DOI: 10.13203/j.whugis2008.10.024
第33卷第10期 武汉大学学报·信息科学版 Vol.33 No.10
2008年10月 Geomatics and Information Science of Wuhan University Oct. 2008

文章编号:1671-8860(2008)10-1062-05 文献标志码:A

基于信任度量的软件下载服务框架

李 建[1,3] 何永忠[2] 徐开勇[1]

(1 信息工程大学电子技术学院,郑州市商城东路12号,450004)
(2 北京交通大学信息安全体系结构研究中心,北京西直门外上园村3号,100044)
(3 广西军区司令部,南宁市植物园路,530021)

摘 要:针对移动终端软件下载方案缺乏信任度量而存在安全隐患的问题,利用身份管理的信任机制、可信计算安全存储和远程平台验证等安全特性,提出了基于信任度量的软件下载服务模型,设计了软件下载服务流程,研究了软件下载服务协议,分析了协议的安全性,比较了不同软件下载方案的安全性,分析结果表明该方案有效地提高了软件下载服务的安全性能。

关键词:信任度量;可信计算;身份管理

中图法分类号:T309

近几年来,随着移动终端功能的不断攀升,它已从只安装设备制造商提供软件的封闭平台,成为了可以从任何软件源安装各种软件的开放平台。由于移动终端操作系统和硬件存在较多的安全漏洞,一些病毒和恶意代码通过软件下载侵入移动终端[1,2]。

研究人员针对移动终端软件下载提出过一些安全方案[3-7]。主要是对下载软件进行了加密和完整性保护,但存在的问题是移动终端下载代理必须绝对信任下载服务器,软件下载前它既不检查服务器的可信度和平台状态,下载后又不进行恶意代码检测。因此,仍然不能保证下载软件的安全。故这种信任是没有根据的,也是有害的,必须将正确的信任机制引入下载服务以确保软件下载安全。

身份管理就是确保仅仅让已知的和授权的身份访问网络、系统和数据的策略、规则、方法和系统[4]。在身份管理体系结构中,各实体的行为是建立在信任基础上的。所谓信任就是指一个范围,在这个范围内,在给定的条件下一方以一个相对安全感愿意依靠另一方,即使可能产生负面结果[5]。

1 可信移动平台

为解决移动终端的安全问题,提供端到端的安全移动解决方案,2004年可信计算组织(TCG)的三个主要成员NTT DoCoMo、IBM、Intel联合制定了可信移动平台(TMP)的硬件体系结构、软件体系结构和协议三个技术标准草案[5-11]。

令S_{K_T}、S_{K_A}、$S_{K_{AD}}$、S_{AIK}分别代表由SRK加密保护的信任密钥、审计密钥、下载代理认证密钥和平台身份认证密钥。T、U、V分别由K_T、K_A、K_{AD}加密保护的信任、审计文件和认证数据,PCR为平台状态信息,W为使用AIK私钥对平台状态的签名,则有:

$$S_{K_T}=E_{K_{\mathrm{SRK}}}(K_T)\quad T=E_{K_T}(\mathrm{Trust})$$
$$S_{K_A}=E_{K_{\mathrm{SRK}}}(K_A)\quad U=E_{K_A}(\mathrm{Audit})$$
$$S_{K_{AD}}=E_{K_{\mathrm{SRK}}}(K_{\mathrm{AD}})\quad V=E_{K_{\mathrm{AD}}}(\mathrm{AD}_T)$$
$$S_{\mathrm{AIK}}=E_{K_{\mathrm{SRK}}}(\mathrm{AIK})\quad W=\mathrm{Sig}_{\mathrm{AIK_{PRI}}}(\mathrm{PCR})$$

2 可信身份体系下载服务流程

可信身份体系采用独立身份管理体系结

收稿日期:2008-08-28。

项目来源:国家863计划资助项目(2006AA01Z440;2007AA01Z40)。

构[12]。在该下载服务模型中,移动终端采用基于可信移动平台的可信移动设备,下载服务/证书提供者采用可信密码模块的应用服务器。下载代理是基于 TCM 的可信下载应用系统,它通过向下载服务/证书提供者提供身份标识和相应的证书等认证信息,软件下载服务/证书提供者经过身份认证,根据 RBAC(基于角色的访问控制)或 PBAC(基于策略的访问控制),向下载代理提供相应的下载服务。本方案将下载过程分为下载前、下载中和下载后三个阶段,对每一阶段都实施信任度量或加密、完整性保护,以确保下载服务的安全。

基于信任度量的可信身份体系下载服务流程分为可信移动平台的软件下载流程和可信平台下载服务提供者的软件下载流程,分别如图 1 和图 2所示。

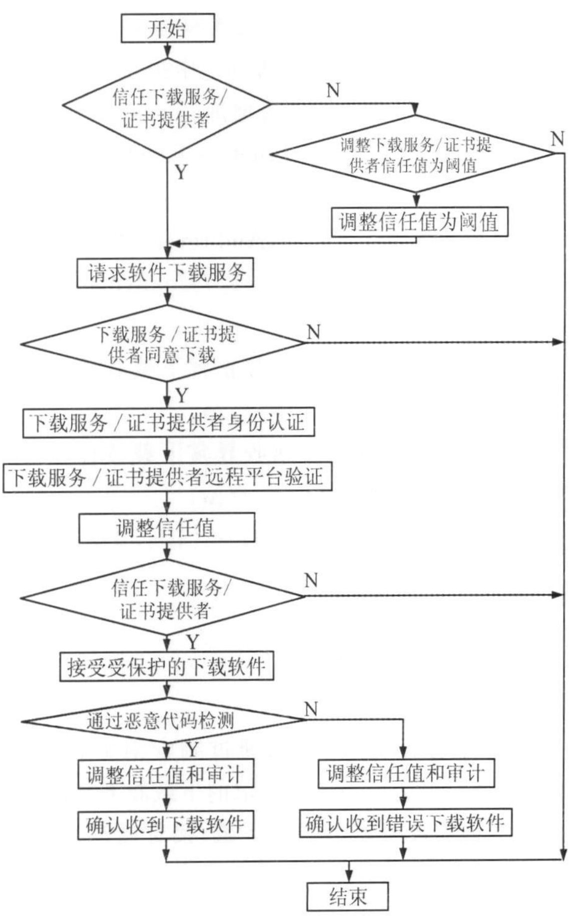

图 1　可信移动平台软件下载流程图

Fig.1　Flow Chart of Downloading Software for TMP

3　可信身份体系下载服务协议

本方案将软件安全下载分为下载前、下载中和下载后三个阶段,如图 3 所示。为了研究方便,

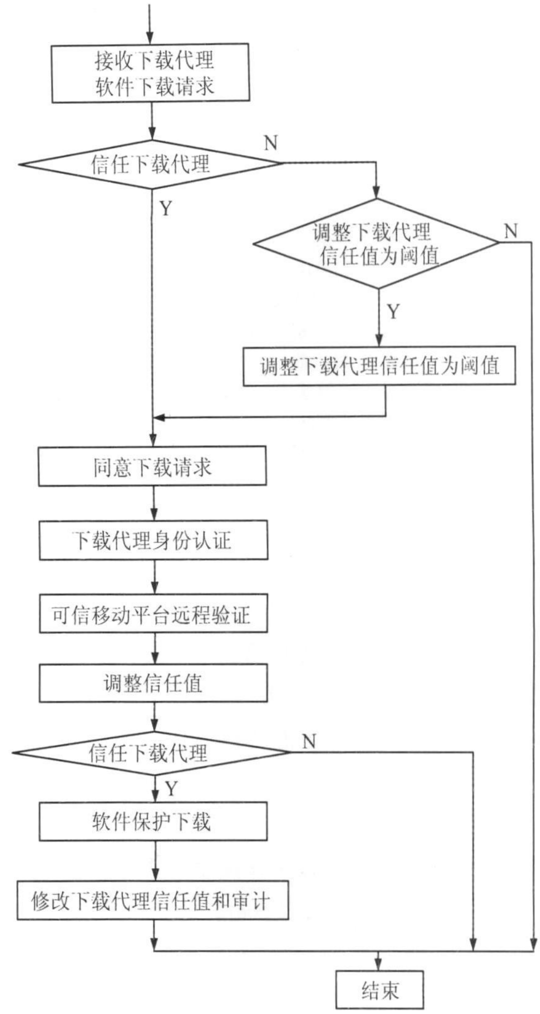

图 2　软件下载服务提供者软件下载流程图

Fig.2　Flow Chart of Downloading Software for Service Provider

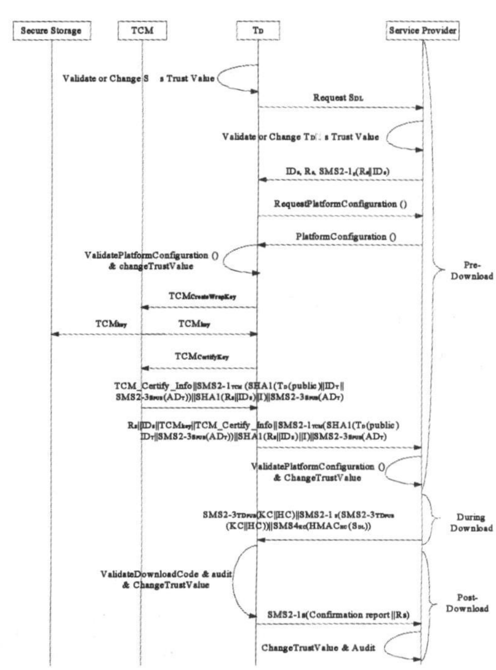

图 3　软件下载协议

Fig.3　Protocol of Downloading Software

先定义以下的缩略语如表1所示。各密码算法均采用文献[12]建议的安全算法。

表1 符号定义

Tab.1 Definition of Symbol

缩略语	含义	缩略语	含义
T_D	下载代理	ID_T	下载代理身份
AD_T	认证数据	S	服务/证书提供者
TCM	可信密码模块	S_{DL}	被下载的软件
$M \parallel N$	数据项 M 和 N 串接	ID_W	实体 W 的身份
W(public)	实体 W 的公钥	W(private)	实体 W 的私钥
R_W	实体 W 随机数	$Cert_W$	实体 W 的证书
SMS2-1	数字签名算法	SMS2-3	公钥加密算法
SMS3	密码杂凑算法	SMS4	对称密码算法
HMAC	消息验证码算法	$Trust_S$	T_D对 S 的信任值
$Trust_T$	S 对 T_D的信任值	$Trust_{ST}$	T_D对 S 的信任阈值
$Trust_{TT}$	S 对 T_D的信任阈值	Δt	信任变化值
Valid(A,B)	$A \geqslant B$,结果为1	Compare(X,Y)	X 和 Y 相等为1

3.1 假定

协议开始时,最初状态是下载代理对下载服务提供者的信任值为阈值 $Trust_{ST}$,下载服务提供者对下载代理的信任值为阈值 $Trust_{TT}$,下载服务可以正常进行。

3.2 软件下载服务协议

4.2.1 软件下载前的信任度量和身份认证

1) T_D: X=Valid($Trust_S$, $Trust_{ST}$)

2) $T_D \rightarrow S$: Request for S_{DL}

3) S: Y=Validate($Trust_T$, $Trust_{TT}$)

4) $S \rightarrow T_D$: ID_S, R_S, SMS2-1_S($R_S \parallel ID_S$)

5) $T_D \rightarrow S$: RequestPlatformConfigur ation()

6) $S \rightarrow T_D$: I=Eventlog()

J=SMS2-1_{TCM}(PCR)

K=Credentials

7) T_D: X=$\mathrm{Verify}_{AIK_{PUB}}$($J$)

Y=SHA1(I)

Z=Compare(X,Y)

如果通过远程平台验证,则增加信任值并继续进行软件下载:$Trust_S = Trust_S + \Delta t$。

如果未通过远程平台验证,则减小信任值并退出软件下载:$Trust_S = Trust_S - \Delta t$ 。

8) $T_D \rightarrow$TCM: $TCM_{CreateWrapKey}$

9) TCM$\rightarrow T_D$: TCM_{key},

TCM$\rightarrow$Secure Storage: TCM_{key}

10) $T_D \rightarrow$TCM: $TCM_{CertifyKey}$

11) TCM$\rightarrow T_D$:

TCM-Certify-Info $\parallel$ SMS2-1_{TCM} (SHA1(T_D(public) $\parallel ID_T \parallel$ SMS2-$3_{S_{PUB}}$ (AD_T)) $\parallel$ SHA1($R_S \parallel ID_S$) $\parallel$ I) $\parallel$ SMS2-$3_{S_{PUB}}$ (AD_T)

12) $T_D \rightarrow S$: $R_S \parallel ID_S \parallel TCM_{key} \parallel$ TCM-Certify-Info $\parallel$ SMS2-1_{TCM} (SHA1(T_D(public) $\parallel ID_T \parallel$ SMS2-$3_{S_{PUB}}$ (AD_T)) $\parallel$ SHA1($R_S \parallel ID_S$) $\parallel$ I) $\parallel$ SMS2-$3_{S_{PUB}}$ (AD_T)

13) S: O=Check(I)

如果通过远程平台验证,则增加信任值并提供下载服务:$Trust_T = Trust_T + \Delta t$。

如果未通过远程平台验证,则减小信任值并禁止下载服务:$Trust_T = Trust_T - \Delta t$。

3.2.2 软件下载中的信息保护

14) $S \rightarrow T_D$: SMS2-$3_{T_{D_{PUB}}}$(KC $\parallel$ HC) $\parallel$ SMS2-1_S(SMS2-$3_{T_{D_{PUB}}}$(KC $\parallel$ TC)) $\parallel$ $\mathrm{SMS4}_{KC}$(HMAC_{HC}(S_{DL}))

3.2.3 软件下载后的代码检测和信任度量

15) T_D: 如果通过文献[12]中提出的判别恶意代码的规则检测,信任值增加:$Trust_S = Trust_S + \Delta t$;反之信任值减小:$Trust_S = Trust_S - \Delta t$。形成审计文件:

$Audit_T$={ID_T, Time, Auditevent, Result}

16) $T_D \rightarrow S$: SMS2-1_S(ConfirmationReport)

如果下载代理确认接收正常下载软件,则增加信任值: $Trust_T = Trust_T + \Delta t$。

如果下载代理确认接收异常下载软件,则减小信任值: $Trust_T = Trust_T - \Delta t$。

形成审计文件: $Audit_S$ = {ID_S, Time, Auditevent, Result}。

4 安全性分析

1) 信任度量。首先,通过判定对方信任初值,可以禁止达不到信任要求的下载服务/证书提供者或移动设备进行软件下载;接着通过下载双方的远程平台验证,对未通过平台验证的一方减少其信任值并中止其软件下载服务;最后,移动终端下载代理对已下载的软件进行恶意代码检测,对未通过检测的减少下载服务/证书提供者的信任值,删除下载软件,向下载代理/服务提供者发出接收不正确的确认信息。而下载服务/证书提供者,在收到接收不正确的确认信息后,将减少下载代理信任值,为今后的下载服务提供信任参考。

2) 下载软件的机密性。本方案使用国产加密算法SMS4和对称密钥保护下载软件 S_{DL} 的安

全,而对称密钥由可信移动平台下载代理公钥加密后送到可信移动平台,而对应的下载代理私钥是受到 TCM 严格保护的,即外来程序无法得到和访问它。如果下载服务提供者有效地保护了对称密钥的安全,一个攻击者通过截获加密保护后的信息,企图提取软件明文信息,其困难程度相当于大整数分解问题 FAC。显然,已知公钥,要推出私钥,在计算上是不可能的。

3) 下载软件的完整性。下载过程中调用信息认证码 HMAC 保护下载软件的完整性,HMAC 密钥与 3)中的对称加密密钥实施了相同的保护,因此,它也达到了 TCM 的保护的安全等级。

4) 数据源认证。由协议的第 11 步可以看到,下载服务/证书提供者对加密密钥 KC 和完整性验证密钥 TC 进行了签名,可信移动平台的下载服务代理 T_D通过验证签名,可以确认数据包来自于下载服务/证书提供者。一个攻击者如果要伪造向下载代理发送的下载软件就必须获得下载服务/证书提供者的签名私钥,而下载服务/证书提供者也是基于 TCM 的平台,其私钥也是受到了 TCM 的严格保护,因此,攻击者要获得签名私钥是不可能的。

为了更好地说明本方案的优势和特点,现将几种下载方案的安全性能进行比较,如表 2 所示。

表 2　三种软件下载方案安全性比较

Tab.2　Comparison of Security Between Several Download Scheme

安全特性	Gallery 方案	Gehrmann 方案	本方案
信任度量	不支持	不支持	支持
安全预警	不支持	不支持	支持
降低下载风险	不支持	不支持	支持
双向认证	支持	支持	支持
软件加密保护	支持	支持	支持
软件完整性保护	支持	支持	支持
数据源认证	支持	支持	支持
抵抗重放攻击	支持	不支持	支持
抵抗中间人攻击	支持	支持	支持
认证信息保护	不支持	不支持	支持
结果审计	不支持	不支持	支持
接收确认	不支持	不支持	支持
软件恶意行为检测	不支持	不支持	支持
软件正确性检测	不支持	不支持	支持
下载软件类别检测	不支持	不支持	支持
软件恢复功能	不支持	不支持	支持
移动平台完整性检测	支持	支持	支持
服务器完整性检测	不支持	不支持	支持

信任作为一个反映服务/证书提供者和下载代理行为和状态的客观物理量,它是动态的。如何使它与身份、角色、策略结合,构成基于动态信任和身份等要素访问的控制模型,使之能够对下载代理的访问权限进行更细粒度的控制,将是今后要研究的一个重要方向。

参 考 文 献

[1] Murmann T, Rossnagel H. How Secure are Current Mobile Operating Systems[EB/OL]. http://sec. cs. kent. ac. uk/cms2004/Program/CMS2004final/p2a2.pdf,2008

[2] Cheng J, Wong S H Y, Yang Hao, et al. SmartSiren: Virus Detection and Alert for Smartphones[C]. The 5th International Conference on Mobile Systems Applications and Services, New York, 2007

[3] Gallery E, Tomlinson A. Protection of Downloadable Software on Sdr Devices[EB/OL]. http://www. sdrforum. org/pages/sdr05/2. 6%20Networking%20and%20Security%202/2.6-04%20Gallery%20et%20al.pdf,2008

[4] Cook P G. Wireless Software Download Security[EB/OL]. http://www. sdrforum.org/uploads/pub_ 17683004_i_ 0069 _v0_ 00_ wireless_ securit y_06_14_04.pdf, 2008

[5] Gehrmann C G, Stahl P. Mobile platform security[EB/OL]. http://www. Ericsson. com/ericsson/corpinfo/pub liccations/review/2006_ 02/files/mobile_ platform_ security.pdf, 2008

[6] Hoffmeyer J, Pyung I L, Ndar M M, et al. Radio Software Download for Commercial Wireless Reconfigurable Devices[J]. IEEE Radio Communication, 2004,42(3):26-32

[7] DoCoMo NTT, IBM,Intel. Trusted Mobile Platform Specification Document [EB/OL]. http:/xml. coverpages.org/TMP-HWAD v10.pdf,2008

[8] National E-Health Transition Authority. Identity Management Glossary of Terms[EB/OL]. http://www.nehta.gov.au/ index.php? option=com_docman&task=cat_ view& gid= 152& Itemid=139,2008

[9] Mcknight D H, Chervany N L. The Meanings of Trust[J]. Trust in Cyber-Societies- LNAI, 2001,2246:27 -54

[10] Barbara Fichtinger, BSc. Trusted Infrastructure for Identities[EB/OL]. http:// andreas. schmidt. novalyst.de/ docs/Fichtinger_ Trusted_ Infrastructures_for_Identities.pdf,2008

[11] 国家密码管理局,可信计算密码支撑平台功能与接口规范[EB/OL]. http://www. oscca. Gov.cn/UpFile/File64.PDF,2008

[12] 王育民,刘建伟. 通信网的安全——理论与技术

[M].西安:西安电子科技大学出版社,2002

第一作者简介:李建,博士生,主要研究方向为信息安全、计算机网络安全。
E-mail:pauljli@sina.com

Software Download Framework Based on Trust Measurement

LI Jian[1,3] *HE Yongzhong*[2] *XU Kaiyong*[1]
(1 Institute of Electronic Technology, Information Engineering University, 12 East Shangchengd Road, Zhengzhou 450004, China)
(2 School of Computer and Information Technology, Beijing Jiaotong University, Xizhimenwai, Shangyuanchun, Beijing 100044, China)
(3 GuangXi Military Area Headquarters, Zhiwuyuan Road, Nanning 530021, China)

Abstract: According to the fact that there are some secure faults in software download schemes due to the lack of trust measurement in software download for mobile equipments, making use of trust mechanism of identity management and secure characteristics such as integrity verification, protect storage, domain isolation, access control and remote platform verifying trusted computing possess, software download service model based on trust measurement of trusted identity management architecture has been put forward, software download service process has been designed, software download service protocol has been studied, the security performance of the protocol has been analyzed, the security performance comparison between several software download schemes has been made, the result shows that the scheme improve security performance of software download effectively.

Key words: trust measurement; trusted computing; identity management

About the first author: LI Jian, Ph.D candidate. His main interest is security of information and computer network.
E-mail: pauljli@sina.com

(上接第1061页)

Active Steganalysis for Stego-image Based on HMT and ICA

LIU Xiaoqin[1] *WANG Jiazhen*[1] *XU Bo*[1] *DENG Gaoming*[1]
(1 Dept. of Computer Engineering, Ordnance Engineering College, 97 West Heping Road, Shijiazhuang 050003, China)

Abstract: Two copies of stego-image are needed in the active steganalysis proposed by Chandramouli, as an improvement, a method of active steganalysis is proposed in which only one copy of stego-image is needed and the practicability is enhanced. An estimate of a cover image by wavelet-domain hidden Markov tree (HMT) is obtained; and the estimate is regarded as another stego-image which is different in the embed ratio. Then cover image and the secret message are separated by using the independent component analysis (ICA). Simulation experiments validate the advantage of HMT model, and give the results of blind separation.

Key words: active steganalysis; HMT model; independent component analysis; simulation

About the first author: LIU Xiaoqin, Ph. D candidate, she is mainly engaged in research on information security.
E-mail: liuxiaoqin1121@163.com