总编号：_____

网络安全奖学金申请书

申 请 人 姓 名　　郑晓峰

学　生　类　别　　硕士研究生

推　荐　单　位　　清华大学

院 系 所 名 称　　计算机科学与技术

填表时间　2016　年　08　月　20　日

中国互联网发展基金会网络安全专项基金办公室制

填 表 说 明

1. 本表用钢笔填写或打印，要求字迹清楚、端正，内容翔实、准确。

2. 封面总编号由中国互联网发展基金会网络安全专项基金办公室统一编写。

3. 申请人所填内容，由推荐单位负责审核。

4. 学生类别是指大学生、硕士研究生或博士研究生，只能选填一种。

5. 如表格篇幅不够，可另附纸。

6. 申请书中所填奖项、专利和论文等须提供支撑材料，作为附件与申请书一并提交。

7. 提供的支撑材料应属于网络安全。

申请人基本情况表

学生类别	硕士研究生	姓名	郑晓峰	性别	男	身份证号	
政治面貌		出生年月		民族		学校	清华大学
院系	计算机科学与技术		入学时间	2012.09		学号	
通信地址			Email			电话	

主要学历和专业技术实习经历

起止年月	学习、实习单位	学历、学位、职务
2002.09-2006.07	解放军信息工程大学	本科
2012.09-至今	清华大学	在读硕士

个人自述

（字数不超过 500 字）

本人现就读于清华大学计算机系，攻读硕士学位，研究方向为网络安全。

硕士期间在国际顶级安全学术会议上发表了两篇学术论文：Cookies Lack Integrity: Real-World Implications, USENIX Security’15（第一作者,CCF 信息安全 A 类会议，该会议有史以来来自中国的第二篇论文，附件 1），Forwarding-Loop Attacks in Content Delivery Networks, NDSS’16（第三作者，CCF 信息安全 B 类会议，杰出论文奖，附件 2、3）。

学术研究的同时，注重与工业界的交流。从实际问题中探索研究方向，同时积极促进学术成果向工业成果的转化。先后向 Google、Apple、Mozilla、Amazon、美国银行、中国建设银行、支付宝等国内外知名企业提交漏洞报告，帮助企业修复了用户隐私泄露、恶意支付等诸多安全漏洞，多次获得相关企业的致谢，并获得 Google 公司 Chromium Security Rewards Program 的奖励(附件 4)。工业界也给予了积极的反馈，Google 根据 Cookies Lack Integrity 论文的研究成果，在其 Chromium 项目中启动了对 Cookie 协议进行修订的实际探索（附件 5），并向 IETF 提交了相关标准草案（附件 6）。

学术研究之余，也积极将研究成果带到各类安全竞赛中进行挑战检验，先后获得了首届信息系统安全技术挑战赛三等奖（附件 7）、腾讯 TSRC 2014 通用软件漏洞最高奖（附件 8）、GeekPwn 2015 第一名（附件 9）。

积极参与学术界和工业界的安全研究交流活动，曾在 InForSec、KCon、XCTF 等会议上进行学术研究报告。

网络安全相关专业课程信息

课程名称	必修/选修	成绩	考试时间
计算机网络安全技术	必修	97	2013.06
专业名称		专业人数及排名	

竞赛信息

竞赛名称	国际/国内赛事	承办单位	排名	获奖等级	时间
首届“信息系统安全技术挑战赛”	国内	信息系统安全技术重点实验室		3	2014
GeekPwn 智能设备破解大赛	国际	碁震	1	1	2015

学术论文

论文名称	刊物名称	排名	时间，卷（期），起止页码
SSL/TLS 在 Web 部署中的安全问题及防范	中国密码学会通讯	1	2014
Cookies Lack Integrity: Real-World Implications	USENIX Security 四大安全顶会之一	1	2015
Forwarding-Loop Attacks in Content Delivery Networks	NDSS 四大安全顶会之一	3	2016

标准

标准名称	标准类型(国际、国家或行业标准)	排名	是否发布	时间

参加科研项目情况

项目名称	课题种类	说明	时间
基于互联网基础设施操控的高级持续网络攻击检测与防范	国家自然科学基金面上项目,61472215	参与人	2015-2018
IPv4 与 IPv6 混合部署网络中的测量与安全研究	清华-伯克利国际合作项目,2015010305	参与人	2015-2015
腾讯安卓应用及系统漏洞挖掘	企业合作项目,20140610	参与人	2014-2015
基于自治治理模型的互联网管理和安全研究	国家 973 课题,2009CB320505	参与人	2014

专利

专利名称	专利类型	排名	是否授权	时间

在网络安全行业的成就（参加众测、漏洞贡献、开源项目贡献等）

名称	说明	时间
CVE-2014-8639 CVE-2015-5841 CVE-2015-1229	Chrome、Firefox、Safari 在处理特殊响应时存在 Cookie 注入的漏洞	2014
建行支付漏洞	支付流程存在漏洞，导致资金被转到攻击者账号（GeekPwn 2014 年演示项目）	2014
中国银联银行卡绑定漏洞	银行卡绑定流程存在漏洞，导致用户的银行卡被绑定到攻击者账号（GeekPwn 2014 年演示项目）	2014
美国银行 Cookie 反射漏洞	存在 Cookie 反射漏洞	2014
Gmail 局部替换漏洞	Gmail 存在漏洞，导致攻击者可伪造受害者的联系人列表（GeekPwn 2014 年演示项目）	2014
CVE-2015-5885	Safari 及 CFNetwork 库存在漏洞，攻击者可以向顶级域名写入恶意 Cookie	2015
CVE-2015-5858	Safari 及 CFNetwork 库存在漏洞，攻击者可以绕过 HTTPS 环境下的 HSTS 防护措施	2015
CVE-2015-2206	PHPMyAdmin 存在 HTTPS BREACH 攻击漏洞	2015
Amazon 恶意购物漏洞	Amazon 的购物支付流程存在漏洞，导致攻击者可以劫持用户的购物操作，进行恶意购物、支付	2015
京东支付漏洞	京东的支付流程存在漏洞，导致攻击者可以劫持用户操作实现恶意支付	2015
支付宝 Session 泄露漏洞	支付宝统一认证存在逻辑错误，导致攻击者可以窃取受 HTTPS 保护的 Session	2015

获奖情况

奖励种类	获奖项目名称	获奖等级	排名	时间
腾讯 TSRC	通用软件漏洞奖	专项奖	1	2014
Google	Chromium Security Rewards Program	专项奖		2015
GeekPwn 智能设备破解大赛	SSL/TLS 已知漏洞攻击	第一名	1	2015
	SSL/TLS 已知漏洞增强			
	SSL/TLS 未知漏洞发现			

教师/导师推荐意见

郑晓峰同学对网络和信息安全方向的研究充满浓厚的兴趣,在清华大学学习期间刻苦钻研，取得了国际学术界和工业界公认的优异的成绩，其中包括：

1）国际顶级学术论文：以晓峰同学为第一作者完成了 USENIX Security’ 15 顶级安全学术会议论文“Cookies lack integrity: Real world implications”，这一会议是计算机学会 CCF 认可的 A 类会议(“指国际上极少数的顶级刊物和会议，鼓励我国学者去突破”)，是该会议有史以来来自中国大陆的第二篇文章，是国际公认的最新研究成果。这项研究推动了 Google 公司修改浏览器、促进了 IETF 修改关于 Web 的国际标准，在学术界和工业界都产生了很大的影响力。2）以晓峰同学为主力队员参加了 2014 年总装某部组织的软件漏洞挖掘竞赛，获得三等奖，在参赛的地方院校中名列前茅。3）以晓峰同学的工作为主，在智能设备破解大赛“极棒（GeekPwn）2014”上做了 HTTPS 劫持的展示，在业界引起强烈反响，被人民日报报道（“攻，是为了更好地防”，2014 年 11 月 3 日） 。4）由于发现浏览器的漏洞，获得腾讯安全响应中心十万元大奖。5）提交主流浏览器 Google Chrome 和 FireFox 漏洞被世界所公认，相关机构因此发布安全公告 CVE-2015-1229、Mozilla CVE-2014-8639。由于发现 Google 公司产品的安全漏洞，获得该公司安全奖励计划的奖励。6）以晓峰同学的研究为基础，向 Amazon、Bank of America、中国建设银行、中国银联等国内外大型企业提交了他们应用或服务产品的安全漏洞，帮助他们增强了服务的安全性。7）以晓峰同学的工作为主，在智能设备破解大赛“极棒（GeekPwn）2015”上获得第一名。8）郑晓峰同学乐于分享他在网络安全领域的知识和经验，先后在工业界和学术界多个知名会议上作特邀报告。

鉴于郑晓峰同学在网络安全领域中的突出贡献,我极力推荐郑晓峰同学申请网络安全奖学金。

签　　字：段海新
职称/职务：研究员/实验室主任
研究方向：网络安全
院系盖章：

年　　月　　日

推荐单位意见

签　　字：

单位盖章：

年　　月　　日

中国互联网发展基金会网络安全专项基金专家委员会意见

签　　字： 年　　月　　日
中国互联网发展基金会网络安全专项基金管理委员会意见
签　　字： 年　　月　　日

【附件 1】

USENIX Security'15 论文

https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-zheng-updated.pdf

Cookies Lack Integrity: Real-World Implications

Xiaofeng Zheng[1,2,3], Jian Jiang[7], Jinjin Liang[1,2,3], Haixin Duan[1,3,4], Shuo Chen[5], Tao Wan[6], and Nicholas Weaver[4,7]

[1]Institute for Network Science and Cyberspace, Tsinghua University
[2]Department of Computer Science and Technology, Tsinghua University
[3]Tsinghua National Laboratory for Information Science and Technology
[4]International Computer Science Institute
[5]Microsoft Research Redmond
[6]Huawei Canada
[7]UC Berkeley

Abstract

A cookie can contain a "secure" flag, indicating that it should be only sent over an HTTPS connection. Yet there is no corresponding flag to indicate how a cookie was set: attackers who act as a man-in-the-midddle even temporarily on an HTTP session can inject cookies which will be attached to subsequent HTTPS connections. Similar attacks can also be launched by a web attacker from a related domain. Although an acknowledged threat, it has not yet been studied thoroughly. This paper aims to fill this gap with an in-depth empirical assessment of cookie injection attacks. We find that cookie-related vulnerabilities are present in important sites (such as Google and Bank of America), and can be made worse by the man-in-the-middle (MITM). However, there is no similar measure to protect its integrity from the same adversary: an HTTP response is allowed to set a secure cookie for its domain. An adversary controlling a related domain is also capable to disrupt a cookie's integrity by making use of the shared cookie scope. Even worse, there is an asymmetry between cookie's read and write operations involving pathing, enabling more subtle form of cookie integrity violation.

The lack of cookie integrity is a known problem, noted in the current specification [2]. However, the real-world implications are under-appreciated. Although the problem has been discussed by several previous researchers [4, 5, 30, 32, 24, 23], none provided in-depth

【附件 2】

NDSS'16 论文

https://www.internetsociety.org/sites/default/files/blogs-media/forwarding-loop-attacks-content-delivery-networks.pdf

Forwarding-Loop Attacks in Content Delivery Networks

Jianjun Chen*†‡, Jian Jiang§, Xiaofeng Zheng*†‡, Haixin Duan†‡¶,
Jinjin Liang*†‡, Kang Li‖, Tao Wan**, Vern Paxson§¶,

*Department of Computer Science and Technology, Tsinghua University
†Institute for Network Science and Cyberspace, Tsinghua University
‡Tsinghua National Laboratory for Information Science and Technology
{chenjj13, zhengxf12, liangjj09}@mails.tsinghua.edu.cn, duanhx@tsinghua.edu.cn
§University of California, Berkeley jiangjian@berkeley.edu
¶International Computer Science Institute vern@icir.org
‖Department of Computer Science, University of Georgia kangli@cs.uga.edu
**Huawei Canada tao.wan@huawei.com

***Abstract*—We describe how malicious customers can attack the availability of Content Delivery Networks (CDNs) by creating forwarding loops inside one CDN or across multiple CDNs. Such forwarding loops cause one request to be processed repeatedly or even indefinitely, resulting in undesired resource consumption and potential Denial-of-Service attacks. To evaluate the practicality of such forwarding-loop attacks, we examined 16 popular CDN providers and found all of them are vulnerable to some form of such attacks. While some CDNs appear to be aware of this threat and have adopted specific forwarding-loop detection mechanisms, we discovered that they can all be bypassed with new attack techniques. Although conceptually simple, a comprehensive defense requires collaboration among all CDNs. Given that hurdle, we also discuss other mitigations that individual CDN can implement immediately. At a higher level, our work underscores the hazards that can arise when a networked system provides users with control over forwarding, particularly in a context that lacks a single point of administrative control.**

In this work we present "forwarding-loop" attacks, which allow malicious CDN customers to attack CDN availability by creating looping requests within a single CDN or across multiple CDNs. Forwarding-loop attacks allow attackers to massively consume CDN resources by building up a large number of requests (or responses) circling between CDN nodes. The impact can become more severe in the (common) case where attackers can manipulate DNS records to dynamically control a loop's IP-level routing on a fine-grained basis.

Although many CDN providers have internal mechanisms (such as appending custom HTTP headers like CloudFlare's CF-Connecting-IP [19]) to detect repeated requests when they circle back, we find that an attacker can bypass such defense mechanisms by using features offered by some other CDNs to filter HTTP headers. Our experiments with 16 commercial CDNs show that all of them are vulnerable to forwarding-loop attacks, even with their existing defense

【附件 3】

NDSS'16 杰出论文奖

NDSS '16

SYMPOSIUM

NETWORK & DISTRIBUTED SYSTEM SECURITY SYMPOSIUM

Distinguished Paper Award

Forwarding-Loop Attacks in Content Delivery Networks

Jianjun Chen, Xiaofeng Zheng, Haixin Duan and Jinjin Liang
Tsinghua University and Tsinghua National Laboratory for Information Science and Technology
Jian Jiang *University of California, Berkeley and*
Kang Li *University of Georgia and*
Tao Wan *Huawei Canada and*
Vern Paxson *University of California, Berkeley and International Computer Science Institute*

Presented at the NDSS Symposium, February 22-24, 2016 in San Diego, California
In recognition of outstanding contributions
in the field of network and distributed system security research.

Srdjan Capkun
Program Chair

Lujo Bauer
General Chair

【附件 4】

CVE 及 Chromium Security Rewards Program 奖励

Vulnerability Summary for CVE-2014-8639

Original release date: 01/14/2015

Last revised: 03/17/2015

Source: US-CERT/NIST

Overview

Mozilla Firefox before 35.0, Firefox ESR 31.x before 31.4, Thunderbird before 31.4, and SeaMonkey before 2.32 do not properly interpret Set-Cookie headers within responses that have a 407 (aka Proxy Authentication Required) status code, which allows remote HTTP proxy servers to conduct session fixation attacks by providing a cookie name that corresponds to the session cookie of the origin server.

Vulnerability Summary for CVE-2015-5841

Original release date: 09/18/2015

Last revised: 10/20/2015

Source: US-CERT/NIST

Overview

The CFNetwork Proxies component in Apple iOS before 9 does not properly handle a Set-Cookie header within a response to an HTTP CONNECT request, which allows remote proxy servers to conduct cookie-injection attacks via a crafted response.

Vulnerability Summary for CVE-2015-1229

Original release date: 03/08/2015

Last revised: 03/16/2015

Source: US-CERT/NIST

Overview

net/http/proxy_client_socket.cc in Google Chrome before 41.0.2272.76 does not properly handle a 407 (aka Proxy Authentication Required) HTTP status code accompanied by a Set-Cookie header, which allows remote proxy servers to conduct cookie-injection attacks via a crafted response.

Vulnerability Summary for CVE-2015-5885

Original release date: 09/18/2015

Last revised: 10/16/2015

Source: US-CERT/NIST

Overview

The CFNetwork Cookies component in Apple iOS before 9 allows remote attackers to track users via vectors involving a cookie for a top-level domain.

Vulnerability Summary for CVE-2015-5858

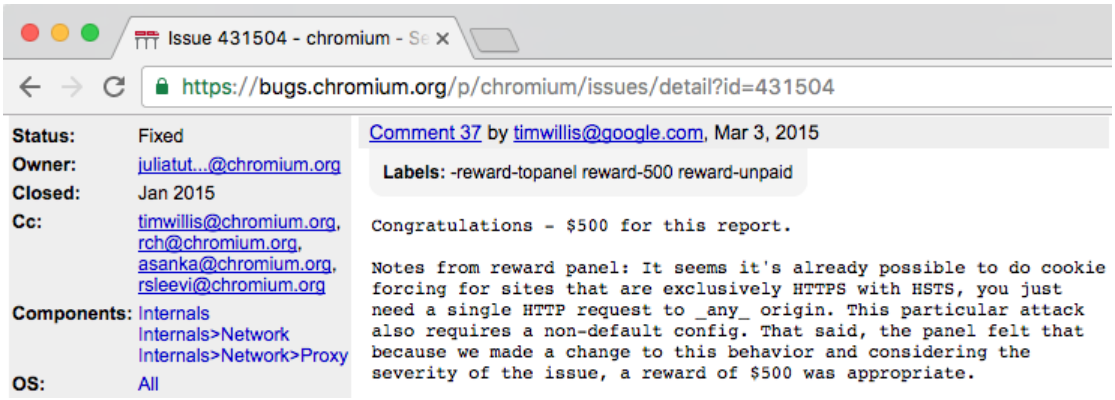
Original release date: 09/18/2015

Last revised: 10/13/2015

Source: US-CERT/NIST

Overview

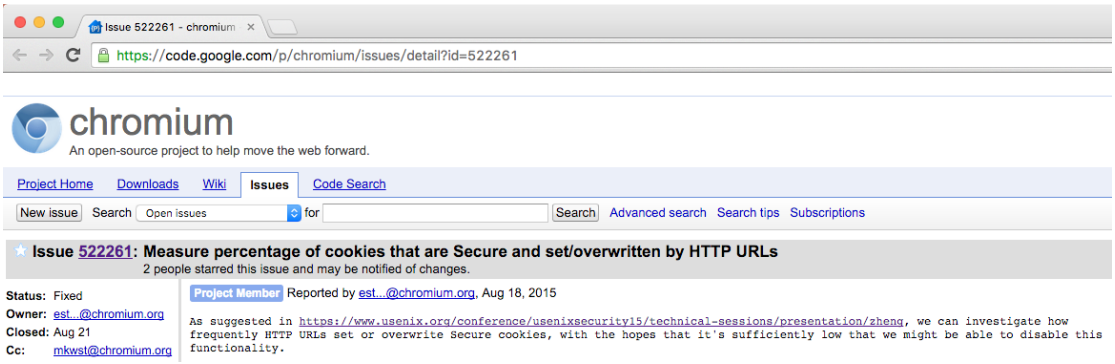
The CFNetwork HTTPProtocol component in Apple iOS before 9 allows remote attackers to bypass the HSTS protection mechanism, and consequently obtain sensitive information, via a crafted URL.



【附件 5】

推进 Chromium 修改

https://bugs.chromium.org/p/chromium/issues/detail?id=522261



【附件 6】

IETF 草案

https://tools.ietf.org/html/draft-west-leave-secure-cookies-alone-05

[Docs] [txt|pdf] [Tracker] [Email] [Diff1] [Diff2] [Nits]

Versions: 00 01 02 03 04 05 draft-ietf-httpbis-cookie-alone

HTTPbis M. West
Internet-Draft Google, Inc
Updates: 6265 (if approved) January 7, 2016
Intended status: Standards Track
Expires: July 10, 2016

Deprecate modification of 'secure' cookies from non-secure origins
draft-west-leave-secure-cookies-alone-05

Abstract

This document updates RFC6265 by removing the ability for a non-secure origin to set cookies with a 'secure' flag, and to overwrite cookies whose 'secure' flag is set. This deprecation improves the isolation between HTTP and HTTPS origins, and reduces the risk of malicious interference.

5.2. Informative References

[COOKIE-INTEGRITY]
Zheng, X., Jiang, J., Liang, J., Duan, H., Chen, S., Wan, T., and N. Weaver, "Cookies Lack Integrity: Real-World Implications", n.d., <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-zheng.pdf>.

【附件 7】

首届“信息系统安全技术挑战赛”获奖证书

【附件 8】

获得腾讯 TSRC 通用漏洞奖

https://security.tencent.com/index.php/user/p/959D8EE0D0D91BCDF300C24B53010C58

【附件 9】

获得 GeekPwn'15 第一名

http://www.tsinghua.edu.cn/publish/newthu/9362/2015/20151129230824258596397/20151129230824258596397_.html