基于 TNC 的网络终端认证模型设计

金 雷 徐开勇 李剑飞 杨天池
(信息工程大学密码工程学院 河南 郑州 450004)

摘 要 针对可信计算平台终端在网络连接认证时存在的安全隐患,提出一个基于可信网络连接框架的网络终端认证模型 TNTAM。该模型通过加入身份认证系统模块、信息访问鉴别模块 IADM 和引入策略管理器来加强终端认证的安全性,实现了用户、改进的认证智能卡以及可信终端三者间的相互认证,并确保了可信终端请求网络服务的可信性和通信安全。对 TNTAM 模型的具体应用流程进行了设计。最后对比分析表明,该模型减小了可信终端在网络认证时存在的安全隐患并为加强终端认证安全提供了一种思路。

关键词 可信终端 智能卡 可信网络连接 终端认证模型 应用流程

中图分类号 TP309 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2015.12.076

DESIGN OF NETWORK TERMINAL AUTHENTICATION MODEL BASED ON TNC

Jin Lei Xu Kaiyong Li Jianfei Yang Tianchi
(*College of Cryptography Engineering, Information Engineering University, Zhengzhou 450004, Henan, China*)

Abstract Aiming at the potential safety hazard existed in network access authentication of the terminal of trusted computational platform, we proposed a TNC frame-based network terminal authentication model TNTAM. The model enhances the security of terminal authentication by adding the identification system module, information access and differentiation module IADM and introducing policy manager, and achieves the mutual authentication between the user, the improved smart authentication card and the trusted terminal, as well as ensures the creditability and communication safety of the trusted terminal when requesting network services. Besides, we designed the specific application procedures of TNTAM. Final comparative analysis indicated that the TNTAM diminished the potential safety hazard of the trusted terminal in network authentication, and it also provided a thought to enhancing the security of terminal authentication.

Keywords Trusted terminal Smart card Trusted network connection (TNC) Terminal authentication model Application procedure

0 引 言

在信息网络迅速发展的今天,网络中的攻击层出不穷,多种多样,反病毒、防火墙等传统防护手段[1]虽然具有一定作用,却已无法从根本上解决信息安全问题。人们从频发的信息安全事件中发现一切隐患的根源来自于终端,只有保证终端的安全接入认证才能保证网络环境的安全。TCG(trusted computing group)的可信网络连接 TNC(trusted network connection)旨在利用可信计算平台技术[2]将终端的可信延伸至网络,从而确保网络连接的可信。它是指终端接入网络之前,对用户身份、平台身份和终端状态依次进行认证,如果都通过则允许终端接入网络,否则转入安全性修补或升级[3]。

为解决网络接入认证的安全问题,国内外学者基于可信计算平台相继开展了一些研究。Pashalid 和 Mitchell 研究设计了单点登录认证系统[4],系统分为用户和服务提供者两部分,实现了用户访问请求的身份认证,但登录标识证书与平台绑定导致用户证书便携性不方便,当平台维护时还存在一定的泄露隐患;George 通过改进可信平台的用户身份认证协议,提出一种智能卡和 PIN 码结合的认证方案[5],实现了智能卡和可信平台终端的相互认证,但是 PIN 码仍然是最大的安全隐患,未摆脱基于口令的认证脆弱性;从 2004 年至今,国内的学者对可信网络连接的改进和终端认证方案的探索从未停止过,如颜菲等人针对网络认证终端缺乏安全保护的问题,提出了一种基于 TNC 的安全认证协议[6],该协议在可信环境下把终端完整性度量和 PKI 技术相结合,确保了通信双方的平台完整性和终端、网络两者之间的认证安全;王佳慧等人提出了扩展的可信网络接入与认证模型[7],该模型通过加入元数据存储点 MAP(metadata access point)和流量控制器和感应器 FC-SS(flow controllers-sensors)保证了终端接入以后的动态完整性。以上研究都在 TNC 框架内解决了终端接入网络的用户和平台身份认证问题,但是依然忽略了用户和平台间相互认证时的通信安全和隐患(如用户智能卡及其信息或口令易被非法窃取等),未提出保证用户和终端间通信及认证安全的具体方案。本文提出的基于 TNC 的网络终端认证模型 TNTAM(TNC network terminal authentication module)通过在终端平台客户端加入身份认证系统模块,利用其指纹识别和 PIN 码绑定的智能卡认证技术,实现用户、智能卡和具

收稿日期:2014-04-24。**金雷**,硕士生,主研领域:密码与信息安全管理。**徐开勇**,研究员。**李剑飞**,硕士生。**杨天池**,博士。

有可信平台模块的可信终端之间的相互认证并保证了认证信道安全;通过加入信息访问判定模块 IADM(information access determine module)提高了网络服务请求认证的效率并降低了服务器端的性能开销;策略管理器的引入保证了网络请求者和接入者的双向认证。

1 TNTAM 模型设计

在可信网络协议和可信计算平台机制下,一个用户要获得网络的完全访问权就必须通过平台认证和授权。TNTAM 是在 TCG 的可信网络连接框架[8]基础上构建的,TNTAM 增加了两个模块和一个策略管理器,如图 1 所示。

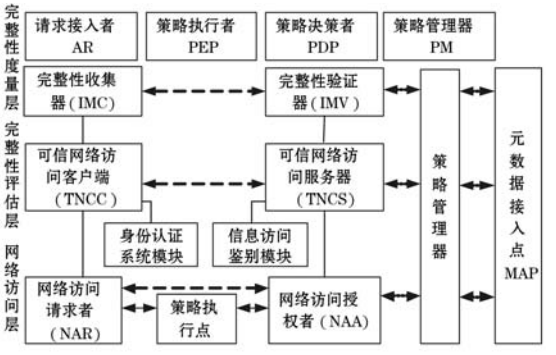

图 1 基于 TNC 的网络终端认证模型

1.1 模型中增加的模块

模型在可信网络访问客户终端加入身份认证系统模块,在可信网络访问服务器中加入信息访问鉴别模块 IADM,并引入了 TCA(trusted connection architecture)架构中策略管理器。下面具体对新增添的功能模块进行详述。

1.1.1 身份认证系统模块

在可信终端的客户端用户认证中,在原有可信计算平台保证终端平台系统完全性的基础上,采用身份认证系统模块来保证用户认证阶段的灵活性和安全性。该模块中用户使用的智能卡具有较强密码运算功能和信息密保功能,卡里存储用户证书以及保密数据,如认证参数、指纹模板 f_u 的哈希值。用户先对智能卡注册,用户的资料由认证服务器端储存在鉴别信息表中进行管理使用,服务器对资料、证书的传送及存储完全加密以确保安全。用户采用 PIN 码及指纹识别[9,10]认证智能卡,智能卡利用其中的数据和终端的可信平台模块实现了它与终端、用户间的双向验证,此模块填补了终端、用户和智能卡无法互相认证的安全漏洞,提高了信息、信道和认证的安全性。其中采用 LCD 和 LED 指示灯[9]的亮起指示平台认证状态和可信与否。

1.1.2 策略管理器

针对可信网络访问请求者单方向网络服务器请求认证,无法验证网络接入管理端的安全隐患,在原始认证框架基础上引入 TCA 架构中的策略管理器来管理身份平台证书和面向终端发布访控策略,并根据元数据接入点 MAP 的动态完整性信息对终端评估策略进行及时调整。策略管理器充当可信第三方的角色,集中实现了证书有效性和平台可信性的校验,这样简化了管理机制,并实现了访问请求者和控制器的双向身份认证,使总体依次构建成终端可信、访问服务器可信和网络连接可信的安全体系架构。

1.1.3 IADM 模块

在可信网络访问服务器中添加一个信息访问鉴别模块 IADM。该模块将用户即将访问的信息进行等级划分,分为公开信息、涉密信息等级别,涉密信息以外的信息资源因其公开性无需进行身份认证,即在终端进行网络服务请求时如果是公开信息服务请求则不必进行身份验证,这样降低了服务器端的性能开销,并使得整体策略决策端的效率更高。

1.2 模型中的层次

TNTAM 架构从上至下分为 3 个层次:完整性度量层、完整性评估层、网络访问层。

1)完整性度量层 对终端平台和接入网关的完整性信息进行收集校验。

2)完整性评估层 根据访问策略和上一层的传递信息,终端对网络接入端的完整性信息进行收集度量。网络接入端对终端的可信性进行收集度量。

3)网络访问层 完成传统连接功能和双向身份认证。

2 TNTAM 应用流程

TNTAM 模型的设计目标是为可信终端的网络访问认证提供支撑,因此应用流程的设计至关重要。通过分析总结本节把 TNTAM 模型的应用流程分为用户和平台身份认证,请求接入双向认证以及服务请求认证等三个阶段,模型简要应用流程如图 2 所示。

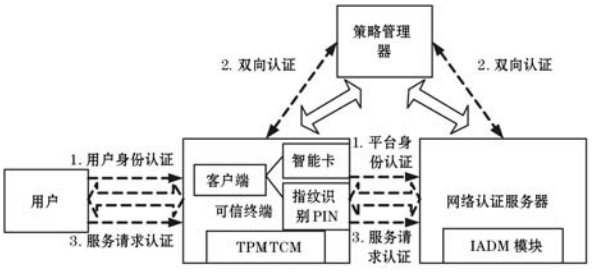

图 2 TNTAM 模型简要应用流程

2.1 用户和平台身份认证

在用户和平台身份认证阶段,可信客户终端通过加入身份认证系统模块,采用改进的智能卡身份认证技术[11,12],结合指纹识别、PIN 码进行多因素结合认证,将可信终端与可信平台模块看作一个整体,过程如图 3 所示。

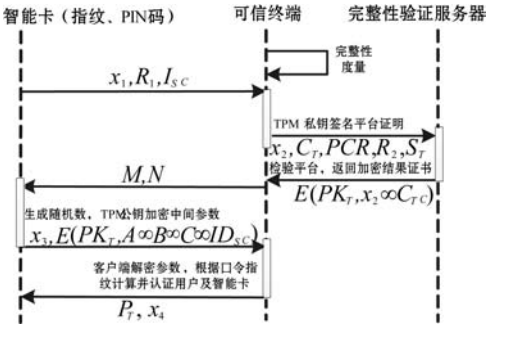

图 3 身份平台认证协议流程

定义 1 P_w 为用户口令,$H(m)$ 为 m 的计算哈希值,∞ 表示连接操作,(X,Y,Z) 为用户接入网络时需要的参数以及用户与终端进行认证的参数。

认证参数(X,Y,Z) 计算式为:

$X = H(ID_u \infty P_w)$;

$Y = H(P_w) \oplus H(f_u)$;

$Z = X \oplus H(ID_u \infty f_u)$;

可信平台模块中存储着自己的私钥 S_T 、证书 C_T 、与指纹识别的共享密钥 K_B 以及用于标示终端平台所有者的 M_T 。其中 $M_T = H(H(P_{w_T}) \oplus H(f_T))$ 。

流程 1　系统加电后终端在可信平台模块作用下进行自身完整性度量。

流程 2　$S_C \longrightarrow T_C : x_1, I_{S_C}, R_1$;

式中 S_C 表示智能卡, T_C 表示可信终端, x_1, I_{s_c}, R_1 分别表示智能卡向终端发送的随机数、智能卡标志和验证请求。

流程 3　$T_C \longrightarrow I_{mv} : x_2, C_T, PCR, S_T, R_2$;

式中 I_{mv} 为完整性验证服务器,可信终端将生成随机数 x_2, 平台配置寄存器值 PCR、平台证书 C_T 、用可信平台模块私钥签名过的平台证明 S_T 以及平台验证请求 R_2 发给完整验证性服务器,等待服务器返回证明证书。其中:

$S_T = S(SK_T, x_1 \infty x_2 \infty ID_T \infty PCR)$, $S(m,n)$ 表示用 m 的私钥对 n 签名。

流程 4　$I_{mv} \longrightarrow T_C : E(PK_T, x_2 \infty C_{T_C})$;

如式中所示,服务器对终端平台验证后,把用可信平台模块公钥加密的验证结果证书 C_{T_c} 返回给可信终端, $E(m,n)$ 表示使用密钥 m 对 n 进行加密。

流程 5　$T_C \longrightarrow S_C : M, N$;

$M = E(PK_{S_C}, x_1 \infty ID_{S_C} \infty ID_T \infty Cred)$;

$N = S(SK_T, x_1 \infty ID_{S_C} \infty ID_T \infty Cred)$;

终端平台将完整性验证报告返回智能卡,由智能卡判断平台状态是否符合完整预期;当符合时,LED 灯指示成功并进入用户认证阶段;当不符合时,LCD 灯指示平台认证出错,认证停止。

流程 6　$S_C \longrightarrow T_C : x_3, E(PK_T, A \infty B \infty C \infty ID_{S_C})$;

$A = H(X \infty x_3)$;

$B = X \oplus H(x_3 \infty ID_T)$;

$C = H(Y \infty x_3)$;

式中 x_3 是生成的随机数,TPM/TCM 把 A、B、C 公钥加密后传给可信终端,可信终端进行用户认证。

流程 7　$T_C \longrightarrow S_C : p_T, x_4$;

客户端接收到 $E(PK_T, A \infty B \infty C \infty ID_{S_C})$ 后进行解密,并根据输入的口令 P'_w 和指纹识别 f'_u 计算 $X' = B \oplus H(x_3 \infty ID_T)$, $A' = H(X' \infty x_3)$ 。当 $A' = A$ 时,则用户为合法用户,否则认证失败并暂停;然后,在可信计算平台模块中计算 $M' = H(H(P'_w) \oplus H(f'_u))$,当 $M' = M_T$ 时,智能卡的使用者为原始用户。

式中 $P_T = H(ID_u \infty f'_u) \oplus x_4$,通过可信平台模块计算后发送到智能卡,由智能卡进行对平台的认证。最后由智能卡进行计算 $X' = P_T \oplus x_4 \oplus Z$,如果 $X' = X$,则平台认证通过。

2.2　请求者和接入方双向认证

访问请求者请求访问受保护的网络,这时访问控制端控制所有访问请求者的访问。引人的策略管理器作为一个可信的第三方,集中管理请求端和决策端的两方行为,并提供两方双向身份认证机制,认证流程如图 4 所示,使得访问请求者与访问控制端一样具有控制连接的能力。这样在终端也能确定接入方的身份可信后,即可发起访问服务请求。

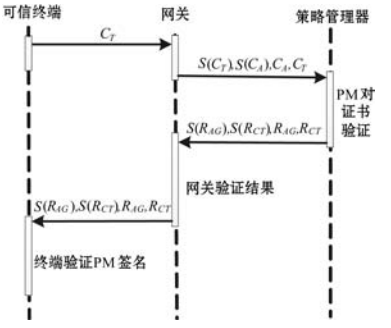

图 4　双向认证协议流程

定义 2　T_C 为可信终端, A_G 为接入网关, P_M 为策略管理器。

流程 1　$T_C \longrightarrow A_G : C_T$;

式中 C_T 为可信终端平台证书。

流程 2　$A_G \longrightarrow P_M : S(C_T), S(C_A), C_T, C_A$;

式中 C_A 为网关证书, $S(x)$ 表示网关 A_G 对 x 的私钥签名。

流程 3　策略管理器首先验证签名证书,如果成功,则验证终端证书。

流程 4　$P_M \longrightarrow A_G : S(R_{CT}), S(R_{AG}), R_{CT}, R_{AG}$;

式中 R_{CT}, R_{AG} 分别表示终端和网关验证结果, $S(x)$ 表示 P_M 对 x 的私钥签名。

流程 5　A_G 验证结果并根据鉴别结论判断是否授权接入。

流程 6　$A_G \longrightarrow T_C : S(R_{CT}), S(R_{AG}), R_{CT}, R_{AG}$ 。

流程 7　T_C 验证 P_M 签名并决定是否接入网络。

2.3　服务请求认证

在身份平台认证通过后,用户即可向可信网络服务器发出访问请求,此时访问请求如果针对公开信息,由于 IADM 模块的加入则无需进行请求验证[13],如果是公开信息以外的服务请求则依据模块判定后进入信息访问前的服务请求认证阶段。基本流程如图 5 所示。

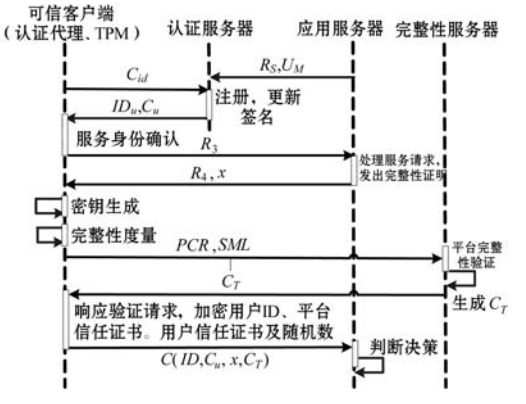

图 5　服务请求认证协议流程

定义 3　应用服务器为 A_s ,认证服务器为 AU_S ,完整性验证服务器为 IN_S 。

流程 1　$A_s \longrightarrow AU_S : R_S, U_M$;

$AU_S \longrightarrow A_S$;

式中 R_S 为注册操作, U_M 为模块签名更新操作。应用服务器通过认证服务器注册,更新签名并被认证中心反向验证自己的合法性。

流程 2 -3 $S_c \longrightarrow AU_S : C_{id}$;

$AU_S \longrightarrow S_C : ID_u, C_u$;

式中 C_{id} 为身份确认请求操作，ID_u, C_u 分别表示用户身份和用户信任证书。

流程 4 -5 $S_c \longrightarrow A_s : R_3$;

$A_s \longrightarrow S_c : R_4, x$;

式中 R_3, R_4 分别为服务请求和完整性证明请求，x 为服务器返回给用户的随机数。

流程 6 -7 可信终端平台生成会话密钥 C_K，平台模块开始对可信平台进行完整性度量。

流程 8 客户端寄存器的数值和日志生成后，认证代理发送到验证服务器验证。

流程 9 -10 度量数据被传送到完整性验证服务器后，服务器按照结果生成度量信任证书 C_T 并传回给客户端。

流程 11 $S_c \longrightarrow A_s : C(ID, C_T, C_u, x)$;

客户端响应用户及平台验证请求，将用户 *ID*、平台信任证书、用户信任证书及随机数在会话密钥加密后返回应用服务器。式中的 $C(x)$ 表示会话密钥对 x 进行加密。

流程 12 服务器验证通过后，如果终端可信，则提供相应的服务。

3 TNTAM 模型分析

3.1 模型优势分析

与传统的终端认证模型相比，本模型具有以下优点。

（1）*终端用户身份认证的安全性* 在该模型中，新加入的身份认证系统模块使用户必须使用与本人绑定的唯一智能卡，并且输入正确 PIN 码与指纹识别才能通过认证。用户在智能卡中保留的资料、口令和指纹信息等与哈希函数关联起来，减小了传统单一口令或者指纹认证的安全隐患，这样即使智能卡信息被攻击，也无法得到智能卡所有的信息。用户初始资料不被简单直接的存储在可信平台模块和智能卡上，并且在实体间的数据传递时，用户密码、指纹信息以及各个生成的随机数都被加密保护，这样使得重要数据得到了新鲜度和完整性保证。这样在 TNTAM 模型中用户对终端平台和智能卡的数据的访控得到加强，并减小了智能卡遗失或者终端被攻破的隐患。

模型中由于可信终端具有可信平台模块，使用户不再依赖认证中心进行在线身份认证，身份认证系统模块中的智能卡和可信终端在与用户交互的过程中如上述主要以哈希和异或计算为主，有效提高了终端的身份认证效率。

（2）*请求认证服务器的高效性* TNTCM 模型通过在可信网络连接服务器中加入 IADM 模块，把请求访问的资源等级划分为公开信息、涉密信息等级别，涉密信息以外的信息资源因其公开性无需进行身份认证，这样提高了网络服务请求认证的效率并降低了服务器端的性能开销，使得整体策略决策端的效率更高。

（3）*终端和服务器双向认证的安全性* TNTAM 中策略管理器的引入为管理机制的简化和终端和网络的双向认证取得了一定提升效果，使终端接入网络前不单单提供自身的可信性证据，还保证了从网络中获取的服务可信。

TNTAM 模型与基础网络认证架构模型[13]性能对比如表 1 所示。

表 1 TNTAM 与现有网络认证架构的对比分析

比较内容	传统网络接入技术	TNC	TCA	TNTAM
接入终端	配套设备，不可信	含 TPM 模块的可信计算平台，可信	含 TCM 模块的可信计算平台，可信	含 TPM/TCM 的可信计算平台，可信
客户端认证	认证方式单一单向易被窃取或攻击	认证方式单一单向易被窃取或攻击	认证方式单一单向易被窃取或攻击	多因素结合认证，强化访控，安全性强；信息交换和认证算法效率高
网络服务器效率	一般	一般	一般	含 IADM 模块，提高了用户服务请求认证效率并降低服务器端性能开销
终端网络双向认证	无	无	含策略管理器，并实现双向认证	含策略管理器，并实现双向认证
终端对网络的恶意攻击隐患	存在	存在	存在	存在但经过改进使相对较小

3.2 模型性能分析

在 TNTAM 的身份认证系统模块中用户、智能卡和终端三者之间的认证使用一次性数据交互，认证信息流量被减少，而且认证过程以哈希计算和异或计算为主，不再使用 TPM 标准方案中的数字签名和验证算法。因此大大提高了用户的认证效率，同时客户端在进行服务器切换时的平台完整性证书有效期保留机制也提高了证明的效率。由于在该模块中采取了智能卡结合 PIN 码和指纹识别的认证系统，所以在整个认证过程中密码运算给整个系统所带来的时间代价必须进行考虑分析。TNTAM 模型整个认证过程的时间代价分为运算时间和通信时间两大部分，运算时间又分为终端可信模块运算时间和智能卡运算时间，由于数据交互时数据传输量较小所以通信时间可以忽略不计。总时间用 t 表示，运算时间为 t_{op}，通信时间为 t_{tr}，终端运算时间为 t_{te}，智能卡运算时间为 t_{ca}。由此我们可得：

$$t_{op} = t_{te} + t_{ca}$$

$$t = t_{op} + t_{tr} = t_{te} + t_{ca} + t_{tr} \approx t_{te} + t_{ca}$$

从整个认证流程可以看出模型中哈希运算共需进行 9 次，在智能卡中进行了 3 次，终端平台的可信计算模块进行了 6 次。加密运算一共需要进行 2 次，智能卡和可信计算模块中各进行了 1 次。解密运算一共需要进行 3 次，智能卡中进行 1 次，可信计算模块进行 2 次。智能卡中得一次哈希运算时间用 t_{hc} 表示，一次加密时间为 t_{ec}，一次解密时间为 t_{dc}；可信计算模块中一次哈希运算时间用 t_{ht} 表示，一次加密时间为 t_{et}，一次解密时间为 t_{dt}。综上可得：

$$t \approx t_{te} + t_{ca} \approx t_{ec} + t_{et} + t_{dc} + 2t_{dt} + 3t_{hc} + 6t_{ht}$$

假设在智能卡和可信平台模块上的加解密 DES 运算、哈希 SHA-1 运算时间均将近 0.2 s，则总时间代价 $t \approx 2.5$ s。由于该模块采用多因素认证，增加的时间复杂度提供了用户和平台的

可信认证和提高安全性的目的,因此可以接受这样的计算代价。

通过在可信网络访问服务器中添加一个信息访问鉴别模块 IADM 把用户即将访问的信息进行等级划分,分为公开信息、涉密信息等级别,涉密信息以外的信息资源因其公开性无需进行完整性检查,这样降低了服务器端的性能开销,并使得模型整体通信效率更高。

3.3　安全性考虑

由于模型中加入新的功能模块和实体,实际应用中就需要考虑更多的安全性和技术支撑问题,如下所述:

IADM 模块的资源安全防护:需要加强对用户的资源访问进行实时监控和控制,避免恶意用户采取恶意攻击方法绕过鉴别系统非法访问资源。

策略管理器和 PDP 之间的安全信道:通过安全协议保证信道安全,只有保证了信道的安全性,才可以保证传输的消息的安全性。

模型中众多接口之间的消息传输也会带来很多的安全性问题,所以必须保证接口之间消息的可靠传输,相应的安全协议是模型应用得到支撑的关键。

4　结　语

本文基于可信网络连接框架提出了一种改进的网络终端认证模型 TNTAM,并对模型的具体应用流程进行了设计。重点阐述了模型的总体设计和具体应用流程,旨在体现可信计算平台在终端接入网络认证时的安全配置思想。新的模型在可信网络连接框架基础上通过在客户终端加入身份认证系统模块,在可信网络服务器端加入信息分级鉴别模块以及引入策略管理器来实现对网络请求者与网络接入者之间的双向认证,为可信终端入网认证时的安全隐患提供了一种可行的解决思路。在下一步工作中,将对模型具体的安全协议和应用支撑进行进一步研究和改进。

参　考　文　献

[1] 冯登国,秦宇,汪丹,等. 可信计算技术研究[J]. 计算机研究与发展,2011,48(8):1332-1349.

[2] 温博为. 可信计算平台技术应用研究[D]. 西安:陕西师范大学,2013.

[3] 王浩,陈泽茂,李铮,等. 基于可信网络连接的多级涉密网安全接入方案[J]. 计算机科学,2012,39(12):65-68.

[4] Pashalidis A, Mitchell C J. Single sign-on using trusted Platforms [M]. Information Security. LNCS 2851, Berlin:SPringer, 2003:54-68.

[5] George P. User authentieation with smart cards in trusted computing architecture[C]//Proeeedings of the International Conference on Security and Management, LasVegas, Nevada, USA, 2004:25-31.

[6] 王佳慧,吴振强,李洁. 扩展的可信网络平台接入与认证[J]. 计算机工程与设计,2010,31(2):239-241.

[7] 颜菲,任江春,戴葵,等. 基于 TNC 的安全认证协议设计与实现[J]. 计算机工程,2007,33(12):160-162.

[8] 马卓,马建峰,李兴华,等. 可证明安全的可信网络连接协议模型[J]. 计算机学报,2011,34(9):1669-1677.

[9] 邱罡. 可信系统保护模型与设计[D]. 西安:西安电子科技大学,2010.

[10] 徐明明. 终端可信接入与远程证明研究[D]. 南京:南京邮电大学,2012.

[11] 张启明. 无线局域网可信接入模型研究[D]. 哈尔滨:哈尔滨工程大学,2012.

[12] 李飞. 基于可信计算的无线网络终端认证机制研究[J]. 科学技术与工程,2011,32(11):8069-8072.

[13] 邓松,林为民,张涛. 基于 TNC 的电力终端安全接入技术研究[J]. 电力系统通信,2012,33(1):78-81.

(上接第 282 页)

参　考　文　献

[1] 周兴社,於志文. 面向老年人生活的智能辅助[J]. 中国计算机学会通讯,2010,6(6):57-67.

[2] 朱旭东,刘志镜. 基于主题隐马尔科夫模型的人体异常行为识别[J]. 计算机科学,2012,39(3):251-275.

[3] Narayanan C Krishnan, Diane J Cook. Activity recognition on streaming sensor data[J]. Pervasive and Mobile Computing, 2010, 10(Part B): 138-154.

[4] Palmes P, Pung H K, Gu T, et al. Object relevance weight pattern mining for activity recognition and segmentation [J]. Pervasive Mobile Computing, 2010, 6(1):43-57.

[5] Liming Chen, Nugent C D, Hui Wang. Knowledge-Driven Approach to Activity Recognition in Smart Homes[J]. Knowledge and Data Engineering, IEEE Transactions on, 2012, 7(24):961-974.

[6] Liming Chen, Jesse Hoey, Chris D Nugent, et al. Sensor-based Activity Recognition[J]. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 2012, 42(6):790-808.

[7] 李娜,侯义斌,黄樟钦. 基于人体加速度特征的实时跌倒识别算法[J]. 小型微型计算机系统,2012,33(11):2410-2413.

[8] Jie Yin, Qiang Yang, J J Pam. Sensor-Based Abnormal Human-Activity Detection[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(8):1082-1090.

[9] Ihnhan Bae. An Ontology-based approach to ADL recognition in smart homes[J]. Future Generation Computer Systems, 2014, 33:32-41.

[10] 邓昌智,敖翔,周明俊,等. 以活动为中心的个人信息管理[J]. 软件学报,2008,19(6):1428-1438.

[11] Bogdan Pogorelc, Matjaž Gams. Home-based health monitoring of the elderly through gait recognition[J]. Journal of Ambient Intelligence and Smart Environments, 2012, 4(5):415-428.

[12] Dario Bonino, Fulvio Corno. DogOnt-Ontology Modeling for Intelligent Domotic Environments[C]. The Semantic Web-ISWC 2008, 5318:790-803.

[13] Ngamnij Arch-int, Somjit Arch-int. Semantic Ontology Mapping for Interoperability of Learning Resource Systems using a rule-based reasoning approach[J]. Expert Systems with Applications, 2013, 40(18): 7428-7443.

[14] 李川. 一种高效的本体匹配算法的研究[D]. 重庆:重庆大学,2011.

[15] 刘秀磊,廖建新,朱晓民,等. 本体匹配中基于抑郁组合的词法分析算法[J]. 电子学报,2012,40(8):1624-1630.

[16] The Apache Software Foundation. What is Jena? [EB/OL]. (2011) [2012-03-31]. http://incubator. Apache. org /jena/about_jena/about. html.