加窗技术的改进证书吊销机制*

王雪颖** 秦志光

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】 分析了现有证书吊销机制在灵活性、可升级性和及时性中的缺陷，针对现有新型证书吊销机制，提出了一种结合加窗证书吊销和增量 CRL 机制的证书吊销机制。该机制结合传统 CRL 机制和在线证书状态机制的优点，既能满足不同的安全需求，又能有效减少资源开销，满足验证者的实时性证书验证请求。

关 键 词 公钥基础设施； 证书； 证书吊销； 证书吊销列表； 加窗证书吊销机制

中图分类号 TP309.2

An Efficient Certificate Revocation Approach Based on Windowed Revocation Mechanism

Wang Xueying Qin Zhiguang

(College of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract Based on the analysis of the algorithm, performance and problem of a novel certificate revocation approach called the windowed revocation mechanism, a new and more efficient certificate revocation mechanism is proposed in this paper. The new mechanism integrates windowed certificate revocation and Delta-CRL mechanism, and uses effective method to avoid replay-attack.It satisfies the scalability and flexibility requirements of certificate revocation mechanism and, as the same time, can provide near real-time certificate status when required. The design and performance of the new mechanism is analyzed in this paper.

Key words public key infrastructure; certificate; certificate revocation; certificate revocation list; windowed certificate revocation

吊销证书信息的发布极有可能成为运营大规模 PKI(Public Key Infrastructure，公钥基础设施)系统成本最昂贵的部分[1]，证书吊销信息如何发布，是决定 PKI 系统，尤其是大规模 PKI 系统能否广泛应用的重要问题。

目前，最常用的方法是使用证书吊销列表(Certificate Revocation List，CRL)来管理证书吊销信息，基本 CRL 机制通过认证中心(Certification Authority，CA)周期性发布 CRL，内容包括该 CA 发放的所有未到有效期但已被吊销的证书。该方案简单易行但及时性差。增量 CRL 机制和在线证书状态验证机制是解决及时性问题的较有效的方案[2]。这两种机制各有优点，但前者性能受峰值带宽限制，并对证书使用率低的验证者不理想，而后者如果面临频繁的验证请求将难以负载。它们的局限性体现在不同的方面，如果能够结合其优点，则能够更好地提供证书吊销服务的及时性。

2002年7月26日收稿
* 国家计算机网络与信息安全管理中心基金资助项目
** 女 25岁 硕士生

本文在融合增量 CRL 与在线证书状态服务优点的基础上，利用加窗机制能够灵活结合其他证书吊销机制的特点，提出了一种改进的证书吊销机制，该机制能够提供及时、高性能、灵活和安全的证书吊销服务。

1 增量 CRL 机制和在线证书状态验证机制

在证书吊销问题中安全性主要通过及时性体现，及时性好则安全性高。通常以易损窗口(Window of Vulnerability，WOV)衡量及时性，其含义是验证者使用一个已被吊销证书的最长时间。小的 WOV 以大的网络或 CPU 资源消耗为代价。不同的验证者有不同的安全要求，好的证书吊销机制能够提供验证者自主地根据安全需求设定 WOV 的灵活性。Freshest Revocation Information 方案提供了有限的灵活性[3]，而通常的证书吊销方案中几乎没有这方面的考虑。

基本 CRL 机制将证书的 WOV 限制到了 CRL 的发布周期，因为 CRL 的长度可能变得很长，发布 CRL 的网络资源消耗使得 CRL 的发布周期不可能设置得太小，因而这种方案及时性差。针对及时性问题，当前两种较为有效的方案是增量 CRL 机制和在线证书状态验证机制。

1.1 增量 CRL 机制

该方案根本思想是把对长度很大的 base-CRL(基量 CRL，包括所有未到有效期但是已被吊销的证书)的请求转变为对短小的 delta-CRL(增量 CRL，仅包括上一次 base-CRL 发布以来吊销的证书)的请求，减少分发 CRL 的平均带宽，同时改善对验证者的响应时间。

增量 CRL 机制主要适用于证书使用率高的验证者，对于证书使用率很低的验证者则意义不大。更重要的是，使用增量 CRL 不能降低对 base-CRL 的峰值请求率，而由于 base-CRL 长度很大，分发 CRL 的峰值带宽限制了增量 CRL 的性能。

1.2 在线证书状态验证机制

在线证书状态验证机制的目的在于使验证者能够实时地对某个证书的状态进行检查，目前最广泛采取的在线证书状态协议是 OCSP(Online Certificate Status Protocol)协议[4]，它对验证者的每个请求产生一个响应，包括证书序列号、证书状态等信息，为防止重放攻击，在响应中包含序列号或时间戳，并经过响应者签名。由于对每个验证者的请求产生签名的响应，当验证者的请求过于频繁，OCSP 这类协议的性能会显著下降，此时信息的处理时间将使在线服务无法为验证者提供预期的及时响应，甚至影响到系统的可用性。

增量 CRL 与在线证书状态验证机制各有优点，但前者性能受峰值带宽限制，并对证书使用率低的验证者不理想，而后者如果面临频繁的验证请求将难以负载。它们的局限性体现在不同的方面，如果能够结合其优点，将能够更好地提供证书吊销服务的及时性。一种新型的证书吊销思想——加窗证书吊销机制(Windowed Certificate Revocation，WCR)提供了我们结合这两种机制的可能性[5, 6]，它同时具有灵活性和可升级性方面的优点。

2 加窗证书吊销机制及其分析

加窗证书吊销机制的实质是结合显式证书吊销机制和隐式证书吊销机制[5~8]，其目的是提供证书吊销方案的灵活性，并通过限制被吊销的证书在 CRL 中的存在时间来减小 CRL 的长度，其中隐式吊销机制也可以理解为一种在线证书状态服务。

加窗机制主要的设计思想是：

1) CA 定期以 CRL 的形式发布吊销信息；

2) 证书缓存：验证者取得证书之后将其缓存，由于证书在未经验证情况下的最长缓存时间取决于验证者为证书设定的清除定时器的值，因此，清除定时器超时的证书将被从缓存中清除；

3) 吊销窗口：被吊销的证书在 CRL 中只存在一段时间，这个时间段称为证书的吊销窗口。

2.1　算法思想

2.1.1　CA 的操作

在加窗吊销机制中，CA 做下面的工作：

1) 布 CRL，CRL 中包括所有未到有效期但已被吊销、吊销时间没有超过该证书吊销窗口的书，此时假设 CA 的 CRL 发布周期为 p；

2) 为每个证书指定吊销窗口，吊销窗口通常设置为 CRL 发布周期的倍数，这里假设为 w，表示该证书的吊销窗口长度为 w 个证书吊销周期。

2.1.2　验证者的定时器设置

验证者的主要工作是对证书的缓存管理，有以下两个定时器对每个证书单独指定：

1) 吊销窗口定时器，用是决定使用证书时验证证书状态的方式，其初始值等于证书的吊销窗口与 CRL 发布周期的乘积，根据上面的参数设定为 wp；

2) 清除定时器，作用是决定某个证书在未经验证的情况下可以使用的最长时间，其值由验证者指定，表明验证者允许的 WOV，此时假定其初始值为π。

验证者可以通过下面的方式获得证书的状态信息：当证书的吊销窗口定时器没有超时，采用显式吊销方式验证证书，即证书的状态信息从当前 CRL 取得；否则采用隐式方式，即验证者尝试向 CA 重新取得该证书，如果成功取得证书则表明证书未被吊销。当验证者获得证书 C 在 t_0 时刻的状态信息并且此时证书 C 未被吊销，那么 C 的两个定时器重置，吊销窗口定时器重置为 t_0+wp，清除定时器则为 $t_0+\pi$。

2.1.3　缓存管理流程

设 t_0为验证者开始取得证书的时刻，t_1为验证者取得 CRL 的发布时刻，在加窗吊销机制中，验证者管理缓存并验证证书状态的流程如图1所示。

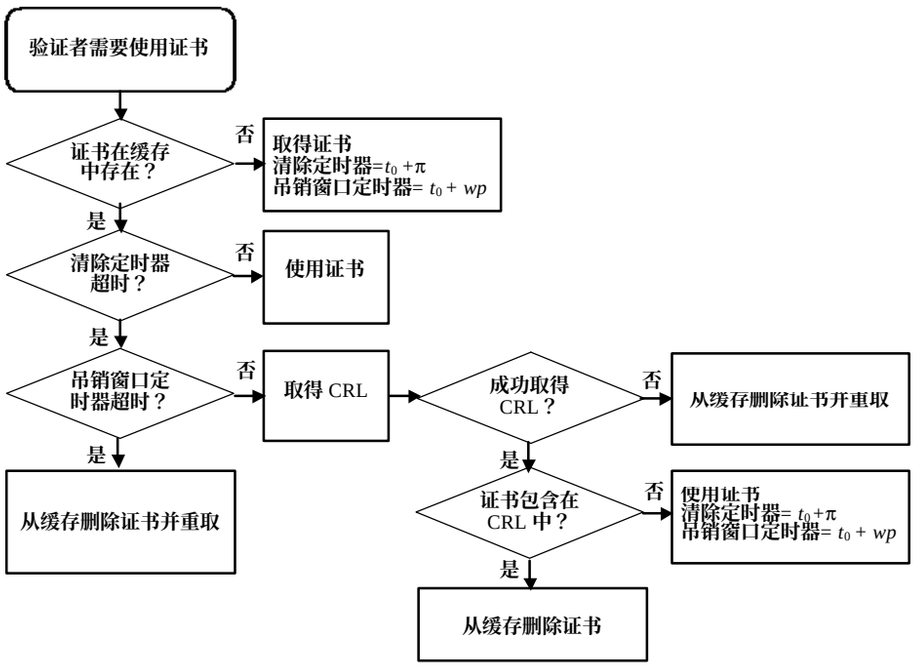

图1　加窗吊销机制的缓存管理流程

图1针对验证者的清除定时器π大于 CRL 发布周期 p 的情况，即通常的情况。而当希望取得小于 CRL 发布周期的及时性时，验证者应将吊销窗口定时器设置为0(无论 CA 如何设置该证书的吊销

窗口 w)，这样，每当清除定时器超时，证书都将从缓存中删除，验证者不下载 CRL，而向 CA 重取证书。

2.2 应用中存在的问题

加窗机制有效地减小了 CRL 长度，并提供了验证者对安全性和资源问题的控制灵活性，以及 CA 在对带宽和 CPU 资源矛盾问题上的控制灵活性。更重要的是结合不同吊销机制的思想设计，可以灵活地与已有的证书吊销机制结合。但是，使用加窗机制存在必须提供有效的机制保证重取证书的过程不受重放攻击的问题。

重放攻击对于证书重取过程或者在线证书状态验证机制问题在加窗机制中显得尤为重要，因为在其他吊销机制中，一次重放攻击影响的范围只是一个证书缓存时间；而在加窗机制中，一次成功的重放攻击就有可能导致验证者使用某个过期的证书直到该证书的有效期结束。图2给出的示例可以清楚地说明这种情况。

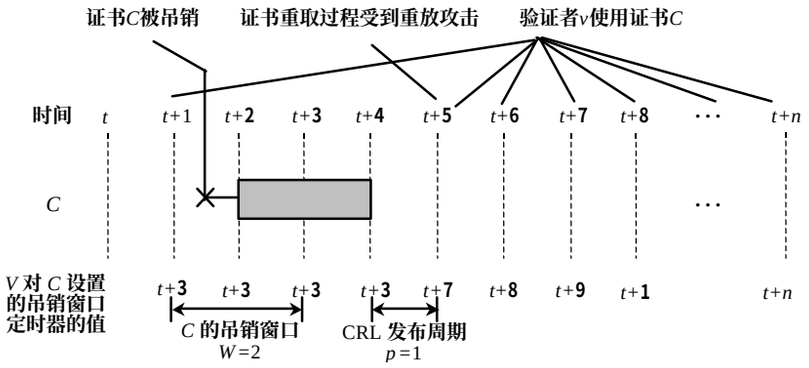

图2 加窗机制受到重放攻击造成长期使用已吊销证书的示例

3 一种提供灵活性、实时性的改进证书吊销机制

本文利用加窗机制能够灵活结合其他证书吊销机制的特点，提出一种改进的证书吊销机制。首先找到一种解决加窗机制重放攻击问题的有效途径，使得加窗机制可以投入实际应用，在此基础上该的机制融合了增量 CRL 和在线证书状态服务的优点，可以提供灵活、高性能和安全的证书吊销服务。

3.1 设计思想

3.1.1 解决加窗吊销机制的防重放攻击问题

使用加窗机制首先必须解决重放攻击问题。文献[5]用定期产生签名的证书响应包的方式防止重放攻击，其过程是指定一个时间间隔，每个时间间隔中 CA 对每个依然有效的证书产生一个响应包(包括证书、时间戳以及 CA 对两者的签名)，当验证者重取证书时，CA 则返回预先产生的包。该方法运用时间戳技术，对防止重放攻击是有效的。但是该方法相当于将验证者的 WOV 下限限制到了产生响应包的时间间隔，验证者无论将清除定时器设置得再小也不可能取得更为及时的证书状态信息。因此，更可取的方案是对验证者的每个证书重取请求单独产生含有时间戳的签名证书响应，或者采用类似 OCSP 协议的方式，返回含有时间戳的签名证书状态响应，此时吊销窗口定时器超时后对证书的处理将不从缓存中删除，而是做一个不能使用的标记，直到验证者重新取得该证书的状态信息。该方案最大的问题是 CA 的 CPU 资源问题，基于太频繁的请求，使在线服务无法负担。因此，必须在保证加窗吊销机制能够减小 CRL 长度这一优越性的前提下，应尽可能地减少验证者对证书的重新索取。下面讨论其修改方案。

3.1.2　结合加窗吊销机制和增量 CRL

该方案结合增量 CRL 和加窗吊销机制，并对验证者在证书吊销窗口定时器超时以后的每个验证要求即时产生包含时间戳的签名响应。

加窗机制的算法思路基本不变，但 CA 在发布 CRL 时，由定期发布基本 CRL 变为发布增量 CRL，此时用一个较长的周期发布 base-CRL 和一个很短的周期发布 delta-CRL。对验证者而言，设置证书的吊销窗口定时器为证书吊销窗口与 delta-CRL 发布周期的乘积。在证书的清除定时器超时、吊销窗口定时器未超时情况下，验证者下载 CRL 来验证证书的状态。下载的 base-CRL 被缓存。每次需要下载 CRL 时，检查缓存中是否有 base-CRL 或者 base-CRL 的缓存时间是否超过其发布周期，如果没有缓存或者已经超时，则重新下载 base-CRL 和当前的 delta-CRL，否则只下载 delta-CRL。当一个证书的吊销窗口定时器超时之后验证者需要使用证书，则访问 CA 的在线证书状态服务。

3.2　实例说明

下面进一步举例说明，结合加窗机制与增量 CRL，可以合理地满足不同验证者的不同验证需要。

设 delta-CRL 的发布周期很小，定为 p，p 为3 min；base-CRL 的发布周期相对 delta-CRL 大得多，设定为 mp，假定为3，即1 440p；一个证书 C，吊销窗口为 w，假定 w 为500。

1) 高频率使用证书的验证者

验证者 $V1$ 30 min(10p 时间)使用一次证书 C。假定他对证书 C 没有特别的及时性要求，则$\pi>p$，设π为5 p(π的取值在此对分析没有实质性的影响)。他对 C 的吊销窗口定时器值为 wp，即500 p。C 吊销以前，$V1$关于 C 的两个定时器在10p 时间就更新一次，于是其吊销窗口定时器始终不会超时，那么 $V1$所有的证书状态信息都从 CRL 获得，绝大多数情况下下载的 CRL 是 delta-CRL。这种结果对 CA 和验证者来说都是理想的：频繁的验证请求被 CRL 满足而没有通过在线服务，不会导致在线服务负担过重，而验证者下载 CRL 的带宽要求也很低。

2) 低频率使用证书的验证者

验证者 $V2$ 10天(4 800p)时间使用一次证书 C，这种情况下，增量吊销机制对于验证者来说意义不大，它反而需要取得比常规 CRL 更多的信息。在吊销机制中，由于 C 的吊销窗口为500，在验证者使用证书时，吊销窗口定时器均已超时。因此 $V2$将不下载 CRL，而要求 CA 的在线服务提供关于证书 C 的状态信息。这种请求因为频率很低，对于 CA 的在线服务是完全可以承受的。

3) 需要很高状态信息及时性的验证者

验证者 $V3$ 对证书 C 的状态有很高的及时性要求($\pi<p$)，此时要求将吊销窗口定时器设置为0，每次使用证书时则通过 CA 的在线服务验证证书状态。原因是 CRL 机制承担了 $V1$情况下的大量证书验证任务，使得在线服务在面临 $V3$这种高及时性的验证要求时可以快速处理。

为了更清晰地说明问题，假设验证者以平均的时间间隔使用证书，在此这种假设并不影响分析的合理性。

3.3　性能优势

结合加窗机制与增量 CRL，使得两种证书吊销机制的性能进一步优化。

1) 相对原始加窗吊销机制的性能改善

使用增量 CRL 进一步节省了验证者下载 CRL 的平均带宽，也加快了对验证者的响应，由于 delta-CRL 的长度很小，CA 可以设置相当小的 delta-CRL 发布周期(p 很小)，对于验证者的部分高及时性的验证请求(当π很小且$\pi>p$)，通过下载 CRL 的方式就可以实现，从而减少了验证者的在线证书验证请求。同时，与增量 CRL 结合使得加窗机制可以将吊销窗口设置得相对的长，证请求进一步减少。于是在线服务只针对及时性要求非常高($\pi<p$，此时 p 已经很小)的验证请求和验证者低频度访问，因此负载很大程度上得到减轻，其响应具有真正的及时性。

2) 充分发挥增量 CRL 机制的性能优势

与加窗机制结合，base-CRL 长度大为减小，从而降低了下载 CRL 的峰值带宽。此外，适当设定吊销窗口值，可使验证请求率很低的验证者在使用证书时吊销窗口定时器超时，则可将直接访问在线服务，而不必通过增量 CRL 机制，使增量 CRL 机制服务于最适用的验证者。

综合上面的分析，结合增量 CRL 和加窗机制的证书吊销方案具有以下特点：

1) 有效减小了下载 CRL 的平均带宽和峰值带宽，可升级性高；
2) 能在需要时提供具有很高及时性的证书状态信息；
3) 增量 CRL 和在线证书状态服务通过结合达到扬长避短的效果；
4) 保持了加窗吊销机制特有的灵活性特点。

4 结 束 语

本文设计的基于加窗证书吊销机制的改进证书吊销方案，通过加窗机制与增量 CRL 结合，并采用对每一个在线证书验证请求即时产生签名响应的方式，可以满足验证者包括实时请求在内的各种证书状态验证要求，是一种灵活而高性能的证书吊销方案。此外，加窗机制因为其独特的能够在安全性和资源消耗之间、网络和 CPU 资源之间灵活调控，可与除了增量 CRL 之外的其他证书服务体系结构和优化机制集成在一起使用。

参 考 文 献

1 Berkovits S, Chokhani S, Furlong A, *et al*. Public key infrastructure study: final report. Produced by the MITRE Corporation for NIST, 1994

2 Housley R, Ford W, Polk W,. *et al*. RFC 2459, internet X.509 public key infrastructure certificate and CRL profile. Internet Engineering Task Force, 1999

3 ITU, ISO/IEC. Final proposed draft amendment on certificate extensions, 1999

4 Myers M, Ankney R, Malpani A, *et al*. RFC 2560, X.509 internet public key infrastructure online certificate status protocol – OCSP. Internet Engineering Task Force, 1999

5 McDaniel P, Jamin S. Windowed key revocation in public key infrastructures. Technical Report CSE-TR-376-98, Electrical Engineering and Computer Science, University of Michigan, 1998

6 McDaniel P, Jamin S. Windowed certificate revocation. In Proceedings of IEEE INFOCOM 2000, 1 406-1 414

7 Cooper D A. A model of certificate revocation. In Proceedings of the Fifteenth Annual Computer Security Applications Conference, 1999

8 McDaniel P, Rubin A. A response to “Can we eliminate certificate revocation Lists？” In Proceedings of Financial Cryptography 2000, International Financial Cryptography Association, 2000