the average amount of vulnerabilities ashigh as 40[1]. In addition, the security status of iOS platformapplications is equally optimistic. Research shows that the iOSsystem,knownforitssecurity,isalsoa hubforvulnerabilities.

The XcodeGhost incident, let NetEase cloud music, WeChat,12306, CITIC Bank, andother well-known domesticAPPsinfectedwiththirdpartymaliciouscode.

Anautomatedsecuritytestingplatformformobileapplications will help application developers to dig out thehiddendangersofmobileapplications,andeffectivelyimprovetheir security monitoring capabilities for mobile applications.Itssignificanceliesin:

1) With the given description and suggestions, developerscan understand the security risks of the software, so that thevulnerabilitiesofmobileapplicationcouldbetimelyandcorrectlydetectedandeliminated.

2) Thenecessaryguidanceforresearchanddevelopmentofmobileapplication'son-lineoperation,couldimprovethesafety and reliability of business, which will reduce the lossescausedbythesafetyaccidenttotheminimum.

3) The security risk analysis of application could provideaccurate data and information for mobile application's design,updateand safetyoptimization.

II. RELATEDWROD

Mobile application security is a rapidly developed field,many new platform architecture, new industry environment,new attack methods, goals and means emerging. At present, inadditiontothetraditionalattacks,thesecurityproblemofmobileplatformsaremainlyreflectedinthreeaspects:

1) The local mobile application problems, which mainlyrefers to the risk of mobile application in configuration, code,compiler process. These vulnerabilities will not only affect thestability of its operation, they also may lead to data loss oridentityhijacking;

2) Thedatacommunicationsecurityproblem,whichmainlyhappenedinthecommunicationprocessbetweenmobileapplicationandserver,suchascleartransmission,thecertificate without checking. These vulnerabilities are likely tobeusedtoperformmaninthemiddleattack,orprotocolanalysisandtraffichijacking,whichharmtheinterestsofmanufacturers;

3) Theserversidesecurity.Mostmobileapplicationinteract with the server by WEB API services, which combinemobile security with WEB security. The attack methods forthiskindofsecurityproblemsaresimilartothoseofthe traditional PC attacks, and also can cause the most damage.Once all the business data is stored on the server, it is withoutdoubtadisaster.

In view of the security threats of these mobile fields, theresearchonmobilesecurityismainlycarriedoutinthefollowingaspects:

1) Access control and privacy protection. The key lies inthemonitorandauthoritycontrolofuseraccesstoprivacydata.RepresentativeresearchincludestheTISSAaccesscontrolschemeproposedbytheNorthCarolinaStateUniversityresearchers[2]andtheSEAndroidproject[3];

2) Mobile operating system security testing. Different fromthe traditional operating system safety, the database of mobilesystemvulnerabilitieshasnotbeenestablishedcurrently,sothesecurityevaluationbasedonvulnerabilityisdifficulttoachievein the mobile terminal. Therefore, security function testing,combined with security risk assessment method is suitable forthe security testing of mobile applications[4]. The key point ofthe security function test is to test whether the system to betested has some specific security functions under a securitymechanismintheevaluationcriteria.Whilebasedontheresults of the security function test, the assessment results ofentire operating system or system security mechanisms couldbegiven.

3) Mobileapplicationsecuritytestingandprotection.Aroundthemaliciouscodedetection,applicationstaticanalysis,dynamic analysis and other aspects, there are many in-depthtechnicalresearchandtooldevelopment.Especiallyintheaspect of automatic testing of mobile applications, the Tencent,Alibaba, 360 and other giants have released products of mobileapplication security testing based on the static analysis anddynamic adjustment of the core functions[5]. But most currentproductsarejustforthelocalmobileapplicationsecuritytesting, lacking of security assessment in data

communicationand server side. In the aspect of safety reinforcement, there aremany commercial companies such as 360, BANGCLE, IJIAMIlaunchedtheirproducts[6].Afterusingtheseproductsforsecurity enhancement, mobile applications can have the abilityofanti-crackandanti-reverse.

Thispaperfocusesonthedesignofsecuritytestingplatform for mobile applications. Despite currently there aremany mobile application security testing tools in the market,problems still exist, such as vulnerability description is notaccurate, vulnerability characteristics is not complete, the falsepositive rate of testing result is high, and lack of testing toolsfor iOS applications. For that reasons, this paper designs anautomatic testing framework. Based on the static and dynamicanalysisidea,testingmethodsbothonlocalmobileapplication,data communication and server side are proposed respectively,which can realize efficient and accurate safety assessment ofmobileapplicationsonbothAndroidandiOSplatform.

III. AUTOMATIONSECURITYTESTINGFRAMEWORK

A. FrameworkOverview

As shown in Figure 1, the proposed mobile applicationsecurityautomationtestingframeworkmainlyincludesuser

interactionmodule,shelldetectionengine,staticanalysisengine, dynamic analysis engine, penetration testing engine,andreportgenerationmodule.

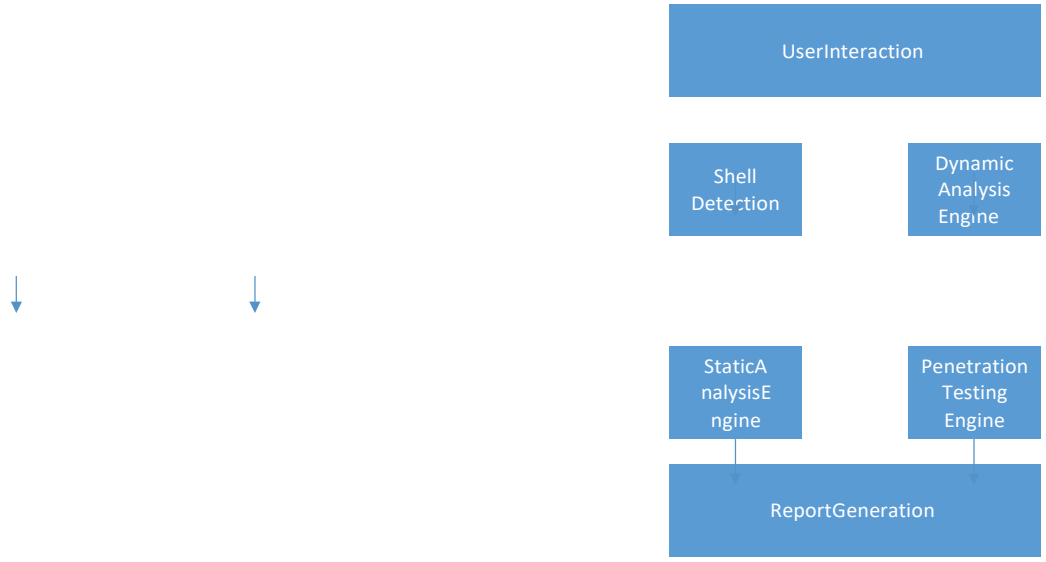

Figure1.Frameworkofsecurityassessment formobileapplications

User interaction module: Users can submit installation filesof mobile application (APK or IPA files), watch the evaluatingprogressandresults,anddownloadtheevaluatingreportsonlinethroughthismodule.

Shell detectionengine: Beforestatic analysisofmobileapplications, shell detection should be processed first. Staticanalysis engine will be customized according to the results ofidentification of shell. The main principle of shell detection iscomparing the feature of shell with the knowledge base, whichisgeneratedbyanalyzingofthecurrentmainstreammanufacturer'sreinforcementtechnology(suchasBANGCLE,IJIAMI,Naga,360andsoon),andthenmakeajudgment.

Static analysis engine: This engine can get the programsource code by disassembly and decompile technology, andthen tests the check list by analyzing the control flow and dataflow in the source code. Static analysis engine will performdifferent operations according to the shell detection result. Ifthe mobile application do not have shelling protection, thisenginewilldisassembletheprogramsourcecode,andcarryoutsafety inspection of the code and the configuration. Otherwise,this engine will mainly do compliance verification of programconfiguration.

Dynamicanalysisengine:Thisenginedeterminethebehavior of a program by collecting the output informationwhen the application is running in a custom operating system.BydeeplycustomizingtheAndroidoperatingsystem,dynamicanalysisenginecancapturealargeamountofruntimeinformation of application, including: file operation, functioncall,logoutput,networktraffic,messagingandsoon.Basedontheseinformation,thisenginecandetermine whethertheprogramhassecurityrisks.

Penetration testing engine: This module will make use ofsensitive information or communication data which is exposedin the static and dynamic analysis to determine the location ofserver,andthenperformpenetrationtestingtotheserver.This

engine mainly combines the traditional web scanner and theexploitsoftheopenvulnerabilitylibrarytoexploitand validatethe vulnerabilities, which basically covers all kinds of websecurityvulnerabilities.

Report generation module: According to the testing resultsstored in the database, this module will generate the final testresults in the form of PDF and WORD, in which each test itemin check list will be given with the vulnerability description,testresultsandrepairsuggestion.

Thefollowingwilldescribe thetechnical details ofthestatic analysis engine, the dynamic analysis engine, and thepenetrationtestingengine.

B. StaticAnalysisTechnology

The static analysis module is composed of two parts, thebinaryanalysismoduleandthesourcecodeanalysismodule.

For Android applications, the binary analysis module canrestore the source code of application by using the officialGoogledisassembletools,andthencallthesourcecodeanalysismoduletoperformsecuritytest.

For iOS applications, for the sake of closure feature, thebinaryanalysismodulecannotdirectlydisassemblethepackageintomorereadablesourcecode.Therefore,thismoduledirectlyanalyzetheunpackediOSbinaryfilebycheckingthedynamiclinklibrary,compiler options in thebinaryheader,directandindirectsymboltables,andthendetermine what kind of security sensitive function were used.And the other binary resource files, such as plist configurationfiles, database files, pictures and cache files are submit to thesourcecodeanalysismoduleforanalysis.

Thesourceanalysismodulemainlyanalyzethesourcecode(Android) or packaged resource files (iOS) analysis generatedbythebinarypackageanalysismodule.Basedonthebyte-codecomparingtechnologyofvulnerabilityfeatures,thesourceanalysis module could locate the security sensitive functionsand check whether there are any sensitive information leakagerisks.

C. DynamicAnalysisTechnology

As shown in Figure 2, the dynamic analysis module installand run the APK file to be tested on the customized virtualAndroid system, while allowing the log monitoring engine,component testing engine, vulnerability fuzz engine and crashrecoveryengineworktogethertocapturetheapplicationbehavior data, such as monitor and intercept log output andcommunicationdata,featurethe behaviorofapplicationandsoon.Subsequently,theinterceptedapplicationbehaviordatawillbeusedandimportedtothedynamicanalysismodulestodetermine whether the vulnerability exists, thus achieving theoverallautomateddynamic detectioneffect.

Logmonitoringengine:thelogofthevirtualAndroidsystem is passed into the file stream and stored in the local testenvironment. At the same time, a child thread is created tomonitorthefilestreamcontinuouslytoachievetheeffectoflogmonitoring.

Component testing engine: This engine sequentially opensorcallseachcomponenttowatchhowtheapplicationisrunning.

Vulnerabilityfuzzengine:ThisengineinteractswithvirtualAndroidsystem,andsendthecustomizedActionorExtra(withcontrollable length, content format) intent into the componentlisted in the Manifest.xml file with Intent Filter function, andthenobservethecomponent'soperationsituation.Ifthecomponentdonotfilteritsdatarigorously,theremayexisthighrisk vulnerabilities such as local denial of service and SQLinjection.

Crashrecoveryengine:Thisenginemonitorscommandoperation in real-time, and provides the interfaces with whichdynamic detection modules could ultimately communicate withthe virtual Android system. If the Android system crashes dueto application running,the initializationstate is resumedandthenextcheckpointtobedetectedcouldbecontinuednormally.

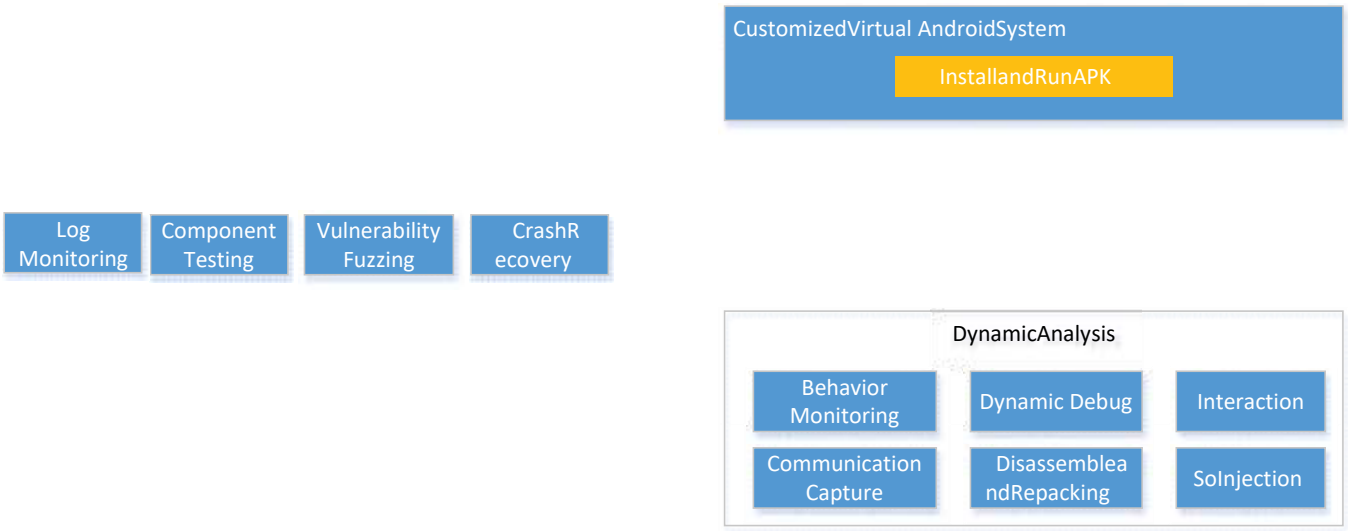

Figure2.ProcessesandModulesofdynamicanalysis

D. ServerSide Penetration Testing

The automated server side penetration testing is a highlightof proposed framework. It can perform vulnerability scanningandsafetyevaluationfortheapplication'sserversideautomatically, so as to realize the multi dimensions of mobileapplicationsecuritytest.

Theprocessofmobileapplicationserverpenetrationtestingis similar to the traditional vulnerability scanning process. Ituses the web scanning engine to do the vulnerability scanningfortheapplicationinterface.Butthedifferenceisthattheapplicationinterfaceisusuallyclearlyknownintraditionalwebapplications, but in mobile applications is not. The interfacesneedtobeextractedby analyzingthecommunication databetweenapplicationclientandserverside,whichwillundoubtedly increase the degree of difficulty, especially if thecommunicationchannelisencrypted.Howtocapturetheplaintextdatafromencryptedcommunicationchannelisagreatchallenge.

In this paper, a common method for capture plaintext databasedonOpenSSLlibraryinjectionisproposed.Thedataencryptioninmobileapplicationisusuallyrealizedbytheopen

source OpenSSL library. Specifically, mobile applications ofAndroidplatformmainlycallrelatedfunctionsrealizedinlibssl.so library to encrypt communication data. As shown inFigure 3, the two most critical functions in the libssl.so libraryare SSL_WRITE and SSL_READ, which are used to send andreceivedata,respectively.Whensendingdata,Androidapplication will pass the plaintext data to the SSL_WRITEfunctiontoencryptthedataandfinallysendout.Whenthedataisreceived,theencrypteddatawillbedecryptedbytheSSL_READ function to plaintext data, which finally is passedtotheAndroidapplication.

penetrationframeworkcanbeeasilyextendedbyintegratingplug-ins.

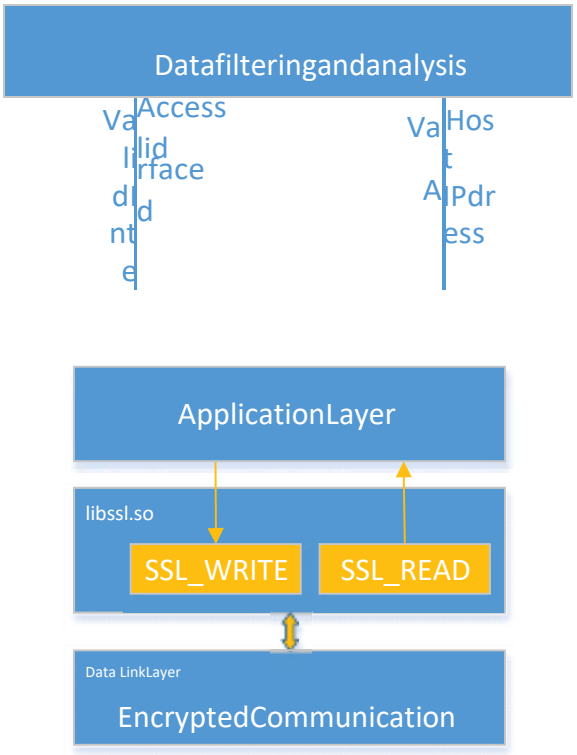

Figure3.Systemcallflowofdata encryptionandtransmission

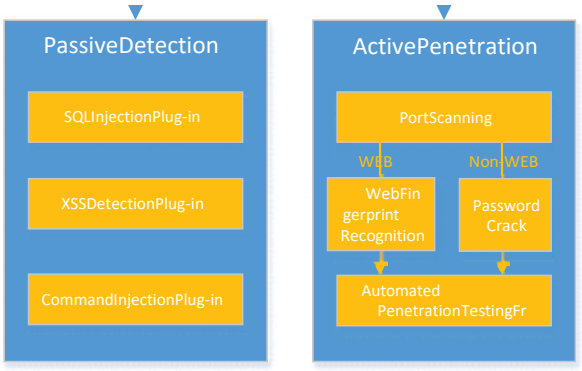

Figure4.Frameworkofautomatedpenetrationtest

SincetheAndroidsystemkernelcanbecustomized,wecancertainlymodifytheopensourcelibssl.solibrary.Sowe

IV. SUMMARY

Inthispaper,amobileapplicationautomationsecuritytesting framework is proposed. This framework support bothAndroid and iOS system, and integrated static analysis anddynamic analysis double engine to realize a multi dimensionvulnerabilitydetectionandevaluationforbothAndroidand realizedaplaintextdataacquisitioninterfaceintothecorrespondingSSL_WRITEandSSL_READfunctionandreplaced the re-compiled libssl.so library in the customizedvirtualAndroidsystem,thenwecancaptureanyencrypteddatamessage inthecommunicationprocess.

After solving the problem of intercepting communicationdata, the next step is how to perform server penetration testingautomatically.AsshowninFigure4,theautomatedpenetrationtestengineconsistsofthreemodules:datafilteringandanalysismodule,passivedetectionmoduleandactivepenetrationmodule. Specifically, the data filtering and analysis module isin charge of plaintext data capture, and extract the effectivehost IP address and access interface between application andserver side, which will be passed to the passive and activedetectionmodule.Accordingtotheaccessinterfaces,thepassive detection module could exploit OWASP mainstreamvulnerabilities by integrating plug-ins such as SQL injection,crosssitescriptingandcommandinjection.Theactivepenetration module is an effective complement to the passivedetection module, which mainly completes the detection ofunknowninterfacesoftheserverside.Inspiredbythetraditional penetration testing idea, this module collects theinformationofportscanningofserverside,andthenimplements the automated penetration testing by integratingtheMetasploitpenetrationframework.Inaddition,theoverall iOSapplications,whichhave90%marketshareinmobilefiled.With thegiven vulnerability knowledge base,the proposedframeworkcouldhelpmobileapplicationdevelopersandrelated management and technical personnel to improve theirsecurity monitoring capabilities of mobileapplications, andhelpenterprisestobuildtheirownmobilesecuritystandards.

REFERENCES

[1] 360InternetSecurityCenter.MobilesafetyreportinChinain2016[R]. Beijing:Qihoo360TechnologyCo.Ltd.2017

[2] Yajin Zhou, Xinwen Zhang, Xuxian Jiang, et al. Taming Information-Stealing Smartphone

Applications(on Android)[C]. In Proceedings ofTRUST2011, Pittsburgh, 2011.

[3] S. Smalley. The Case for Security Enhanced (SE)Android[J]. AndroidBuildersSummit, 2012.

[4] JieTang,Quan-fangLu,HongWen.IntelligentMobileTerminalSystemSecurityRiskAssessmentBasedonAHPAlgorithm[J]. Information Securityand Technology.2013(03)

[5] Jing-chaoFeng.Designandimplementationofautomatictestingplatformbased on Android system[D]. JilinUniversity. 2015.

[6] Yuan-yiXia,LeiWang,Min-lingWang.MobileApplicationReinforcementMethodinIntelligentTerminal.INFORMATION&COMMUNICATIONS. 2016(2).