SSL 技术详解手册

SSL 技术详解手册

SSL（安全套接层）是一个基于标准的加密协议，提供加密和身份识别服务。SSL 广泛应用于在互联网上提供加密的通讯。SSL 最普通的应用是在网络浏览器中通过 HTTPS 实现的。然而，SSL 是一种透明的协议，对用户基本上是不可见的，它可应用于任何基于 TCP/IP 的应用程序。本技术手册将介绍 SSL 协议的作用和使用，包括如何配置具有 SSL 保护的 FTP 服务器，企业如何生成可信 SSL 证书等内容。

SSL 协议基础知识

SSL（安全套接层）是一个基于标准的加密协议，提供加密和身份识别服务。SSL 广泛应用于在互联网上提供加密的通讯。由于 SSL 所处的位置，SSL 能够向客户机提供有选择地保护单一应用程序的能力，而不是对整个一组应用程序进行加密。那么 SSL 究竟处于什么位置，起到什么作用？

- ❖详解 SSL 协议
- ❖SSL 协议使用的最新测试细节

SSL 服务提供的安全保护

如何通过 Internet 在两个服务器间建立进行通讯的 SSL 连接？如何配置具有 SSL 保护的 FTP 服务器？又该如何通过启用 Exchange 2010 SSL 减负功能，优化 Exchange 2010 各访问协议和客户端访问服务连接到 CAS 服务器的负载？

- 创建服务器间的 SSL 连接
- 如何配置具有 SSL 保护的 FTP 服务器？
- 通过 SSL 发送的电子邮件是否需要加密
- Exchange 2010 SSL 减负功能全面配置指南

如何生成可信 SSL 证书

许多用户和一些企业过分得依赖 SSL，认为 SSL 是网络安全的万能药。然而，在网站上使用 SSL 时并不能使企业免受所有网络安全漏洞的影响，即使在最佳的情况下 SSL 也只是在客户和服务器之间提供了加密的链接。

- SSL 漏洞：企业如何生成可信 SSL 证书（上）
- SSL 漏洞：企业如何生成可信 SSL 证书（下）

详解 SSL 协议

问：我经常听人们说 SSL 位于网络层和应用层之间，这是什么意思?

答：这是一个非常好的问题。我想回答这个问题的最好方法是从检查协议的目的开始。在计算机领域，协议是管理数据在两个端点之间传输的一套规则。这套规则包括连接、通讯和实时数据交换的句法、语义和同步执行。然而，大多数通讯和网络协议都不是单独发挥作用的，这些协议在一个称作协议堆栈的地方分层次地放在一起。协议堆栈是需要共同合作的协议的具体结合，在这个协议堆栈中的每一个协议都执行专门的任务。SSL(安全套接层)是一个基于标准的加密协议，提供加密和身份识别服务。SSL 广泛应用于在互联网上提供加密的通讯。SSL 最普通的应用是在网络浏览器中通过 HTTPS 实现的。然而，SSL 是一种透明的协议，对用户基本上是不可见的，它可应用于任何基于 TCP/IP 的应用程序。

正如你想象的那样，设法保证一个协议栈能够完成其预定的任务和保证不同的协议都在一起工作是非常复杂的。为了帮助工程师概念化协议栈，人们开发了各种模型，每一种模型都提供一个网络协议应该如何工作的简要说明。OSI(开放系统互连)模型可能是最被广泛应用的，它使用 7 层结构把各种协议以及服务组织在一起。早期的 TCP/IP 模型使用 4 层或者 5 层。这两种模型接近最上面的层在逻辑上更接近用户，接近最下面的层在逻辑上更接近数据的物理传输。

根据 OSI 模型，应用层(7 层)为应用程序处理提供普通的应用服务。网络层(3 层)解决把数据包从网络的一个地方传送到另一个地方的问题。SSL 是一种不同寻常的协议，它不只在一个层上工作。SSL 既不是网络层协议也不是应用层协议，它是位于这两层之间的一种协议。

由于 SSL 所处的位置，SSL 能够向客户机提供有选择地保护单一应用程序的能力，而不是对整个一组应用程序进行加密。这个过程能够在不用担心 3 层(网络层)的情况下完成。由于这些原因，当使用 SSL 对网络通讯进行加密的时候，实际上只加密了应用层数据。这与 IPsec 协议不同。IPsec 协议在网络层工作，加密在 IP 层中的所有通讯数据。

(作者：Michael Cobb 来源：TechTarget 中国)

黑帽大会 2010：SSL 协议使用的最新测试细节

安全研究人员 Ivan Ristic 一直在默默地调查数百万个注册域名，以查明和测试 SSL 协议的实施情况。

Ristic 是 Qualys 公司的工程部总监，负责 SSL 实验室的管理工作。该实验室从事非商业性的研究工作，于去年被 Qualys 公司收购。该实验室的网站利用 SSL 测试工具检查配置问题和协议错误，而这些缺陷有可能被中间人攻击（man-in-the-middle attacks）所利用，诱骗人们交出自己的敏感数据。

“我们正试着在互联网上找到尽可能多的 SSL 服务器，并对它们一一进行评估”，Ristic 说，“我们的目标是弄明白 SSL 真正的使用现状。我们需要知道我们是否安全，如果存在安全隐患，我们还需要知道这些安全问题究竟是什么，可以采取哪些措施来解决这些问题。”

Ristic 计划于本月下旬在 Las Vegas 举办的 Black Hat 大会上详细陈诉 SSL 目前的研究细节。Ristic 表示，在审查的约 1.2 亿个域名中，约 72 万个域名使用了 SSL 认证。在本次采访中，Ristic 解释了研究人员需要对 SSL 进行重点关注的原因，尽管大家都认为它是一个近乎完美的安全协议。

请介绍下 SSL 实验室，它是怎样成为 Qualys 公司一部分的呢？

Ristic：SSL 实验室是一个重点关注 SSL 和 TLS 协议的研究组织，是我在大约一年前创立的，这来源于我对 SSL 的狂热爱好。当我发现 SSL 是一个如此优秀的协议时，我对 SSL 便着了迷。SSL 是最成功的协议之一，是网络安全的支柱，可我们在研究它的使用情况、帮助各地的用户配置 SSL 以及正确使用 SSL 等方面花的时间却很少。在我所创建的这个网站上，有大量可以帮助人们了解如何正确配置 SSL 的信息和工具。Qualys 公司非常看重我所做的研究。在收购之前，我可以说是一边负责 SSL 实验室，一边做其他的事情。而 Qualys 公司给我提供了一次机会，使我能够把精力全部放在这项研究上。

为什么缺乏对 SSL 的研究？

Ristic：我认为其中的原因是，SSL 在最初阶段就取得了许多令人激动的研究成果。该协议自创立以来大约有 15 年了。多年来，不知道什么原因，我们没有重视 SSL，反而研究应用安全领域、甚至是网络安全领域等其他方面的问题去了。我觉得，人们过去对 SSL 有一种约定

俗成的看法，那就是没有必要对它进行认真思考，这不得不说是一件令人惋惜的事。不过，几年下来，这种情况有了比较明显的改观。关于 SSL，我们已经有了不少新的认识。有几个相互独立工作的研究人员发现，SSL 不仅在实施过程中存在许多问题，其协议本身也存在一些需要解决的细小问题。现在，对 SSL 的研究又成了一个热点，越来越多的人开始不再沉默，并致力于解决 SSL 的问题。

许多问题都是源于配置吗？

Ristic：是的。实施工作中存在问题，协议本身也存在一些小问题。如果您是一名普通用户，您不必对协议问题关注太多。这是 SSL 厂商需要关心的问题，是研究人员改善该协议需要解决的问题。作为一个普通用户，您只需要保持系统更新。如果您保持了系统更新，那么您就可以应对这些问题了。至于配置问题，您可以马上对其进行了解，并且在半小时或几个小时内就能把问题解决。然而，大多数人根本没有意识到他们的配置存在问题。

配置是在线 SSL 评估工具的基础吗？所有这些问题都需要检查一遍吗？

Ristic：是的。在线工具分为两部分：第一部分是系统方法，它详细阐明了如何进行 SSL 评估；第二部分是工具。如果您键入了网站域名，该工具将转到该域名，并找到后台所有的 SSL 服务器，甚至是相同域名下的多个 SSL 服务器，然后对服务器逐一进行评估。评估的结果很容易看懂，因为我们对每种网站的配置方式都进行了总结，分成 A 至 F 级并用 0 到 100 进行编号。所以，即使您没有深入研究 SSL，也会很容易明白。而如果您是技术用户，我们还会提供更多的技术信息。这两类用户对此都感到满意。

您曾经谈到过 SSL renegotiation 漏洞。这是一个什么问题？

Ristic：renegotiation 漏洞是去年年底发现的。基本上，这个问题来自 SSL 的某一特殊层面，这是 SSL 的优势也是劣势。SSL 被设计成协议无关的，所以它位于一个独立的网络层。这使得它适用于任何底层的网络协议。您可以使用 SSL 保护 HTTP、电子邮件的 SMTP 协议、IMAP、LDAP 以及其他协议。而要想让这些不同的协议都与 SSL 一起使用，几乎不需要做什么工作。但是，我们现在明白了，当您部署一个没有直接连接到 SSL 的协议时，威胁就会被引入。最终，我们将被迫面对不匹配问题，以及其他一些您可能无法处理的 SSL 问题，因为您对其完全不了解。其本质是允许攻击者打开两个连接，并诱使用户把这两个连接当成一个来使用，由此攻击者便可以向有漏洞的网站引入任意内容。这一点修复起来相对快速，但实际上现在的问题是，所有的 SSL 服务器都需要打补丁。在对正在打补丁的无数服务器进行调查时，该漏洞便是我要检查的重点之一，以便了解当系统问题出现时管理员的反应速度有多快。

您的测试是用 2000 个数据包对单个服务器进行快速测试吗？

Ristic：这项评估的设计在构想之初是打算包含大量评估测试的，但在没有一个完整的SSL连接的情况下，只能在一个非常低的层次进行实施，不过这也使得速度非常快。一次测试需要进行约200次连接，数据交换的速度为250 kbts。我们不希望所测试的服务器超负荷运转，不过测试本身并不会损害任何服务器。我们正试着尽可能多的找到互联网上的SSL服务器，并对它们一一进行评估。我们的目标是弄明白SSL真正的使用现状。我们需要知道我们是否安全，如果存在安全隐患，我们还需要知道这些安全问题究竟是什么，可以采取哪些措施来解决这些问题。”

网站有数百万个，但只有相对较少的网站使用了SSL认证。这是否属实？

Ristic：是的。总共约有2亿个注册域名，在测试中我调查了其中的60%（1.2亿个）。弄明白所调查的1.2亿个网站都支持哪些服务，只是我工作的开始。我还想了解每个域名所代表的网站是否都真实存在，所运行的网站又是否安全。最终我们发现，约1/4的域名都无法访问。在所测试的域名中，约77%有一个服务器。大约2200万个域名有Web服务器，约3%的域名可能具备有效的SSL认证。我还发现，大约有72万个网站是安全的，在测试的第二阶段我还将对其进行更深入的评估。目前，我们在SSL领域面临着一个重大的问题：如果托管一百万个网站，您可以把它们全放在一个IP地址上；可对于每一个安全的网站来讲，您只能拥有一个独立的专用IP地址。这一问题很难解决，阻碍了SSL在世界范围内的普及。

您已经参与了开源Web应用程序防火墙ModSecurity项目。对于Trustwave收购Breach Security以及ModSecurity项目，您作何反应？

Ristic：收购可能会影响ModSecurity项目，但我们并不知道他们以后对ModSecurity有什么打算。说实话，ModSecurity项目在Breach Security下并没有良好发展，所以我认为收购可能会让情况变得更好一些。虽然他们在维护ModSecurity项目上做得的确很好，但在过去几年里我们没有看到ModSecurity取得过什么进展。我仍然会以贡献者的身份参与此项目，如果有时间还将继续作出自己的努力。

为什么ModSecurity项目的进展不大？

Ristic：我认为是因为ModSecurity与Breach Security的利益不一致造成的，因为Breach Security除了ModSecurity还有他们自己的产品。不幸的是，在ModSecurity被收购后，Breach Security并没有将其融入到自己的产品线中。如果当初他们做到了这一点，ModSecurity会因此而受益，因为ModSecurity也会成为Breach Security利益的一部分。

(作者：Robert Westervelt 译者：Sean 来源：TechTarget中国)

创建服务器间的 SSL 连接

问：我如何通过 Internet 在两个服务器间建立进行通讯的 SSL 连接呢？SSL 连接不仅仅是作为网络服务器或者网络客户端，而是类似于服务器/客户端的需要交互的两个应用程序，且将 Internet 作为其网络的一部分。怎样的设置才是最好、最安全的？

答：实际上，在服务器间建立 SSL 连接有许多种方式，不过最适合您所述情况的方式依赖于您计划使用的网络协议类型。正如您所知的那样，安全套接字层(SSL)在 TCP/IP 连接中允许对数据进行加密来进行保护。最常用的 SSL 的实施方式是 HTTPS 协议：一个替代的 HTTP 在 Web 上进行安全、加密传输的协议。

在两个服务器间建立安全连接最简单的方式是使用"安全 Shell 指令"(SSH),其利用 SSL 来建立一个类似于远程连接方式的服务器间连接。这项技术被内置于 Linux/Unix 系统中，对于 Windows 系统，也同样有类似的免费的实现，包括 OpenSSH 和 PuTTY。

如果您正在建立这样一个客户端应用程序，您需要针对您所使用的编程环境配置相应的 SSL 开发包。SSL 的实现非常普遍，几乎适合任何的开发环境。我经常使用的是 Crypt:SSLeay，一个 Perl 语言的开发包来实现，然而任何适合您开发环境的标准 SSL 开发包都能正常工作。

(作者：Mike Chapple　译者：行久　来源：TechTarget 中国)

如何配置具有 SSL 保护的 FTP 服务器？

问：有没有可能在 5R2 版 OS/400 操作系统中设置一个具有 SSL 功能之 FTP 服务器?

答：答案是肯定。iSeries FTP 服务器既支持 TLS(传输层安全)又支持 SSL(安全套接层)保护之进程，包括客户身份识别和自动登录，以便为通过 FTP 控制和数据连接传输之数据进行加密。在你能够设置你之 FTP 服务器使用 SSL 之前，你必须要在你之 iSeries 服务器上安装必要之程序和设置数字证书。不过，在我们考察如何设置你之 FTP 服务器之前，了解 FTP 协议是非常重要的。

FTP 使用两个 TCP 连接，一个连接用于控制，另一个连接用于数据。标准之控制连接使用 TCP 端口 21，默认之数据连接是端口 20。要开始一个安全之 FTP 进程，用户可以连接没有加密之 TCP 端口 21，然后协商身份识别和加密选项。这个过程称作显示控制。另一方面，当用户选择安全 FTP 端口之时候，这种连接是隐式连接，通常使用 990 端口，在这个端口之连接是 TLS/SSL。对这个控制连接进行加密之主要原因是在登录 FTP 服务器时隐藏口令。没有安全控制连接，FTP 协议不允许你拥有一个安全之数据连接。

当你为控制连接使用 TLS/SSL 加密之时候，这个 FTP 客户端软件也在为在 FTP 数据连接上发送之数据加密。加密具有很高之性能成本，在数据连接中可以绕过这种加密措施以便在不降低网络性能之情况下发送非机密之文件，而且仍可以通过不暴露口令之方式保护系统。iSeries FTP 服务器提供了这两种选择。为了在你之 iSeries V5R2 服务器上设置具有 SSL 功能之 FTP 服务器，你需要确保这个服务器安装了如下软件：

- OS/400 操作系统 V5R2 版或者以上版本。
- TCP/IP 连接工具。
- 用于 iSeries 服务器之 128 位“Cryptographic Access Provider”。
- IBM 之数字证书管理器。
- IBM HTTP 服务器。

下一步你需要进行如下操作：

1. 创建一个本之证书授权，或者使用数字证书管理器设置 FTP 服务器使用与这个 FTP 服务器有关之公开证书。

2. 要求 FTP 服务器对客户进行身份识别。

3. 在 FTP 服务器上启用 SSL 功能。

（作者：Michael Cobb 译者：Shirley 来源：TechTarget 中国）

通过 SSL 发送的电子邮件是否需要加密

问：当在电子邮件客户端软件中使用 SSL 时，电子邮件附件会通过一个加密的隧道传输吗?

答：所有通过 SSL 连接传输的通讯都是加密的，无论它是一个网页、一个文件还是一个电子邮件附件。在这个问题中，电子邮件附件是在电子邮件客户端与一台 SMTP(简单邮件传输协议)或者 IMAP 服务器之间传输的。在一个 SSL 连接上，电子邮件信息和附件都使用 SMTP，并且在最终达到收件人电子邮件信箱之前也能要在几台机器之间传送。这与 FTP 那样的协议工作方式不同。那种协议是在两台机器之间直接传送文件。

当你通过 SSL 发送电子邮件和附件的时候，邮件从这台电脑传送到电子邮件服务器。当收件人收取这封电子邮件的时候，这个邮件信息和附件再次通过 SSL 传送到它们的 PC。然而，如果一封电子邮件是发送到机构外部的某个人的，这封电子邮件就可能以不加密的明文方式传送。尽管有这种局限性，使用 SSL 肯定比使用在整个互联网和其它公共网络上的 SMTP 连接好一些。

要使用 SSL，你必须在你的邮件服务器上安装一个数字证书并且加密邮件集以及邮件传输。仅仅加密 SMTP 协议只保护传送到微软 Exchange 服务器的邮件，而不保护 POP3 或者 IMAP4 邮件。重要的是要记住，你的信息即使是在 SSL 连接上发送的也只是在传输过程中是加密的。这个邮件信息在邮件服务器或者收件人的 PC 和任何备份介质上都是以明文显示的。

因此，要保证邮件信息和附件的安全，明智的方法是在发送电子邮件之前对邮件进行加密。使用文件加密不仅能够在传输过程中保护附件，而且还能在 PC 存储附件的时候保护文件，并且在邮件通过任何邮件服务器和达到收件人的机器的时候提供保护。我还建议对任何重要的信息进行签名。然而，永远不要向某些人盲送(blind carbon copy)加密的电子邮件，因为大多数电子邮件客户端软件都很容易看到是谁盲送的邮件!

(作者：Michael Cobb 来源：TechTarget 中国)

Exchange 2010 SSL 减负功能全面配置指南

当企业中采用硬件负载均衡设备来平衡 CAS 阵列（客户端访问服务器阵列）中各 CAS 服务器的负载流量时，我们可以部署并采用 Exchange 2010 的 SSL 减负功能来优化 Exchange 2010 各访问协议和客户端访问服务连接到 CAS 服务器的负载。

通过启用 SSL 减负功能，管理员可以将 CAS 服务器的 SSL 入站连接完全交给负载均衡（NLB）设备接管。这样做的好处在于：可以将占用 CAS 服务器 CPU 的 SSL 工作量（加密和解密任务）转交给 NLB 设备，以释放出更多的资源让 CAS 服务器来处理更多其它任务和负担其它功能。这样处理的另一个原因是，管理员可以充分利用好网络的 7 层模型。例如：使用 SSL 减负到 NLB 设备基于 Cookies 的持久性处理功能和配置反向 SSL 等。

注意：

如果您启用了 Exchange 2010 CAS 服务器的 SSL 减负功能，NLB 设备到 CAS 服务器之间所有用户密码都将通过明文方式传送，因此您需要一个安全的网络环境以保证密码不被侦听和截取。

为 Outlook Web App (OWA)启用 SSL 减负

要为 Outlook Web App (OWA)启用 SSL 减负功能，必需在 CAS 阵列的所有 CAS 服务器上执行如下两个步骤：首先，你需要在 CAS 服务器的注册表的如下路径中添加一个 SSL 减负功能的 REG_DWORD 值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange OWA

在此注册表路径下创建名称为“SSLOffloaded”的 REG_DWORD 值，并将值设置为“1”

其次，我们需要禁用 OWA 虚拟目录的 SSL 要求。打开 IIS 管理器——展开 Default Web Site——选中“OWA”虚拟目录——双击“SSL 设置”——取消对“要求 SSL”的勾选”

配置完成后，执行“iisreset /noforce”命令重启 IIS，以使配置生效。

为 Exchange Control Panel (ECP)启用 SSL 减负

与配置 OWA 的方式不同，启用 Exchange Control Panel (ECP) 减负功能时我们不再需要对注册表进行更改，这是因为 ECP 减负的注册表与 OWA SSL 减负使用的注册表值相同。

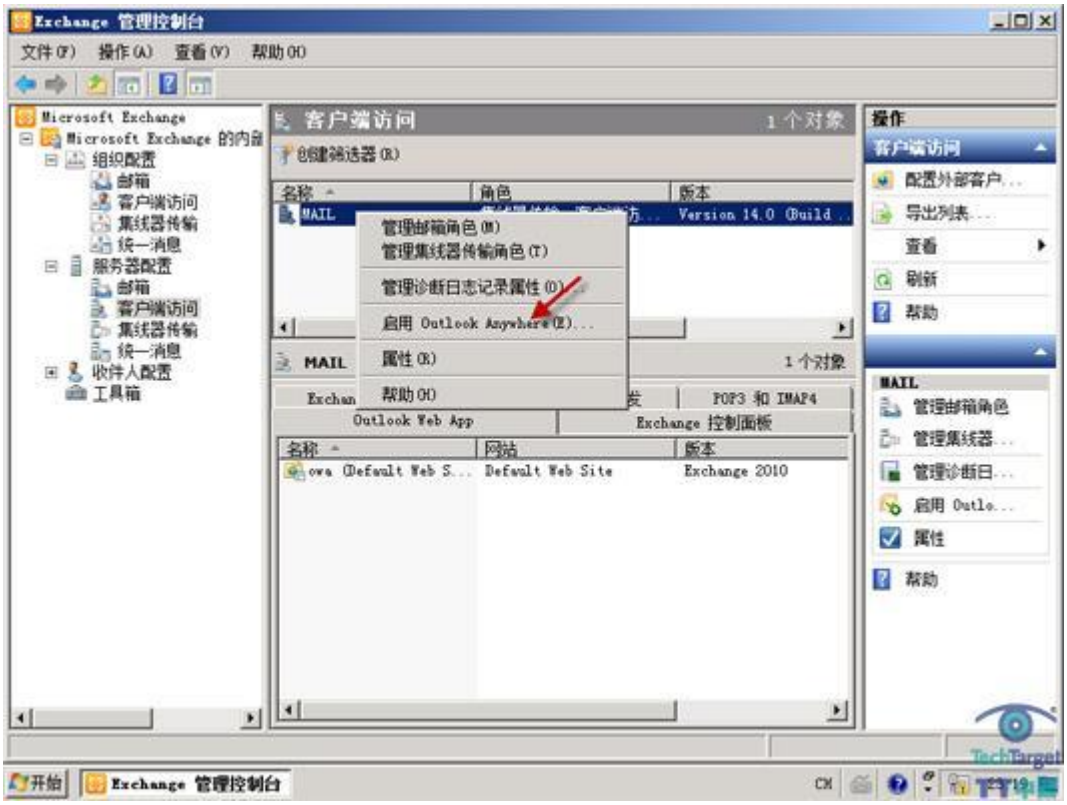
下面我们还在需要禁用 ECP 虚拟目录的 SSL 要求。打开 IIS 管理器——展开 Default Web Site——选中“ECP”虚拟目录——双击“SSL 设置”

同样的，取消对“要求 SSL”的勾选”

配置完成后，执行“iisreset /noforce”命令重启 IIS，以使配置生效。

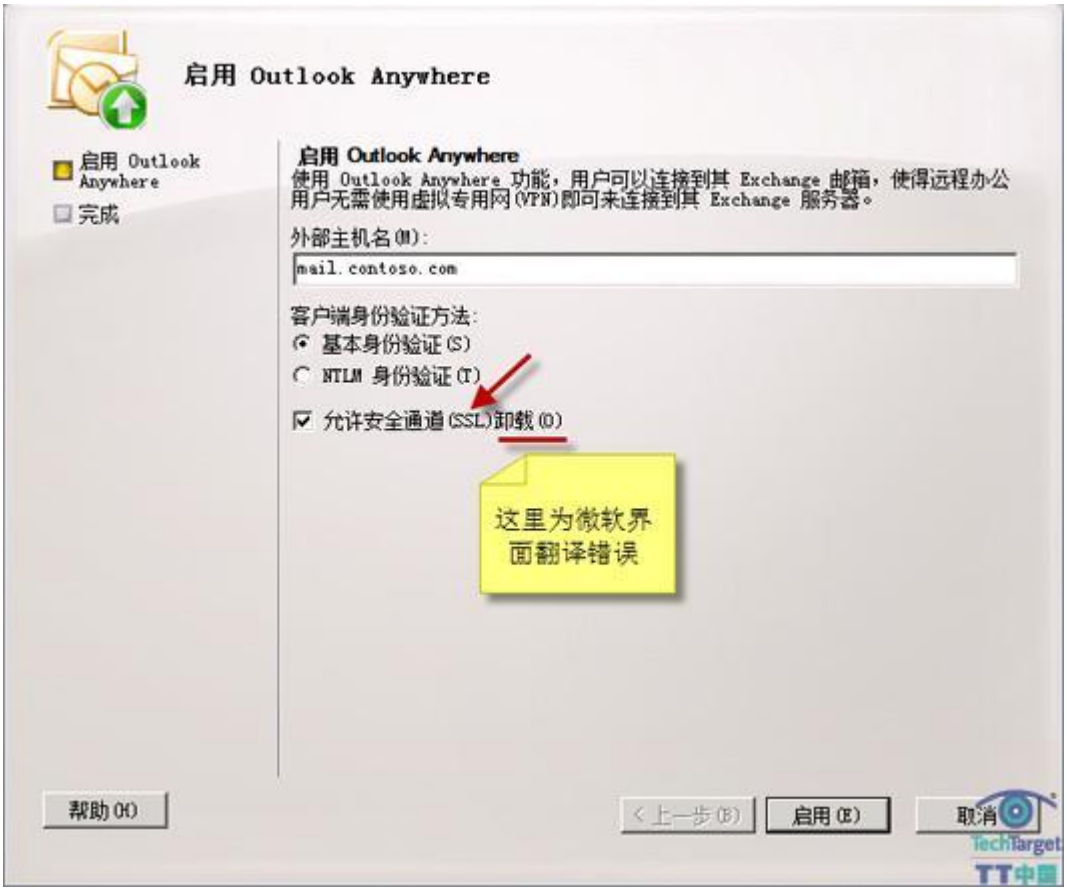
为 Outlook Anywhere (OA)启用 SSL 减负

要为 Outlook Anywhere 启用 SSL 减负，只需要一步操作。但首先我们需要通过 Exchange 管理控制台（EMC）或 Exchange 命令行管理程序（EMS）来确定当前的服务器是否已经启用了 Outlook Anywhere。



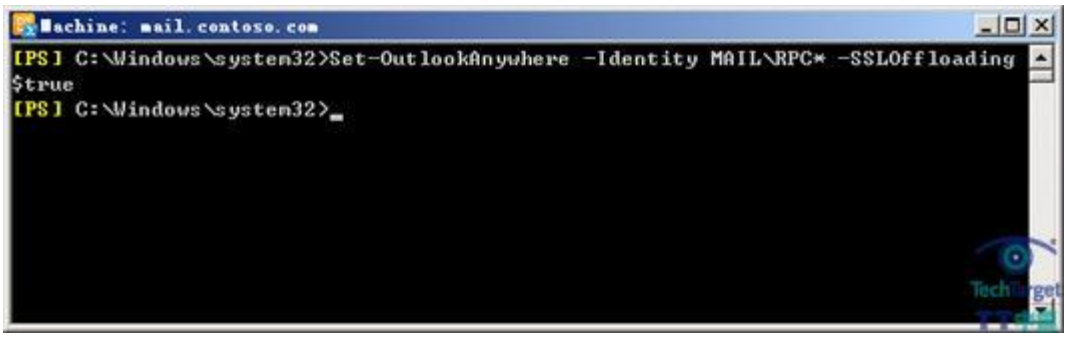
如果您的服务器当前并未启用 Outlook Anywhere 功能，我们可以在配置 SSL 减负时通过“启用 Outlook Anywhere 向导”来进行启用：在 CAS 服务器上打开 EMC（Exchange 管理控制台）——如下图所示，选择“启用 Outlook Anywhere”

在弹出的向导中选中“允许安全通道（SSL）减负”如下图：



如果您的服务器当前并已启用了 Outlook Anywhere 功能，我们则需要使用 Set-OutlookAnywhere cmdlet 来启用 SSL 减负。在我们的实例中，打开 EMS（Exchange 命令行管理程序）执行如下命令：

Set-OutlookAnywhere -Identity CAS 服务器\RPC* -SSLOffloading $true



执行上述命令后，将自动禁用 RPC 虚拟目录的“要求 SSL”选项，这意味着我们不需要再对 IIS 进行手动配置。

为 Exchange ActiveSync (EAS)启用 SSL 减负

Exchange ActiveSync (EAS)启用 SSL 减负功能也非常简单，与前面介绍的方法类似，我们只需在 IIS 中取消“Microsoft-Server-ActiveSync”虚拟目录“SSL 设置”中的“要求 SSL”选项再重启 IIS 即可。

注意：

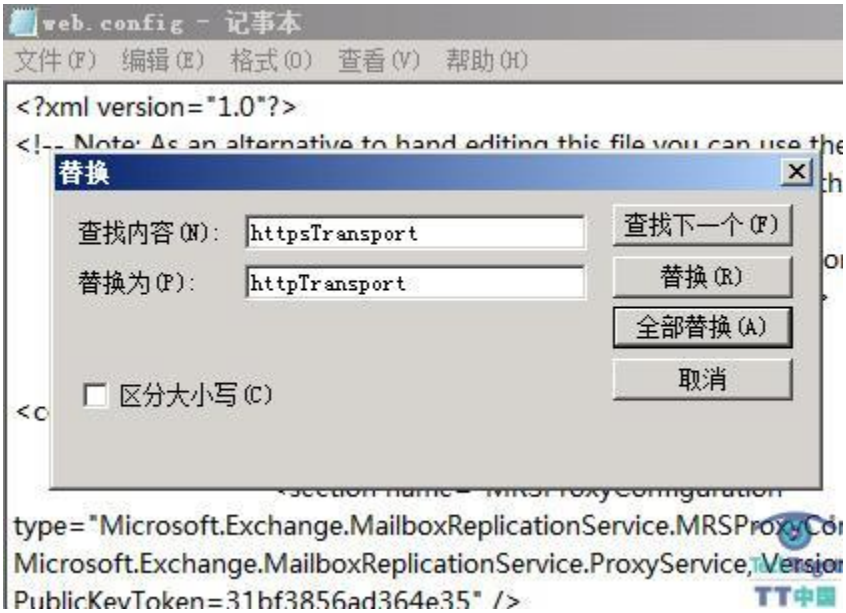
Exchange ActiveSync 只支持 Internet 访问的 SSL 减负，并不支持活动目录站点 CAS 代理之间的 SSL 减负。

为 Exchange Web Services (EWS)启用 SSL 减负

要为 Exchange Web services 启用 SSL 减负功能，必需在 CAS 阵列的所有 CAS 服务器上执行如下三个步骤：

1、 在 IIS 中取消“EWS”虚拟目录“SSL 设置”中的“要求 SSL”选项再重启 IIS

2、 更改 EWS 虚拟目录中的 web.config 配置文件。在 C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews 目录中找到并用记事本打开 web.config 配置文件，将所有的“httpsTransport”替换为“httpTransport”



3、 使用“iisreset /noforce”命令重启 IIS。

注意：

在 Exchange 2010 SP1 中，我们只需要在 IIS 中对 EWS 虚拟目录进行配置即可实现 SSL 减负功能，不再需要对 web.config 配置文件进行修改。

为自动发布服务(AS)启用 SSL 减负

要为自动发布服务启用 SSL 减负功能与配置 EWS 减负类似，管理员必需在 CAS 阵列的所有 CAS 服务器上执行如下三个步骤：

1. 在 IIS 中取消“Autodiscover”虚拟目录“SSL 设置”中的“要求 SSL”选项再重启 IIS

2. 更改 Autodiscover 虚拟目录中的 web.config 配置文件。在 C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Autodiscover 目录中找到并用记事本打开 web.config 配置文件，将所有的“httpsTransport”替换为“httpTransport”

3. 使用“iisreset /noforce”命令重启 IIS。

(作者：付林　来源：TechTarget 中国)

SSL 漏洞：企业如何生成可信 SSL 证书（上）

在拉斯维加斯举办的 2010 年黑帽安全大会和 Defcon 黑客大会上，有几份报告是关于 SSL（安全套接层）现状和 SSL 漏洞及攻击的。

许多用户和一些企业过分得依赖 SSL，认为 SSL 是网络安全的万能药。然而，在网站上使用 SSL 时并不能使企业免受所有网络安全漏洞的影响，即使在最佳的情况下 SSL 也只是在客户和服务器之间提供了加密的链接。在这篇文章中，我们将讲述为何企业应该仔细评估 SSL 最新漏洞对计算环境可能造成的风险，以及应该采用哪些措施来降低这些风险。

SSL 现状：SSL 漏洞和攻击

SSL 是在 1994 年由 Netscape（美国网景公司）研发的，目的是为新兴通讯媒介（即因特网）上的电子商务建立起安全的连接。自那时起，人们又对 SSL 进行了几次改进，例如传输层安全协议（TLS），但是 SSL 仍存在许多漏洞和攻击。Defcon 2010 上的 EFF SSL 考察计划（SSL Observatory Project），以及在 2010 黑帽安全大会上 Qualys 公司的 SSL 实验室报告，都向人们展示了当前 SSL 所存在的不足。

作为研究的一部分，EFF 项目收集了在互联网上使用的 SSL 证书，并记录了 SSL 客户和服务器之间的一些有趣行为。其中一个最大的发现是：有大量使用 SSL 的服务器和认证中心（CA）存在安全隐患，极易受到透明的中间人（man-in-the-middle）攻击。而这些服务器和认证中心中的大部分仍然被他们的企业用户所信赖。

来自 Qualys 公司 SSL 实验室的报告专注于密码选择、SSL 协议以及目前 SSL 在互联网上应用时存在的不足。报告中很重要的一点是：网络浏览器只需安装 10 到 20 个根（root）证书授予机构就可以在大多数网站上使用 SSL 功能，而不是像 IE 和 Firefox 一样将所有的认证中心设为默认。那些狡猾、有野心的攻击者会选择攻击这十多个 CA，而每个 CA 都可以为 DNS（域名服务器）进行认证，所以攻击能在网络上造成巨大的危害，这确实是一件值得关注的事。

该报告记录描述了使用认证度低的证书会造成的攻击，这些证书是在 DebianLinux 操作系统中生成的，它们在 OpenSSL 补丁发布之前生成，该补丁可以移除证书中存在的一项问题。这些证书的危害在于，它们能够导致中间人攻击、碰撞攻击（collision attacks），还有黑客

暴力破解认证中心根密钥以伪造任何类型的证书进而导致的攻击。SSL renegotiation 漏洞也可以被黑客利用，进而控制 SSL 的链接。

知晓何种配置易受攻击，确定一个企业的特定风险，这些工作都比较困难，尤其是现在 SSL 的设置越来越复杂。目前许多 SSL 设置都包括负载均衡、通配型证书等。所以说，企业目前所面临的威胁不是微不足道的，但确定哪些系统易受攻击这一点还是可以做到的。

利用上述研究小组的新成果，黑客不仅能够确定一家企业的 SSL 服务器，还可以获知 SSL 在这些服务器上的使用情况。一旦黑客发现某台 SSL 服务器的安全性较低，他就可以利用这一点发起攻击（如中间人攻击），从而对 SSL 上的网络流量进行查看和操控。这些攻击还能危及其他的协议，所以为了安全起见，用户还可以使用与 EFF 和 Qualys 研究人员同样的方法，扩大对这些危害的了解深度，去研究其他一些使用了 SSL 的非 HTTP 协议，例如 IMAP、SMTP 等。这样能够更深入认识服务器上 SSL 的使用情况，这样才能帮助你了解在加密过程中哪些地方使用了安全性低的证书和协议，以及黑客可能会在系统的哪些地方发起攻击。

要确定客户是否容易受到上述攻击的威胁，可以检测目前所使用的浏览器版本，有两种方法：被动流量分析或检查客户端。这项检测有助于确定 SSL 服务器所默认的可信赖认证中心，以及这些认证中心能否被用来攻击系统，或攻击由该认证中心所建立的连接。这项检测对非 HTTP 协议也有效，但因为非 HTTP 协议所支持和使用的加密选项或许不同，所以检测的工程会更复杂些。

（作者：Nick Lewis　译者：Sean　来源：TechTarget 中国）

SSL 漏洞：企业如何生成可信 SSL 证书（下）

企业 SSL 防御策略

要使企业和用户抵御来自 SSL 的威胁，就需要了解企业在哪些地方使用了 SSL，以及是如何使用的。这项工作可以使用与 EFF 和 Qualys 类似的方法，除此之外还有另外两种方法：监测网络流量，或者在客户端和服务器软件上执行应用程序详细清单（inventories）。在这一步完成后，你首先需要认识到，除非自己的企业在 PKI（公钥基础设施）和 SSL 使用方面经验丰富，否则使用行业标准的 SSL 或认证中心是不明智的，因为它们极易导致 SSL 的配置问题。在客户端这一方面，你还需要使用最新的软件和安全配置（其中默认的可信赖认证中心清单是时刻更新的），才能预防由于 SSL 漏洞导致的攻击。如果企业确实有使用复杂 SSL 配置的必要（例如使用 SSL 加速器和只支持某种类型认证的智能卡），并且拥有处理这种复杂配置的专业知识，那么这项配置需要小心地管理，因为 SSL 会导致不安全的配置，这一点在上述的报告中已经证明了。

最后一项控制只涉及授权（白名单）企业使用的浏览器中所部署的必要认证中心，可以抵制来自潜在恶意认证中心的攻击。然而，这可能需要花费很大的精力，不仅要发现这些必要的认证中心是什么，还要禁用其他的认证中心。

用户可以在一开始就使用 Qualys SSL 实验室报告中所提出的 17 种可信赖的 SSL 证书授予机构，随后再根据自己的需要进行添加。同时，可以考虑使用扩展验证证书，因为扩展验证证书与当前标准的证书相比提供了更高的安全保证。当前的标准证书不仅要考虑授予证书的认证中心，还要考虑向网络浏览器表明所访问网站的合法性。但是，EV（扩展验证）证书不会这么麻烦，它会帮助用户区分不同类型的证书，以及这些证书的授予单位。升级后安全性更高的浏览器会在地址栏上显示一个绿条，以表明使用了扩展验证证书。

结论

虽然 SSL 的安全风险日益严重，但是 SSL/TLS 协议一直在改进，服务器和客户系统也致力于应对这些漏洞和攻击。操作系统和应用程序供应商所附带的 SSL 管理和支持工具的性能有了大幅度的提高。这些工具被用户广泛的应用于维护 SSL 的安全性以及它的相关系统，这些做法对保护互联网隐私是极其重要的。企业应当经常关注人们对认证中心的讨论，从而获悉在浏览

器的证书信任名单中哪些认证中心是默认的，从而避免那些不信任的认证中心被添加在信任名单中。

（作者：Nick Lewis 译者：Sean 来源：TechTarget 中国）