基于可信计算的远程认证在 DRM 中的应用

闫建红
（太原师范学院 计算机系 山西 太原 030012）

【摘 要】：本文通过对 TPM 进行介绍，重点对 TPM 在认证协议中用到的相关技术做了详细的说明，并指出在远程认证过程中容易出现的问题，提出了一种基于可信平台的远程认证的完整性协议，并将其在 DRM 中如何应用做了简要说明。

【关键词】：可信计算；远程认证；DRM

引言

1.1 TCG 的背景知识

随着网络和计算机的普及，计算机的安全日趋复杂，系统安全问题层出不穷，信任危机也在制约着信息化的发展过程。可信计算技术有别于传统的技术，给我们提供了安全的硬件结构即安全芯片。由 TCG 定义的 TPM[1]为平台提供了硬件度量、安全存储和身份认证的功能，系统的所有安全认证和安全调用都通过 TPM 来完成。TPM 存储了平台配置信息和加密密钥，并内置加密引擎和用于产生密钥的随机数发生器。TPM 支持行业保证的密码应用编程接口，在硬件中生成、存储和管理密钥，并利用系统平台的存储和计算资源，为加密算法和密钥提供硬件保护。

TCG 的核心是 TPM，是 pc 机主板上的小型安全卫士，TPM 用一个信任根来提供服务，因为它的硬件在理论上是很难被攻击，因此，也就假定它是可信的。根据其使用说明，TPM 不是用来抗攻击的，而是在认证过程中当主机被攻击时能够发现证据。

TPM 能创建和存储密钥，既可以是对称的，也可以是非对称的。当产生这些密钥时可能被标识为可迁移的或不可迁移的，相对于不可迁移密钥时，可迁移密钥可以再不同的 TPM 之间互相传输。由于 TPM 有限的存储能力，TPM 也可以将存储密钥放到硬盘上。TPM 自己有能力进行一些计算，如：它可以产生密钥和解密等。

TPM 还提供了不同的签名密钥，其中重要的是签注密钥 Endorsement Key (EK)，它产生于生产 TPM 的厂商，是独一无二地代表着 TPM 身份，被用来证明 TPM 是一个真正的 TPM。除此之外，EK 还用来获取身份证明密钥（Attestation Identity Key AIK），由 TPM 内部产生 AIK，用 EK 的私钥部分来签名，公共部分被传给了可信第三方 Privacy-CA，由第三方证明其是一个真正的 TPM，并颁发证书给 TPM，证书包含了平台的身份识别，身份标识等常用的信息，这个证书后来被用来验证平台配置的真实性。

1.2 远程认证

认证是确认信息是否正确的过程。通过认证，外部实体可以确认保护区域、保护能力和信任源是否可信，通过认证就是将某个身份与某个主体进行绑定。基于网络的认证机制要求某个主体向某个单一的系统进行认证。远程计算机对包含有 TPM 平台的计算机的安全性进行认证，称为基于可信平台的远程认证。

1.3 数字权限管理技术 DRM

DRM 英文全称 Digital Rights Management，指的是内容数字版权加密保护技术，DRM 技术的工作原理是，首先建立数字节目授权中心。编码压缩后的数字节目内容，可以利用密钥进行加密保护，加密的数字节目头部存放着 KeyID 和节目授权中心的 URL。用户在点播时，根据节目头部的 KeyID 和 URL 信息，就可以通过数字节目授权中心的验证授权后送出相关的密钥解密，节目方可播放在数字权限管理技术 DRM 和企业安全方面我们都要求客户端平台是可信的，并且和所定义的策略是一致的。这就要求当敏感数据需要传输之前需要认证。为了这个目标，必须定义所使用的的策略以加强客户软件的安全性。由于策略加强机制是在客户端上被执行。攻击者可以通过修改客户端软件来破坏这个机制运行。

2.可信平台的远程认证

为了防止这种情况的发生，在服务器端决定发送敏感数据时，必须先通过远程认证来验证客户端的平台状态。发送者必须确保自己的平台是可信的。远程认证并不都是能做到克服伪装攻击，一个攻击者能控制一个伪装主机和诚实主机，并且能在远程认证中，证明它的伪装主机就是诚实主机。攻击者将所有的认证请求截获，然后在发送给具有安全可信状态的客户端，诚实主机客户端一定会回答，它仅仅是传输给请求者，而这时的攻击是一种伪装攻击。攻击者操纵诚实客户端，恶意的客户端平台很可能借助诚实客户端来证明是可信的，则就可能使受保护的数字产品接下来被传到了假装的可信平台。这样的结果的原因就是没有对这些客户端软件平台用任何策略的保护。

克服伪装攻击是保护数字权限管理系统的关键问题，由于这个原因，内容提供者和内容接受者必须确认一种策略，定义一种有效地准入机制来认证是否是 DRM 的客户端。在发送保护的数字产品之前，内容提供者必须首先认证接受者平台的状态，内容必须被加密并绑定到某台机器上。因此，内容提供者必须确保被绑定密钥的实体是经过认证的可信平台而不是另外一台机器。

远程认证是用来验证一个远程实体的配置，在客户端准备接受服务器端的数据时，服务器端在进行通信过程中要进行完整性报告的验证。这种机制可以用来作为很多不同的应用程序进行使用，在 DRM 应用中可以在 DRM 客户端执行，通过执行一定的策略，可以使受保护的数字产品不会被非法拷贝和使用。

在本协议中，用到 TPM 中的平台配置寄存器 PCRs，它是用来存储平台状态的配置信息的寄存器，在加电进行初始化后，用来存储软件完整性数据，软件部件被 TPM 测量并将相应的 hash 值储存到 PCRs，通过式子

Extend(PCRN, value)=SHA1(PCRN, ||value)

扩展前面的 PCRs 旧值，每次测量的事件被创建并存储到 SML 中，由 PCRs 和 SML 一起来验证平台的环境配置状态。为了确定这个值是真正的值，我们要用不可迁移密码来签名，即 AIK。远程认证比较这些值是否和参考值一样来证明平台是否可信。TCG 假定可信操作系统在启动过程中测量了每个过程的 HASH 值。

3、完整性报告协议

远程认证的概念使完整性报告协议发展起来 。在本文中所述的一种完整性报告协议如图：

图 1 中说明了 A 对远程的 B 进行验证，其中 B 内置有 TPM

在第 1 步 A 创建一个挑战序列序列 nonce；

第 2 步 A 发送这个挑战序列 nonce；

第 3.1 步 B 从受 TPM 保护的存储根密钥中取出 AIK，假设这个 AIK 已经通过 EK 向可信第三方申请了身份证明密钥；

第 3.2 步 用 AIK 私钥对 PCR 值和 nonce 进行加密；

第 3.3 步 从 TPM 中获得 SML 的值；

第 4 步：B 向 A 发送 AIK 证书公钥、对 PCR 和 nonce 进行签名后的值、和 SML；

第 5.1 步　验证 AIK 证书公钥，这一步由 A 向可信第三方来验证，A 向可信第三方将 AIK 公钥证书，由可信第三方从列表中来验证 AIK 是一个真正的 TPM，这样就可以避免伪装的客户端来假装它是诚实的客户端，因为 AIK 是唯一的；

第 5.2 步　A 用 B 的 AIK 公钥解密 nonce，PCR 验证其是否真正是由 B 发送而来；

第 5.3 步　A 用 PCR 值来验证 nonce 和 SML；

协议的整个证明过程中，A 能够验证远程客户端平台是否是可信的，没有被感染。

在这个协议中，由于使用了 nonce，每次请求都不一样，这样即使被第三方窃听，它也无法保证每次都能通过，所以避免了重放攻击。由可信第三方来验证 AIK 证书，也避免了伪装客户端进行冒名顶替，因为只有具有可信平台的计算机才能达到 AIK 证书，并且，只用该平台拥有这个 AIK 的私钥。

4.结论

在 DRM 系统中，我们可以先通过可信计算的远程认证协议证明 DRM 客户端是可信的平台，在此基础上可以用 Diffie-Hellman (DH)方法来产生会话密钥，也可以将客户端产生的对称密钥经过加密之后发送给服务器端，用密钥对数字产品进行加密，防止被攻击者被拷贝和非法使用，防止获得服务器的数据和系统的访问权限，防止不可信的计算机攻陷服务器，保证了服务器的安全。上面主要讨论了如何对远程实体进行验证，如何有效快捷建立一个加密的通道来传输相关数据将是以后的的研究工作。

参考文献：

1.Trusted Computing Group. TCG TPM Specification part 1 -Design Principles[S]. USA: Trusted Computing Group, 2006: 16-26.

2.Reiner Sailer, Xiaolan Zhang, Trent Jaeger, and Leendert van Doorn. Design and Implementation of a TCG-based Integrity Measurement Architecture.In 13th USENIX Security Symposium. IBM T. J. Watson Research Center, August 2004

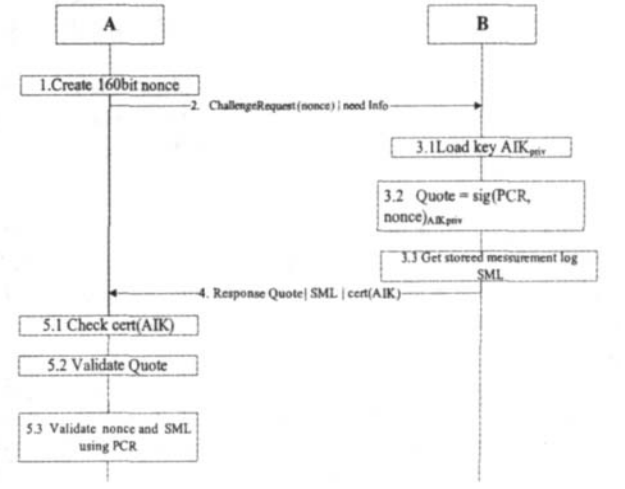

图 1 完整性报告协议

(上接第 165 页)

3.3 检测 MREL 端子电压

打开点火开关，测量 MREL 端子电压，如果有 12V 电压，表示正常。如果没有电压，必须更换 ECU 插头或 ECU。

3.4 检测 EFI 继电器

(1)关闭点火开关，拔下 EFI 继电器，用万用表电压档测量继电器的 4 个插孔的电压，有 12V 电压的表示继电器的 5 端子正常。

(2)打开点火开关，检测电压，应该有两个端子有电压，一个是 5 端子，一个是 2 端子，否则，应该修复 ECU 的 MREL 端子导线。

(3)用万用表的欧姆档测量继电器的任意两个端子的电阻，导通的表示 1 和 2 端子，另外剩下的就是 3 和 5 端子；用蓄电池搭接 1 和 2 端子，则 3 和 5 端子应该导通(如图 3 所示)，否则更换继电器。

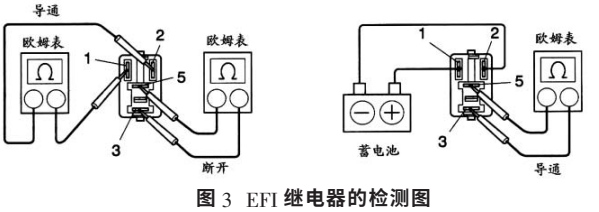

图 3　EFI 继电器的检测图

(4)分别检测继电器 1 端子的插孔与蓄电池负极(搭铁)和继电器 3 端子的插孔与 ECU 的+B 端子的导线，如果不导通应该更换或修复导线。

当然，上述检测方法只是针对线路的断路情况以及部件损坏情况，进行检修，而在实践当中，还可能出现线路短路，插头和插孔腐蚀、脏污、接触不良，插头松动等故障，在此不一一例举，测量的步骤和方法与上述情况大致相同。

4.结束语

经过实践检验，不管是什么类型的汽车发动机电脑控制系统的电源电路，只要按照以上方法和步骤，都能顺利排除故障。对于其他机电产品的电脑控制系统的电源电路，都可以参照或仿照这种检测方法。以上检测方法是本人经多年的实践总结，不断地摸索和研究所得成果，此次拿出来与大家共同学习、交流，欢迎多提宝贵意见。

参考文献：

1. 王秀红，田有为. 《汽车发动机电控技术》[J]. 大连理工大学出版社，2007.

2.李百华.《汽车发动机电控技术》[J].人民邮电出版社，2009.

(上接第 177 页)

量非常大时，所有的子进程都在很频繁的读写外存和处理业务，这个时候系统很有可能会遭遇读写外存"风暴"，从而导致很多时间都被浪费在等待读写外存上面。此时太过频繁的读写外存已经成为系统的性能瓶颈。

为了能有效地提高系统的性能，我们需要大大降低读写外存的次数。当程序需要保存消息时，不再直接写文件或入库，而是充分利用外部存储器的特点（即磁盘驱动器一次能从外存中读写多少字节量），以这个字节量作为基量，比较待保存消息的大小，若接近或大于基量，则直接写文件或入库；若明显小于基量，则先保存到预置的内存中，等到内存中所保存的消息的总大小接近或超过基量时，再一次性把内存中的消息全部写入文件或入库。在实际测试中，发现很多待记录的消息都明显小于基量，因此通过这次改进，有效地减少了单笔业务处理的时间，从总体上大大提高了系统的处理容量。