两篇Web PKI相关的文章

Web PKI是目前最大、最重要的密码系统之一。Web PKI的核心是负责SSL证书颁发和维护的CA生态系统。这些证书颁发给web服务提供商，并在SSL/TLS协议中使用。因此，Web PKI能够对Web服务器进行身份验证，从而在web浏览器和服务器之间进行安全的加密链接。

但是随着互联网的不断发展，Web PKI在许多方面不能提供所需的安全性。比如，为了实现互操作性（即，应尽可能多地验证合法的web服务证书），在当前浏览器和操作系统中默认情况下完全受信任的CA的数量一直在增长。目前，大约有1500个可信CA。由于这些受信任的CA中的每一个都可以为任何web服务或域签署证书，因此信任单个恶意CA（即事实上不可信的CA）可能会破坏整个web PKI的安全性。

对于这个问题，在第一篇文章中，作者提出通过建立信任视图，将可信CA的数量减少到用户真正需要的数量来降低这种风险。信任视图是在用户本地与信任决策相关的一个知识库，包含之前收集的关于其他实体及其密钥的所有信息，并且是在用于信任验证的过程中逐步构建的。一个实体的信任视图：一组受信任的证书、一组不受信任的证书、一组公钥信任评估。

受信任证书是以前用于建立与另一个实体的可信连接的所有证书。不可信证书是指那些被评估为连接不可信的证书。

信任评估表示在先前的信任验证期间为相应的公钥-证书对收集的所有信息。它是一个五元组 (k; ca; S; okl; oit)：

S是k的一组证书。这些证书的主题是ca。该集合包含所有主题为ca和公钥为k的证书，这些证书之前已由e1验证。

Okl是一种观点。它代表了e1关于k是否属于ca（k的关键合法性）的意见。

Oit也是一种观点。它表示e1在ca中对颁发可信任证书的信任（也可以说是使用k时，颁发者对ca的信任）。

为了决定与实体e2的连接是否可信，实体e1运行信任验证算法

我们现在描述信任验证算法。它将实体e1的信任视图和实体e2的证书的认证路径作为输入，并计算e2的密钥的密钥合法性，（密钥合法性由应用程序的安全级别来确定，安全级别是介于0和1之间的实数。安全级别越高，评估可信连接所需的密钥合法性就越高。安全级别的分配是一个主观的过程，依赖于e1的风险状况，这里不再赘述），通过密钥合法性决定与e2的密钥建立的连接是否被认为是可信的。信任视图中可用的信息可能不足以完成信任验证。在这种情况下，还有一种验证服务被用作后备机制。

为了验证这种方法是否有效，作者设计了一个攻击者模型（首先假设攻击者是不会攻击用户系统的，即不会破坏用户的信任视图，另外假设ca本身通常不是恶意的，）攻击者通过使用ca的密钥颁发恶意证书来实施攻击。如果想要对特定用户组进行攻击的话，当用户获得一个证书后，有两种情况，要么它之前接受过这个证书，要么对这个证书相关联的ca有足够的信任，否则就会验证失败，需要查询验证服务来重新确认证书。攻击者必须破坏在每个用户的信任视图中具有高信任级别的CA，否则，当信任验证失败的用户使用验证服务检查证书时，就会检测到攻击。由于信任视图是特定于用户的，并且不公开可见，因此很难识别出这样一个受所有用户信任的CA，并且攻击者是否能够设法破坏该CA也是值得怀疑的。因此大大减少了能够成功攻击用户的数量，从而降低可能的损害。如果是对特定服务进行攻击，也面临同样的问题，就是需要找到一个被所有用户充分信任的ca，不会触发验证服务，但是由于不同用户信任视图不同，也很难找到这样的ca进行大范围攻击。

因此，信任视图可以帮助用户维护一组最小的受信任CA，并最大限度地降低了由于CA故障或泄露而颁发的恶意证书的风险，从而提高web pki系统的安全性。

另一篇文章的题目是Evaluating web pkis

这篇文章提供了一个对公钥证书管理系统的评估框架，作者首先对现有的证书管理方案进行了分类，

经典的基于ca的证书管理系统是当前部署的pki，它在ca信任方面缺乏灵活性，并且很难预防和检测攻击。所以人们提出了几种建议来加强当前的证书管理系统。作者根据每种设计原则，将领先的证书管理系统分为三类，即差异检测、范围限制和证书透明管理。我们为大家介绍每一类方案的特点并举例进行说明。

首先，差异观察是一个旨在检测不可信CA的概念，使浏览器能够验证接收到的证书是否与其他人提供的证书不同。

2008年，Wendlandt、Andersen和Perrig实现了一个名为Perspectives的Firefox插件。提出了通过要求不同的公正服务器（也称为观察者）检测同一服务器的公钥是否一致，从而提高首次使用身份验证的信任安全性。每个观察者将所有观察到的密钥或证书与相应的时间戳一起存储，并定期检查更新和撤销。当客户端想要与服务器建立安全连接时，客户端会向服务器和多个观察者请求服务器的公钥，然后比较接收到的密钥。如果获得的公钥是一致的，则客户端认为公钥是可信的，并使用该密钥来建立安全连接。否则，这可能表明攻击者通过向客户端提供不同的公钥发起了中间人（MITM）攻击。

范围限制限制旨在通过限制CA可以担保的领域范围来降低CA的权力。

Langley等人在Google Chrome中实现了一种公钥固定的方法，通过指定特定网站授权哪些CA为其颁发证书来限制CA权力，可以保护用户通信免受未经授权的CA错误颁发证书的攻击者的攻击。

证书透明管理是一个旨在使CA的行为透明的概念。其基本思想是使用一个公开可见的日志来记录已颁发的证书。

Certificate transparency(CT)由谷歌提出，通过使证书颁发透明，让域所有者能够有效地检测错误颁发的证书。更详细地说，域所有者向日志维护者请求签名确认，称他们的证书包含在日志中，然后他们可以将此确认与相应的证书一起提供给web浏览器。只有在证书和签名的确认都有效的情况下，浏览器才接受证书。由于CA的行为是透明的，CT不要求用户盲目信任CA，即CA的行为可以验证。这使得CT能够提供信任灵活性。

在介绍完这些证书管理系统的分类及应用后，作者以系统的方式对这些方案进行了评估，评估标准包括16项，分为信任Trust、有效性Availability、安全Security、可用性Usability、隐私Privacy五个方面，涵盖了web证书管理系统所需的功能和安全问题。



可以看到，在这三类中，最后一类基于透明的公共日志，在实际应用中最成功。

文章提供的评估框架也有助于正在进行的研究Web证书管理的替代方案。

这两篇文章对我们未来的研究方向有很大的启示。

针对公钥证书管理系统的研究:

1. 开发更加灵活和安全的证书管理系统：可以探索如何设计更加灵活和安全的证书管理系统，例如采用去中心化的方式、使用区块链技术等。

3. 提高SSL/TLS验证和身份验证的安全性：可以研究如何提高SSL/TLS验证和身份验证的安全性，例如采用多因素身份认证、使用更加安全的密码算法等。

4. 平衡安全性和可用性：可以探索如何在保障安全性的同时保持系统的可用性，例如采用自适应访问控制策略、优化证书更新流程等。

5. 处理各种攻击：可以研究如何应对各种攻击，例如钓鱼攻击、中间人攻击等。这需要开发新的防御机制，并不断更新和改进现有防御机制。

加强Web PKI系统的安全性

1. 进一步探索和改进trust views的建立和管理机制，以提高其效率和可扩展性。

2. 研究如何将trust views与其他安全机制集成，例如基于策略的安全机制。

3. 探索如何在不同的应用场景中使用trust views，并评估其实际效果。

4. 研究如何在Web PKI中使用更先进的密码学技术来提高安全性，并将其与trust views相结合。