PKI证书服务的安全增强技术

王琼霄 王聪丽 林璟锵 宋 利
(中国科学院数据与通信保护研究教育中心 北京 100093)
(信息安全国家重点实验室(中国科学院信息工程研究所) 北京 100093)
(中国科学院大学网络空间安全学院 北京 100049)
(wangqiongxiao@iie.ac.cn)

Security Enhancement of Certificate Services in Public Key Infrastructures

Wang Qiongxiao, Wang Congli, Lin Jingqiang, and Song Li
(*Data Assurance and Communications Security Research Center*, *Chinese Academy of Sciences*, *Beijing* 100093)
(*State Key Laboratory of Information Security* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)
(*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049)

Abstract Based on public key cryptography, public key infrastructures (PKIs) provide security services for a range of network activities, such as authentication, data integrity, data source authentication, etc. Besides, PKIs build the foundation of many Internet security protocols, including SSL/TLS. A certification authority (CA) is the fully-trusted party in a PKI system, and is responsible for issuing digital certificate for an entity after validating the entity's identity information. A certification is capable for identifying a person or a server, in which the security attributes of the subject may be included. However, in recent years, fraudulent certificates appear frequently, which bringing the vulnerabilities to PKI-based applications. Fraudulent certificates may appear if a CA didn't validate the entity's information carefully, or it wasn't built with adequate security property. In order to solve these problems, security enhancements of PKI systems are proposed. In this paper, we analyze the security problems of CAs and discuss existing security enhancements of certificate services in PKI systems.

Key words public key infrastructure; digital certificate; certificate authority; certificate transparency; SSL/TLS

摘 要 公钥基础设施(public key infrastructure, PKI)基于公钥密码学提供身份鉴别、数据完整性、数据源鉴别等安全服务,是SSL/TLS等重要网络安全协议的基础.PKI体系的安全性依赖于对证书认证中心(certificate authority, CA)的绝对信任,CA实现对于用户身份信息的审核确认,并为其签发相应的数字证书,数字证书可用于表示个人用户、服务器等不同实体的身份,也可包含身份主

收稿日期:2018-10-15
基金项目:国家重点研发计划项目(2016YFB0800500)

体所具有的安全属性等信息. 然而,近年来 CA 签发虚假证书或证书被伪造的情况时有发生,CA 未经严格履行用户审核、CA 自身存在安全漏洞等原因导致上述问题的产生,严重影响了 PKI 应用的安全性. 为解决 CA 单点失效导致证书服务不可信的问题,针对不同应用场景提出了新的 PKI 证书服务安全增强技术方案. 针对证书服务不可信问题进行分析,对主要的 PKI 数字证书服务安全增强研究方案及其应用情况进行分类介绍.

关键词 公钥基础设施;数字证书;证书认证中心;证书透明化;SSL/TLS

中图法分类号 TP309

公钥基础设施(public key infrastructure, PKI)基于公钥密码学提供数据机密性、数据完整性、数据源鉴别等安全服务. 尤其在互联网应用中,PKI 为网络安全提供了重要的安全保障服务,如 SSL/TLS,S/MIME 协议等广泛使用的网络安全通信都是 PKI 的具体应用. SSL/TLS 协议在传输层提供数据安全保护,并提供客户端对服务器的单向认证或客户端与服务器之间的双向认证. HTTPS 是使用 SSL 协议的安全 HTTP 通信协议,浏览器可以通过服务器提供的 SSL 证书有效认证服务器的真伪,避免访问虚假网站,并进一步实现浏览器与服务器之间的加密通信,保护用户敏感信息的传输安全. HTTPS 目前已被越来越多的网站、浏览器采用,例如,Google 公司一直在全面推行 HTTPS 应用,并宣布于 2018 年 7 月起 Chrome 浏览器的地址栏把所有 HTTP 标示为不安全网站. 根据对部分国家用户的网页访问统计,通过 Chrome 浏览器加载的网页在 Windows 平台中有约 77%使用 HTTPS,通过 Firefox 浏览器加载的网页有约 75%使用 HTTPS. 在我国,近 2 年 HTTPS 的应用数量也快速增长,2018 年前 3 个月,机构证书月均增长量超过 300 张,远高于 2017 年的证书增长量.

HTTPS 的广泛使用可以有效实现对于网站服务器的认证并保护网络传输数据的安全性,PKI 证书服务的安全性是 HTTPS 安全的重要基础. 近年来,PKI 证书服务的安全事件时有发生,如 CA 签发虚假证书导致合法网络应用身份被冒用,造成用户敏感数据泄露. CA 签发虚假证书是指 CA 机构为证书持者签发与其真实身份不相符的数字证书,证书持有者由此冒充合法网站身份. 在这种情况下,浏览器和服务器之间即使使用了 HTTPS,由于虚假服务器具有合法 CA 签发的有效数字证书,浏览器也无法发现服务器的虚假身份,而将其认定为证书里所声称的网络应用,导致用户访问虚假服务,进而导致中间人攻击、数据泄露等.

为解决 PKI 系统中 CA 可能签发虚假证书的问题,国内外已有不少研究,用以加强 PKI 证书服务的可信度,为基于 PKI 实现的安全方案提供更好的安全保障. 本文将针对 PKI 证书服务安全问题、已有方案、部分方案的应用情况等进行分析与介绍.

1 PKI 基本安全模型

PKI 是基于公钥密码学的安全服务体系,基本结构由证书认证机构(certificate authority, CA)、证书持有者(certificate holder)也称为订户、依赖方(relying party)三方构成.

1) CA 是一个独立的可信第三方,为证书持有者签发数字证书,数字证书中声明了证书持有者的身份和公钥. CA 在签发证书前应用对证书持有者的身份信息进行核实验证,并根据其核验结果为其签发证书.

2) 证书持有者向 CA 申请数字证书,并向 CA 提供必要的信息以证明其身份及能力,获得由 CA 签发的证书;证书持有者在与依赖方进行交互时,需向依赖方提供由 CA 签发的数字证书证明其有效身份.

3) 依赖方是证书的验证方,依赖方与证书持有者进行交互(如建立通信连接)时,需获取证书持有者的数字证书,验证数字证书的真实性和有效性. 依赖方可以指定其信任的 CA 列表,若证书

持有者提供的数字证书不是受信 CA 签发的数字证书，依赖方将不认可该证书所声明的信息.

PKI 基本模型如图 1 所示：

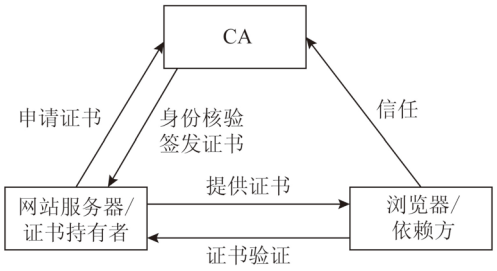

图 1　PKI 基本模型

在 HTTPS 协议中，一般使用浏览器对网站服务器的单向认证模型，在此情况下，网站服务器是 PKI 体系中的证书持有者，浏览器是依赖方. 用户通过浏览器访问 HTTPS 网站时，网站服务器向浏览器提供标明其身份的数字证书，浏览器验证服务器证书，进一步与服务器之间建立安全信道，完成网站页面的加载. 对于证书验证不通过或未能提供可信 CA 签发的证书的服务器，浏览器可以按照自身的安全策略作相应处理. 例如，Chrome 浏览器将所有非 HTTPS 网站或非可信 CA 签发证书的 HTTPS 网站在地址栏标记为不安全网站，用户可根据提示自行决定是否继续访问该网站.

2　PKI 证书服务的安全问题

PKI 证书服务的安全依赖于 CA 的完全可信. CA 是现有 PKI 体系的信任基点，一旦 CA 发生安全问题，基于 PKI 实现的安全协议、安全方案也无法达到预期的安全性. 在理论分析中，我们会假定 CA 是绝对安全的可信第三方，但是在实际应用中，CA 无法实现无条件的安全. 近年来，有多次 CA 机构发生安全事件，使得 PKI 证书服务自身的安全成为产业界、学术界共同关注的问题，PKI 证书服务的安全性增强技术成为重要的研究方向.

证书服务的安全问题主要体现在 CA 因攻击等原因而签发虚假证书或攻击者利用正常数据伪造证书等. CA 可能因为网络入侵等原因签发虚假数字证书，或者由于使用了不合适的算法而导致证书伪造.

2.1　CA 签发虚假证书

由于 CA 机构数量众多，每个 CA 的技术能力、管理水平存在巨大差异，可能由于管理、技术等问题而签发虚假证书.

1）CA 未严格审核证书申请信息签发虚假证书

2001 年 1 月，VeriSign 给谎称是微软员工的人签发了 2 个主体名为“Microsoft Corporation”代码签名证书[1]，利用这些证书可以对 ActiveX，Java Applet 等代码进行数字签名.

2008 年 7 月，安全研究人员 Mike[2] 利用在 live. com 注册的 sslcertificate@live. com 邮箱，在 VeriSign 子公司 Thawte 成功申请到了证书主体名为“login. live. com”的证书，而 login. live. com 是 Microsoft 的单点登录验证中心，有几百万用户，该证书一旦被用于恶意攻击，攻击者就可获得数百万用户的账号信息. Thawte 对用户信息进行审核时未实施足够检查，误认为 sslcertificate@live. com 邮箱属于 live. com 的管理员.

2008 年 12 月，StartCom 的 CEO&COO Eddy[3] 发现 CertStart（Comodo 丹麦合作伙伴）可以在没有进行域名所有权验证的情况下给申请者签发证书，并先后获取了称为 startcom. org 和 mozilla. org 的证书.

2011 年 8 月，TURKTRUST 错误地为订户签发了 2 张中间 CA 证书[4]，而且其中 1 张中间 CA 证书被用来签发 google. com 的虚假证书.

2）CA 未告知证书持有者私自签发证书

CA 机构由于自身业务需求或受政治、经济等因素影响，可能在未告知合法证书持有者的情况下，私下签发代表该证书持有者的数字证书. 2013 年 12 月，Google 发现与法国信息系统安全局（ANSSI）有关的中间 CA 发布了多个 Google 域名的虚假证书[5]，ANSSI 伪造证书是全球首例被曝光的国家级伪造证书劫持加密通信事件，在网络安全行业影响恶劣.

2015 年 9 月，赛门铁克旗下的 Thawte CA 在 Google 不知情下为 Google 域名生成了有效期 1 天的预签证书，赛门铁克经内部审查后证实，共发现了 76 个域名的 164 个问题证书[6]；2017 年 3 月 Google 和 Firefox 的调查人员发现赛门铁克没有按照行业规则，误签发了 127 张 SSL 证书，进一步调查发现涉及的问题证书可能高达 3 万多张[7].

赛门铁克作为全球最大的 CA 服务商之一发生如此大规模的虚假证书问题，对 CA 行业的正常发展产生了巨大影响. 2017 年 7 月，Google 宣布不再信任赛门铁克旗下所有 SSL 证书[8]；此后赛门铁克声称会改用新的 PKI 安全机制[8]. 但由于其之前发生的安全事件，截至目前 Google，Mozilla 等公司都宣布不再信任 2017 年 12 月 1 日前赛门铁克签发的所有 SSL 证书[9].

3) CA 被黑客攻击而签发虚假证书

CA 系统可能存在安全漏洞，CA 系统被黑客攻陷后，会导致 CA 被黑客操控而签发虚假证书.

2011 年 3 月，黑客入侵 Comodo 证书认证机构并签发了包括 mail. google. com，www. google. com，login. yahoo. com，addons. mozilla. org 等在内的 9 个虚假证书[10]. 事后，Comodo 撤销了所有的虚假证书，Microsoft，Google，Mozilla 也都发布了撤销这些证书的补丁.

2011 年 8 月底，荷兰 CA 机构 DigiNotar 的服务器遭受黑客入侵事件被曝光[11]. DigiNotar 在 7 月 19 日已发现系统被入侵，但是并没有及时向外界公布. 黑客入侵 DigiNotar 后，至少签发了 531 个虚假数字证书，包括 Google、Microsoft、Yahoo、Twitter、Facebook、中情局等在内的网站. 黑客利用这些数字证书实施中间人攻击，并导致伊朗 30 万 Gmail 用户的信息被监听、泄露. 该事件发生后，各主流浏览器均不再信任 DigiNotar 签发的证书，DigiNotar 也因此事件而最终破产.

2014 年 7 月，印度国家信息中心（NIC）使用 Indian CCA 根证书签发的中间 CA 证书签发了多个 Google 和 Yahoo 域名的虚假证书. Indian CCA 是被 Windows root certificate store 所信任的，这些虚假证书可被用于发起大范围的中间人攻击. Indian CCA 已经撤销了 NIC 持有的中间 CA 证书，声称 NIC 的证书签发系统遭到了黑客入侵[12-13]. 事后微软发布了操作系统紧急更新，屏蔽了黑客签发的 45 个影响重大的虚假 SSL 证书[12].

2.2 攻击者伪造虚假证书

除 CA 自身系统运行、管理上存在的问题外，如果 CA 机构在数字签发过程中采用了不安全的密码算法，攻击者就可以利用 CA 签发的合法证书构造虚假证书.

2008 年 12 月，Sotirov 和 Stevens 等人[14]利用 MD5 杂凑算法中的弱点来构造碰撞（2 张完全不一样的证书，却拥有相同的 MD5 散列值），成功伪造了 1 张 RapidSSL 签发的中间 CA 证书. 利用 MD5 算法的碰撞弱点，攻击者可以利用真实证书来伪造虚假证书. 攻击者向 RapidSSL 请求 1 张合法的网站证书，然后使用 MD5 杂凑算法生成 1 张与之前合法证书具有相同杂凑值的新证书，这个新证书是虚假的中间 CA 证书. 由于 2 张证书的 MD5 杂凑值一致，从 RapidSSL 获得的数字签名可以直接用在伪造的中间 CA 证书中，攻击者就可以进一步签发任何域名证书.

2012 年 5 月，中东地区出现的火焰病毒包含 1 个伪造的数字签名. 微软在终端服务授权服务证书中，错误地启用了代码签名功能，并且该证书使用 MD5 作为签名算法. 火焰病毒利用该漏洞，将病毒代码伪装成具有微软签名的合法代码[15].

3 PKI 安全增强方案

为解决 PKI 体系存在的安全问题，尤其是上述介绍的 CA 不可信导致虚假证书的问题，学术界、产业界针对 PKI 安全增强技术开展了很多研究. 研究主要基于 HTTPS，SSL 等具体应用开展，在这些场景中 PKI 证书持有者为网站服务器，依赖方为浏览器客户端.

现有的研究成果主要包括以下几类：

1) 客户端增加信任策略. 客户端在接收、验证服务器数字证书时，不仅验证证书签名、证书链的正确性及有效性，客户端还会根据自定义的信任策略对数字证书的签发者、数字证书的一致性等进行验证.

2) 证书主体发布限定策略. 由证书持有者（如域名服务器）声明哪些 CA 可以为其签发数字证书，客户端接收、验证数字证书时依据证书持有者声明的 CA 列表，验证数字证书是否由符合要求的 CA 签发.

3) 证书透明化. 将 CA 证书签发操作发布在公开、可审计的日志服务中，证书持有者、依赖方可以通过对公开日志的查阅发现虚假证书.

上述方案从不同的角度出发，实现对于虚假证书的限制、识别、发现. 下面，本文对典型的 PKI 安全增强方案原理及应用情况进行介绍.

3.1 客户端增加信任策略

在访问 HTTPS 网站时，浏览器与网站服务器之间进行 SSL/TLS 握手协商，验证服务器证书的正确性和有效性. 由于虚假证书是由合法 CA 签发的证书，如果仅从证书签名是否正确、证书是否在有效期内等方面进行验证，客户端无法判别接收到的服务器是否为虚假证书.

HPKP[16]，Certificate Patrol[17]，TACK[18] 等方案提出客户端记录首次/上一次访问网站时获取到的数字证书，并在每次访问该网站时比较证书的一致性，以避免持有不同来源数字证书（虚假证书）的网站仿冒合法网站. 这种在客户端绑定域名和证书信息的方法也称为 Pinning 方案.

CA-TMS[19]，Policy Engine[20]，CAge[21] 等方案提出，根据 CA 签发证书的数量、类型、特点等信息分析 CA 的一般性服务范围，并以此作为验证策略，对证书的签发者进行验证，不符合 CA 证书签发范围的证书，被认为是不合法/虚假证书. 例如，某 CA 一般只签发后缀名为.ac.cn，.gov.cn 的域名证书，当客户端收到由 CA1 签发的后缀名为.com 的域名证书时，会认为该证书为非法证书. 分析 CA 服务特性，自动判定 CA 服务范围的方法，需要分析大量证书签发情况，才能达到较好的效果，由于 CA 数量众多、服务类型多且存在动态变化的可能性，所以实际操作性并不高.

2015 年，IEFT 发布 RFC 7469，规定了 Pinning 方案在 HTTPS 访问中的具体使用方式，称为 HPKP. 网站通过 HTTPS 报文的 Public-Key-Pinning（PKP）头部向浏览器声明网站绑定的证书（公钥）信息，其中包含：

1）绑定有效期；

2）多个证书主体公钥信息的消息摘要，相应的证书可能是终端证书、中间 CA 证书或者根 CA 证书；

3）声明该 Pinning 是否适用于子域名；

4）用以报告虚假证书的 URI.

对于首次访问的网站，浏览器根据在 SSL 协议中验证通过的数字证书、收到的 HPKP 头部信息，实现网站与 HPKP 中指定证书的绑定操作. 实施绑定前，客户端需对 HPKP 中的证书信息与 SSL 协议中使用的服务器证书链进行比较，证书链上应至少有 1 个证书与 HPKP 头部中的证书信息一致. 浏览器再次访问该网站时，对 SSL 协议中获得的网站证书链与已绑定的证书信息进行一致性比较，当存在与已绑定证书一致的证书时，浏览器将判定接收到的网站证书正确，完成网站连接. 如果验证失败，浏览器发出警告，根据用户决定是否接受证书并更新绑定，或将可能的虚假证书上报至相关 URI.

HPKP 方案已被 Firefox 35 及以上版本、Chrome 38 及以上版本等浏览器支持. 但是，根据文献[22]对 Alexa 排名前 100 万的网站进行的分析，结果显示截至 2017 年，仅有 0.02%的网站支持使用 HPKP 方案.

以 HPKP 为代表的 Pinning 方案，都是基于 Trust on First Use 假设，也就是如果浏览器初次访问的网站是正确的网站，后续可以发现虚假证书；如果初次建立连接的网站是虚假网站，则会将该网站认为是真实的网站进行绑定，反而会影响后续的真实网站访问.

3.2 证书主体发布限定策略

证书主体也可以对其数字证书的安全规则进行定义与声明，例如，证书应由哪些指定的 CA 签发. 依赖方可以根据证书主体发布的规则验证数字证书，如 DANE[23]；CA 机构可以根据证书主体发布的规则为其签发数字证书，如 CAA[24]，DANE，CAA 等都是基于 DNSSEC[25-26] 提出的服务器证书安全增强方案. 由网站（域名所有者）自定义安全规则，限定 CA 的服务范围，可以防止任意 CA 都能签发任意证书持有者身份的数字证书，由此降低因 CA 单点失效而给 PKI 证书服务带来的整体安全威胁.

DANE[23] 支持网站（域名所有者）在域名的 DNSSEC TLSA 资源记录中声明网站的证书信息和网站证书的验证规则. 根据内容的不同，TLSA 资源记录主要包括以下几类.

1）CA Constraints：浏览器应只接收由指定 CA 签发的数字证书；

2）Service Certificate Constraints：浏览器应只接收指定的数字证书；

3）Trust Anchor Assertion：浏览器应使用指定的根证书验证网站证书.

浏览器在域名解析或 SSL/TLS 协商时获得域名的 TLSA 资源记录，并根据 TLSA 资源记录

的内容来验证 SSL/TLS 协议中使用的服务器证书. 若验证通过,则完成相应的 SSL/TLS 协议连接;反之,浏览器中断本次 SSL/TLS 连接. DANE 允许网站通过 PKI 系统之外的方式,规定并发布自身证书的信任规则. 对于支持 DANE 的网站,网站证书不仅需要由合法的 CA 机构签发,而且必须由网站限定的 CA 签发,攻击者无法使用任意被攻击的 CA 签发符合 DANE 规则的证书,增加了攻击者构造虚假证书的难度,降低了虚假证书攻击成功的可能性.

CAA[24]支持网站(域名所有者)在域名的 DNSSEC CAA 资源记录中声明哪些 CA 可以签发该网站的证书. CAA 资源记录还可以进一步规定签发证书的类型、是否允许签发通配符证书等. 与 DANE 不同,CAA 资源记录是事前的,由 CA 机构在签发证书时检查,CAA 资源记录不作为浏览器验证数字证书的依据. 当 CA 机构接到证书申请请求时,需要在 DNSSEC 中检查是否有相应的 CAA 资源记录的存在. CAA 资源记录作为证书主体声明的"证书策略",可以降低 CA 机构错误签发证书的可能性,其有效性依赖于 CA 机构是否遵守 CAA 规定. CAA 无法强制性地阻止 CA 机构签发虚假证书,也无法帮助发现虚假证书. CAA 可以用于评估 CA 机构的证书服务.

3.3 证书透明化方案

虚假证书能带来严重安全威胁的重要原因之一是,证书由 CA 机构签发并直接发放给证书申请者,被仿冒身份的网站没有有效的途径获知哪些 CA 签发了代表该网站身份的数字证书. 必须在虚假证书被使用一段时间、传播了一定范围之后,被仿冒身份的网站才有可能发现. 证书透明化方案(certificate transparency)[27]要求所有 CA 机构将签发的证书公开记录在特定 Log Server 中. Log Server 以 Merkle Tree 的形式存储服务器证书,具有 append-only 特性,且日志的内容对所有人公开. 所有人(包括网站管理员)都可以公开查询各 CA 签发了哪些数字证书,从而及时发现虚假证书.

证书透明化方案在传统 PKI 模型中引入新的角色:

1) 日志服务器(log server). 维护公开的日志,接收 CA 或者网站管理员提交的有效证书. 日志信息发布采用只增模式、不可删除,确保(虚假)证书提交发布之后不会被删除.

2) 监视机构(monitor). 周期性地访问公开日志服务器,检测可疑证书.

3) 审查机构(auditor). 定期地检查日志服务器,监督日志服务器是否正确运行,包括日志服务器是否始终保持自增特性,是否在接收提交之后及时发布证书.

日志服务器是独立于 CA、网站(证书持有者)、浏览器(依赖方)的第三方服务,监视机构和审查机构的功能可以是 PKI 体系之外的角色承担,也可以由 PKI 体系内已有角色承担. 证书透明化方案的典型角色部署方式如图 2 所示:

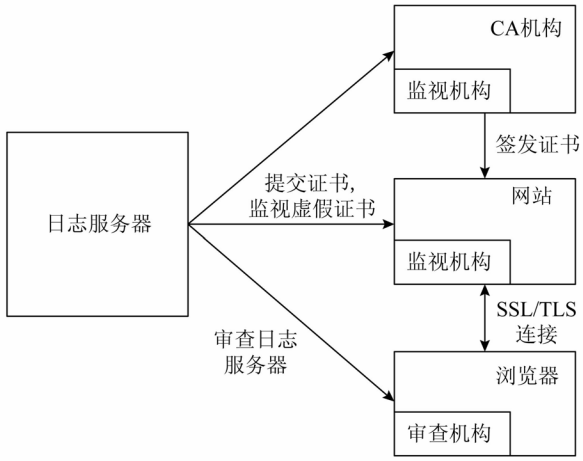

图 2 证书透明方案中各系统角色的典型部署方式

浏览器验证证书时,要求证书必须已经在公开日志中发布. 日志服务器为每一个在日志中发布的证书签发 SCT(signed certificate cimestamp),浏览器验证网站证书时需同时得到相应的 SCT 并验证. 如果浏览器验证的证书没有相应 SCT,说明证书未被公开发布,浏览器拒绝该证书. 如果敌手使用虚假证书发起攻击,也必须将虚假证书发布在公开的日志中. 此时,虚假证书就可以被利益相关方发现,如网站(真实的域名所有者)或者 CA 机构.

证书透明方案中,浏览器有 3 种方式获得日志服务器签发的 SCT 凭证:

1) 从 X.509 证书扩展项获得 SCT. CA 在证书签发前将预证书提交给公开日志服务器并获得 SCT,之后将对应的 SCT 作为证书扩展包含到正

式的证书中；网站的 TLS 服务器无需作任何改变，仅需要将证书传递给浏览器.

2）从 TLS 扩展项获得 SCT. 网站的 TLS 服务器向公开日志服务器提交证书并获得 SCT，在 TLS 链接建立时，TLS 服务器通过 TLS 扩展将 SCT 发送给浏览器，此时 CA 不需要作任何改变.

3）从 OCSP Stapling 的扩展项获得 SCT. CA 签发证书，提交给公开日志服务器并获得 SCT；TLS 链接协商时，网站的 TLS 服务器查询 CA，获得 SCT 并包含在 TLS 的 OCSP Stapling 扩展中；这种方式要求 TLS 服务器支持 OCSP Stapling.

浏览器的 SCT 提供方式统计图如图 3 所示：

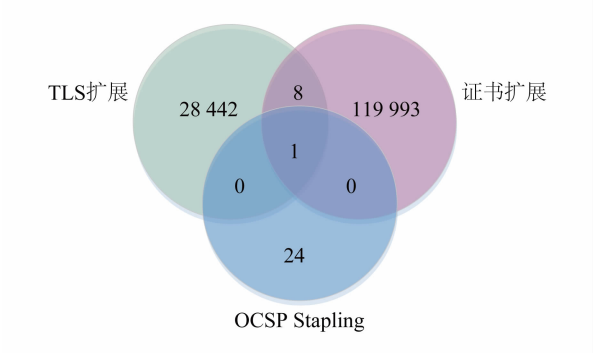

图 3　SCT 提供方式统计图

AKI[28]，ARPKI[29]等方案从多方面扩展了证书透明方案，网站可以在数字证书扩展中声明其相信的 CA 机构、日志服务器以及证书由多个 CA 机构签名等.

目前证书透明化方案已被不少网站、CA 机构、浏览器、开源软件支持. 2017 年 10 月 6 日，文献[30]对 Alexa 排名前 100 万域名进行了扫描，结果显示，有 563 866 个网站返回了合法证书，其中有 148 468（26. 33%）个网站同时提供了 SCT，也就是有 14. 8%的网站支持证书透明化.

Chrome 浏览器已全面支持证书透明化，Firefox，OpenSSL 等软件也都实现了对证书透明化的支持，此外，苹果的 macOS 和 iOS 平台也增加了对证书透明化的支持. 2013 年 9 月，DigiCert[31]成为首个支持证书透明化的 CA 机构. 截至目前，Comodo，VeriSign，GlobalSign，RapidSSL，WoSign 等主流 CA 机构均支持证书透明化技术. 在证书透明化（CT）官方网站上[32]，目前已登记日志服务的数量共有 72 个，如表 1 所示：

表 1　证书透明化日志服务的分布情况

Log Operator 所在国家或个人	Log Operator	Log Server 数量
美国	Google	25
	Cloudflare	5
	DigiCert	16
	Certly	1
	Comodo CA Limited	3
	Venafi	2
	Akamai	1
	Let's Encrypt	1
西班牙	Izenpe	2
中国	WoSign	3
	Wang Shengnan	1
	GDCA	3
	CNNIC	1
	StartCom	1
	Beijing PuChuangSiDa Technology Ltd.	1
	SHECA	2
个人	Matt Palmer	1
英国	Up in the Air Consulting	1
北欧	NORDUnet	2

证书透明化方案在传统 PKI 体系的基础上引入新的角色，通过公开日志发布 CA 签发的数字证书，监视机构通过对公开日志的检查可以及时发现其中虚假证书，从而避免 CA 因攻击等其他原因而签发虚假证书的情况. 证书透明化需要调整数字证书签发或验证流程，方案的部署应用需要由 CA 或网站服务器及浏览器端作相应的改造.

4　总　　结

PKI 技术是网络环境中提供身份鉴别、数据完成性、数据源鉴别等安全服务的重要支撑，PKI 证书服务的安全性对于当前的互联网安全至关重要. 针对 PKI 系统中 CA 不完全可信、可能签发虚假证书的问题，目前已有较多研究成果及实用系统.

现有解决方案中，除了证书透明化有较大范围的部署，其他方案的部署都非常有限. 在解决问题的同时，现有解决方案也有新的缺陷，包括 Pin-

ning 方案的初始化难题、证书主体策略的强制力度有限、证书透明化方案的滞后性等等. 进一步分析现有问题并提出更好的数字证书服务安全增强解决方案,仍然是当前 PKI 和信任管理的重要研究内容.

参 考 文 献

[1] Microsoft. Microsoft security bulletin MS01-017: Erroneous veriSign-issued digital certificates pose spoofing Hazard [OL]. (2003-06-23)[2018-10-15]. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2001/ms01-017

[2] Mike Z. Criminal charges are not pursued: Hacking PKI [OL]. 2008 [2018-10-15]. https://defcon.org/images/defcon-17/dc-17-presentations/defcon-17-zusman-hacking_pki.pdf

[3] SSL Shopper. SSL certificate for Mozilla.com issued without validation [OL]. (2008-12-23) [2018-10-15]. https://www.sslshopper.com/article-ssl-certificate-for-mozilla.com-issued-without-validation.html

[4] Google Security Blog. Enhancing digital certificate security [OL]. (2013-01-03) [2018-10-15]. https://security.googleblog.com/2013/01/enhancing-digital-certificate-security.html

[5] Google Security Blog. Further improving digital certificate security [OL]. (2013-12-07) [2018-10-15]. https://security.googleblog.com/2013/12/further-improving-digital-certificate.html

[6] Google Security Blog. Sustaining digital certificate security [OL]. (2015-10-28)[2018-10-15]. https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html

[7] Sleevi R. Intent to deprecate and Remove: Trust in existing symantec-issued certificates [OL]. (2017-03-24) [2018-10-15]. https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ

[8] Fisher D. Intent to deprecate and remove: Trust in existing symantec-issued certificates [OL]. (2017-07-28) [2018-10-15]. https://groups.google.com/a/chromium.org/forum/#!topic/blink-dev/eUAKwjihhBs%5B1-25%5D

[9] Ristić I. Monitoring of symantec certificates [OL]. (2017-08-15) [2018-10-15]. https://www.hardenize.com/blog/monitoring-of-symantec-certificates

[10] Mozilla Security Blog. Comodo certificate issue—Follow up [OL]. (2011-03-25)[2018-10-15]. https://blog.mozilla.org/security/2011/03/25/comodo-certificate-issue-follow-up/

[11] VASCO Data Security International Inc. DigiNotar reports security incident [OL]. (2011-08-30) [2018-10-15]. https://www.vasco.com/about-vasco/press/2011/news_diginotar_reports_security_incident.html

[12] CA Security Council. In the wake of unauthorized certificate issuance by the Indian CA NIC, can government CAs still be considered "Trusted Third Parties" [OL]. (2014-07-24) [2018-10-15]. https://casecurity.org/2014/07/24/unauth orized-certificate-issuance/

[13] Google. Maintaining digital certificate security [OL]. (2014-07-08) [2018-10-15]. https://security.googleblog.com/2014/07/maintaining-digital-certificate-security.html

[14] Sotirov A, Stevens M, Appelbaum J, et al. MD5 considered harmful today [OL]. (2008-12-30) [2018-10-15]. http://www.win.tue.nl/hashclash/rogue-ca/

[15] Wikipedia. Flame (malware) [OL]. (2018-11-21) [2018-12-11]. https://en.wikipedia.org/wiki/Flame_(malware)

[16] Evans C, Palmer C, Sleevi R. Public key pinning extension for HTTP[S/OL]. IETF RFC 7469, 2015[2018-10-15]. https://tools.ietf.org/html/rfc7469

[17] Modell M, Toth G, Loesch C, et al. Certificate patrol [OL]. 2014[2018-12-11]. http://patrol.psyced.org/

[18] Marlinspike M, Perrin T. Trust assertions for certificate keys [OL]. (2013-01-07) [2018-10-15]. http://tack.io/draft.html

[19] Braun J, Volk F, Classen J, et al. CA trust management for the Web PKI[J]. Journal of Computer Security, 2014, 22(6):913-959

[20] Abadi M, Birrell A, Mironov I, et al. Global authentication in an untrustworthy world [C] //Proc of the 16th USENIX Conf on Hot Topics in Operating Systems. Berkeley, CA: USENIX Association, 2013: 19-19

[21] Kasten J, Wustrow E, Halderman J A. Cage: Taming certificate authorities by inferring restricted scopes [C] //Proc of the 17th Int Conf on Financial Cryptography and Data Security. Berlin: Springer, 2013: 329-337

[22] Amann J, Gasser O, Scheitle Q, et al. Mission accomplished?: HTTPS security after diginotar [C] //Proc of the 2017 Internet Measurement Conf. New York: ACM, 2017: 325-340

[23] Schlyter J, Hoffman P. The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA [S/OL]. IETF RFC 6698, 2012[2018-10-15]. https://tools.ietf.org/html/rfc6698

[24] Hallam-Baker P, Stradling R. DNS certification authority authorization (CAA) resource record [S/OL]. IETF RFC 6844, 2013 [2018-10-15]. https://tools.ietf.org/html/rfc6844

[25] Larson M, Massey D, Rose S, et al. DNS security introduction and requirements [S/OL]. IETF RFC 4033, 2005 [2018-10-15]. https://tools.ietf.org/html/rfc4033

[26] Ateniese G, Mangard S. A new approach to DNS security (DNSSEC)[C] //Proc of the 8th ACM Conf on Computer and Communications Security. New York: ACM, 2001: 86-95

[27] Laurie B, Langley A, Kasper E. Certificate transparency [S/OL]. IETF RFC 6962, 2013 [2018-10-15]. https://tools.ietf.org/html/rfc6962

[28] Kim H J, Huang L S, Perring A, et al. Accountable key infrastructure (AKI): A proposal for a public-key validation infrastructure [C] //Proc of the 22nd Int World Wide Web Conf on Steering Committee. New York: ACM, 2013: 679-690

[29] Basin D, Cremers C, Kim H J, et al. ARPKI: Attack resilient public-key infrastructure [C] //Proc of the 2014 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2014: 382-393

[30] Nykvist C, Sjöström L, Gustafsson J, et al. Server-Side adoption of certificate transparency [C] //Proc of the 19th Int Conf on Passive and Active Network Measurement. Berlin: Springer, 2018: 186-199

[31] Dark Reading Reports. DigiCert announces certificate transparency support [OL]. (2013-09-24) [2018-10-15]. https://web.archive.org/web/20131010015324/http://www.darkreading.com/privacy/digicert-announces-certificate-transpare/240161779

[32] Google. Certificate Transparency [OL]. 2013 [2018-10-15]. https://www.certificate-transparency.org/

王琼霄

博士，高级工程师，主要研究方向为可信身份管理、网络认证、密码应用技术等.

wangqiongxiao@iie.ac.cn

王聪丽

硕士研究生，主要研究方向为网络安全、公钥基础设施等.

wangcongli@iie.ac.cn

林璟锵

博士，研究员，主要研究方向为应用密码学、网络与系统安全.

linjingqiang@iie.ac.cn

宋　利

硕士，工程师，主要研究方向为可信身份管理、网络认证等.

songli@iie.ac.cn