An End-to-End Measurement of Certificate Revocation in the Web's PKI

DEC 24TH, 2015

论文下载：https://www.cs.umd.edu/~dml/papers/revocations_imc15.pdf

Abstract & Introduction

- 这篇文章主要研究了PKI体系中证书吊销的相关问题，主要包括以下3点：
    - 服务器对证书的吊销和替换；
    - CA提供CRL和OCSP的情况；
    - 不同平台中不同浏览器对吊销证书的处理方法。

Data Collection

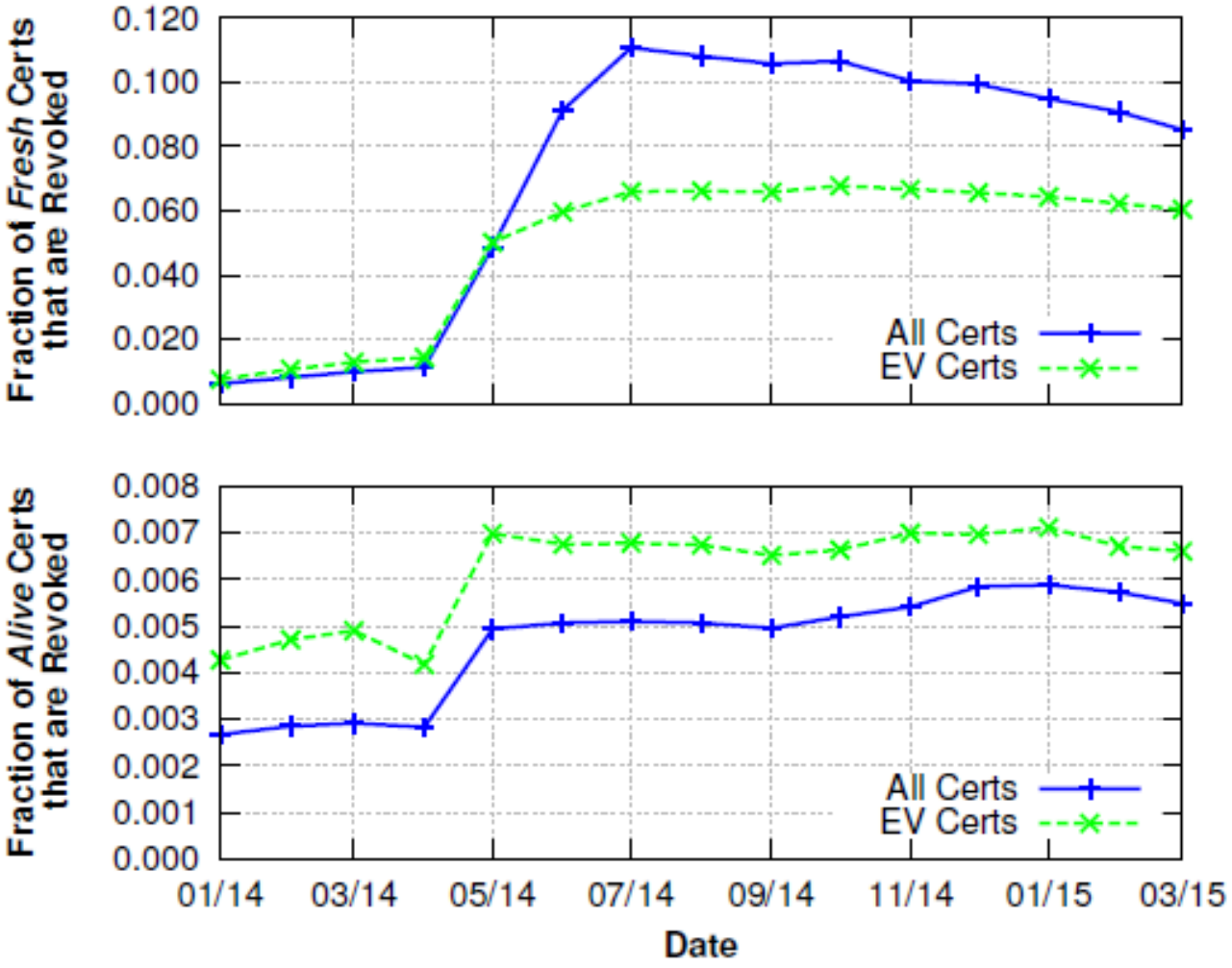
- SSL Certificate：

    - 作者用Rapid7工具扫描整个IPv4地址空间的443端口，进行了74次扫描，得到38,514,130个不同的证书。
    - 预处理证书共得到1,946个中间证书，称为Intermediate Set。
    - 用OpenSSL校验证书，排除不合法证书，除了有日期错误的，得到5,067,476个证书，称为Leaf Set，其中2,291,511个（45.2%）个在最新的443端口扫描中出现。
- Obtaining Revocation Information：
    - Leaf set中，99.9%的证书提供了一个潜在可达的CRL发布点，95%的提供了一个OCSP响应点。4,384（0.09%）的证书什么都没提供。，也就意味着它们不可能被吊销。
    - Intermediate Set中，98.9%的证书提供了CRL，48.5%的提供了OCSP。
    - CRLS：得到2,800个不同的CRL。
    - OCSP：观察到499个不同的OCSP响应点。
- Definitions：
    - Fresh：证书有效期内的时间称为fresh period。
    - Lifetime：证书被服务器使用就称它alive，理论上证书的lifetime应该是fresh period的严格子集，实际上不是。

Website Admin Behavior

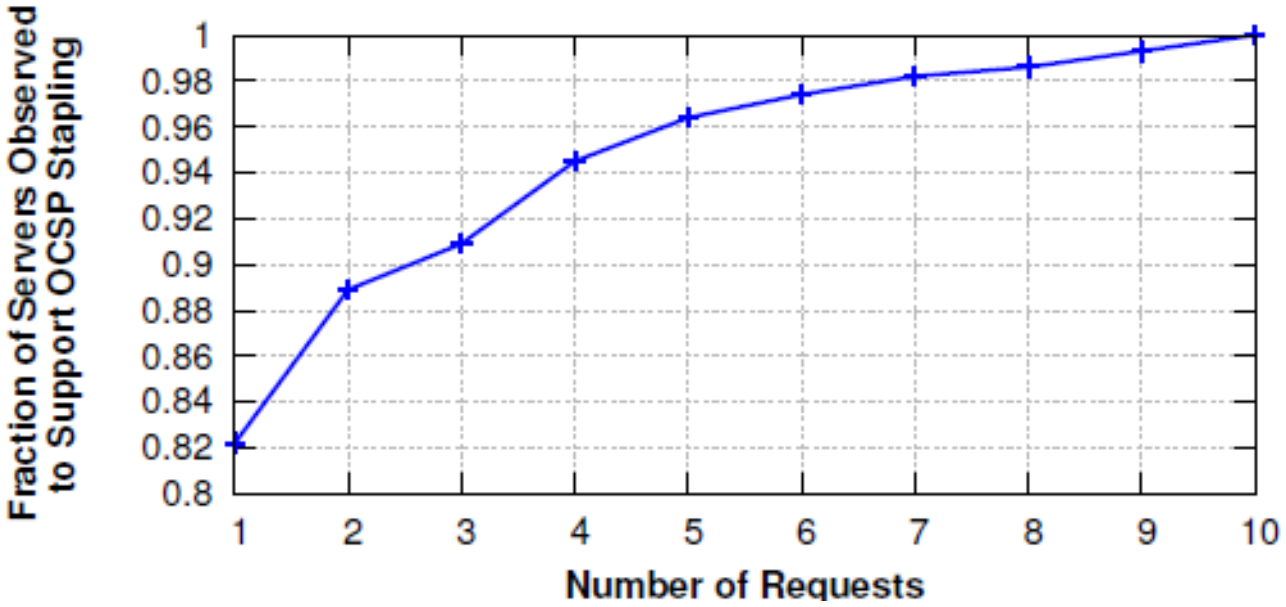
- Frequency of Revocations：

    - 收集到的证书里8%的是被吊销的，大部分是由于Heartbleed吊销的。
    - 少于1%的证书是alive，即仍被使用。
    - EV证书中，6%的已被吊销，0.5%的alive证书被吊销。



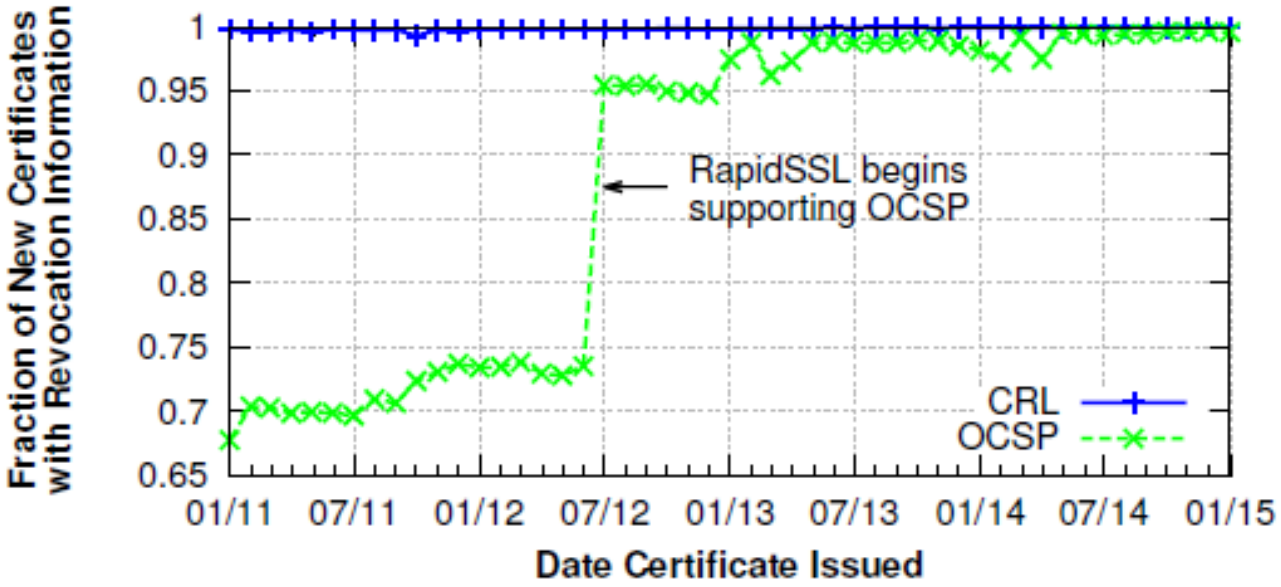
- Reasons for Revocation：大部分吊销证书都没有CRL reason code（用来说明证书为什么被吊销：”Unspecified”、”Key Compromised”、”Privilege Withdrawn”）
- OCSP Stapling：要求服务器端实现这个支持（CRL和OCSP都只涉及CA）。
    - 服务器有时候没有缓存一个合法的staple也不会再response里包含staple。

- 随机选取20,000个服务器，连接它们测试对OCSP Staple的支持情况。
- 在TLS握手扫描的数据中，2.6%的服务器支持OCSP stapling。
  - 扫描涉及的2,298,778个证书里，5.19%的被至少一个支持OCSP Stapling的服务器使用，所有使用某证书的服务器都支持OCSP Stapling的证书占3.09%。
  - EV证书中，3.15%的被至少一个支持OCSP Stapling的服务器使用，所有使用某证书的服务器都支持OCSP Stapling的证书占1.95%。



CA Behavior

- Availability of Revocation Information: CRL会带来带宽负担。OCSP会影响页面加载时间。



- Size of Revocation Information:
  - CRL大小和里面记录数时线形相关的。平均每条记录38 bytes。
  - CRL最大有76MB。95%的CRL会在24小时内过期。
  - 有一种减小CRL大小的技术是每个CRL只包含某CA所签发证书的子集。

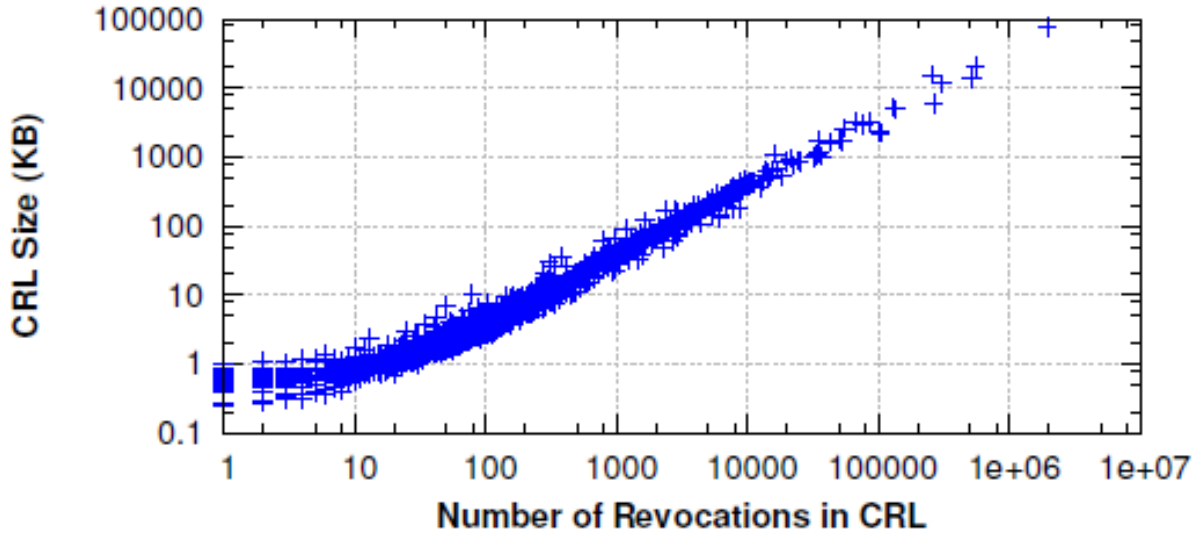


Figure 5: Scatterplot of the number of entries in CRLs versus CRL file size, for all 2,800 CRLs we crawled. As expected, a linear correlation is observed.

CA	Unique CRLs	Certificates Total	Certificates Revoked	Avg. CRL size (KB)
GoDaddy	322	1,050,014	277,500	1,184.0
RapidSSL	5	626,774	2,153	34.5
Comodo	30	447,506	7,169	517.6
PositiveSSL	3	415,075	8,177	441.3
GeoTrust	27	335,380	3,081	12.9
Verisign	37	311,788	15,438	205.2
Thawte	32	278,563	4,446	25.4
GlobalSign	26	247,819	24,242	2,050.0
StartCom	17	236,776	1,752	240.5

Table 1: Number of CRLs, certificates (total and revoked), and the average CRL size per certificate for the largest CAs.

Client Behavior

- Methodology: 生成了一个root证书装到浏览器里，再用这个root证书生成中间证书和叶子证书给浏览器测试。测试集包含不同的证书链长度和吊销协议的组合。
  - Chain Length：每个链有0-3个中间证书。
  - Revocation Protocol：部分证书有CRL，有的有OCSP，有的都有，也配置了支持OCSP stapling的服务器。
  - Extended Validation：生成了部分EV证书，叶子证书包含一个OID说明它是EV证书。
  - Unavailable Revocation Information：设置4种情况看浏览器如何处理证书：
    - 吊销服务器的域名不存在。
    - 吊销服务器返回HTTP 404.
    - 吊销服务器不响应。
    - 吊销服务器返回unknown。

- Desktop Browsers:设置了不同的浏览器/操作系统组合，每个组合设置一个VM，操作系统包括Ubuntu 14.04, Windows 8.1, OS X 10.10.2。共有30个不同的组合。

		Desktop Browsers										Mobile Browsers			
		Chrome 44			Firefox	Opera		Safari	IE			iOS	Andr. 4.1–5.1		IE
		OS X	Win.	Lin.	40	12.17	31.0	6–8	7–9	10	11	6–8	Stock	Chrome	8.0
	CRL														
Int. 1	Revoked	EV	✓	EV	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	EV	✓	–	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
Int. 2+	Revoked	EV	EV	EV	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Leaf	Revoked	EV	EV	EV	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	A	✓	✗	✗	✗	✗
	OCSP														
Int. 1	Revoked	EV	EV	EV	EV	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	L/W	✗	✓	✓	✓	✗	✗	✗	✗
Int. 2+	Revoked	EV	EV	EV	EV	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Leaf	Revoked	EV	EV	EV	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
	Unavailable	✗	✗	–	✗	✗	✗	✗	✗	A	✓	✗	✗	✗	✗
Reject `unknown` status		✗	✗	–	✓	✓	✗	✗	✗	✗	✗	–	–	–	–
Try CRL on failure		EV	EV	–	✗	✗	L/W	✓	✓	✓	✓	–	–	–	–
OCSP Stapling															
Request OCSP staple		✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	I	I	✗
Respect `revoked` staple		✗	✓	–	✓	✓	L/W	–	✓	✓	✓	–	–	–	–

Table 2: Browser test results, when intermediate (Int.) and leaf certificates are either revoked or have revocation information unavailable. ✓ means browser passes test in all cases; ✗ means browser fails test in all cases. Other keys include EV (browser passes only for EV certificates), L/W (browser passes only on Linux and Windows), A (browser pops up an alert), and I (browser requests OCSP staple but ignores the response).

- Mobile Browsers:用的都是模拟器来测。包含iOS/Android/Windows Phone。
  - iOS 67/8：Safari不检查任何证书吊销信息。
  - Android：4.¾4.4/5.1这3个版本下进行测试。
    - Stock、Chrome：不检查吊销信息，但是流量里有请求OCSP staple，请求回来的信息没有用来检查证书。
    - Firefox：没能导入根证书。
  - Windows Phone：不检查吊销信息。

CRLSets

- 谷歌针对一小部分吊销证书设置的，Firefox有一个类似的项目OneCRL（只包含8个吊销证书）。
- CRLSet：

- 文件大小不能超过250KB；
- 内部CRL合集；
- 一个CRL的条目数太多就会从Set移除。
- 这里面的吊销证书要有CRLSet reason code。