可信网络连接研究

张焕国[1),2)] 陈 璐[1)] 张立强[3)]

[1)](武汉大学计算机学院 武汉 430072)

[2)](空天信息安全与可信计算教育部重点实验室 武汉 430072)

[3)](武汉大学软件工程国家重点实验室 武汉 430072)

摘 要 文中详细地介绍了可信网络连接的发展历程、体系结构、消息流程、相关规范,对 TCG 的可信网络连接架构的优点与局限性进行了分析.针对如何将可信计算机制拓展到网络,使得网络成为可信的计算环境这一问题进行了分析论述,并对可信网络连接技术未来的发展趋势进行了展望.

关键词 可信计算;可信网络连接;可信网络;网络安全;信息安全

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2009.00706

Research on Trusted Network Connection

ZHANG Huan-Guo[1),2)] CHEN Lu[1)] ZHANG Li-Qiang[3)]

[1)](*School of Computer, Wuhan University, Wuhan* 430072)

[2)](*Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, Wuhan University, Wuhan* 430072)

[3)](*State Key Laboratory of Software Engineering, Wuhan University, Wuhan* 430072)

Abstract This paper introduces the development history, architecture, information flow and related specification of Trusted Network Connection in details. Analyses are given on Trusted Network Connection architecture; merits and restriction are pointed out. Focusing on how to extend the Trusted Computing mechanism into network and make network to be a trusted computing environment, related research work are analyzed and summarized. Some future research trends and development on Trusted Network Connection are advised.

Keywords trusted computing; trusted network connection; trusted network; network security; information security

1 引 言

自从 2003 年可信计算组织(Trusted Computing Group,TCG)① 成立以来,可信计算技术得到了迅速的发展.人们已经意识到,在面对现有各种安全风险与威胁时,不仅需要自顶向下的安全体系设计,还需要从终端开始自底向上地保证计算系统的可信;不仅要保证终端计算环境的可信,还要把终端计算环境的可信扩展到网络,使得网络成为一个可信的计算环境.

2004 年 5 月 TCG 成立了可信网络连接分组② (Trusted Network Connection Sub Group, TNC-SG),主要负责研究及制定可信网络连接(Trusted

收稿日期:2009-07-24;最终修改稿收到日期:2009-11-03.本课题得到国家"八六三"高技术研究发展计划项目基金(2006AA01Z442,2007AA01Z411)、国家自然科学基金(60673071,60970115)资助.**张焕国**,男,1945 年生,教授,研究领域为信息安全、可信计算等.E-mail: liss@whu.edu.cn. **陈 璐**,女,1979 年生,博士研究生,研究方向为可信计算、网络安全. **张立强**(通信作者),男,1979 年生,博士,讲师,研究方向为可信计算、网络安全. E-mail: whujking@126.com.

① TCG Web Site. https://www.trustedcomputinggroup.org

② TNC Web Site. https://www.trustedcomputinggroup.org/network/

Network Connection，TNC）框架[①]及相关的标准[②③④⑤⑥⑦⑧]. 经过几年的发展，TNC 已经具有 70 多名成员，形成了以 TNC 架构为核心、多种组件之间交互接口为支撑的规范体系结构，实现了与 Microsoft 的网络访问保护（Network Access Protection，NAP）[⑨]之间的互操作，并将一些规范作为建议草稿提交到互联网工程任务组（International Engineer Task Force，IETF）的网络访问控制（Network Access Control，NAC）规范中. 目前已经有多家企业的产品支持 TNC 体系结构，如 Extreme Networks、HP ProCureve、Juniper Networks、Meru Networks、OpSwat、Patchlink、Q1Labs、StillSecure、Wave Systems 等；也有开放源代码的软件，如 libTNC[⑩]、FHH[⑪]、Xsupplicant[⑫] 等.

TNC 是对可信平台应用的扩展，也是可信计算机制与网络接入控制机制的结合. 它是指在终端接入网络之前，对用户的身份进行认证. 如果认证通过，对终端平台的身份进行认证，如果认证通过，对终端的平台可信状态进行度量，如果度量结果满足网络接入的安全策略，则允许终端接入网络，否则将终端连接到指定的隔离区域，对其进行安全性修补和升级. TNC 旨在将终端的可信状态延续到网络中，使信任链从终端扩展到网络. TNC 是网络接入控制的一种实现方式，是一种主动性的防御方法，能够将大部分的潜在攻击在发生之前进行抑制.

TNC 是从技术层面上将可信计算机制延伸到网络的一种尝试. 但是，TNC 在研究层面还有很多基本的问题亟待解决. TNC 的理论研究落后于技术开发，至今尚没有公认的可信网络环境理论模型；远程证明是 TNC 的基础，但是目前尚缺少软件动态可信性的度量方法与理论，缺少经过形式化验证的远程证明协议；一些关键的技术如软件动态可信性度量机制等尚待攻克.

虽然 TNC 的发展目前还存在一些问题. 但是 TNC 的出发点是为了从终端入手解决网络的安全和可信问题，无论是理论还是技术都非常符合解决网络可信的需求. 目前，各国研究机构和大学、企业的研究部门、军事和国防机构都对 TNC 开展了深入的研究. 针对这种情况，本文将 TNC 技术的现状和发展进行了介绍和总结，对 TNC 的优势与局限性进行了分析，对如何将可信机制延伸到网络的研究进行了分析，并对 TNC 的未来发展趋势进行了探讨，力求对 TNC 技术的研究与发展进行客观和全面的介绍.

本文第 2 节对 TCG 的 TNC 架构与规范进行介绍；第 3 节对 TNC 架构进行分析；第 4 节对如何将可信机制延伸到网络的研究进行分析；第 5 节对 TNC 的未来发展趋势进行探讨；第 6 节对我们的研究工作做简单介绍；第 7 节给出结论.

2　TNC 架构与规范

2.1　TNC 的发展历程

2004 年 5 月 TCG 建立了 TNC-SG，意图在网络访问控制和终端安全领域制定开放的规范. 2005 年 5 月，TNC V1.0 版本的架构规范和相应的接口规范发布，其确定了 TNC 的核心，并在 Interop LasVegas 中进行了理念的展示. 2006 年 5 月，TNC V1.1 版本的架构规范发布，其添加了完整性度量模型的相关内容，展示了完整性度量与验证的示例，包括第一个部署实例以及无线局域网、完整性度量与验证、网络访问、服务器通信等相关的产品. 2007 年 5 月，TNC V1.2 版本的架构规范发布，其中增加了与 Microsoft NAP 之间的互操作，对一些已有规范进行了更新，并包括了一些新的接口规范，使更多的产品开始支持 TNC 架构. 2008 年，TNC 架构中最上层的 IF-M 接口规范进入了公开评审阶段，这意味着耗时 3 年多的 TNC 架构规范终于完整公开.

---

① TCG Specification Trusted Network Connect—TNC Architecture for Interoperability Revision 1.1[EB/OL]. Trusted Computing Group，2006.5. http://www.trustedcomputinggroup.org

② TCG Specification Trusted Network Connect — TNC IF-PEP：Protocol Binding for Radius Revision 0.7[EB/OL]. 2007.5. https://www.trustedcomputinggroup.org

③ TCG Specification Trusted Network Connect—TNC IF-T：Protocol Binding for Tunneled EAP Methods. Revision 10[EB/OL]. 2007.5. https://www.trustedcomputinggroup.org

④ TCG Specification Trusted Network Connect — TNC IF-TNCCS：TLV Binding Revision 10[EB/OL]. 2008.1. https://www.trustedcomputinggroup.org

⑤ TCG Specification Trusted Network Connect — TNC IF-IMC Revision 8[EB/OL]. 2007.2. https://www.trustedcomputinggroup.org

⑥ TCG Specification Trusted Network Connect — TNC IF-IMV Revision 8[EB/OL]. 2007.2. https://www.trustedcomputinggroup.org

⑦ TCG Specification Trusted Network Connect—TNC IF-M：TLV Binding Revision 30[EB/OL]. 2008.1. https://www.trustedcomputinggroup.org

⑧ TCG Specification Trusted Network Connect — TNC IF-PTS Revision 1.0[EB/OL]. 2006.11. https://www.trustedcomputinggroup.org

⑨ Network Access Protection Platform Architecture[EB/OL]. Microsoft Corporation. http://www.microsoft.com/technet/network/nap/

⑩ Open Source Project for TNC. http://sourceforge.net/projects/libtnc

⑪ Open Source Project for TNC. http://tnc.inform.fh-hannover.de

⑫ Open Source Project for 802.1X. http://open1x.sourceforge.net/

2008 年 4 月，TNC V1.3 版本的架构规范发布，其增加了可信网络连接协议 IF-MAP[①]（Interface for Metadata Access Point），使得 TNC 架构具有安全信息共享和动态策略调整功能. 2009 年 5 月，TNC TNC1.4 版本的架构规范发布[②]，其中增加了 IF-T：Binding to TLS[③]、Federated TNC[④] 和 Clientless Endpoint Support Profile[⑤] 3 个规范，进一步对跨域场景和无 TNC 客户端的场景进行支持.

2.2 TNC 架构

TNC 基础架构如图 1 所示，包括 3 个实体、3 个层次和若干个接口组件. 该架构在传统的网络接入层次上增加了完整性评估层与完整性度量层，实现对接入平台的身份验证与完整性验证.

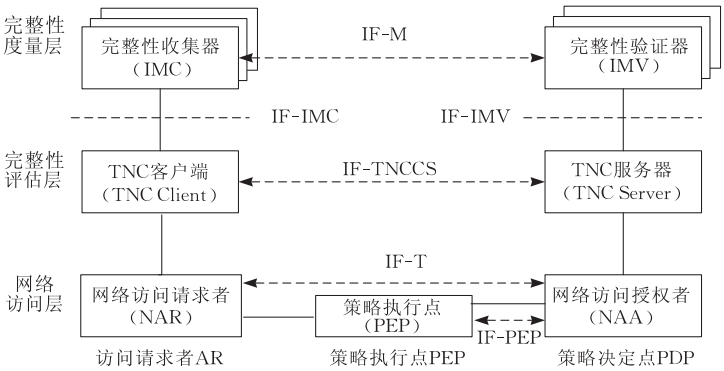

图 1 TNC 基础架构

3 个实体分别是访问请求者（Access Requestor，AR）、策略执行点（Policy Enforcement Point，PEP）和策略决定点（Policy Decision Point，PDP）. 其中 AR 发出访问请求，收集平台完整性可信信息，发送给 PDP，申请建立网络连接；PDP 根据本地安全策略对 AR 的访问请求进行决策判定，判定依据包括 AR 的身份与 AR 的平台完整性状态，判定结果为允许/禁止/隔离；PEP 控制对被保护网络的访问，执行 PDP 的访问控制决策.

AR 包括 3 个组件：网络访问请求者（Network Access Requestor，NAR）发出访问请求，申请建立网络连接，在一个 AR 中可以有多个 NAR；TNC 客户端（TNC Client，TNCC）收集完整性度量收集器（Integrity Measurement Collector，IMC）的完整性测量信息，同时测量并报告平台和 IMC 自身的完整性信息；IMC 测量 AR 中各个组件的完整性，在一个 AR 上可以有多个不同的 IMC.

PDP 包括 3 个组件：网络访问授权者（Network Access Authority，NAA）对 AR 的网络访问请求进行决策. NAA 可以咨询上层的可信网络连接服务器（Trusted Network Connection Server，TNCS）来确定 AR 的完整性状态是否与 PDP 的安全策略一致，从而决定 AR 的访问请求是否被允许；TNCS 负责与 TNCC 之间的通信，收集来自完整性度量验证器（Integrity Measurement Verifier，IMV）的决策，形成一个全局的访问决策传递给 NAA；IMV 将 IMC 传递过来的 AR 各个部件的完整性测量信息进行验证，并给出访问决策意见.

3 个层次分别是网络访问层、完整性评估层与完整性度量层. 网络访问层支持传统的网络连接技术，如 802.1X 和 VPN 等机制. 完整性评估层进行平台的认证，并评估 AR 的完整性. 完整性度量层收集和校验 AR 的完整性相关信息.

在 TNC 架构中存在多个实体，为了实现实体之间的互操作，需要制定实体之间的接口. 接口自底向上包括 IF-PEP、IF-T、IF-TNCCS、IF-IMC、IF-IMV 和 IF-M. IF-PEP 为 PDP 和 PEP 之间的接口，维护 PDP 和 PEP 之间的信息传输；IF-T 维护 AR 和 PDP 之间的信息传输，并对上层接口协议提供封装，针对 EAP 方法和 TLS 分别制定了规范；IF-TNCCS 是 TNCC 和 TNCS 之间的接口，定义了 TNCC 与 TNCS 之间传递信息的协议；IF-IMC 是

① TCG Specification Trusted Network Connect IF-MAP Revision 25[EB/OL]. 2008.4. https://www.trustedcomputinggroup.org

② TCG Trusted Network Connect TNC Architecture for Interoperability Specification Version 1.4[EB/OL]. 2009.5. http://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14

③ TCG Trusted Network Connect TNC IF-T: Binding to TLS [EB/OL]. 2009.5. http://www.trustedcomputinggroup.org/resources/tnc_ift_binding_to_tls_version_10_revision_16

④ TCG Trusted Network Connect TNC Federated TNC [EB/OL]. 2009.5. http://www.trustedcomputinggroup.org/resources/federated_tnc_version_10_revision_26

⑤ TCG Trusted Network Connect Clientless Endpoint Support Profile [EB/OL]. 2009.5. http://www.trustedcomputinggroup.org/resources/tnc_clientless_endpoint_support_profile_version_10_revision_13

TNCC 与各个 IMC 组件之间的接口，定义了 TNCC 与 IMC 之间传递信息的协议；IF-IMV 是 TNCS 与各个 IMV 组件之间的接口，定义了 TNCS 与 IMV 之间传递信息的协议；IF-M 是 IMC 与 IMV 之间的接口，定义了 IMC 与 IMV 之间传递消息的协议. 目前各个接口的定义都已经公布，接口与协议的定义非常详细，有的甚至给出了编程语言与操作系统的绑定.

在 TNC 架构中，平台的完整性状态将直接导致其是否被允许访问网络. 如果终端由于某些原因不能符合相关安全策略时，TNC 架构还考虑提供终端修补措施. 在修补阶段中终端连接的是隔离区域. TNC 并没有强制要求终端具有可信平台，但是如果终端具有可信平台，那么针对可信平台的相关特性 TNC 还提供了相应的接口(见本文第 2 页注释⑧). 具有可信平台与修补功能的 TNC 架构如图 2 所示.

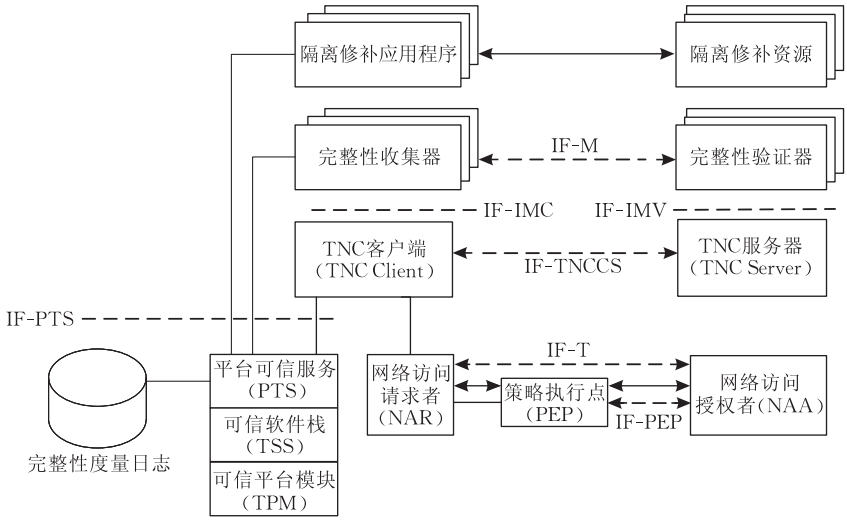

图 2　带有可信平台模块和修补功能的 TNC 架构

图 2 中的修补层由两个实体组成：配置和修补应用程序(Provisioning & Remediation Application，PRA)与配置和修补资源(Provisioning & Remediation Resource，PRR)组成. PRA 可以作为 AR 的一个组成部分，向 IMC 提供某种类型的完整性信息. PRR 作为修补更新资源，能够对 AR 上某些组件进行更新，使其通过完整性检查. 平台可信服务接口(Platform Trust Services，IF-PTS)将可信软件栈(Trusted Software Stack，TSS)的相关功能进行封装，向 AR 的各个组件提供可信平台的功能，包括密钥存储、非对称加解密、随机数、平台身份和平台完整性报告等. 完整性度量日志将平台中组件的度量信息保存起来.

2.3　TNC 基本流程

以 TNC1.4 版本为例，一次完整的 TNC 基本流程如图 3 所示.

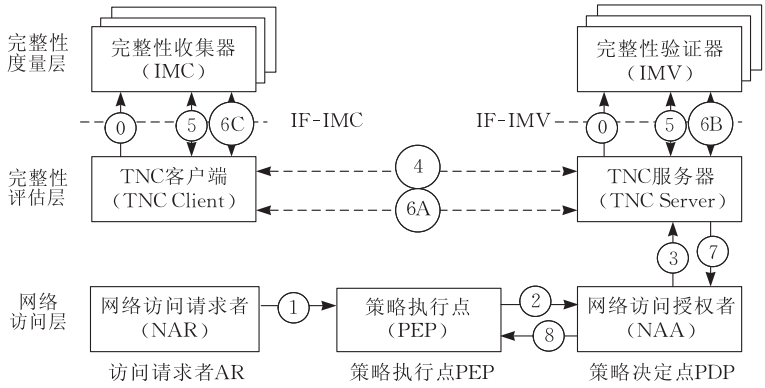

图 3　TNC 流程

具体流程如下：

1. 在进行网络连接和平台完整性验证之前，TNCC 需要对每一个 IMC 进行初始化. 同样，TNCS 也要对 IMV 进行初始化.

2. 当有网络连接请求发生时，NAR 向 PEP 发送一个连接请求.

3. 接收到 NAR 的访问请求之后，PEP 向 NAA 发送一个网络访问决策请求. 假定 NAA 已经设置成按照用户认证、平台认证和完整性检查的顺序进行操作. 如果有一个认证失败，则其后的认证将不会发生. 用户认证可以发生在 NAA 和 AR 之间. 平台认证和完整性检查发生在 AR 和 TNCS 之间.

4. 假定 AR 和 NAA 之间的用户认证成功完成，则 NAA 通知 TNCS 有一个连接请求到来.

5. TNCS 和 TNCC 进行平台验证.

6. 假定 TNCC 和 TNCS 之间的平台验证成功完成. TNCS 通知 IMV 新的连接请求已经发生，需要进行完整性验证. 同时 TNCC 通知 IMC 新的连接请求已经发生，需要准备完整性相关信息. IMC 通过 IF-IMC 向 TNCC 返回 IF-M 消息.

7a. TNCC 和 TNCS 交换完整性验证相关的各种信息. 这些信息将会被 NAR、PEP 和 NAA 转发，直到 AR 的完整性状态满足 TNCS 的要求.

7b. TNCS 将每个 IMC 信息发送给相应的 IMV. IMV 对 IMC 信息进行分析. 如果 IMV 需要更多的完整性信息，它将通过 IF-IMV 接口向 TNCS 发送信息. 如果 IMV 已经对 IMC 的完整性信息做出判断，它将结果通过 IF-IMV 接口发送给 TNCS.

7c. TNCC 也要转发来自 TNCS 的信息给相应的 IMC，并将来自 IMC 的信息发给 TNCS.

8. 当 TNCS 完成和 TNCC 的完整性检查握手之后，它发送 TNCS 推荐操作给 NAA.

9. NAA 发送网络访问决策给 PEP 来实施. NAA 也必须向 TNCS 说明它最后的网络访问决定，这个决定也将会发送给 TNCC. PEP 执行 NAA 的决策，这一次的网络连接过程结束.

上述的流程没有包括完整性验证没有通过的情况. 如果完整性验证没有通过，AR 可以通过 PRA 来访问 PRR，对相关的组件进行更新和修复，然后再次执行上述流程. 更新和修复的过程可能会重复多次直到完整性验证通过.

2.4 TNC 的支撑技术

尽管完整性度量与报告是 TNC 的核心技术，但是 TNC 架构中采用了现有的一些技术来为上层的可信计算机制提供支撑. 这主要包括网络访问技术、安全的消息传输技术与用户身份认证技术.

TNC 的网络访问层基于现有的网络访问技术，主要包括 802.1X、虚拟专用网 VPN 和点对点协议 PPP. 802.1X 为局域网提供基于端口的访问控制，能够通过受控端口与非受控端口对网络连接进行控制，这也是目前应用的最为广泛的网络接入方法. VPN 使用 IPSec 协议或安全套接字 SSL 在 Internet 上建立安全连接，保证数据传输的安全，提供远程接入功能. PPP 协议是用于在两个网络节点间建立连接的数据链路协议，能够提供连接认证和传输加密功能.

TNC 架构中需要在多个实体的多个组件中传递消息，因此安全的消息传输技术也很关键. 可扩展认证协议（Extensible Authentication Protocol，EAP）提供了认证框架，支持不同的 EAP 方法. 它不仅可以传输认证信息，而且通过 EAP 方法还可以传递终端完整性度量信息. HTTP 协议和 HTTPS 适用于传输应用程序相关的信息. TLS 可以传递完整性报告和完整性检查的消息握手.

在网络访问控制的用户身份认证中，TNC 并没有强制使用任何协议，但是可以利用现有的 RADIUS 协议和 Diameter 协议.

可以看出，在可信网络连接架构中，底层的网络访问层基本上沿用了现有的网络访问控制技术，尤其是认证协议. 消息传输也使用了现有的规范，使得整个可信网络连接架构易于兼容现有的网络接入.

3 TNC 架构分析

TNC 架构是一个开放的、支持异构环境的网络访问控制架构，建立在 TCG 相关规范和其它广泛应用的行业标准与规范之上. 它在设计过程中，既要考虑架构的安全性，又要考虑与现有标准和技术的兼容性，在一定程度上进行了折中考虑，因此，TNC 既具有一定的优点，也具有一定的局限性. 下面分别针对它的优点和局限性进行分析.

3.1 TNC 的优点

(1) 开放性. TNC 架构本身就是针对互操作的，所有规范都面向公众开放，研究者可以免费获得相关的规范文档. 另外，它采用了很多现有的标准与规范，如 EAP、802.1X 等，使得该架构可以适应多种环境的需要，没有与某个具体的产品相绑定. 它与 NAC 架构、NAP 架构的互操作也说明了该架构的开放性.

(2) 安全性. TNC 是对传统网络接入控制技术的扩展，在传统的基于用户身份认证的基础上增加了平台身份认证与完整性验证. 这将对接入网络的终端提出更高的要求，反过来这也增强了提供接入的网络的安全性. 同时每个规范中针对安全问题与隐私问题都具有相应的探讨与解决方案.

(3) 指导性. TNC 的规范内容详细，考虑的问题全面，很多接口定义规范提供了具体的消息流程、

XML Schema 和相关操作系统和编程语言的绑定，如 IF-IMC、IF-IMV 和 IF-TNCCS 等，易于指导产品的实现.

(4) 系统性. TNC 规范自身为一个完整的体系结构，每一个相应的接口都具有子规范进行详细定义，有关完整性度量、报告等核心问题专门有完整性工作组(Integrity Working Group，IWG)制定相应规范与参考模型，与可信计算整体规范既有关联，又自成一个体系.

3.2　TNC 的局限性

虽然 TNC 具有上述的优点，但是它也有一定的局限性，有些局限性是与可信计算本身相关的.

(1) 理论研究滞后. 目前在可信计算领域存在着技术超前于理论的状况，TNC 也不例外. 如何将信任链从终端扩展到网络，使得网络成为一个可信计算环境，这是一个亟需研究的理论问题. TNC 从技术的手段将可信计算技术应用到网络接入控制，但是这种接入的方式尚缺乏可信理论的支撑.

(2) 局限于完整性. TNC 对终端的可信验证基于完整性. 完整性只能保证信息的来源可信与未被修改，并不能保证信息的内容可信. 而且，目前基于完整性的可信验证只能确保软件的静态可信，尚不能确保软件的动态可信. 因此 TNC 并不能完全保证接入终端的平台可信. 另外，目前 TNC 基于完整性验证的架构比较复杂，难于扩展，实现成本高.

(3) 单向性的可信评估. TNC 的出发点是保证网络的安全性，因此该架构没有考虑如何保护终端的安全. 终端在接入网络之前，除了要提供自身的平台可信性证据之外，还应该具有对接入网络进行可信性评估，否则无法保证从网络中获取的服务可信.

(4) 缺乏安全协议支持. TNC 架构中，多个实体需要进行信息交互，如 TNCC 与 TNCS 之间、TNCC 与 IMC 之间、TNCS 与 IMV 之间、IMC 与 IMV 之间都需要进行大量的信息交互，但是 TNC 架构本身并没有给出相应的安全协议，只是简单地介绍了如何进行消息的传递.

(5) 缺乏网络接入后的安全保护. TNC 只是在终端接入网络的过程中对终端进行了平台认证与完整性验证，在终端接入网络之后就没有相应的措施对网络和终端进行保护. 终端平台有可能在接入之后发生状态的改变，因此有必要增加整个接入过程的控制机制. 在 TNC1.3 架构中增加了安全信息动态共享，在一定程度上增强了动态控制功能.

(6) 应用范围具有局限性. TNC 应用目前局限在企业内部网络，难以提供分布式、多层次、电信级、跨网络域的网络访问控制架构. 在 TNC1.4 架构中增加了对跨网络域认证的支持以及对无 TNC 客户端场景的支持，在一定程度上改善了应用的局限性.

4　相关研究

虽然 TNC 只是一种技术架构，但是它开创性地提出了将可信计算机制引入网络，引起了国内外研究者对此更加深入和广泛的研究，核心问题就是如何将信任链从终端扩展到网络，使得网络成为一种可信的计算环境. 针对这个目标，众多学者对以下几个方面进行了深入的研究，包括：(1) 可信网络连接与可信网络体系结构研究；(2) 远程证明与远端可信研究；(3) 可信传输与资源共享研究. 下面对其中的每一个方面进行介绍.

4.1　可信网络连接与可信网络体系结构研究

目前国际上网络访问控制架构主要为微软的网络访问保护 NAP 架构、思科的网络访问控制 NAC 架构①和 TNC 架构. 这 3 种结构都基于以下机制：终端接入网络之前，对终端的平台状态进行度量，如果度量结果满足网络接入的安全策略，则允许终端接入网络，否则将终端连接到指定的隔离区域，对其进行安全性修补和升级. NAC、NAP 和 TNC 技术的目标和实现技术具有很大相似性，同时，由于 3 种技术的发布者自身的背景，3 种技术又存在不同的偏重性，NAC 偏重于接入设备，NAP 偏重于终端和接入服务器，TNC 偏重于可信计算. 在产品方面，Juniper 公司已经研制出符合 TNC 规范的统一接入控制 2.0 的产品②，华为公司推出了 EAD 解决方案③，天融信公司推出了可信网络架构 TNA④.

1983 年美国国防部制定了世界上第一个《可信计算机系统评价准则》TCSEC(Trusted Computer System Evaluation Criteria)[1]，作为补充又推出了可信网络解释 TNI(Trusted Network Interpretation)[2]. TNI 主要强调了信息的秘密性，而对完整性、真实性考虑较少，强调了系统安全性的评价，却没有给出达到这种安全性的系统结构和技术路线.

在可信网络方面，NewArch 项目[1] 提出了“信任调节透明性”(trust-modulated transparency)原

① Cisco Network Admission Control Architecture[EB/OL]. Cisco Corporation. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
② Juniper Product. http://cn.juniper.net/products/ua/
③ Huawei Product. http://www.huawei.com
④ 李鸿培. 可信网络架构概述. 北京天融信公司，2005.11

则，希望将现实社会中的信任关系映射到网络. 基于交互用户双方的信任需求声明，网络可以提供一定范围的服务，若双方完全信任，则其交互是透明、无约束的，否则需要被检查、过滤和约束. 美国高级研究计划局提出的 CHAT(Composable High-Assurance Trustworthy Systems)项目②研究了如何在对安全性、可靠性、可生存性及其它必要属性具有严格要求的条件下，设计出可以验证的可信网络. TRIAD (Trustworthy Refinement through Intrusion-Aware Design)项目[3]研究了通过引入入侵检测设计机制来提高网络系统的可信性.

全国信息安全技术标准化委员会于 2005 年 1 月成立了我国可信计算工作小组. 2007 年 2 月，北京工业大学牵头组织可信计算关键标准的研究，包括芯片、主板、软件和网络 4 个标准. 在可信网络连接标准制定过程中，采用三元、三层、对等、集中管理的可信网络连接架构，如图 4 所示. 通过引入一个策略管理器作为可信第三方，对访问请求者和访问控制器进行集中管理，网络访问控制层和可信平台评估层执行基于策略管理器为可信第三方的三元对等鉴别协议，实现访问请求者和访问控制器之间的双向用户身份认证和双向平台可信性评估. 该架构采用国家自主知识产权的鉴别协议，将访问请求者和访问控制器作为对等实体，以策略管理器为可信第三方，既简化了身份管理、策略管理和证书管理机制，又保证了终端与网络的双向认证，具有很大的创新性.

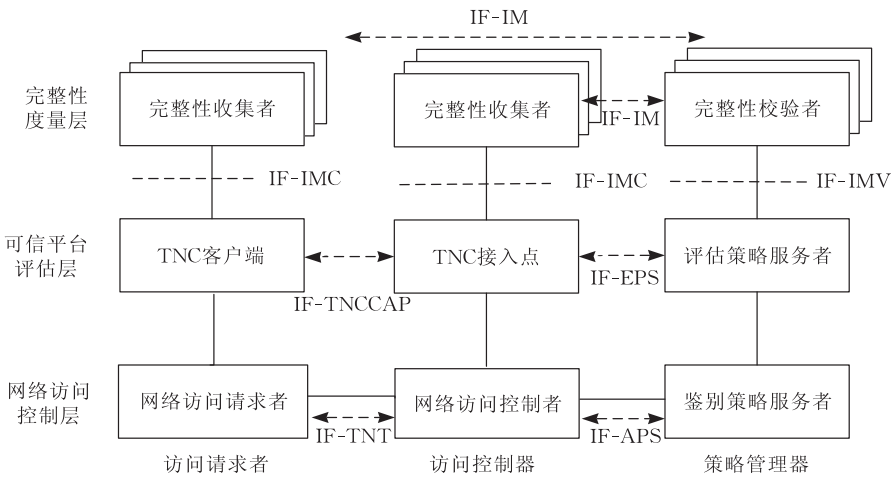

图 4 中国可信网络连接架构

国内学者也开展了可信网络的研究。林闯等人[4-5]提出了可信网络的概念，意图从网络体系结构层面增加安全机制的方式来解决现有网络的脆弱性问题，在保障网络中信息的秘密性、真实性、完整性和可用性的同时，保障网络的安全性、可生存性与可控性. 通过将信任机制集成在网络体系结构中对安全机制进行增强. 提出了可信网络的设计原则，从行为可信的角度对可信网络进行了定义，指出网络与用户的行为及其结果可预期、可管理. 闵应骅认为[6]可信网络是能够提供可信服务的网络，并且服务可以论证其可信赖的. 这里的可信性包括可用性、可靠性、可维护性、安全性、健壮性与可测试性等. 田立勤等[7]针对网络中用户的行为可信进行了研究，在用户身份可信的基础上增加了对用户行为可信的控制与管理，利用贝叶斯网络对用户行为进行多属性条件下的可信预测，基于用户安全行为可信属性进行风险分析与博弈分析，计算出混合的纳什均衡策略，为网络可信提供决策. 周明天等[8]认为可信计算是一个保障体系，其目标是网络可信. 可信计算机系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统. 在可信计算的体系结构中包括可信网络连接与可信网络服务器，确保交易可信. 在可信网络连接中包括物理设备可信、传输可信与接入可信部分，接入可信对应着 TCG 的 TNC. 可信网络服务器中在传统的安全服务器基础上，除了终端安全技术之外，还需要研究服务器的服务可信与对共享资源的保护. 对此我们也提出了自己的学术观点[9-10]：可信性包含许多属性，但是现阶段关注的主要属性是可靠性和安全性. 因此可以通俗地说，可信≈可靠＋安全. 可信网络不仅要解决接入可信问题，还要解决接入之后的网络传输和数据共享的可

① David Clark, Karen Sollins, John Wroclawski, NewArch Project: Future-Generation Internet Architecture [EB/OL]. http://www.isi.edu/newarch/iDOCS/final.finalreport.pdf

② Neumann P G. Principled assuredly trustworthy composable architectures[EB/OL]. http://www.csl.sri.com/neumann/chats4.html

信问题.不过,网络的可信性问题还是近年来随着人们对网络安全的日益重视才开始的,大部分的工作是就可信网络在理论与技术的某个局部目标展开的,并没有形成完整的体系,可信网络的许多研究还处在探索阶段.

4.2　远程证明与远端可信研究

远程证明是指网络中的两个节点,一个节点将自身的某些平台相关信息使用约定的格式向另一个节点报告,使得另外一个节点能够对该节点提供的相关信息进行验证.远程证明的初衷就是允许两个节点在进行交互之前判断对方的平台状态,如果平台状态符合交互要求则允许节点交互,它进一步抽象了网络连接的层次.远程证明机制建立在可信度量、可信报告的基础之上,但是可以脱离可信平台而存在.远程证明为平台间可信交互提供了一个强有力的方式,因此被广泛用于 P2P 网络、Adhoc 网络和 Web Service 等环境中.

可信度量与可信报告是远程证明的关键技术.目前,TNC 架构中采用的是基于 Hash 函数的度量算法,使用平台配置寄存器(Platform Configuration Register,PCR)和存储度量日志(Stored Measurment Log, SML)进行报告.这种机制具有非常大的局限性,具有不便于软件升级、不适应系统配置动态变化、容易绑定到某个特殊的产品以及容易泄露平台配置等缺点.很多研究者在此基础上进行研究,对完整性的度量和报告机制进行拓展和改进,加入软件正确性、风险评估等特性,充实可信度量和报告的机制,使其更加易于实现,减少缺陷,提高安全和可信性.

针对远程证明的研究主要集中在远程证明的协议和协议交换信息及格式等方面.对远程证明协议的研究包括:使用形式化对协议进行验证以发现协议的安全漏洞并进行改进[34];更改协议的形式,由带有可信第三方的协议改为直接匿名通信的协议[35]等;对协议交换信息及格式的研究包括:对基于二进制度量的信息进行扩充,包括基于属性的信息[36]、基于语义的信息[37]等;对信息的格式进行扩充,包括基于 XML 描述的完整性参考值的报告等.

远端可信与远程证明非常相似,只不过远端可信要求提供的证据比远程证明更加具体,往往对某个平台、某个实体或者某个任务进行验证.远端可信的相关研究包括 Pioneer 系统基于准确计算对方代码执行时间的方法判断远端平台可信[15];SWATT 采用类似的方法验证嵌入系统的完整性[16];Haldar 提出了基于语言虚拟机的方法[14];Sadeghi 提出基于属性的远程证明方式验证远端平台可信[13];Rick 等提出一个检查远端平台真实性的方法[17];Chen 提出带有验证原语的方法确认远程软件执行的可信①;Falcarin 提出了 aspect-oriented 编程的方法验证远端可信[18].

4.3　可信传输与可信资源共享研究

联网的根本目的在于数据传输和资源共享.网络连接仅仅是网络业务处理的第一步,因此仅有网络连接的可信是不够的,还需要数据传输的可信和资源共享的可信.TCG 目前只研究了 TNC,尚缺少对数据传输的可信和资源共享的可信的研究[9].

可信传输具有两个层面的含义:传输数据可信和传输行为可信.传输数据可信是指数据在传输过程中是可信的(安全的和可靠的)以及网络实体间在网络交换过程中的收发都能提供可信证据,在每一次转报过程中都要提供经手的证明[8].由于 TCP/IP 协议设计时只考虑数据的转发,而没有考虑数据传输的安全,因此最好的解决方法是对其进行扩展.传输行为的可信是指在传输过程中,主体的传输行为的历史记录反映主体行为是否违反安全规则的统计特性以及对传输行为的实时监督.目前,研究行为可信比较典型的是人工智能中智能代理研究.曲延文对软件行为进行了深层次的刻画,提出了软件行为学[19].

基于可信硬件的资源共享目前也是研究热点.数字产品(软件、数据、媒体)的使用管理涉及可信资源共享.在数字版权管理系统中,数字内容的解密使用、使用权利的解析验证由客户端 DRM 应用程序负责,需要采用各种技术手段来确保数字内容的可信应用.可信计算能够支持保护数字版权,因此可信计算对于资源共享具有独特的优势.Sandhu 等提出了基于可信计算平台的安全信息共享模型 PEI[20-21].基于可信计算技术的访问控制模型[22]扩展、基于可信计算技术增强网格安全[23]也促进了资源共享的研究.

5　TNC 的发展趋势

随着可信计算研究的不断深入,目前针对终端

① Chen Yu-Qun, Venkatesan Ramarathnam et al. Oblivious hashing: A stealthy software integrity verification primitive. Microsoft Research Report [EB/OL]. http://research.microsoft.com/~yuqunc/papers/ohash.pdf

的可信性研究必然会拓展到网络中.网络连接只是网络活动的第一步,连网的主要目的是数据交换和资源共享,这方面还缺少可信技术规范[9].我们认为将可信计算思想和机制引入到网络中,使得网络成为一个可信的计算环境,将会是后续的研究热点.网络环境比终端更加复杂,需要从理论层面和技术层面同时进行研究.不但需要对可信度量、可信报告等可信计算核心机制进行深入研究,还需要从理论层面对可信网络环境进行研究,对网络中数据的可信传输与资源的可信共享进行研究.下面对每一个内容进行探讨.

5.1 可信网络环境的理论模型

研究如何将可信计算机制引入到网络中,使得网络成为可信的计算环境,首先要研究现有网络中各个节点之间的信任关系,研究终端平台上各个组件之间的信任关系,对节点与组件之间的关系进行刻画,建立可信网络环境的理论模型.人们已经对信任模型进行了深入的研究,信任模型是对传统安全模型的扩展和增强.目前,基于各种数学理论的网络信任模型很多.可信网络环境的理论模型具有可信计算自身的特点,和这些网络信任模型既有联系,又有区别.我们可以根据网络信任模型的构造理论、构造方法、相应的数学基础,根据可信计算平台的可信根、信任链的特点,构造可信网络环境的理论模型.

目前网络信任模型多用于网络中不同节点间信任关系的描述,这些模型都从某些特定的方面描述了信任度在信息系统中的表示和计算方法,但仍存在下列问题:(1)这些模型只考虑节点在网络中的行为、声誉等因素,而未考虑节点本身的计算环境是否值得信任.这一点往往正是容易被攻击者利用而对网络实施攻击的主要途径.(2)缺少在不同网络信任模型之间建立一种信任评价比较尺度的研究.(3)没有反映评价者自身的权威性对评价结果的影响度.(4)评价信任度的粒度比较粗,大多仅用信任、不信任、不确定来简单刻画.

在网络信任模型中,每个节点都有自己的信任度,节点是对等的,都可发起和接受其它节点的信任度量.而在 TNC 中,节点并非都是对等的,总是存在一个节点作为度量的决策者,其它节点接受该节点的策略决策.因此研究可信网络环境的理论模型时,可以借鉴信任模型的某些思想.比如,对平台可信性的度量,其实就是考察组成平台的各组件是否值得信任.在网络中可信的度量并不是任何组件都可以发起的,也不需要两两组件间都要自发进行信任的度量来决定是否通信,需要有一定的组织结构,由某些组件来完成可信性度量的功能,一旦这些组件判定其它组件为可信,就可以相互信任相互通信.

5.2 可信度量与可信报告研究

目前 TNC 的度量采用的是基于数据完整性度量的方法,虽然可以保证系统的数据完整性,但是并不能完全保证系统的可信性.根据我们的"在现阶段可信≈可靠+安全"的学术观点[9-10],数据完整性只是可信性的一个组成部分.可信度量应当对系统的可信性(主要是可靠性和安全性)进行度量,而不是只对数据完整性进行度量.但是,由于进行可信性的度量在技术上尚有许多困难,因此目前基于数据完整性的度量仍然是有积极意义的.

可信度量的一种方法是借鉴采用系统评测的方法.这种方式能够在很大程度上保证系统的正确性.同时,基于系统安全评估与预警的方式,对系统各个组件进行安全风险评估,可以消除多个组件之间关联的风险.可信的度量凭据应能全面表现节点状况,获得全面、真实可靠、划分粒度适中、满足应用的基础信息,在尽量不影响网络正常流量的情况下,完成包含身份、行为和环境信息的实时凭据提取和生成.

可信报告与可信度量紧密相关.可信报告需要设计高效、安全、可扩展的报告协议.目前可信计算规范对于底层安全传输协议进行了规定,考虑到可能存在的中间人攻击,并给出了相应的解决方案,但是没有给出具体的协议(见本文第 2 页注释③).应当对可信报告协议进行形式化分析和验证,消除潜在的安全漏洞.

5.3 可信网络传输与可信资源共享研究

可信传输方面,除了继续采用密码对数据加密和对通信进行认证之外,还可以通过对传输协议进行扩展,为传输的每一个数据报增加可信标签,用于传输路径上的信息定位、服务质量监督等功能.同时,通过传输行为进行实时监控与审计,保证传输行为的可信.IPv6 具有非常好的可扩展性,通过分析 IPv6 扩展的方式,在 IPv6 上增加可信标签和行为监控,可以进行可信传输方面的实验研究.

可信资源共享方面,可以借助传统的访问控制理论和方法、网格的访问控制理论和方法、P2P 环境下的访问控制理论和方法以及安全多方计算的理论和方法,并对这些理论与方法进行可信性增强,设计层次化、跨可信域的、基于可信硬件的访问控制方法,达到主体对客体的安全访问,实现资源的可信共享.访问控制模型可以结合信任关系进行扩展,访问控制机制可以通过可信硬件进行增强和改进,同时将访问控制模型和信任模型结合起来.

在研究资源共享的过程中，授权是重要的环节.现有的授权模型大多依据身份、角色、访问控制策略或其它历史信息做出判断，并没有考虑在用户连接、授权过程中及授权后，用户行为或平台环境发生改变该如何处理.当授权完成后，无法对授权结果进行自动调整，不能适应普适计算、面向服务计算等分布计算环境中交互行为不可预知性和动态性的要求.当存在不同敏感程度的资源需要保护时，还应能提供多级安全保护的能力.所以，需要将体现用户行为和平台环境的信任度与通常的访问控制机制相结合，尽量使所计算的信任度与用户真实情况相符，以得到最佳的授权结果.而且还应根据资源提供者对哪些信任凭据更关注，其信任度计算方式是否与环境相适应，并结合资源共享过程中用户的行为变化，不断调整授权策略，得到与环境相适应的基于用户行为的动态授权.

6　我们的工作

在国家 863 计划项目的支持下，我们对可信网络连接的一些理论与关键技术进行了研究[24].在可信网络连接理论方面，对可信的概念进行了研究和定义，提出了统一网络访问控制架构，并对 BLP 模型进行了可信扩展；在可信度量与报告方面，提出了可信度量模型，对可信报告协议进行了拓展，并对远程代码可信执行问题进行了研究；在可信网络连接系统实现方面，遵从 TNC 1.2 架构规范，在网络访问控制架构的基础上实现了客户端与服务器端的双向平台认证，包括平台配置及环境的度量和报告，实现了可信网络连接原型系统；在可信资源共享方面，基于信任理论与可信环境构造理论对访问控制机制进行扩展.具体内容包括：

(1)针对目前可信网络连接架构缺乏延续性、局限于静态完整性的现状，在分析现有网络访问控制架构的基础上，根据可信网络连接的需求，对信任与可信概念进行研究，给出了符合可信网络连接本质的概念定义.通过分析网络访问控制机制的局限性，结合可信网络连接的本质要求，提出了融合网络访问控制机制、网络安全机制和系统访问控制机制的统一网络访问控制 UNAC 模型，将只关注秘密性的 BLP 模型进行动态可信性扩展，提出了 TE-BLP 模型，使其能够通过可信度与统一网络访问控制模型结合起来[24].

(2)针对目前可信度量机制缺乏系统度量模型、基于静态完整性的现状，提出一套完整的可信度量流程模型，涵盖可信度量的需求、目标、细化内容、度量机制、度量结果等阶段，在度量机制中提出了可信度量模型 TMM，该模型能够刻画可信度量的需求、目标和细化内容，利用层次化分析方法确定模型中各个组件的权重值，通过度量函数计算可信度.对证据的可信生成、可信存储与可信报告进行研究，改进了 TCG 的可信报告机制，提出了一种安全的远程证明协议 TRP，该协议能够实现证据信息的可信报告，保证信息的秘密性、新鲜性、真实性和完整性.提出了远端代码可信执行问题，并基于虚拟化技术与行为可信技术分别提出解决该问题的远端代码可信执行框架，并论证了两种框架的安全等价性[24-26].

(3)针对目前可信网络连接架构缺乏系统实现的现状，从底到上实现了完整的可信网络连接原型系统.研究了可信网络连接的支撑技术，对基于端口的访问控制技术及与之相关的 EAP、RADIUS 等网络协议进行研究，在此基础上设计和实现网络接入系统并支持多种认证方式.研究了可信网络连接的关键机制，对远程证明的方法和在可信网络连接中的应用进行研究，设计并实现了基于完整性挑战与完整性验证协议的远程证明，实现了系统平台间双向证明.实现基于远程证明的完整性度量器和验证器，并完成了可信网络连接的整体流程[24].

(4)在实现可信网络连接的基础上，提出了一种基于信任度角色的授权预测控制模型.从网络节点行为可信的角度出发，利用可信计算技术提供的密码功能和平台环境保护功能，将体现用户行为和平台环境的信任度与访问控制机制相结合，根据资源共享过程中用户行为的变化，预测并能及时调整授权策略，从而得到动态合理的授权控制以保障资源共享过程的安全可靠[27-29].

在将来的工作中，我们计划通过对基于信任度的角色授权模型进行预测控制，实现全面的、动态的连接及授权体系，收集更完备的上下文证据信息，使其能够更好地反映用户及其平台的可信度，并实现 MAP 服务器以方便灵活地进行动态接入控制，同时优化体现环境要求的信任度计算参数以更好地实现可信可控的资源共享.

7　结　论

TNC 目前已经迈出了将可信计算机制向网络延伸的第一步.国内外的研究者已对其进行了广泛深入的研究，取得了许多重要的研究成果.但是，如何将可信计算机制引入到网络，使得网络成为可信

计算环境的研究才刚刚开始.目前,就如何将信任链扩展到网络的研究而言也存在很多问题,如可信网络模型、内容可信、行为可信、传输可信、资源可信共享等,有待学术界与产业界研究解决.

参 考 文 献

[1] Department of Defense Computer Security Center. DoD 5200.28-STD. Department of Defense Trusted Computer System Evaluation Criteria. USA: DOD, December 1985

[2] National Computer Security Center. NCSC-TG-005. Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria. USA: DOD, July 1987

[3] Ellison R J, Moore A P. Trustworthy refinement through intrusion-aware design (TRIAD): An overview//Proceedings of the 3rd Annual High Confidence Software and Systems Conference, 2003

[4] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. Chinese Journal of Computers, 2005, 28(5): 751-758(in Chinese)
(林闯,彭雪海. 可信网络研究. 计算机学报, 2005, 28(5): 751-758)

[5] Lin Chuang, Ren Feng-Yuan. The new controllable and extensible generation internet. Journal of Software, 2004, 15(12): 1815-1821(in Chinese)
(林闯,任丰原. 可控可信可扩展的新一代互联. 软件学报, 2004, 15(12): 1815-1821)

[6] Min Ying-Hua. Trusted system and network. Computer Engineering & Science, 2001, 23(5): 21-23(in Chinese)
(闵应骅. 可信系统与网络. 计算机工程与科学, 2001, 23(5): 21-23)

[7] Tian Li-Qin, Lin Chuang. A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network. Chinese Journal of Computers, 2007, 30(11): 1930-1938(in Chinese)
(田立勤,林闯. 可信网络中一种基于行为信任预测的博弈控制机制. 计算机学报, 2007, 30(11): 1930-1938)

[8] Zhou Ming-Tian, Tang Liang. Development of trusted computing. Journal of Electronic Science and Technology of China, 2006, 35(4): 686-697(in Chinese)
(周明天,谭良. 可信计算及其进展. 电子科技大学学报, 2006, 35(4): 686-697)

[9] Shen Chang-Xiang, Zhang Huan-Guo, Feng Deng-Guo, Cao Zhen-Fu, Huang Ji-Wu. Survey of information security. Science in Chian Series F, 2007, 50(3): 273-298

[10] Zhang Huan-Guo, Luo Jie et al. Research development of trusted computing. Journal of Wuhan University (Natural Science Edition), 2006, 52(5): 513-518(in Chinese)
(张焕国,罗捷等. 可信计算研究进展. 武汉大学学报(理学版), 2006, 52(5): 513-518)

[11] Stumpf Frederic, Tagreschi Omid, Roder Patrick, Eckert Claudia. A robust integrity reporting protocol for remote attestation//Proceedings of the 2nd Workshop on Advances in Trusted Computing. Tokey, Japan, 2006

[12] Brickell E, Camenisch J, Chen L. Direct anonymous attestation//Proceedings of the 11th ACM Conference on Computer and Communications Security. NY, USA: ACM Press, 2004: 67-77

[13] Sadeghi A-R, Stuble C. Property-based attestation for computing platforms: Caring about properties, not mechanisms//Proceedings of the 2004 Workshop on New Security Paradigms, 2005: 67-77

[14] Haldar Vivek, Franz Michael. Symmetric behavior-based trust: A new paradigm for internet computing//Proceedings of the 2004 Workshop on New Security Paradigms, 2004: 79-84

[15] Seshadri A, Luk M, Shi E, Perrig A, van Doorn L, Khosla P. Pioneer: Verifying integrity and guaranteeing execution of code on legacy platforms//Proceedings of the Symposium on Operating System Principles, 2005: 1-16

[16] Seshadri A, Perrig A, van Doorn L, Khosla P. SWATT: Software-based attestation for embedded devices//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, 2004: 272-282

[17] Kennell Rick, Jamieson Leah H. Establishing the genuinity of remote computer systems//Proceedings of the USENIX Security. Washington, 2003: 295-310

[18] Falcarin P, Scandariato R, Baldi M. Remote trust with aspect-oriented programming//Proceedings of the Advanced Information Networking and Applications. Vienna, Austria, 2006: 461-465

[19] Qu Yan-Wen. Software Behavior. Beijing: Publishing House of Electronics Industry, 2004(in Chinese)
(曲延文. 软件行为学. 北京: 电子工业出版社, 2004)

[20] Sandhu R, Ranganathan K, Zhang X. Secure information sharing enabled by trusted computing and PEI models//Proceedings of the ACM Symposium on Information, Computer, and Communication Security, 2006

[21] Krishnan R, Sandhu R, Ranganathan K. PEI models towards scalable, usable and high-assurance information sharing//Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, 2007: 145-150

[22] Sandhu R, Zhang X. Peer-to-peer access control architecture using trusted computing technology//Proceedings of the SACMAT05, 2005: 147-158

[23] Mao Wen-Bo, Yan Fei, Chen Chun-Run. Daonity: Grid security with behaviour conformity from trusted computing//Proceedings of the 1st ACM Workshop on Scalable Trusted Computing. 2006: 43-46

[24] Zhang Li-Qing. Some theories and key technologies of trusted network connection [Ph. D. dissertation]. Wuhan University, Wuhan, 2008(in Chinese)
(张立强. 可信网络连接的一些理论与关键技术研究[博士学位论文]. 武汉大学, 武汉, 2008)

[25] Zhang Li-Qiang, Chen Lu, Zhang Huan-Guo, Yan Fei. Trusted code remote execution through trusted computing and virtualization//Proceedings of the SNPD 2007. Qingdao, 2007: 39-44

[26] Zhang Li-Qiang, Zhang Huan-Guo, Zhang Xian-Tao, Chen Lu. A new mechanism for trusted code remote execution// Proceedings of the CISW 2007. Harbin, 2007: 574-578

[27] Wen Song. Research on access control based trusted computing [Ph. D. dissertation]. Wuhan University, Wuhan, 2009 (in Chinese)
(文松. 基于可信计算的访问控制研究[博士论文]. 武汉大学, 武汉, 2009)

[28] Chen Lu, Zhang Huan-Guo, Zhang Li-Qiang, Li Song, Cai Liang. A peer-to-peer resource sharing scheme using trusted computing technology. Wuhan University of Natural Sciences, 2008, 13(5): 523-527

[29] Chen Lu, Zhang Huan-Guo, Zhang Li-Qiang, Cai Liang. A new information measurement scheme based on TPM for trusted network access//Proceedings of the MEMS 2007. 2007: 574-577

ZHANG Huan-Guo, born in 1945, professor. His research interests include information security, cryptography, trusted computing etc.

CHEN Lu, born in 1979, Ph. D. candidate. Her research interests include information security and Trusted Computing.

ZHANG Li-Qiang, born in 1979, Ph. D.. His research interests include information security and Trusted Computing.

Background

This work is supported by the National High Technology Research and Development Program (863 Program) of China (grant No. 2006AA01Z442 and No. 2007AA01Z411), the National Natural Science Foundation of China (grant No. 60673071 and No. 60970115).

The projects are involved in the key theory and technology of Trusted Network Connection. The researches and applications of Trusted Network Connection have yielded substantial achievements. Many research organizations have been taking deep researches into Trusted Computing and Network Access Control theory and technology, but Trusted Network Connection itself is still in a situation which the development of technology exceeds the development of theory. This paper introduces the development history, architecture, specifications, related researches, merits, restrictions, research trends and future directions of TNC in details. This authors' work focuses on extending the Trusted Computing mechanism from endpoint to network, both in theory extension and demonstration system. Aiming at current situation of Trusted Network Connection which lacks continuity and has limits in static integrity, the authors proposed the Unified Network Access Control model, TE-BLP model, Trusted Measurement Model, and Trusted Resource Sharing Model. Aiming at the current situation of trust report which lacking trusted evidence transporting mechanism, the authors proposed a secure remote attestation protocol TRP and trusted code remote execution mechanism. To improve the current situation that Trusted Network Connection lacks whole system implementation, the authors also designed and implemented Trusted Network Connection prototype which complies with Trusted Network Connection specification 1.2.