清华大学网络科学与网络空间研究院

个　人　陈　述

✧ 我的学术背景和做过的相关研究工作：

在第一学期通过开学选拔进入四川大学网络空间安全学院卓越人才班（以下简称网安卓越班）后，我便开始了自己在网络空间安全方面的研究。在第一学年，获得了国家奖学金和四川大学年度一等奖学金。在平时的课程中，我积极回答老师问题，参与课堂互动。同时在专业课课程项目中均担任组长，锻炼自己的管理能力和团队协作能力，并且均取得了不错的成绩。在项目的汇报过程中，总是担任上台汇报的职责，很好地锻炼了自己的表达能力和上台演讲能力。在前五学习的课程学习中，取得了必修均分 90.72 的成绩，在全年级 172 名同学中排名第 2，网络空间卓越人才班 18 名同学中排名第 1。在前六学习的课程学习中，取得了必修均分 91 的成绩，预计在全年级 172 名同学中排名第 2。

网安卓越班中的大部分同学都是通过 18 年我院的自主招生进入的川大，都是早期就接触过网络安全方面的比赛或者实践的同学。在进入网安卓越班后，我在同学们的耳濡目染下，开始了对网安的早期认识。在同学们的引领下，在大一参加了很多 CTF 比赛，包括湖湘杯等。由于 CTF 比赛的特殊性（考察的知识点相对较广，需要对计算机知识有很多的涉猎），因此我在大一参加比赛的时候，并没有取得特别好的成果。但是在比赛中，仍然学到了很多安全方面的实操能力，对 Web 安全、密码学、逆向和 Pwn 等知识有了初步的认识和实践能力。

在大二下学期，我进入黄诚老师的课题组（https://chenghuang.org/），在黄诚老师的教导下进行挖矿代码检测的相关工作。在研究过程中，我在黄诚老师的指导下，独立收集数据并完成了实验。并且在写作过程中，提高了自己的英语表达水平。这篇论文最终被投递至 IEEE TrustCom 2021 会议，被会议主办方转投至 IEEE CSE 2021 会议，并被接受。

在大三上学期末，我进入李贝贝老师的课题组（https://li-beibei.github.io/），和几位同学一起进行联邦学习的相关研究。我所进行的研究是联邦学习中的拜占庭攻击的防御方法研究。我在阅读了已有的联邦学习中的抗拜占庭方法后提出了自己的方法：通过一种声望机制来对拜占庭攻击者进行发现。在确定思路后，我在李贝贝老师的指导下独立完成了该实验和论文，并且和李贝贝老师反复讨论修改后，将该论文投递至 IEEE ISCC 2021（CCF-C，已接收），近期对该论文的实验进行了进一步扩展，并对论文进行了扩展，准备将该论文投至 IEEE TIFS（CCF-A）。并且辅助合作同学完成了一篇联邦学习的非独立同分布问题解决方法的相关论文，现投至 IEEE GlobeCom 2021（CCF-C，已接收）。

✧ 研究计划

大四：在保研结束后，进入导师实验室，熟悉实验室的基本工作，以备好在正式进入硕士学习阶段后能够更快地参加导师课题组的日常工作。同时开始自主学习导师的方向的知识，为后面的硕士学习打好基础。并且广泛地阅读导师研究方向的相关文献，开始构思硕士期间文章的思路。

硕士一年级：硕士上学期巩固理论基础，认真学习研究方向相关的课程；巩固研究基础，根据自身研究方向针对性地研读国内外文献，培养自己的逻辑与独立思考的能力，增加对自己研究方向的了解程度。硕士下学期就开始在老师的指导下进行实验，为硕士二年级发文章打好基础。

硕士二年级：将工作重点放在对科研工作上，在完成并发表 1-2 篇高水平论文。如果有机会，希望能够后在硕士学业结束后继续深造，通过硕博连读的方式继续攻读博士学位。