异步图书
www.epubit.com.cn

闫建红 著

可信计算

远程证明与应用

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

闫建红 著

可信计算

远程证明与应用

人民邮电出版社
北京

图书在版编目（CIP）数据

可信计算远程证明与应用 / 闫建红著. -- 北京 : 人民邮电出版社, 2017.12
ISBN 978-7-115-47578-7

Ⅰ. ①可… Ⅱ. ①闫… Ⅲ. ①电子计算机－安全技术 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2018)第002155号

内 容 提 要

可信计算是信息安全的一种新技术和新体系结构。远程证明是可信计算平台的重要功能之一。本书在国内外学者部分研究成果的基础上，介绍了作者在可信计算中的远程证明及其应用方面多年的研究成果。本书分为8章，主要包含了信息安全概述、可信计算、基于混合加密的可信软件栈数据封装、动态属性证明协议、度量行为信息基的可信证明、可信远程证明在DRM中的应用、基于TPM的物联网安全等内容。

本书可作为信息安全及相关专业高年级本科生和研究生教材，也可供从事信息和网络安全、可信计算相关研究和开发的人员参考。

◆ 著　　闫建红
责任编辑　傅道坤
责任印制　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京印匠彩色印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：11
字数：221千字　　2017年12月第1版
印数：1－1 200册　　2017年12月北京第1次印刷

定价：69.00元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字20170147号

关 于 作 者

闫建红，副教授，博士，于 1994 年在哈尔滨建筑大学计算机系获学士学位，2004 年在太原理工大学计算机软件与理论专业获硕士学位，2012 年在太原理工大学计算机应用技术专业获博士学位，当前主要从事网络安全、机器学习等方面的教学与科研工作。先后主持与参与山西省自然基金项目、山西省基础平台项目、山西省科技高等学校科技项目等 5 项工作，近年来以第一作者的身份在国内外学术刊物上发表论文 10 多篇（其中 SCI、EI 索引两篇，核心期刊以上 8 篇），参与编写学术著作和教材两部。

致　谢

在本书的写作过程中，得到了单位领导、同事、老师、同学、家人的大力支持和无私帮助，在此谨向他们表示衷心的感谢！

首先感谢太原师范学院和计算机系的领导对我的帮助和鼓励，给我提供了优越的工作环境；感谢在一起工作的同事，使我能在一个轻松的氛围中工作。

感谢我的老师彭新光教授。彭教授胸怀宽广，他渊博的学识和敏锐、活跃、开放式的思维，对前沿技术不懈的追求，严谨求实的治学态度，孜孜不倦的科研精神，使我受益匪浅。

感谢我的家人，感谢父亲的鼓励和开导，生活中指引我前进；感谢母亲对我人格的塑造；感谢哥哥多年以来对母亲的照顾；感谢我的丈夫对我工作上的支持和理解；感谢我的孩子，他懂事、自立，使我能全身心投入到工作中，我心中备感欣慰。

感谢所有对本书出版提供帮助的单位、项目和个人！

最后，向曾经给予我帮助，但未曾在上面提到的所有老师、同事、同学和朋友一并致谢！

前　言

信息技术（Information Technology，IT）是当今社会中最具活力的生产要素和战略资源。淘宝、微信、支付宝等技术和工具深入应用在社会的方方面面。信息技术的迅速发展给人们的生活带来更大便利的同时，危害信息安全的事件也不断发生，如敌对势力、恶意软件、黑客的攻击。信息安全关乎我们的生活，也关系到国家和社会的安全。如 2013 年爆发的“棱镜门”事件，世界各地的网民之前绝不会想到他们在使用谷歌、Facebook、苹果等知名公司的网络产品进行社交、办公或存储信息时，他们屏幕的背后正隐藏着美国情报部门的身影。2014 年 12 月，12306 官网遭受撞库攻击，10 多万用户数据遭泄露。2015 年 7 月，意大利专业黑客公司 HackingTeam 被黑，400GB 内部资料以及攻击工具被泄露。2016 年夏季，美国民主党全国委员会、筹款委员会、竞选团队被黑客组织入侵，近 2 万封邮件被维基解密披露，邮件显示希拉里涉嫌抹黑竞争对手并可能涉嫌洗钱等财务问题。2017 年 5 月中旬出现的勒索病毒 WannaCry 席卷全球网络等。鉴于此，信息安全在当今社会中的位置将越来越重要。

网络和信息安全技术也在不断变化和发展中，传统的安全技术——防火墙、杀毒软件、入侵检测已不能保证信息的安全。面对各种各样的恶意攻击和病毒，我们往往通过加大病毒库、砌高防火墙、增加入侵检测的复杂度等手段防御，但问题依然层出不穷，尤其对于在计算机硬盘上驻存的一些恶意程序更显得无能为力，这些恶意程序会破坏系统，并在网络肆意传播。整个信息安全状况令人担忧：误报率多、安全投入增加、维护与管理成本高且更加复杂，使得使用信息系统的效率降低；尤其对一些新的病毒攻击，入侵检测毫无防御能力。

针对这些问题，我们需要改变过去的思维方式，改变被动防御的局面。在用户终端，如果每个用户每次进入网络时都需要授权和证明，操作需要验证，就会防患于未然，攻击性事故就会减少。只有将绝大多数不安全因素从终端源头进行控制，并从芯片、主板、BIOS、操作系统入手，综合采取措施才能提高网络的安全性。

可信计算（Trusted Computing，TC）正是以此为出发点，包括硬件层面、操作系统层面、应用程序层面，通过在平台内部引入可信硬件设备作为可信根，采用软硬件相结合的技术，建立一条信任链，一级认证一级，一级信任一级，把信任关系扩大到整个计算机系统，这样就能确保计算机系统是可信的。可信计算的主要思想是在计算机中的主板上嵌入一个安全芯片，通过其提供的度量、身份证明和密钥功能来提高系统的安全性。可信计算组织（Trusted Computing Group，TCG）已经对可信计算的相关技术和规范做了详细的定义，其核心是称为可信平台模块（Trusted Platform Module，TPM）的安全芯

片。每个 TCG 平台都拥有一个 TPM，以密码技术为支持，以安全操作系统为核心，从而提供了一种对终端平台运行环境、配置进行可信评估的技术。PC 平台上的体系结构主要分为 3 层：TPM、TSS（TCG Software Stack，TCG 软件栈）和应用软件。可信计算技术可以用在各种不同的设备上，包括安全协处理器、密码加速器、个人令牌、软件狗以及增强型 CPU、安全设备和多功能设备等，可以有效地解决因不安全终端接入网络而引起的安全威胁事件，将病毒、蠕虫等各类攻击真正拒绝于网络之外。可信计算技术在未来的网络安全领域将有广泛的应用前景。

远程证明是指一个节点将自己平台的某些信息使用约定的格式和协议向另一个节点报告，使得另一节点能够获得这些信息，并判定该平台的可信状态，其目的是保证两个节点的身份和安全属性符合对方的要求，其平台状态是可靠的。而在可信计算平台上的“远程证明”是指在平台上使用身份认证密钥对当前存储的 PCR 值进行签名，然后报告给远程挑战者其平台的状态。这是建立在可信度量、可信报告基础之上的技术，也是实现可信网络的重要基石。远程证明对于实现高可信网络服务环境，加固信息安全纵深防御体系有极其重大的理论和应用价值，对云计算、移动设备，数字版权管理、物联网等安全网络应用系统领域的可信证明，也具有较好的技术参考价值和应用前景。

远程证明中的相关对象需要加密存储。为了提高加密效率，必须对可信计算的软件架构进行研究，尤其是对其中的密封、绑定等关键技术进行分析，这样不仅能方便用户使用，还能为其安全性提供分析基础，从而降低安全风险。如果改进其中制约性能的密码算法，也能提高远程证明中对象的加密存储效率。

远程证明建立在 TSS 和应用软件之间，而行为证明是在应用软件安装之后，对远程行为进行度量。为了解决这个问题，首先要进行远程证明，目前有二进制证明和属性证明两种方法。属性证明能隐藏平台软件和硬件的配置信息，是静态的，不能动态验证现在正在运行的平台实时信息。因此需要设计能动态验证运行平台的实时信息且不会暴露平台配置信息的方法，以保证协议的可行性和保密性。

为了确认验证之后应用程序是否有恶意行为，是否已经被恶意攻击，有必要对验证之后的行为进行控制和度量。软件行为学是建立在范畴论等数学基础上的类型描述语言，它作为描述软件行为语义范畴的方法，是建立数学方法与程序设计的桥梁。软件行为的可信判定方法通过动态度量对平台软件行为进行可信判定。根据可信计算动态度量的实际需求，软件行为可以作为平台的行为证明模型，基于行为的验证保证在平台验证安全后，对远程的行为进行监控。经过组合之后的度量，可确保平台应用软件运行时的可信。

可信计算的远程证明可以应用到数字版权管理（Digital Rights Management，DRM）中。DRM 技术所面临的问题之一是如何确保数字内容的使用是安全的，确保可信的用户不会得到受保护的数字产品的非法拷贝。这就要求必须建立某种机制，保证设备是可信的，而仅仅靠传统上的密钥保护显然是不够的。目前，DRM 系统的安全瓶颈在于用户端软件和数字内容许可证的保护。可信计算技术的产生和发展为 DRM 的安全使用提供了

很好的技术支持。授权用户可以得到数字内容的解密密钥，而密钥又被硬件芯片所保护，加密技术绑定硬件，从而防止了非法拷贝。在 DRM 中，数字内容的解密使用、权利的解析验证由客户端负责，需要使用各种技术手段保证数字内容的可信使用。通过将 DRM 系统和可信计算的新技术结合起来，用户可以更安全和更可靠地使用数字产品。

可信计算可以严格地进行身份识别、信任启动、平台认证和加密传输。物联网可以利用这些功能，解决过去只依靠软件机制进行安全保护所带来的软件漏洞问题，防止恶意软件利用漏洞攻击。感知层进行身份认证和加密存储，网络层进行可信网络连接，应用层防止数据泄密，这样利用 TPM 进行层层保护，可以保证物联网系统安全可靠地运行。

本书聚焦于可信计算和远程证明。为了提高证明中相关数据的加密存储效率，本书介绍了对软件栈进行的研究，对远程证明中的静态和暴露隐私的问题进行的改进，对平台安全属性证明之后的行为证明进行的研究，对可信计算的远程证明在 DRM 中的应用进行的设计，对基于 TPM 的物联网在可信启动、平台认证和在传输数据中的远程认证进行的设计。

本书内容共分 8 章，具体如下。

第 1 章，“信息安全概述”：主要介绍信息安全的现状，以及各种攻击手段和防御措施，还介绍了传统信息安全技术存在的局限性。

第 2 章，“可信计算”：综述了可信计算在国内外的发展状况和安全基础设施的基本概念，对可信计算进行了简要介绍，对可信计算的研究方向进行了说明；接着对可信计算平台体系结构做了详细描述；然后对可信计算平台的核心机制进行分析；最后详细对 TCG 提出的两种远程证明方案进行了探讨，为后面章节做了知识上的铺垫。

第 3 章，“基于混合加密的可信软件栈数据封装”：介绍了可信计算软件栈的结构，详细说明密封和解封的过程，分析并指出可信计算的 RSA 密钥机制是制约速度的原因。为此，本章提出将混合密钥机制的思想引入可信计算的设计，改进可信密码模块功能函数。

第 4 章，“动态属性证明协议”：对证明协议的表示进行了定义，并对属性证明协议进行形式化表示。本章提出了动态属性证明方案，在基于证书的属性证明的基础上加入二进制验证机制，增加了对系统实时状态的验证；还从证明协议、证明模型和实验 3 个方面对动态属性证明协议进行了详细的介绍，并对其安全性进行了分析。

第 5 章，“度量行为信息基的可信证明”：在软件行为学理论的基础上，根据可信计算动态度量的实际需求，定义了基于软件行为证明的动态度量相关概念，将 Merkle 散列树引入行为树中，对行为进行动态度量。本章还设计了证明度量行为信息基模型，并通过实验进行分析。

第 6 章，“可信远程证明在 DRM 中的应用”：介绍了 DRM 系统的基本原理，详细讨论 DRM 内容的完整性机制，指出其存在的技术问题。本章在可信计算的平台上对 DRM 系统的模型进行了设计，详细分析其过程，对用户的身份证明、许可证服务器和用户的

远程证明、RS 对 DRM 控制器的安全属性证明协议进行了设计。本章对内容下载、权利协商和权利包的相关协议进行了整体设计，最后对该设计进行了安全性分析。

第 7 章，“基于 TPM 的物联网安全”：分析了物联网安全所面临的问题，指出基于 TPM 的物联网系统解决步骤，设计了利用 TPM 的密钥系统进行身份认证；利用平台度量功能进行平台认证和加密存储，利用绑定功能进行远程传输和远程认证；最后使用基于 TPM 的软件栈进行实现。

第 8 章，“总结与展望”：对本书做了总结，对下一步的研究进行了展望，并指出可信计算的研究领域和发展方向，最后探讨了下一步信息安全的热点问题。

本书论述的可信计算远程证明的观点有以下特点。

（1）基于混合加密的可信软件栈数据封装

分析可信计算软件栈的结构，尤其对密封和解封过程进行研究。TSS 层与数据密封有关的功能接口函数是 Tspi_Data_Seal 和 Tspi_Data_Unseal，用 Sealing 方法加密数据，并且用解封方法对其进行解密。随着数据块的增大，解封时间基本以线性增加，对更大数据的密封将需要更长的时间。指出可信计算的 RSA 密钥机制是制约速度的原因，为此，提出将混合密钥机制的思想引入到可信计算的设计中，改进可信密码模块功能函数。改进后的方法能有效地减少加密时间，比较适合对较大的数据量进行密封，从而以较小的性能代价保障了用户数据的安全。

（2）动态属性证明协议

二进制方法和基于属性证书的证明是可信远程证明的两种证明方法。属性证明能隐藏平台软件和硬件的配置信息，是静态的，不能动态验证正在运行的平台的实时信息。本书结合这两种方法的优点，提出了一种基于动态属性的证明协议，并将二进制证明、属性证明结合到该协议中。在获得属性证书的过程中依赖于第三方，第三方提供了加解密服务。在第二阶段的动态属性证明中，其不再是静态的，而是示证者和验证者的一次二进制证明。第一阶段所得到的证书在后面可以多次使用。而可信第三方作为属性配置证书的颁发者可以离线；第二阶段是建立在示证者和验证者之间的证明。通过比较证书中的平台配置寄存器（Platform Configuration Register，PCR）值和实时得到的 PCR 值，检验当前示证者是否满足一定的属性要求，以便验证者允许示证者使用它的服务。

（3）度量行为信息基的可信证明

提出将 Merkle 散列树应用到 TPM 的行为证明中，利用其灵活性和计算时间短的特性完成对行为的动态验证。给出创建证明度量行为信息基 AM_AIB 的过程，根据当前行为的度量值，得到该时刻的 root_hash 值，并且将 root_hash 用于远程证明。利用 Merkle 散列树计算时间短的特性，在验证过程中只验证客户端的 root_hash，以保护客户端的隐私。root_hash 由 TPM 签名，传递给服务器端验证，如果和服务器端的 root_hash 一致，表明该行为是可信的。还可根据行为特性设计不同粒度的行为信息基。该模型验证方式

灵活，能提高时间性能、保护平台隐私，还克服了基于属性验证的静态特点，确保了平台应用软件运行时可信。

（4）基于可信远程证明的数字版权管理

在基于可信计算的平台上对 DRM 系统的模型进行了设计。提出内容服务器（Content Server，CS）对用户的身份证明使用 DAA 方法，从而保护了用户的隐私，防止了 DoS 攻击；在许可证服务器（Right Server，RS）和用户的远程证明中，提出将密钥协议引入可信计算，在 TPM 内部产生相应的 RSA 密钥，用 RSA 密钥产生用来加密的会话密钥，对数字内容权限加密，并通过生成的随机数防止重放攻击，防止恶意程序攻击。RS 对 DRM 控制器的安全属性证明使用动态属性的远程证明方法，通过度量行为信息基对系统的行为进行实时的监控。对内容下载、权利协商和权利包的相关协议进行了一个整体的设计，通过安全性分析，指出其能保证 DRM 内容和 RO（Rights Object）的完整性和机密性，防止对 CS 和 RS 的攻击，具有不可否认性，并保证了 DRM 控制器的安全性。

（5）基于 TPM 的物联网安全

传统的物联网使用软件机制进行保护，但恶意软件常常利用软件漏洞篡改环境和数据，使平台在一个不可靠、不安全的环境下运行。基于 TPM 的物联网就是利用其特有的软硬件机制，利用 TPM 严格的平台度量功能和密钥体系，保障物联网在感知层、网络层和应用层的平台存储和传输的安全。

本书提到的实验使用 TPM Emulator 模拟 TPM 芯片。对可信软件栈的改进，TSS 采用的是开源软件 Trousers 0.3.6。应用程序首先通过 TSPI 接口调用相关的函数，再通过 TCS 使用 TDDL，通过 TDDLI 接口使用 TPM。对于远程证明，先进行远程平台的属性证明。对于验证平台的安全属性是否达到远程的安全要求，根据本书提出的思想，可不断地进行远程的属性验证，然后载入应用程序；之后，验证应用程序的行为是否可信，即本书的度量行为信息基的可信证明，验证行为的动态特性。本书中，动态属性证明和度量行为信息基的可信证明使用的是可信协议栈 IAIK jTSS，安装 Open JDK 1.6.0，通过虚拟机 JDK 进行程序设计，采用 Eclipse 3.2 开发工具，使用 TPM 的相关接口函数，借助度量行为信息基理论在 Java 虚拟平台上验证客户端和服务器端之间的远程证明，对基于行为的远程证明进行验证。

通过在理论上对可信协议栈、可信计算的远程证明、可信计算的应用模型的建立，分析其安全性、性能，然后通过可信计算实验平台进行验证。验证时先进行理论研究，再通过实验证明。在可信计算平台下，设计了基于可信计算的 DRM 系统模型。对数字版权管理的相关协议进行了讨论和设计。在已建立的可信平台、可信软件栈的基础上，嵌入一个媒体播放软件，对数字内容的加密、许可证的发放等技术进行了研究。在物联网系统的每个节点中嵌入 TPM 芯片，在此基础上进行安全策略的研究。在感知层利用密钥进行身份识别，利用平台寄存器状态进行平台安全认证和密封；在网络层利用可信计算网络协议进行网络连接；在应用层绑定数据不被泄露，使用基于 TPM 的软件栈进行编

程。总的来说，在理论方面，进行模型的抽象、形式化的表示、安全性的证明；在实验方面，搭建可信计算平台，通过实验进行验证和分析。

本书对外部内容和观点的引用按原始出处列入了参考文献，在此向所引内容和观点的作者表示感谢。如有因各种原因造成的引注错误和疏漏，请广大读者指出。

本书主要内容是围绕山西省自然科学基金项目《可信虚拟语义认证研究》（No.2009011022-2）、山西省留学基金项目《虚拟可信安全服务研究》（No. 2009-28）、山西省高校创新项目《基于可信网络连接的动态远程认证》（No. 20101115）部分工作展开的，且受到了山西省自然科学基金项目《不平衡数据流重抽样和学习算法研究》（No. 2015011039）资助。

作者一直对可信计算和远程认证进行理论和应用的研究，本书是作者多年工作成果的总结。限于作者的学识水平和时间仓促，书中难免存在错误及不妥之处，恳请广大读者和业界同仁不吝赐教。希望本书能对可信计算与远程证明的理论和应用起到一定参考作用。

目　录

第 1 章　信息安全概述

1.1　信息安全现状

信息安全的概念在 20 世纪经历了一个漫长的历史阶段，20 世纪 90 年代以后受到了人们的充分重视。进入 21 世纪，随着信息技术的不断发展，信息安全问题也日益凸显。信息安全是防止对知识、事实、数据或能力进行非授权使用、误用、篡改或拒绝使用所采取的措施。信息安全关系到网络系统的正常使用、用户资产和信息资源的安全，也关系到企事业机构的信息化建设与发展和国家安全与社会稳定。因此，信息安全不仅成为各国关注的焦点，也成为热门研究和人才需求的新领域。

网络空间面临的安全挑战日益复杂，当前主要体现在以下几个方面。

- 针对工业控制系统的网络安全攻击日益增多，多起重要的工业控制系统发生了安全事件。如 2016 年 3 月，美国纽约鲍曼水坝的一个小型防洪控制系统遭受攻击；2016 年 8 月，卡巴斯基安全实验室揭露了针对工业控制行业的“食尸鬼”网络攻击活动，该攻击主要对中东和其他国家的工业企业发起定向网络入侵。
- 移动互联网恶意程序趋利性更加明确，移动互联网黑色产业链已经成熟。通过分析恶意程序行为发现，以诱骗欺诈、恶意扣费、锁屏勒索等攫取经济利益为目的的应用程序骤增。
- 大量物联网相关的智能设备遭受恶意程序攻击形成僵尸网络，该僵尸网络被用于发起大流量 DDoS 攻击。如 2016 年年底，因美国东海岸大规模断网事件和德国电信大量用户访问网络异常事件，Mirai 恶意程序受到广泛关注。
- 网站数据和个人信息的泄露屡见不鲜，“衍生灾害”严重。美国大选中，候选人希拉里的邮件泄露，直接影响到大选的进程；雅虎两次泄露账户信息涉及约 15 亿的个人账户，致使美国电信运营商威瑞森 48 亿美元收购雅虎的计划搁置甚至可能取消。

- 敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全。2017 年 5 月，英国、意大利、俄罗斯等多个国家爆发勒索病毒攻击，我国大批高校也出现感染情况，众多师生的电脑文件被病毒加密，只有支付赎金才能恢复。美国一家名为 Check Point 的软件技术公司日前发布年中报告，认为 2017 年上半年勒索病毒攻击在总体网络攻击中的比重较之去年同期几乎翻倍，从 26%上升到 48%。对敲诈勒索软件攻击对象分析发现，勒索软件已逐渐由针对个人终端设备延伸至企业用户。

我国的信息安全局势也很严峻。据国家互联网应急中心（CNCERT）监测[1]，2016 年抽样监测获得的主要数据中，在木马和僵尸程序监测方面，控制服务器 IP 地址总数为 96 670 个，较 2015 年减少 8.0%，受控主机 IP 地址总数为 25 840 694 个，较 2015 年下降 10.1%。在“飞客”蠕虫监测方面，全球互联网月均有 465 万余台主机 IP 地址被感染，其中，我国境内感染的主机 IP 地址数量月均近 67 万台。在移动互联网安全监测方面，捕获及通过厂商交换获得的移动互联网恶意程序样本数量为 2 053 501 个，相比 2015 年增长 39.0%。按行为属性统计，流氓行为类的恶意程序数量居首位。按操作系统统计，主要针对 Android 平台的移动互联网恶意程序占 99.9%。在网站安全监测方面，监测到仿冒我国境内网站的钓鱼页面 177 988 个，涉及 IP 地址 20 089 个，在这 20 089 个 IP 地址中，85.4%位于境外。被篡改网站数量为 16 758 个，较 2015 年的 24 550 个减少 31.7%。监测到境内 82 072 个网站被植入后门，其中政府网站有 2 361 个。

从数据来看，2016 年移动互联网恶意程序捕获数量、网站后门攻击数量以及安全漏洞收录数量较 2015 年有所上升，而木马和僵尸网络感染数量、拒绝服务攻击事件数量、网页仿冒和网页篡改页面数量等均有所下降。有鉴于此，我们需要预警与处置安全漏洞，接收与处理网络安全事件，保护计算机系统中硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露，使系统能够正常、连续运行。

1.2　信息攻击手段和防御措施

进行网络攻击是一件系统性很强的工作，其主要工作流程是：收集情报→远程攻击→

远程登录→取得普通用户的权限→取得超级用户的权限→留下后门→清除日志。主要内容包括目标分析、文档获取、密码破解、日志清除等技术。

网络攻击主要有如下技术。

（1）扫描、监听、嗅探

端口扫描是一种获取主机信息的方法。利用端口扫描程序扫描网络上的一台主机，可以从扫描的端口数目和端口号来判断出目标主机运行的操作系统，再结合其他扫描信息进而掌握一个局域网的构造。针对端口扫描，其防范措施一般是关闭那些不使用的端口。

网络监听和嗅探工具可以监听网络的状态、数据流动情况以及网络上传输的信息。但此类工具也会被一些黑客利用，当网卡设置为混杂模式，此网段上的信息便被截获。通常的检测与防护方法是：对于有可能运行监听程序的机器，用正确的 MAC 地址和错误的物理地址去 ping，运行监听程序的机器会有响应；使用安全的网络拓朴结构隔断网络阻止监听；对一些重要数据进行加密，即使被截获，信息也不易泄露。

（2）电子欺骗

电子欺骗是通过伪造源于一个可信任地址的数据包以使一台机器认证另一台机器的电子攻击手段。它可分为 IP 电子欺骗、ARP 电子欺骗和 DNS 电子欺骗 3 种类型。IP 电子欺骗技术就是通过伪造某台主机的 IP 地址，使得某台主机能够伪装成另外一台主机；而这台主机往往具有某种特权或被另外的主机所信任。ARP 电子欺骗是一种更改 ARP Cache 的技术。Cache 中含有 IP 与物理地址的映射信息，如果攻击者更改了 Cache 中的 IP/物理地址对，来自目标的数据包就能发送到攻击者的物理地址。当攻击者危害 DNS 服务器并明确地更改主机名/IP 地址映射表时，DNS 欺骗就会发生。这些改变被写入 DNS 服务器上的转换表。因此，当一个客户机请求查询时，用户只能得到这个伪造的地址，而该地址是一个完全处于攻击者控制下的机器的 IP 地址。

（3）DoS 拒绝服务

DoS 拒绝服务就是利用合理的服务请求来占用过多的服务资源，致使服务超载，无法响应其他的请求。这些服务资源包括网络带宽、文件系统空间容量、开放的进程或者向内的连接。分布式拒绝服务攻击（DDoS）是利用攻击者已经侵入并控制的主机（可能是数百台），对某一单机发起攻击。在悬殊的带宽力量对比下，被攻击的主机会很快失去