谁在篡改我的可信根证书仓库？

张一铭，刘保君

清华大学网络科学与网络空间研究院

或许曾经在12306网站购票的过程中，你已经习惯于随手下载并信任陌生根证书。但是你是否也思考和怀疑过：信任陌生根证书对于终端设备而言究竟意味着什么？攻击者有没有可能同样隐蔽地植入恶意根证书？

研究论文“Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem”[1]，互联网公钥基础设施领域本地可信根证书仓库的安全性现状测量与分析，发表于国际网络安全领域顶级学术会议 CCS 2021。这项研究工作是由来自清华大学以及加州大学尔湾分校等多位研究人员共同完成的。

【研究背景】

HTTPS协议是互联网基础网络协议之一，它为客户端和服务器之间数据传输的机密性和完整性提供了安全保障。实际上，HTTPS协议的安全特性是由数字签名证书提供的

（图一绿色区域）。可信第三方证书颁发机构（Certification Authoritie，CA）签名的数字证书，在网络交互过程中可以通过验证。

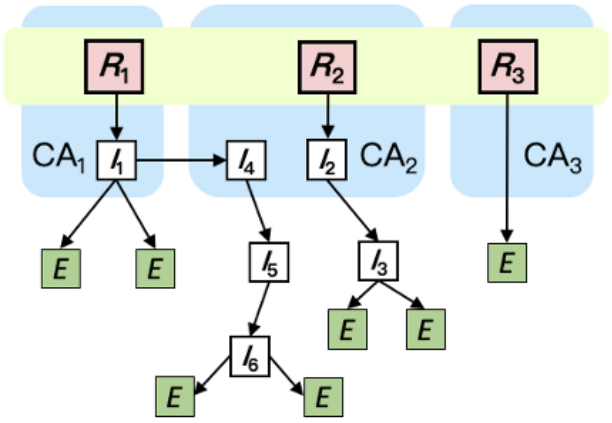

图1： 互联网公钥基础设施森林状安全信任模型

考虑到数字签名证书的重要作用，可信第三方证书颁发机构必须经过严格的安全性审查，并受到规范监管。作为当前最佳安全实践，主流操作系统通常会维护可信证书颁发机构的根证书列表（图一红色区域），并将其存储为终端设备的可信根证书仓库，也被称为Root CA Store。由该列表内根证书签发的数字证书链将被用户视为安全可信。

截至目前，关于“如何管理本地可信根证书仓库”仍然缺乏统一的标准或规范。譬如，尽管Windows系统会为用户预置Root CA Store，却为其保留了修改Root Store、植入第三方根证书的权限，并将判断第三方根证书是否可信的责任交给互联网用户。这种安全性设计并不合理。事实上，政府机构以及企业、本地软件甚至是恶意软件，都可能将其持有的根证书植入到操作系统的Root CA Store。此类由第三方植入的根证书未经严格安全审查，其签发行为亦不受社区监管，安全风险极高。而信任存在安全性缺陷的根证书，将从

根本上破坏HTTPS协议的信任模型，使网络通信面临窃听或劫持风险。2015年，联想电脑即在设备出厂时默认安装广告软件，植入不可信的根证书，使得即使用户访问加密后的网页内容也可被篡改 [2]。

我们认为，作为网络通信的安全根基，用户实际使用的（可能已被第三方修改后的）本地根证书仓库或许并不可靠。而该问题尚未获得安全社区的足够重视。我们的研究工作主要试图回答以下问题:

1）在互联网用户的本地根证书仓库中，究竟存在着多少未受监管的第三方根证书?

2）上述根证书存在何种安全性缺陷，影响了多少HTTPS网络流量?

3）此类根证书包含哪些类型，主要来源或途径是什么，谁是背后的操控者?

【主要研究结论】

结论一：在互联网用户本地根证书仓库中，我们发现了至少*117万*个未受监管的根证书，影响了约0.54%的HTTPS网络链接。

通过对大量异常HTTPS网络链接的分析，对比公共可信根证书列表，我们定位出119万未受监管的根证书。值得注意的是，其中绝大部分（117万个）已经植入本地根证书仓库，正在被终端设备所信任。

结论二：通过对上述根证书进行聚类关联分析，我们识别出了持有这些根证书的*5005个组织/团伙*，其在实际影响与规模方面呈现出显著的长尾效应。

下图展示了证书组织规模与影响分布，位于头部的100个组织持有97.5%未受监管的根证书，影响了超过98.9%的不安全HTTPS网络链接。

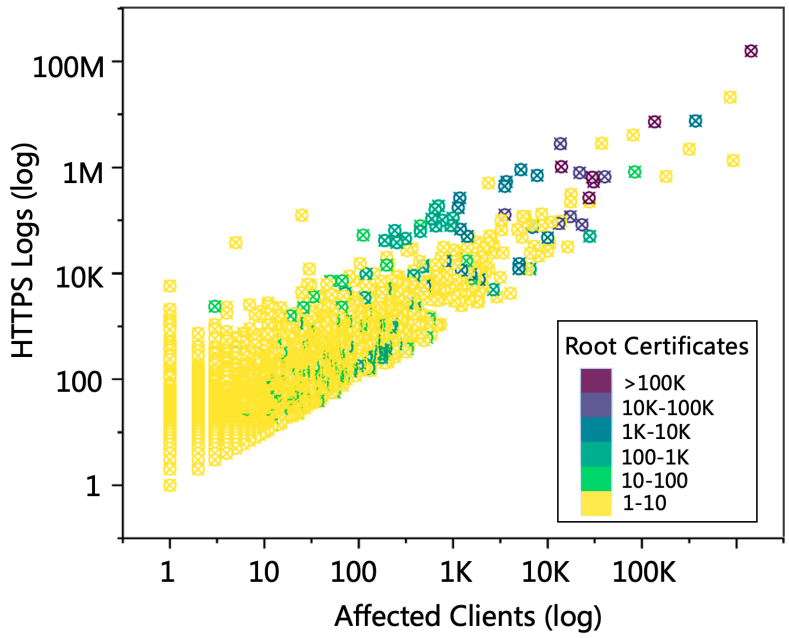

图2：未受监管根证书组织的规模及影响分布图

结论三：关于未受监管根证书的类别/来源，除了典型的企业或安全软件自建根证书以外，我们还发现了攻击者仿冒知名证书颁发机构伪造恶意根证书的现象，影响颇为严重。

通过对影响最大的组织进行逐一分析，我们发现，目前未受监管的根证书来源主要包括：1）企业及政府机构的自建根证书；2）攻击者仿冒知名证书颁发机构伪造的根证书；3）本地安全软件或网络代理软件生成的根证书。

类别	组织数量	根证书数量	影响终端规模	典型案例
Enterprise Self-built	24	48	199,743 (3.94%)	CN = SZSE ROOT CA, O = Shenzhen Stock Exchange
Digital Authentication	13	18	539,711 (10.65%)	CN = CFCA ACS CA, O = China Financial Certificate

				Authentication
Government Self-built	13	16	62,032 (1.22%)	O = National E-Government Network Administration Center
Fake Authentications	11	817,532	2,798,985 (55.21%)	CN = VeriSlgn Class 3 Public Primary Certification Authority - G4
Packet Filter	11	15,587	73,725 (1.45%)	CN = NetFilterSDK 2
Proxy/VPN	10	90,131	1,029,648 (20.31%)	CN = koolproxy.com, O = KoolProxy inc
Security Software	2	7,187	4,719 (0.09%)	O = Beijing SkyGuard Network Technology Co., Ltd
Parent Control	1	7,554	7,787 (0.15%)	CN = UniAccessAgentFW 2
Unknown	15	207,957	289,198 (5.07%)	CN = VRV NDF RootCA 2

其中特别值得注意的是虚假根证书仿冒知名证书颁发机构的现象。攻击者利用根证书字段伪装为知名权威认证机构，有利于逃逸安全厂商检测。此外，数据显示，虚假根证书签发了大量知名域名的数字证书。而由于其已被广泛植入本地信任列表，终端设备对此类非法证书几乎不会产生任何告警信息。

攻击者仿冒的根证书名称（红色为修改部分）	根证书数量	影响域名规模
GlobalSignature Certificates CA 2	1	74,555
VeriSlgn Class 3 Public Primary Certification Authority - G4	2	210
GlobalSign Root CA	1,419	6,023
Small DigiCert Baltimore Root 2	135,258	30,316
GlobalSign Root CA R3	136,196	47,347
Certum Trusted NetWork CA 2	254,414	1,137,121

【讨论与总结】

本研究通过测量研究披露了客户端可信根证书仓库的脆弱性，大量第三方根证书正广泛存在于网络用户本地信任列表，带来了严重的安全隐患。因此，安全社区应当重新审视互联网公钥基础设施中本地可信根证书仓库的安全特性。操作系统及浏览器等应用应当采取更为严苛的检查与限制策略，并在本地根证书仓库被修改时更为明确地告知终端用户安全风险。

在后续的工作中，我们将探索客户端可信根证书仓库管理的最佳安全实践，努力清除终端设备中的非法根证书，尽最大可能改善我国互联网用户终端的安全性现状。

对于上述工作感兴趣的读者，欢迎阅读完整论文：

https://dl.acm.org/doi/pdf/10.1145/3460120.3484768

【作者简介】

张一铭，清华大学计算机系博士研究生，主要研究方向为网络安全。

刘保君，清华大学网络研究院博士后，主要研究方向为网络安全与网络测量。

【参考文献】

[1] Zhang Y, Liu B, Lu C, et al. Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web P KI Ecosystem[C]//ACM conference on Computer and Communications Security (CCS). 2021.

[2] King B G. Lenovo's Superfish fallout: Can we forgive and forget?[J]. Fortune, 2015.