我是北京邮电大学网络技术研究院研二的学生，靳国栋。我的本科同样也就读于北京邮电大学上，读的是计算机科学与技术专业，大四以优异的成绩保研到了网络技术研究院的计算机科学与技术专业。

研一上学期，由于实验室不要求进入实验室，所以有机会进入百度地图事业部去做手机Webview的开发，在实习期间，主要负责百度地图手机应用的百度身边功能的页面的开发，分别开发了百度地图手机版和百度地图Ipad版，其中Ipad版由我一人负责有1.0到2.0的大改版，用了将近1个月的时间，手机版主要是在现有的版本上添加新功能，需要和产品经理，后台数据工程师还有UE相互沟通，最终也是成功上线，主要做的功能有KTV预定，百度印象，评论二级页等功能；

在研究生期间主要进行IMS网络安全方面的研究，IMS网络是电信网3G、4G的核心网络，IMS网络的安全显得尤其重要，我所做的工作就是从攻击者的角度来测试IMS网络的安全性。IMS项目组有11个成员，我担任组长，项目期间共同开发了IMS网络测试仪，语言用的是Ruby，界面用的是QT-Ruby，界面用的是QT-Ruby推荐的框架，后台用的是metasploit渗透性测试框架，我负责测试仪的主控模块、IP伪装模块、松散路由模块，在开发过程中负责组员任务分配、方案决策以及协调组员间的合作。现在，IMS网络测试仪功能基本齐备，明年项目将会结题，由于我即将毕业，IMS网络测试仪主要任务大部分移交给下一届了。

现在我的毕设工作是基于C语言的危险函数研究SIP协议栈的不稳定性，该项研究是基于一种假设，假设软件的不稳定性大部分是由C语言危险函数的直接或者间接的不正确调用造成的。通过阅读多篇相关论文，以及现有的软件安全现状，发现这种假设是合理的。通过为C语言危险函数和其对应的畸形值，构建C语言危险函数库；为SIP协议栈在源代码级别上建立源代码模型；再根据SIP协议规范和SIP协议栈的实现，找出SIP协议栈中对应SIP协议规范中SIP头字段的顶层函数；在SIP协议栈中遍历调用C语言危险函数的函数，然后反向溯源找到与SIP头字段对应的顶层函数；顶层函数对应SIP协议规范的某个SIP头字段，然后对该SIP头字段注入相应的畸形值，产生畸形测试报文，然后测试该报文是否会触发到SIP协议栈的危险函数。这样就可以得到一组含有畸形值得SIP报文，由于SIP协议规定SIP头字段是被独立处理的，所以，为了减小畸形SIP报文的数量，需要一个畸形SIP报文携带多个畸形值，以减少被目标网络发现的概率。