项目的话，我现在做的项目是IMS网络安全相关的项目。IMS网络是基于IP的多媒体子系统，它到来的目的是为了替代软交换或者和软交换互补互利，现在中国已经有地方部署了IMS网络了，比如广东。由于IMS网络是基于IP的网络，所以网络的安全性有待评估。又因为IMS网络使用SIP协议作为网络的会话控制协议，且SIP协议和HTTP协议类似是应用层的协议、易于扩展使之成为了现代实时通信协议中的重要协议，但是SIP协议本身存在的漏洞，导致IMS网络的安全性不可保证。我在大四的时候开始做IMS网络安全相关的项目，当时负责与IMS网络关联的一个实体HSS，用户归属服务器，存放用户和IMS网络中其他服务器的信息。当时负责研究IMS网络的SQL注入的相关问题，遇到的最大的问题是从UE到HSS要经过IMS网络的P-CSCF、I-CSCF并且经过SIP协议到Demetiar协议的转换才能将用户的注册消息发送到HSS服务器上，如何在UE中的注册消息中修改某些信息，以达到SQL注入的效果，这是我的贡献，最后经过协议分析，抓包，验证，最终确定了一些SIP字段最终会被HSS服务器处理；消息到了HSS服务器只是第一步，如何进行HSS服务器的SQL注入，这是我的贡献，首先查看HSS处理数据库的源代码，找出数据库处理中的问题，最后的结论是没有问题，HSS数据库使用了Hebernate持久性工具来操作数据库，Hibernate使用了非法字符过滤、SQL语句预处理（关闭），单条语句执行预处理，返回值类型检测、预处理参数检测5条检测方法，发现可以使用非法字符，但是使用非法字符后发现非法字符被过滤了，'变为\'，原来MYSQL数据库配置成过滤SQL语句中的数据,导致SQL语句错误例如：select \* from table where id = 1 and 'a' = 'a'; 通过Hibernate后变为，select \* from table where id = 1 and \'a\' = \'a\'；但是通过MYSQL后变为select \* from table where id = 1 and \\\'a\\\' = \\\'a\\\',SQL语句报错，这是想到改变MYSQL的配置，关闭非法字符过滤，注入成功。

上了研究生之后，在百度地图做过一些手机WebView方面的工作；回到实验室后，当上了IMS项目组组长，想过负责了IMS网络测试仪的IP伪装功能、松散路由远程信令传送功能和系统的主控模块。问题：主控模块的多进程同步问题，有时候会因为某个进程出现问题后导致系统被挂起。多进程调试，是其中比较困难的一步；之后开始研究SIP协议栈的安全性问题，从SIP协议和开源的SIP协议栈以及C语言危险库函数入手；首先从SIP协议栈的源码中找到危险库函数的位置，然后对SIP协议栈的源代码进行建模，反向溯源找到与SIP协议相关的顶层函数，危险库函数对应相应的触发值，这样我就得到了SIP消息的某个头字段对应SIP协议栈的某个危险库函数了；根据SIP协议对SIP协议进行拆分，对SIP协议栈中的每个独立的字符串建立模板，这样将与危险库函数对应的SIP头字段的部分替换为触发值，其他的设置为正常值，进行测试，这样就能够在源代码级别测试出SIP协议栈的一部分漏洞，在实验的过程中确实找到了一些漏洞，比如malloc函数，对于一个畸形的SIP消息，其某个头字段的长度超过了1W，而服务器依然正常处理这个字符，造成资源浪费。

我是北京邮电大学网络技术研究院研二的学生，靳国栋。我的本科也是在北京邮电大学上的，读的是计算机科学与技术专业，大四以优异的成绩保研到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，所以有机会去百度地图事业部去做手机Webview的开发，在实习期间，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，明天项目将会结题，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。