计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2017,26(10):124−132 [doi: 10.15888/j.cnki.csa.005999]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

Web 网站 SSL/TLS 协议配置安全研究①

胡仁林 [1,2], 张立武 [2]

[1](中国科学院大学, 北京 100049)
[2](中国科学院 软件研究所, 北京 100190)

摘　要: SSL/TLS 协议是目前通信安全和身份认证方面应用最为广泛的安全协议之一, 对于保障信息系统的安全有着十分重要的作用. 然而, 由于 SSL/TLS 协议的复杂性, 使得 Web 网站在实现和部署 SSL/TLS 协议时, 很容易出现代码实现漏洞、部署配置缺陷和证书密钥管理问题等安全缺陷. 这类安全问题在 Web 网站中经常发生, 也造成了许多安全事件, 影响了大批网站. 因此, 本文首先针对 Web 网站中安全检测与分析存在工具匮乏、检测内容单一、欠缺详细分析与建议等问题, 设计并实现了 Web 网站 SSL/TLS 协议部署配置安全漏洞扫描分析系统, 本系统主要从 SSL/TLS 协议基础配置、密码套件支持以及主流攻击测试三方面进行扫描分析; 之后使用该检测系统对 Alexa 排名前 100 万网站进行扫描, 并做了详细的统计与分析, 发现了不安全密码套件 3DES 普遍被支持、关键扩展 OCSP Stapling 支持率不足 25%、仍然有不少网站存在 HeartBleed 攻击等严重问题; 最后, 针对扫描结果中出现的主要问题给出了相应的解决方案或建议.

关键词: Web 网站; SSL/TLS 协议; 安全漏洞扫描; 基础配置; 密码套件

引用格式: 胡仁林,张立武.Web 网站 SSL/TLS 协议配置安全研究.计算机系统应用,2017,26(10):124–132. http://www.c-s-a.org.cn/1003-3254/5999.html

Research on Security Vulnerability of SSL/TLS Protocol Configuration in Web Sites

HU Ren-Lin[1,2], ZHANG Li-Wu[2]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract: The SSL/TLS protocol is one of the most widely used security protocols in communication security and identity authentication. It plays a very important role in ensuring the security of information system. However, due to the complexity of the SSL/TLS protocol, web sites are prone to security vulnerabilities such as code implementation vulnerabilities, deployment configuration defects and certificate key management problems when implementing and deploying SSL/TLS protocols. This type of security problems often occurs in Web sites, which also causes a lot of network security events, affecting a large number of sites. However, the existing methods to analyze and detect web security cannot satisfy the need. First, there are very few tools in this field, and their targets tend to focus on some certain aspects. In addition, these problems need to be further explored to acquire more detailed analysis and recommendations. In this paper, we design and implement a detection system to test the SSL/TLS protocol deployment of web site based on SSL/TLS. Our system performs vulnerability scanning and analysis mainly from three aspects: protocol basic configuration, cipher suites support, and typical attack test. We use it to scan the top 1 million websites of Alexa, and give detailed statistics and analysis. We found that the unsafe cipher suite 3DES is generally supported and the critical expansion OCSP Stapling support rate is less than 25%. What's more serious is that there are still many sites suffering from HeartBleed attacks and many other serious problems. Finally, the corresponding solutions or suggestions are given

① 基金项目: 国家自然科学基金 (61472409,61303247); 国家重点基础研究计划 (973 计划)(2013CB338003)
收稿时间: 2017-01-22; 采用时间: 2017-02-17

© 中国科学院软件研究所 http://www.c-s-a.org.cn

for the main problems in the scanning results.

Key words: Web sites; SSL/TLS; security vulnerability scanning; protocol basic configuration; cipher suites

1 引言

SSL/TLS 协议[1]作为网络信息系统中应用最为广泛的协议之一, 对于保障信息系统的安全有着十分重要的作用. HTTPS 是超文本传输协议 HTTP 和 SSL/TLS 协议的组合, 它提供了 Web 网站的安全通信需求. 目前各大浏览器产商、搜索引擎公司以及相关研究组织的一系列项目与决策都推动着 HTTPS 的快速发展. 据 Chrome 和 Firefox 所给出的数据表明[2,3], 现在全世界范围内超过一半的网页采用了 HTTPS.

由于 SSL/TLS 协议的复杂性, 使得 Web 应用系统在实现和部署 SSL/TLS 协议时, 很容易出现代码实现漏洞、部署配置缺陷和证书密钥管理问题等安全缺陷. 例如, 2014 年 3 月公布的 HeartBleed 漏洞[4], 由于广泛使用的开源组件 OpenSSL 存在实现缺陷, 造成了超过 50 万台服务器受到攻击, 导致服务器私钥和用户会话 Cookie 及密码被盗; 2016 年 3 月, 公布的 DROWN 漏洞主要利用弱加密算法对 RSA 进行破解, 这种类型攻击很可能使目前至少三分之一的 HTTPS 服务器瘫痪; 2015 年 8 月, 清华大学郑晓峰等人[5]公布了一个存在于主要浏览器的 Web Cookie 注入漏洞, 攻击者通过此漏洞可以窃取私密的私人会话数据, 导致 Google、Amazon、Apple 以及中国银联等网站都受此影响.

针对以上 SSL/TLS 协议实现和部署配置方面的安全缺陷, 实时在线的对 Web 服务器进行安全检测, 并报告存在的漏洞风险, 具有十分重要的意义. 对 Web 网站中 SSL/TLS 协议实现与部署配置方面进行检测, 一般来说主要分为如下三个部分: HTTPS 基础配置、密码套件支持以及攻击测试. 这三者之间既相互关联, 也相互制约, 基础配置和密码套件存在问题不仅可能导致相应的攻击, 也可能导致会话无法成功建立, 而类似 HeartBleed 这类攻击则是对其所配置的 SSL 开源组件实现方面的检测.

近年来, 与 SSL/TLS 协议部署配置相关的安全检测受到了研究者的广泛关注. Qualys SSL Labs[6]是 Ivan Ristić等人于 2009 年发起的一个项目, 一个在线版全球知名的 HTTPS 网站检测工具, 它提供服务器/客户端安全检测、SSL Pluse(全球 HTTPS 网站统计报告) 以及相关 API 接口调用; 针对密码套件方面的分析, Mozilla 的开源项目 CipherScan[7]可以实现对目标服务器进行密码套件的全面扫描与分析, 同时它也提供简单的证书验证、扩展支持以及密钥大小的扫描分析服务; TLS-Attacker[8]是由 Juraj Somorovsky 开发并维护, 用于测试评估 TLS 实现库的开源框架, 它可以自定义 TLS 消息序列、任意地动态修改 TLS 消息内容, 以检测可能存在的问题.

一方面, 以上开源项目基本都是针对单个网站进行测试, 并不适用于大范围的高效测试; 另外, 它们还存在以下不足与缺陷:

SSL Pluse 统计数据不全面, 受限于网站管理人员是否愿意公开其网站配置信息;

SSL Labs 对密码套件扫描不全面, 只针对最高的 SSL/TLS 版本进行了测试;

TLS-Attacker 本身是针对 SSL/TLS 开源组件 (如 OpenSSL、GnuTLS 等) 进行测试与分析, 而非实际 HTTPS 网站.

综上所述, 目前缺乏一个涵盖 SSL/TLS 协议基础配置、密码套件支持以及主流攻击测试方面的 Web 网站 SSL/TLS 协议部署配置安全检测分析系统. 因此本文主要通过设计开发一个 Web 网站安全检测分析系统, 对 Alexa 排名靠前的 HTTPS 网站进行深入的统计调研分析, 发现并分析存在的主要问题, 最后给出相应的建议.

2 相关工作

在 SSL/TLS 客户端检测方面, Jeff Hodges 等人[9]创建了 How's My SSL 网站, 它是一个针对 SSL 客户端安全配置的在线检测工具, 从协议版本、基本配置扩展以及攻击测试等方面给予了详尽的测试分析, 并且提供了相关 API 接口以供本地测试调用.

著名网络安全公司 High-Tech Bridge SA 在 2015 年 10 月推出的一个验证任何基于 SSL/TLS 协议服务器配置的在线检测评估工具 High-Tech Bridge Free SSL Server Test[10], 它主要以 NIST guidelines[11]、PCI DSS requirements[12]以及 HIPAA guidance[13]作

© 中国科学院软件研究所 http://www.c-s-a.org.cn

为网站安全评估准则, 对 HTTPS 网站的 SSL/TLS 协议的部署配置进行检测评估, 最后并给出相应的安全等级.

SSL/TLS Deployment Best Practices[14]是 Qualys SSL Labs 于 2012 年开始的一个项目, 主要针对 SSL/TLS 协议在应用中部署配置容易导致的常见问题给出了相应的最佳部署建议. 目的是让已经不堪重负的系统管理人员尽可能花少量时间就能完成 HTTPS 安全站点的搭建.

2.1 组织结构

本文的后续章节安排如下: 第 3 节阐述了 Web 网站 SSL/TLS 协议配置安全检测系统的研究与设计工作, 详细描述了关键模块的实现细节; 第 4 节结合我们的检测系统对实际 Web 网站进行检测后的结果与分析; 第 5 节针对扫描中出现的主流问题给出了相应的解决方案或建议; 第 6 节总结了本文的工作.

3 Web 网站 SSL/TLS 协议配置安全检测系统设计与实现

3.1 设计目标

本检测系统旨在针对 SSL/TLS 协议在 Web 网站中的基础配置、密码套件支持以及主流攻击测试方面进行检测与分析. 本系统主要在现有的开源项目上进行改进与集成, 我们认为 Web 网站 SSL/TLS 协议安全检测系统应当具备以下特性:

(1) 检测要全面详细. 对 Web 网站中 SSL/TLS 协议的实现与部署进行分析, 需要全面深入地检测 SSL/TLS 协议部署配置的各个方面, 如各协议版本下的密码套件支持情况等.

(2) 高效性. 由于是对 Alexa 排名前 100 万网站的测试, 因此我们需要高效地完成测试与分析. 引入多线程、多进程思想, 并结合考虑到 SSL/TLS 协议中等待时间限制等问题, 设计了适用于 SSL/TLS 协议攻击测试的特定并发程序.

(3) 可扩展性. 主流攻击测试方面应该具有可扩展性, 面向接口编程, 对于新型攻击的出现, 只需要编写相应的攻击代码, 并引入到主程序中, 即可实现对新型攻击的测试.

3.2 设计思想

本检测系统对 Web 网站的 SSL/TLS 协议部署配置方面进行全面检测与分析. 针对 SSL/TLS 协议基础配置方面, 我们将使用 SSL Labs 提供的 API 接口, 对其请求进行封装, 并根据其 API 接口要求进行特定的并发程序开发; 对于密码套件支持方面, 我们将借助 CipherScan 扫描工具, 将其以构件形式封装到本系统中, 并使用相关命令进行调用; 对于主流攻击测试方面, 我们将使用 TLS-Attacker 工具, 并对其整体架构、高效性进行重新设计与实现, 使其能够对实际的 Web 网站进行高效测试. 之后, 再将上述三个关键模块整合进行本系统, 进行集成开发, 获取的相关数据存储在 MySQL 本地数据库或以文件形式存储; 最后, 对数据进行相应的分析, 并对外提供报表输出接口, 将分析结果、解决方案或建议以报表形式呈现出来.

3.3 系统架构

本检测系统逻辑架构图如图 1 所示. 主要由数据收集层、存储层、数据分析层、应用层四个相对独立的构件组成. 数据收集层主要从 SSL/TLS 协议基础配置、密码套件支持以及主流攻击测试三个方面进行数据收集, 分别用到 SSL Labs 的接口服务、CipherScan 密码套件扫描工具以及 TLS-Attacker 攻击测试工具. 数据收集层扫描获取的数据一般存储于 MySQL 本地数据库或者以文件形式存储. 数据分析层主要对对收集来的数据从基础配置、密码套件支持以及主流攻击测试三个方面进行深入的统计分析. 应用层主要是根据统计分析的结果, 输出分析报表, 并对存在的主要问题给出相应的解决方案或建议.

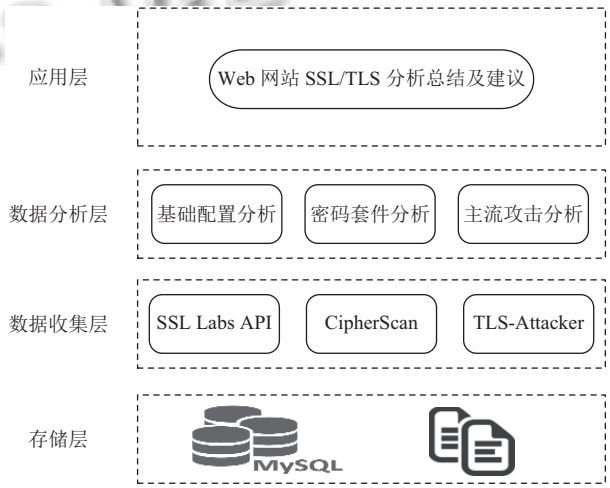

图 1 系统逻辑层次图

数据分析层是本系统的核心层, 它主要包括 SSL/TLS 协议基础配置分析模块、密码套件支持分析

© 中国科学院软件研究所 http://www.c-s-a.org.cn

模块、主流攻击测试分析模块, 如图 2 所示.

图 2 安全配置分析检测内容示意图

SSL/TLS 协议基础配置分析模块. 基础配置方面的检测主要包括: 证书验证、协议版本以及配置扩展支持情况. 其中证书验证方面又具体包含了证书签名算法、证书有效期检验、证书域名匹配、证书私钥大小以及证书链完整性等等; 协议版本支持方面, 要分别测试 Web 服务器对 SSL2.0、SSL3、TLS1.0、TLS1.1 以及 TLS1.2 的支持情况; 最后再测试 Web 服务器对 NIST guidelines[11]中所规定扩展的支持情况.

SSL/TLS 协议密码套件支持分析模块. 通过在各版本 SSL/TLS 协议建立情况下, 测试其对所有密码套件的支持情况. 具体统计分析其密钥协商算法、会话密钥强度以及完美前向安全套件的支持情况.

SSL/TLS 协议主流攻击测试分析模块. 本文中主要针对 SSL/TLS 协议中目前出现的主流攻击进行了测试与分析, 包括: HeartBleed 攻击、POODLE 攻击、PaddingOraclce 攻击、InvalidCurve 攻击等. 统计分析了各类攻击的结果, 并给出了相应的解决建议.

3.4 SSL/TLS 协议基础配置检测模块

在 1.1 节中, 我们已经提到虽然 Qualys SSL Labs 提供了比较全面的 HTTPS 服务器部署配置检测, 然而其 SSL Pluse 统计数据受限于网站管理人员是否愿意公开其网站部署信息, 并且对密码套件扫描方面并不全面. 基于以上原因, 我们将利用其公开的 API 接口, 进行请求的封装, 获取 Alexa 排名前 100 万网站的 HTTPS 部署配置信息.

根据 Qualys SSL Labs 提供的最新 API 文档: SSL Labs API Documentation v1.24.4[15], 我们对 SSL Labs 接口进行了封装, 并使用 Retrofit2 开源框架简化了 HTTP 请求处理, 然后使用 Gson 对返回的数据转成 Pojo 对象, 接着使用 Hibernate 作为数据持久层存储框架, 最后将所有解析后的数据存储到 MySQL 本地数据库, 大致示意图如图 3.

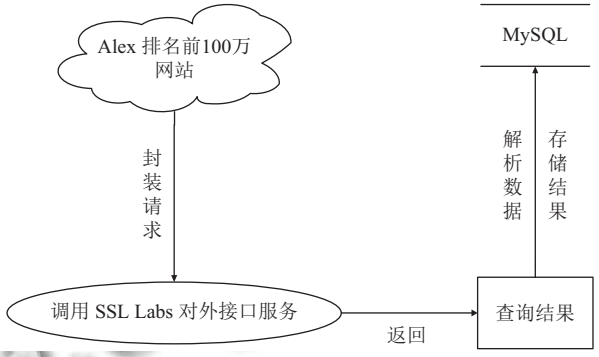

图 3 SSL Labs 接口调用示意图

另一方面, 为了加快数据收集工作的进行, 但是又不能超过 API 文档中规定的最大请求数量 (为了防止滥用 API 接口, SSL Labs 规定允许同时发起的最大请求数量为 25), 我们设计了特定的多线程并发程序, 大体思想如下: 使用 Java 线程池, 并设定线程池大小为最大请求数量 25, 监测已发起的请求数量, 一旦某个请求返回了响应结果, 就执行请求队列消息中的下一个请求, 使得请求数量一直处于饱和状态, 最大限度地使用 SSL Labs 提供的 API 接口进行数据的获取.

目前单进程下可以完成平均每分钟 5 个网站的测评速度. 最终, 从 SSL Labs 获取的网站基础配置数据存储于 MySQL 本地数据库中.

3.5 SSL/TLS 协议密码套件检测模块

我们将 CipherScan 嵌入到本系统中, 以实现对目标 HTTPS 服务器密码套件扫描和分析. 先部署所需要的 Python 运行环境, 然后通过 Shell 命令执行脚本文件.

扫描结果以文件形式存储于本地.

3.6 SSL/TLS 协议攻击测试模块

TLS-Attacker 虽然能对 SSL/TLS 开源组件 (如 OpenSSL、GnuTLS) 的实现进行主动测试, 然而针对实际的 HTTPS 服务器却会产生各种各样的异常情况. 因此, 我们主要从以下三个方面对 TLS-Attacker 进行改进:

(1) 我们重新设计并实现了攻击代码的整体架构, 修改代码接口使其能够对指定的服务器进行攻击测试, 并采用工厂模式来创建新的攻击类型.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

(2) 为了加快攻击测试, 我们增加了多线程并发特性, 并且注意到攻击测试过程中消息等待时间限制等一系列 SSL/TLS 协议实现问题, 通过设定超时时间或者在规定时间内未响应的请求进行重新发送, 这两种方式解决了因为时间限制问题导致的攻击异常.

(3) 数据存储方面, 我们使用了 Hibernate 持久层框架, 将攻击测试结果存入 MySQL 本地数据库, 方便后期对数据进行提取和分析.

4 实验结果与分析

所有实验均在一台 10 核 CPU、16 G 内存的 CentOS 服务器上进行; 使用本测试系统的测试步骤如下:

(1) 对 Alexa 排名前 100 万网站进行数据收集工作, 并存储于 MySQL 本地数据库中;

(2) 对数据库中数据从基础配置、密码套件支持以及攻击测试三方面进行相关统计分析;

(3) 结合当前 SSL/TLS 协议安全现状, 对统计结果进行更细致的分析;

(4) 对扫描中发现的主要问题, 提出相应的解决方案或建议.

下面将从 SSL/TLS 协议基础配置、密码套件支持以及主流攻击测试三方面详细阐述相关实验结果. 注意, 下文中涉及到的所有表, 如无特别说明, 百分比 (%) 均是指占全部 HTTPS 网站总数的百分比, SSL Pluse(%) 是指 SSL Pluse 统计的百分比, PFS 百分比 (%) 是指占所有 PFS 密码套件的百分比, “-”表示 SSL Pluse 无此类统计数据.

4.1 Web 网站 SSL/TLS 协议基础配置

目前, 已使用该检测系统完成 Alexa 排名前 100 万网站的基础配置数据收集与分析工作. 从总体上来看, 超过 55.4% 的网站可通过 HTTPS 访问. 下面从证书验证、协议版本、配置扩展三方面进行详细分析与总结.

4.1.1 证书验证

(1) 证书签名算法

由表 1 可知, 证书签名算法以 sha256WithRSA 为主, 占 86.1%; sha1WithRSA 在 2017 年即将被各大浏览器产商所淘汰, 但目前仍然有 5.3% 的 HTTPS 网站使用该签名算法.

(2) 证书私钥大小

由表 2 可知, 目前主要是 RSA 2048bits 私钥, 占 85.6%; 仍然有 21 个 HTTPS 网站使用 1024bits 的 RSA 私钥; 更加高效又安全的 ECDSA 256bits 目前占到将近 12%.

表 1 证书签名算法

证书签名算法	总计	百分比(%)
None	10359	1.8697
ecdsaWithSHA256	63100	11.389
sha1WithRSA	29544	5.3324
sha256WithRSA	477256	86.1405
sha384WithRSA	5	0.0009
sha512WithRSA	60	0.0108

表 2 证书私钥大小 (部分)

证书私钥大小	总计	百分比(%)	SSL Pluse(%)
ECDSA 256	66442	11.9922	-
RSA 1024	21	0.0038	0.00005
RSA 2048	479886	86.6151	93.1
RSA 3072	150	0.0271	2.1
RSA 4096	26364	4.7585	4.8

(3) 证书链完整性

由表 3 可知, 不完整证书链占到 HTTPS 网站的 3.1%, 而不受信证书证书占 22.2%; 证书链的不完整并不一定说明证书不可信, 因为可以通过加入可信中间 CA 证书的方式来构造完整的证书链.

表 3 证书链完整性 (基数是 709652 个 hosts)

证书链	总计	百分比(%)	SSL Pluse(%)
完整	529449	74.6068	97.0
不完整	22333	3.147	3.0
不受信证书	157870	22.2461	-

4.1.2 协议版本

由表 4 可知, TLS1.2 和 TLS1.1 已经成为主流协议版本, 都超过了 85%, 相比于 SSL Pluse 的结果支持率更高; 仍然有 12.3% 的 HTTPS 网站支持不安全的 TLS1.0 及以下版本; 仍然存在少数网站支持或仅支持 SSLv2 或 SSLv3, 如有 17 个 HTTPS 网站仅支持 SSLv2.

表 4 协议版本

协议版本	总计	百分比(%)	SSL Pluse(%)
SSL2	17623	3.1808	5.8
SSL2 Only	17	0.0031	-
SSL3	98238	17.7311	18.6
SSL3 Only	1159	0.2092	-
TLS1	543101	98.0249	95.4
TLS1 or lower Only	68307	12.3288	-
TLS1.1	473247	85.4169	80.6
TLS1.2	482460	87.0797	83.2
TLS1.2 Only	2594	0.4682	-
TLS1.2, 1.1	9606	1.7338	-

© 中国科学院软件研究所 http://www.c-s-a.org.cn

4.1.3 配置扩展

由图 4 可知, 只有 23.2% 的 HTTPS 网站支持 OCSP Stapling 扩展, 而根据最新 (2017 年 1 月 3 日) 的 SSL Pluse 显示在其所调研的 139741 个网站中, 有 25.0% 的网站支持 该扩展, 因此说明实际的 HTTPS 环境中, OCSP Stapling 扩展的支持率更低, 然而 OCSP Stapling 这一扩展对于缓解中间 CA 压力、提高服务器响应速度、改善用户体验有着十分重要的作用, NIST guidelines[11] 已经将其作为关键扩展, 并规定所有 SSL/TLS 应用都应该实现.

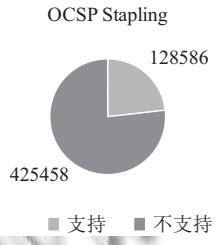

图 4 OCSP Stapling 扩展

另外, 我们还对重协商扩展以及 TLS 压缩算法进行了调研分析, 结果如下:

由表 5、表 6 可知, 根据我们的调研研究结果, 不安全的重协商扩展支持率为 2.9%, 而最新的 SSL Pluse (2017 年 1 月 3 日) 的调查结果为 1.1%, 由于我们数据来源是 Alexa 排名前 100 万的网站, 而 SSL Pluse 只调研了 139741 个网站数据, 因此在调研方法相同的情况下, 我们的数据说明了现实 HTTPS 环境中对不安全重协商扩展的支持更为严重; 而由于支持 TLS 压缩算法 (zlib) 导致 CRIME 攻击[16]的网站, 比 SSL Pluse 的调研结果要小将近 0.7%, 同理现实 HTTPS 环境中对 TLS 压缩算法支持率更低.

表 5 重协商扩展

重协商	总计	百分比(%)	SSL Pluse(%)
False	5199	0.9384	2.3
insecure	15950	2.8738	1.1
secure	532895	96.1828	96.5

表 6 TLS 压缩算法扩展

TLS压缩算法	总计	百分比(%)	SSL Pluse(%)
1(zlib compression)	7539	1.3607	2
False	5199	0.9384	0
NONE	541306	97.7009	98

4.2 Web 网站 SSL/TLS 协议密码套件

总的来说, Alexa 前 100 万网站中有 603391 个网站开启了 SSL/TLS, 占总数的 60.3%. 下面对这 603391 个网站从密钥交换算法、会话密钥强度、完美前向安全性等方面进行分析.

4.2.1 会话密钥强度

由表 7 可知:

(1) 从文献[17]中我们得知 3DES 安全性目前已经和 RC4 属于同一级别, 然而由上表可知有 532905 个 HTTPS 网站 (88.3%) 支持 3DES, 相比之下 RC4 目前存在 153525 个 HTTPS 网站 (25.4%) 支持 RC4 密码套件, 因此不安全的 3DES 套件应该开始引起重视;

(2) 仍然存在少数 HTTPS 网站只支持 3DES/RC4, 优先选择 3DES 的占 0.3%, 优先选择 RC4 的占 2.1%, 仍然有 1.1% 的 HTTPS 网站强制在 TLS1.1 及以上版本中支持 RC4;

(3) 有 8.8% 的 HTTPS 服务器支持 NULL、Export Key Exchange、RC4 等不安全的密码套件, 详见 NIST guidelines[11]中对不安全密码套件划分.

表 7 密码套件扫描结果 (部分)

会话密钥强度	总计	百分比(%)
3DES	532905	88.3184
3DES Only	550	0.0912
3DES Preferred	1719	0.2849
3DES forced in TLS1.1+	992	0.1644
AES	599329	99.3268
AES-CBC	598756	99.2318
AES-GCM	509780	84.4858
Insecure	53186	8.8145
RC4	153525	25.4437
RC4 Only	140	0.0232
RC4 Preferred	12783	2.1185
RC4 forced in TLS1.1+	6911	1.1454

4.2.2 密钥协商算法

由表 8 可知:

(1) 密钥协商算法主要以 RSA 和 ECDHE 为主, 并且 ECDHE 支持率高过 RSA;

(2) 仅有 2 个 HTTPS 网站支持易导致 Invalid Curve 攻击的 ECDH 密码套件;

(3) 仍然有少数 HTTPS 网站支持不安全的密钥协商算法, 如 ECDH/ADH/AECDH.

4.2.3 完美前向安全 (Perfect Forward Secrecy, PFS)

由表 9 可知:

(1) 已经有高达 95.4% 的 HTTPS 网站支持完美前向安全, 并且有 90.1% 的 HTTPS 网站优先选择 PFS 密码套件;

© 中国科学院软件研究所 http://www.c-s-a.org.cn

(2) 虽然有超过 32.5% 的网站使用 2048bits 的 DH 参数, 但是使用不安全的 1024bits 的 DH 参数仍然高达 19.2%, DH 参数最高支持 8192bits;

(3) 在 ECDH 方面, 主要使用曲线 P-256(82.9%) 来完成握手, 并且优先选择 ECDH(P-256) 套件的 HTTPS 网站高在 77.1%.

表 8 密钥协商算法

密钥协商算法	总计	百分比(%)
ADH	918	0.1521
AECDH	9574	1.5876
DHE	327644	54.3004
ECDH	2	0.0003
ECDHE	532966	88.6258
ECDHE and DHE	285103	47.2501
RSA	517470	85.7603

表 9 PFS(部分)

完美前向安全性	总计	百分比(%)	PFS百分比(%)
Prefer PFS	543950	90.1488	0
Support PFS	575507	95.3788	0
DH, 1024bits	115821	19.195	35.3496
DH, 2048bits	196265	32.527	59.9019
ECDH, P-256, 256bits	500295	82.9139	93.87
Prefer DH, 1024bits	42440	7.0336	12.9531
Prefer ECDH, P-256, 256bits	465038	77.0708	87.2547

4.3 Web 应用 SSL/TLS 协议攻击测试

目前, 使用该检测系统已完成 Alexa 前 10 万网站的攻击测试. 检测的攻击有: Bleichanbacher[18]、Invalid-Curve[19]、Heartbleed[4]、POODLE[20]、PaddingOracle[21] 以及 CVE2016-2107[8], 下面简单介绍一下这几种攻击:

(1) Bleichanbacher 攻击[18]: 敌手通过向服务器发送大量基于 PKCS#1 格式加密的消息, 从得到的不同错误响应消息中解密出预主密钥, 从而获取 TLS 会话密钥.

(2) InvalidCurve 攻击[19]: 某些椭圆曲线密码学库在处理输入时忽略了“点是否位于曲线上”这一检查, 从而导致无效椭圆曲线攻击, 使得服务器私钥泄露.

(3) Heartbleed 攻击[4]: OpenSSL 在实现 TLS 的心跳扩展时没有对输入进行适当验证, 导致敌手可以通过发送特定消息来引发缓冲区过读, 从而获取服务器或客户端的私密信息.

(4) POODLE 攻击[20]: 一种针对 SSLv3 的降级攻击, 由于 SSL 是先认证后加密, 使得 MAC 并没有对 Padding 部分进行保护, 从而导致敌手发起攻击, 获取会话 Cookie.

(5) PaddingOracle 攻击[21]: 它是一种针对 CBC 加密模式的攻击, 如果服务器对消息填充的有效性响应不同的错误消息, 那就说明可能存在该攻击.

(6) CVE2016-2107 攻击[8]: OpenSSL 开启 AES-NI 后, 对 CBC 模式填充检测逻辑存在漏洞, 且握手未完成时服务器报错信息以明文返回, 使得攻击者可利用不同响应来探测特定位置的字节, 从而解密明文.

由图 5 可知:

(1) 在所测试的 Alexa 前 10 万网站中, HTTPS 访问不可达网站将近 75%, 可能原因: 部分国外网站国内无法访问, 另一部分网站本身就不支持 HTTPS;

(2) 在 25217 个 HTTPS 访问可达的网站中, 有 21669 个 (超过 85%) 网站存在或多或少的攻击.

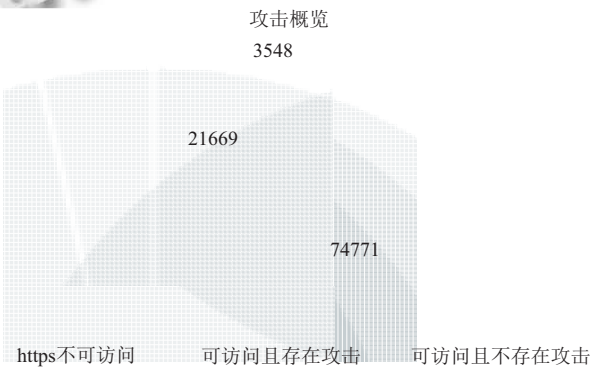

图 5 TLS-Attacker 攻击概览

表 10 显示了 6 种攻击的测试总结, 由表可知:

(1) PaddingOracle 攻击和 Poodle 攻击最为突出, 分别占 85.72%、12.84%;

(2) 仍然有 13 个网站存在 HeartBleed 攻击, 这 13 个网站涵盖购物、交友、保险金融以及视频等领域;

(3) Invalid Curve 攻击实现是针对 ECDH 密码套件, 没有网站存在这类攻击, 说明所测试的网站中都不支持 ECDH 套件.

表 10 TLS-Attacker 攻击结果

攻击名称	攻击成功	百分比(%)
Bleichanbacher	49	0.19
InvalidCurve	0	0
HeartBleed	13	0.05
Poodle	3237	12.84
PaddingOracle	21617	85.72
CVE2016-2107	4	0.015

5 SSL/TLS 协议部署建议

通过对 Alexa 排名前 100 万网站的检测与分析,

© 中国科学院软件研究所 http://www.c-s-a.org.cn

我们发现了 SSL/TLS 协议在 Web 应用中部署实现时, 在基础配置、密码套件支持以及攻击测试方面存在的一些问题, 现在针对以上发现的突出问题, 给出以下解决方案或建议.

5.1 Web 网站中 SSL/TLS 协议基础配置建议

(1) 证书. 首先必须要从可信 CA 处获取有效证书; 然后要确保证书链的完整性, 证书链可从 CA 中心获取; 最后, 至少选择 SHA256 强度的签名算法, 如果目前仍然使用 SHA1 杂凑函数签名, 应该立即进行更新;

(2) 私钥. 如果使用 RSA 证书, 那么必须保证私钥强度至少是 2048bits; 如果使用 ECDSA 证书, 私钥强度至少为 256bits; 另外, 从性能和效率上考虑, 应该优先选择 ECDSA 私钥;

(3) 协议版本. 针对目前 TLS 各版本的安全现状, 只应该支持 TLS1.1 或 TLS1.2; 针对老客户端兼容问题, 应该给客户发送更新通知, 使其更新到兼容版本, 以支持安全的 TLS 版本; 在商用领域, 不应该为了兼容老客户端, 而部署不安全的 SSL/TLS 版本, 从而导致更加严重的安全问题;

(4) 配置扩展. 实现 NIST guidelines[11]中规定的关键扩展, 如 TLS 证书状态查询扩展 (OCSP Stapling)、Trusted CA Indication 以及服务器名称指示扩展 (SNI) 等. 对于 HSTS(HTTP Strict Transport Security, HSTS) 以及 HSTS preloading 这类优秀扩展, 应该尽量实现, 它们对于降低会话劫持风险, 抵御未知的新型攻击具有很好的效果.

5.2 Web 网站中 SSL/TLS 协议密码套件支持建议

(1) 使用更加安全的加密套件. 根据现有的 TLS1.3 草案, 未来 TLS1.3 协议规定只能使用 128bit 或者更强的加密认证套件 AEAD; 因此我们应该禁用 NULL、Export Key Exchange、RC4 以及 3DES 这些不安全的密码套件, 转而使用更加安全的 AEAD 密码套件;

(2) 支持前向安全性. 支持 PFS 能够保证在私钥泄露的情况下, 以前的会话内容也无法破解. 因此, 我们建议使用 DHE 或 ECDHE 密钥协商算法, 并且至少使用 2048bits 的 DHE, 或者 256bits 以上的 ECDHE 算法;

(3) 控制加密套件的选择. 在进行 SSL/TLS 协议握手过程中, 对于客户端发送过来的密码套件列表, 服务器应该选择其中安全性最高的密码套件, 而不应该随机选择或者选择第一个密码套件.

5.3 Web 网站中 SSL/TLS 协议主流攻击防御建议

(1) 关闭 TLS 压缩, 使其免遭 CRIME 攻击;

(2) 不要支持 3DES 密码套件, 使其免遭 Sweet32 攻击;

(3) 关闭 SSL2.0、SSL3.0 和 TLS1.0, 防止 POODLE 攻击;

(4) 使用安全的 CBC 加密模式套件, 防止 Beast、PaddingOracle 攻击;

(5) 对于仍然遭受 HeartBleed 以及 CVE2016-2107 这类由于 TLS 开源组件实现漏洞导致的攻击, 应该尽快更新其开源组件.

6 结语

针对 SSL/TLS 协议在 Web 应用中部署配置方面存在的问题, 本文首先设计并实现了针对 Web 网站的 SSL/TLS 协议配置安全检测系统, 然后基于该检测系统对 Alexa 排名前 100 万网站的从基础配置、密码套件支持以及攻击测试三个方面进行了扫描, 统计并分析了 SSL/TLS 协议部署配置情况, 并发现了一些问题, 如普遍支持不安全的 3DES 密码套件、OCSP Stapling 等关键扩展部署率较低、仍然有不少网站存在 HeartBleed 严重攻击等问题, 针对上述问题本文最后给出了相应的解决方案或建议.

参考文献

1 Dierks T. The Transport Layer Security (TLS) Protocol Version 1.2. IETF, RFC 5246. 2008.

2 Sawers P. Google: HTTPS now represents more than 50% of all pages loaded through Chrome on the desktop. http://venturebeat.com/2016/11/04/google-transparency-report-https/. [2016].

3 Aas J. Mozilla telemetry shows more than 50% of page loads were HTTPS yesterday. First time that has ever happened. https://twitter.com/0xjosh/status/786971412959420424. [2016].

4 Durumeric Z, Kasten J, Adrian D, *et al*. Thematter of heartbleed. Proc. of the 2014 Conference on Internet Measurement Conference. Vancouver, BC, Canada. 2014. 475–488.

5 Zheng XF, Jiang J, Lian JJ, *et al*. Cookies lack integrity: Real-world implications. USENIX Security Symposiu. 2015. 707–721.

6 Ristić I. Qualys SSL labs. https://www.ssllabs.com/index.html.

7 Mozilla. CipherScan. https://github.com/mozilla/cipherscan.

8 Somorovsky J. Systematic fuzzing and testing of TLS libra-

© 中国科学院软件研究所 http://www.c-s-a.org.cn

ries. Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria. 2016. 1492–1504.

9 Hodges J. How's My SSL? https://www.howsmyssl.com/.

10 SA HTB. High-tech bridge free SSL server test. https://www.htbridge.com/ssl/. [2015].

11 Polk T, Mckay K, Chokhani S. Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. NIST Special Publication 800-52. U.S. Department of Commerce, 2014.

12 PCI Security Standards Council. Requirements and security assessment procedures. Wakefield, MA. USA: PCI Security Standards Council, 2016.

13 Centers for Disease Control and Prevention. HIPAA privacy rule and public health. Guidance from CDC and the U.S. Department of Health and Human Services. MMWR Suppl, 2003, 52: 1–17.

14 Ristić I. Ssl and Tls deployment best practices. https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices. [2017].

15 Ristić I. Ssl labs Api documentation. https://www. ssllabs.com/projects/ssllabs-apis/index.html. [2016].

16 Duong T, Rizzo J. The CRIME attack. Presentation at Ekoparty Security Conference. 2012.

17 Bhargavan K, Leurent G. On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN. Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria. 2016. 456–467.

18 Nleichenbacher D. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. Proc. of the 18th Annual International Cryptology Conference on Advances in Cryptology. London, UK. 1998. 1–12.

19 Jager T, Schwenk J, Somorovsky J. Practical invalid curve attacks on TLS-ECDH. 20th European Symposium on Research in Computer Security. Vienna, Austria. 2015. 407–425.

20 Möller B, Duong T, Kotowicz K. This poodle bites: Exploiting the SSL 3.0 fallback. Security Advisory, 2014.

21 Rizzo J, Duong T. Practical padding oracle attacks. Proc. of the 4th USENIX Conference on Offensive Technologies. Washington, DC, USA. 2010. 1–8.

www.c-s-a.org.cn

© 中国科学院软件研究所 http://www.c-s-a.org.cn