

总编号：\_\_\_\_\_

## 网络安全奖学金申请书

申请人姓名	_____陈建军_____
学生类别	_____博士研究生_____
推荐单位	_____清华大学_____
院系所名称	_____计算机系_____

填表时间 \_\_\_\_\_2016\_\_\_\_\_年\_\_8\_\_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	博士 研究生	姓名	陈建军	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	计算机系		入学时间	2013.9		学号	
通信地址			Email			电话	
<b>主要学历和专业技术实习经历</b>							
起止年月	学习、实习单位					学历、学位、职务	
2015.9-2016.3	美国加州大学伯克利分校					访问学者	
2013.9-2015.7	清华大学					网络安全助研	
2013.9-至今	清华大学					保送直博生	
2009.9-2013.7	武汉大学					本科生	
<b>个人自述</b> (字数不超过 500 字)							
<p>我在清华大学段海新教授指导下研究网络安全，曾在美国加州大学伯克利分校在 Vern Paxson 教授指导下进行访问研究。目前我的成果不仅受到了安全学术界的认可，也对工业界产生很大影响。</p> <p>学术科研方面，在 CDN 安全、入侵检测、HTTP 协议安全方向发表网络安全国际顶级会议三篇 (NDSS, CCS, IEEE S&amp;P)。2016 年 2 月，关于 CDN 转发循环攻击的研究在 NDSS 会议上以第一作者发表，并获得“杰出论文奖”，这是国内首次由大陆研究机构在网络安全顶级会议获得该奖。5 月，关于检测被入侵网站的研究在 IEEE S&amp;P 上发表。8 月，CCS 会议上以第一作者投稿的关于 HTTP 协议攻击的论文已经被录用。</p> <p>工业漏洞方面，发现了国内外厂商 (比如 BAT) 和开源软件 (比如 Squid) 的多个安全漏洞。2015 年 6 月，影响 16 家 CDN 厂商的 DoS 攻击漏洞，收到了 CloudFlare, Verizon, 百度, 腾讯等厂商的致谢和奖励。国际漏洞响应协调中心 (CERT/CC) 为该漏洞发布了安全公告 (VU#938151)，被日本等多国安全响应中心转载并翻译。2016 年，发现了一系列 HTTP 协议攻击。著名开源代理软件 Squid 为该漏洞紧急发布了两条安全公告 (CVE-2016-4553, CVE-2016-4554)，并且将其评为危险级别最高 (Blocker) 的漏洞。该漏洞也收到了来自 Akamai, 阿里巴巴, 腾讯等厂商的致谢与现金奖励。此外，该漏洞还影响 Palo Alto Networks, 华为等防火墙产品，并促使他们调整了产品。目前该漏洞仍在披露之中，更多厂商继续在确认与与修复中。此外，我还积极参与了蜜网安全开源社区 (HoneyNet Project) 和 Squid 的开发与内部安全测试。</p>							

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	98	2014	
高等计算机网络		必修	94	2013	
计算机网络管理		选修	93	2014	
无线网络与移动计算		选修	90	2014	
Web 与信息检索		选修	85	2014	
现代优化算法设计与实践		选修	88	2014	
专业名称		计算机科学与技术	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
Plaid CTF	国际	美国 PPP	7		2014
SIGINT CTF	国际	德国 CCCAC	3		2013
UCSB iCTF	国际	美国 UCSB	6		2013
学术论文					
论文名称		刊物名称	作者排名	时间	
[1] Host of Troubles: Multiple Host Ambiguities in HTTP Implementations		CCS (国际四大顶级安全会议之一, CCF A类)	1/6	2016. 8	
[2] Forwarding-Loop Attacks in Content Delivery Networks		NDSS (国际四大顶级安全会议之一, CCF B类)	1/8	2016. 2	
[3] Seeking Nonsense, Looking for Trouble: Efficient Promotional-Infection Detection through Semantic Inconsistency Search		IEEE S&P (国际四大顶级安全会议之一, CCF A类)	6/12	2016. 5	
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	在研		2015/1-2018/12
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	已结题		2015/1-2015/12
腾讯安卓应用及系统漏洞挖掘	企业合作项目	已结题		2014/6-2015/1
基于自治治理模型的互联网管理和安全研究	国家 973 课题	已结题		2009/1-2014/12
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-2016-4553	被 Squid 团队评为最严重级别(Blocker)漏洞			2016
CVE-2016-4554	从 Squid1.0 开始潜伏 20 年的高危漏洞			2016
VU#938151	影响 16 个主流 CDN 厂商的 DoS 攻击漏洞			2015
IPv6 Attack Detector	项目负责人，由蜜网安全开源组织(Honeynet Project)支持，Google 赞助			2013
获奖情况				
奖励种类	获奖项目名称	获奖等级	排名	时间
杰出论文奖	NDSS 会议杰出论文奖	国际	国内首个安全顶会杰出论文奖	2016

## 教师/导师推荐意见

陈建军同学以其敏锐的思维和辛苦的努力，成为我实验室学术研究成果最多、也是影响最大的同学。在入学以来，陈建军同学在以下几个方面都取得了国际学术界公认的优秀成果：

(1) CDN 循环转发攻击：CDN 作为互联网基础设施的可用性非常重要，陈建军发现了 CDN 设计的安全漏洞可能导致大规模攻击，这一成果发表在四大安全顶级会议之一 NDSS 2016，并获“杰出论文奖”，这是四大安全会议上国内唯一的最佳论文奖。

(2) 发现了互联网应用最广泛的协议 HTTP 的重大安全漏洞 Host of Trouble，可能导致缓存污染、防火墙绕过等攻击，成果发表在国际四大顶级会议之一 CCS 2016。虽然目前这一会议还没有召开，部分研究成果毒鱿鱼 (squison) 攻击的概念已经在网络上广为传播，并协助相关厂商修复了相关的安全漏洞。

(3) 提出了基于语义不一致的检测方法检测被攻破的网站，这一成果发表在四大安全会议之一 Security & Privacy。这项合作研究的创新思想是陈建军同学最先提出的。

(4) 陈建军同学的上述研究成果已经帮助 CDN 厂商、防火墙厂商、以及开源软件组织等修复了相关的漏洞，包括微软、Akamai、百度、腾讯、阿里巴巴、华为、Squid、Apache 等，为互联网基础软件和基础设施的安全做出了重要贡献。

鉴于陈建军同学在网络安全领域所作出的突出贡献，我极力推荐陈建军同学申请“网络安全奖学金”

签字：段海新

职称/职务：研究员/研究室主任

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