大作业（助教邮箱：netsec19@163.com）

1. 校内访问http://www.engineeringvillage2.org/，并结合scholar.google以及相关知名国际会议主页（也可以直接访问各电子期刊数据库等）查询本课程相关领域最新的研究内容和研究点，并以某个方向为题撰写原创性小论文一篇。（不少于6页，正文字体为5号字体，单倍行距，英文参考文献如果是会议论文请主要参照**2016**之后的，而如果是期刊论文则主要参考2017年之后的，直接相关的参考文献不少于**8**篇。论文不要拘泥于翻译多篇文献，要从整体上进行把握，反映一个方向）。论文方向可选择PKI体系、IP安全、Key Agreement、传输层安全、DNS安全、Wireless Security、Email Security、Web security、Trust、 block chain、机器学习在网络安全领域的应用等等，不限于此，但必须是与网络安全和网络安全协议相关的内容（强调是网络安全，而不是泛信息安全）。提交报告请在文末列出详细的参考文献[注1]，同时在文中的引用处进行标注。材料必须是在自己读懂的基础上进行总结的，而不是直接翻译，同时**不要将报告变成科普，需要有深度具有学术性**。如果疑是抄袭，一经确实做0分处理。（该选题需要由2-3人组成，过程中及时跟任课老师、助教进行讨论和沟通，尽量避免选题重复）推荐！

2. 论文翻译，从列表中选择1篇。（1-2人成组，理解的基础上翻译；IEEE双栏排版模式低于7页的只能1人成组。），可以自行组织和整理，但要求翻译稿可读性好，部分相关基础在论文中不够清楚的，需要调研其他文献。最终成稿内容不少于6页（正文字体为5号字体，单倍行距）。

3. 相关IETF 工作组调研（主要调研2016之后的RFC和工作组草案，工作组草案是以draft-ietf开头的），理解思路和基本原理，可以由多个草案综合而成，最终成稿内容不少于6页（正文字体为5号字体，单倍行距，该选题1-2人成组，每个选题不得超过2组），可选择的IETF工作组为：

（1）TCP Increased Security (tcpinc) https://datatracker.ietf.org/wg/tcpinc/documents/

（2）IP Security Maintenance and Extensions (ipsecme)

https://datatracker.ietf.org/wg/ipsecme/documents/

（3）Transport Layer Security (tls) https://datatracker.ietf.org/wg/tls/documents/

4. 热点调研类选题：举例如，Block Chain的原理以及相关改进和拓展工作（不能只有原理，改进和拓展的调研需要有一定深度）、TLS的改进机制以及可能的漏洞分析、机器学习在网络安全领域的开创性应用。（1-2人成组）

5. IPSec VPN类实验：查找资料进行StrongsWan、Openswan相关实验，提交演示系统的描述、拓扑布置、参数设置流程、实验测试，**抓包分析流程**，期望对课程相关内容有深层次的理解。（2人成组，该选题不超过3组，先到新得），推荐！

6. 其他VPN 技术及实验（例如PPTP、SSLVPN、OPENVPN等，包含各个网络层次VPN 的实现技术小结，具体实验实现，平台描述、软件选型、具体配置、使用实例）。给予演示过程截图，提交的安装和测试文档，**抓包分析流程**。（2人成组，该选题不超过3组，先到新得），推荐！

7. OpenCA系统的安装和维护（具体实验实现：平台描述、软件选型、具体配置、使用实例，在数据库的使用如果存在问题，请简单修改代码。http://www.openca.org/）。最后需要提供基于虚拟机的演示系统流程截图和安装和测试文档。（2-3人成组，该选题不超过3组，先到新得），（另外也可以基于EJBCA搭建PKI系统）推荐！

8. 基于FreeRadius服务器的无线用户接入认证和流量控制（包括FreeRADIUS服务器的安装和配置，无线AP的安装和配置）。给出**演示系统的流程截图**，安装和测试文档。（2人成组，该选题不超过3组，先到新得），推荐！

9、防火墙软件Iptables的使用，至少包括功能测试以及抓包分析（NAT处理）、应用层过滤模块安装（如L7filter模块）。给出演示的流程截图，配置和测试文档。（2人成组，该选题不超过3组，先到新得），推荐！

10、其他选题：其他由助教认可的网络安全类实验（需要跟本课程教学内容相关，且涉及相关前沿技术，统一由田航宇同学负责），推荐！

注意事项：

1、文档中所有字体均为5号字体，单倍行距，标题可以为黑体加粗。**请认真完成大作业，抄袭直接以0分计，零容忍。评定按照提交材料和讲述所反应的工作量、创新性和主动性等进行综合评定。**

2、自由组合分组，分组为1-3人组成，组的组成以及选题请提前发送给助教。（hnythyq@mail.ustc.edu.cn），在选题确认之后再进行具体工作（**5月5日**前完成确认工作，可以提前完成）。对于扎堆的题目可能会进行适当的分流（采取先到先得的原则）。**6月1日**前将最终报告通过email 发送给助教，同时准备8分钟的PPT，同组中每个同学都需要做好准备，最终会抽取一定数量的组和个人，介绍工作结果（初定6月3日和6月6日）。**完成时间较为紧张，请控制好时间。**

3、部分实验内容需要大家对于Linux系统有一定程度的熟悉，遇到问题查询Google，baidu。

4、文档和PPT使用Latex编辑，且排版整洁者，有额外加分。

5、综述类选题要求70%以上文献为权威文献，即来源为CCF推荐的网络安全权威期刊和会议。

http://www.ccf.org.cn/xspj/wlyxxaq/

6、参考文献表示格式

[1] Author. Title. Technical Report, Report No., Publishing place : Publisher, Year .

Wei Li, Kaiping Xue, Yingjie Xue, Jianan Hong, TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage, IEEE Transactions on Parallel Distributed Systems, 27(5): 1484-1496, 2016

Dan Ni, Kaiping Xue, Peilin Hong, OCPS: Offset Compensation based Packet Scheduling Mechanism for Multipath TCP, IEEE International Conference on Communications(ICC2015), London UK, Jun. 2015

7、实验过程涉及到 TCPDUMP/Wireshark 等抓包工具的使用，自行从网上获取帮助文档。