RSA PRESS

Mc Graw Hill Education

XML安全基础

XML Security

开发和部署坚实的XML安全策略

学习XML签名的结构和语法

有效地阻止XML特有的安全漏洞

Blake Dournaee 著

周永彬 贺也平 刘娟 译 卿斯汉 审校

清华大学出版社

XML 安全基础

[美] Blake Dournaee 著
周永彬 贺也平 刘娟 译
卿斯汉 审校

清华大学出版社
北京

ISBN: 0-07-219399-9
XML Security
Blake Dournaee

图书在版编目(CIP)数据

XML 安全基础/(美)多尼著;周永彬,贺也平,刘娟译.—北京:清华大学出版社,2003.8
书名原文:XML Security
ISBN 7 - 302 - 06632 - 9

Ⅰ.X… Ⅱ.①多… ②周… ③贺… ④刘… Ⅲ.可扩充语言,XML - 程序设计 Ⅳ.TP312

中国版本图书馆 CIP 数据核字(2003)第 036166 号

--

出 版 者:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
http://www.tup.com.cn
责任编辑:冯志强
印 刷 者:世界知识印刷厂
发 行 者:新华书店总店北京发行所
开 本:787×960 1/16 **印张**:22.75 **字数**:478 千字
版 次:2003 年 8 月第 1 版 2003 年 8 月第 1 次印刷
书 号:ISBN 7 - 302 - 06632 - 9/TP • 4960
印 数:0001~4000
定 价:42.00 元

序

XML 和安全的结合本身就是一个新领域，它和“传统”的应用安全不同，有着自己显著的特点。XML 安全和传统的应用安全有着共同的理论基础——密码学，但是完全理解 XML 安全必须要有一个全新的视角，同时也需要一个新颖的概念性工具。我们认为 Blake Dournaee 所著的《XML 安全基础》一书恰好满足了这一要求，它比较全面地介绍了 XML 以及 XML 加密、XML 签名等内容，并给出了一些实际的应用实例以及相关的解决建议，是一本值得推荐的好书。

本书是一本高级科普读物，介绍的内容比较广泛，要想了解细节的读者还得进一步阅读相关的资料。不过，我们相信，本书的翻译出版必将有助于国内 IT 专业人员、大专院校师生和相关人员对 XML 安全以及密码学应用的更好的理解。

本书的翻译出版得到国家重点基础研究发展规划资助项目（编号：G1999035810）和国家自然科学基金资助项目（编号：60083007）的支持，在此表示感谢。

感谢清华大学出版社冯志强编辑耐心细致的工作，感谢他的大力支持与帮助。感谢本书译稿的复审和终审人员，感谢他们为本书的出版提出的宝贵意见。最后，感谢所有帮助和支持我们的人。

2003 年 4 月于

中国科学院信息安全技术工程研究中心

致谢

我首先要感谢的人是我的父亲，他的无私奉献和爱给了我无尽的灵感。我同样也要感谢 Ilan Zohar，他一丝不苟地审校了本书，他激励我进入职业和研究生涯。他指出了我概念上的一些错误并帮助提高了本书的技术精确性。

Jason Gillis 做了大量的工作，他审校了几章书稿，我把他作为良师；还有 Clint Chan，他提供了大量的反馈信息。如果没有 Jason Gillis、Clint Chan、Catherine Huang、Patrick Lee 以及 Eleanor Huie（他 1999 年聘用我作为 BSAFE 开发支持小组的一个成员）的合理决策，这本书可能根本就不存在。

我特别想感谢 Daisy Wise，她帮助我编写算法类。如果没有她的耐心和投入，我可能还在重写类而不是写作本书。David Rutstein 帮助我鼓足勇气干下去，同时她作为一个合作者也完全投入到本书的工作中。

感谢 Dale Gundersen 在第 2 章中所做的杰出的工作，他给出了我所见到的最精巧的密码机。同样感谢 Bryan Reed，在本书的写作过程中，他给我提供了大量的支持和帮助。

感谢 Steven Elliot，他给了我写作本书的机会；同样感谢 Tracy Dunkelberger、Alexander Corona 和 Beth Brown，他们帮助我尽可能减少写作过程带来的艰辛。

需要特别提出的其他人包括 Rosie M. Faifua，他在本书的整个写作过程中都给予我支持。也要感谢 Stephanie Blossom 和 Chris Jones，因为本书的许多章节都是在他们的公寓写成的。此外，要感谢经常惠顾 San Luis Obispo 的人们，他们在适当的时候给我带来了欢乐。

然而，最重要的还是 Jeremy Crisp 的协作和鼓励，他虽然没有做什么工作，但在本书中仍然要有他的名字。

作者简介

Blake Dournaee 于 1999 年加入 RSA 安全公司的开发人员支持小组，专门负责 BSAFE 密码工具包的支持和培训。他从 San Luis Obispo 的加利福尼亚理工州立大学获得计算机学士学位，目前他是马萨诸塞大学的研究生。

审校者简介

Ilan Zohar 目前在 HP 公司工作，曾经参与了多种安全项目，最近则专注于 XML 安全标准的实现工作。以前，他在 RSA 安全公司的 RSA BSAFE™ CryptoC 小组工作。Ilan 于 1999 年在斯坦福大学毕业，获得电子工程硕士学位，在斯坦福他就专注于密码学及其在信息安全中的应用研究。Ilan 还拥有以色列海法的以色列理工大学的数学硕士学位，Cum Laude 的电子工程硕士学位以及 Summa Cum Laude 的数学和电子工程学士学位。你可以通过 ilan@stanfordalumni.org 和 Ilan 联系。

前言

写作本书的灵感来自一个无伤大雅的个人故事。很难相信在我的生活中的一些事件能使我写出一本完整的书。

有相当一段时间我对 XML 安全知之甚少，现在好多了（我希望这能够说服读者相信我多少还是知道一些这方面知识的。我们拭目以待）。特别地，我记得曾经研究过全新的“XML 签名”主题。那时，我对 XML 一无所知，仅仅知道安全的一些知识。不用说，在毫无目的地看过 XML 签名候选推荐标准之后，我立即意识到 XML 和安全的结合本身就是一个新领域，它带有自己的显著特点，而且它不同于“传统”的应用安全。尽管 XML 安全和传统的应用安全有着共同的基础，但是完全理解 XML 安全却需要全新的角度以及一套全新的概念性工具。当认识到这一点的时候，我看到了摆在面前的研究和工作领域。我仅仅希望以一种简单、容易理解的方式来解释一些知识。你手头的这本木讷、笨拙的图书就代表着我在这方面的尝试。

目录一览

目录

第 1 章

引　言

本章将讨论以下主题：

- 本书简介
- 各章简介

本书是 XML 安全的入门简介。大家应该高兴，因为你们将学习到大量的知识。本书内容包括了大量关于应用安全领域和 XML 安全领域的知识，它把大篇幅的知识汇合成短小篇章，使大家感到简单、易学。

本书是不全面的，它在 XML 安全发展的过程中所起的作用简直是微乎其微。技术的特性远远超过了一本书的范畴。基于此原因，我们要特别注重去理解概念问题，而避开一些细枝末节。本书的目的是为了介绍概念，要达到此目的往往要忽略一些细节问题。大家应该读完此书，并能够以一种易懂的方式来解释 XML 安全的基础知识，而不是卖弄关于 XML 安全的百科知识。

在 XML 安全的海洋里遨游之前，我们需要定义所谈论的内容。什么是 XML 安全？此书涉及的范围是什么？XML 是保证数据的可移植性的一种有效可行的技术。XML 安全是将“应用安全”运用到 XML 结构上去的应用。要分解应用安全这门学科的一个简单方法就是要区分数据保密和认证。继续定义下去，我们可能作出代换，并得出以下定义：XML 安全是把数据保密和认证应用到 XML 结构上去的应用。

并非所有的读者对数据保密和认证都有很多的认识。因此，我们在书的开始部分提供了有关安全概念的基础知识。这是第 2 章的重点。对于密码学的高深知识，安全基础部分仅提供的极少的内容。利用这里提供的有关资料可以进行密码学的学习，但是建议读者去查看参考文献部分和其他有关安全的文章。第 2 章忽略了许多有关密码算法的特定细节。例如，我们介绍了 3DES（一种特定的密码算法）并从高层次的观点来分析它的工作原理，但是我们将算法作为一种黑盒子并忽略了其具体细节。

同样，也并非所有读者对 XML 都有深入的了解。这一内容无论是在深度上还是在广度上都可以和应用安全相提并论，并且需要大量的概念性的预备知识。如果读者没有理解一些关于 XML 的基本知识，他就不能容易地读懂本书的信息。庆幸的是，第 3 章提供了关于 XML 的基础知识。第 3 章介绍了作为 XML 基础的一些细节和基本概念，因为这些知识与 XML 安全有关。写作第 3 章的目的是想传递为了了解大多数 XML 安全所需的最少的 XML 知识。

其他 XML 资料对于准确描述具体细节问题可能是有帮助的，但是它们并不是必需的。为了使读者弄明白 XML 安全，XML 的基

本知识包括了了解 XML 安全所需要掌握的知识。

在掌握了基础安全的必备知识后，第 4 章开始真正学习 XML。本章我们首先要介绍 XML 签名建议推荐标准。我们在本书中提到的所有有关 XML 的技术都源自一种由 WWW. W3C 提出的标准。你可能想知道在 W3C 背后的故事。我不能对 W3C 进行一一介绍，但 W3C 对自己进行了介绍(源自 www. w3. org)：

W3C 提出了多种互操作技术(规范、指南、软件和工具)来引导 Web 充分发挥它的潜能，即作为 W3C 一种用于信息、商务、交流和共同理解的论坛。

至少有三种主要 W3C 活动与 XML 安全直接有关，这些活动包括 XML 签名、XML 加密和 XML 密钥管理规范(XKMS)。可能有人会认为与 XML 安全有关的一系列活动不能到此结束，还应该介绍其他诸如信任断言(XTASS)或者传送协议(SOAP)等技术。尽管可以这样认为，但是以上提到的三种活动必定是最基础的，因为它们定义了用于基本的密码操作的机制，而且还考虑到了信任的建立问题。

第 4 章开始探讨 XML 签名以及它的工作原理。在三种核心的 XML 安全技术中，XML 签名提议推荐标准是最成熟的一种技术，它的地位也最高。在达到一定高度而成为一种 W3C 推荐之前，W3C 规范要经历一个过程，W3CRecommendation 是 W3C 规范的最高样式。在写作本书的时候，XML 签名规范是处于 Proposed Recommendation 标准的状态，这是在完全成熟并成为一种 W3C 推荐标准之前的一个阶段。在关于 XML 签名的整个讨论中，我使用了缩短的词组 XML 签名推荐标准，而没有用冗长的 XML 签名提议推荐标准。我这样做是为了使讨论简明扼要。XML 签名建议推荐标准的说法太啰嗦，无法成为有趣的普通谈话。但是大家应该明白 XML 签名规范只是一种建议推荐标准，无论我可能混淆的词汇用法如何。

因为 XML 签名技术很成熟，与其有关的内容包括三章：第 4 章主要介绍 XML 签名的语法；第 5 章主要是对 XML 签名处理规则的介绍；第 6 章是对建议使用的说明和常见问题解答的总结。我们会发现：仅仅 XML 的复杂性就足以使那些极聪明的人震惊，此外，我们还会发现，在我们努力对此有一个概念性理解的过程中，它可以提供一种最好的框架，让我们尝试新思想。

一旦完全了解了 XML 签名的工作原理，我们就可以转入第 7