考核课有两次：选课人数为 111 人，每组 6-7 人，共 18 组。每次课 9 篇文章，每篇 10 分钟讲解时间，3 分钟提问。每次考核课有效时间为 117 分钟。

每组每人均需提交 pdf 版本阅读报告，报告以**小组组号+选课名单编号+姓名**命名发送给助教。报告内容为 2 页 A4，主要讲：文章的优缺点分析；对体系结构安全发展的启示；存在的不足。勿超页、勿翻译、要有自己的见解。纸质阅读报告尽快提交，最晚于汇报后两周内提交。

最终成绩：课堂汇报*0.4 + 阅读报告*0.4 + 平时成绩*0.2。

助教邮箱：yangzhengbang@iie.ac.cn

1. 先自由进行分组，将名单统一告知助教；
2. 组队后再选择哪篇文章（注意：人数不够时先自己找队员），告知助教，以免冲突。

# 第一次课（5 月 24 日）为宋威老师提问：

1、CFI
Finding Cracks in Shields: On the Security of Control Flow Integrity Mechanisms
CCS 2020
https://dl.acm.org/doi/10.1145/3372297.3417867

2. Break user ASLR
ASLR on the Line: Practical Cache Attacks on the MMU
https://www.cs.vu.nl/~herbertb/download/papers/anc_ndss17.pdf

3. Finding Eviction Sets
Theory and Practice of Finding Eviction Sets
https://vwzq.net/papers/evictionsets18.pdf

4． TLB-based Attacks
TLB;DR: Enhancing TLB-based Attacks with TLB Desynchronized Reverse Engineering
https://www.usenix.org/system/files/sec22fall_tatar.pdf

5. Prime+Scope
Prime+Scope: Overcoming the Observer Effect for High-Precision Cache Contention Attacks
https://dl.acm.org/doi/10.1145/3460120.3484816

6. Conflict-Based Cache
MIRAGE: Mitigating Conflict-Based Cache Attacks with a Practical Fully-Associative Design
https://www.usenix.org/system/files/sec21fall-saileshwar.pdf

7． Contention-Based Cache
Cyclone: Detecting Contention-Based Cache Information Leaks Through Cyclic Interference
https://spark.ece.utexas.edu/pubs/MICRO-19-cyclone.pdf

8. Attack Intel Xeon non-inclusive LLC
Attack directories, not caches: Side-channel attacks in a non-inclusive world
http://iacoma.cs.uiuc.edu/iacoma-papers/ssp19.pdf

9. Random Cache
New attacks and defense for encrypted-address cache
http://memlab.ece.gatech.edu/papers/ISCA_2019_1.pdf

# 第二次课（5 月 31 日）为朱子元老师提问：

10. 代码复用攻击 COOP
Counterfeit Object-oriented Programming On the Difficulty of Preventing Code Reuse Attacks in C++ Applications
S&P 2015
https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2015/03/28/COOP-Oakland15.pdf

11. 代码指针完整性
Code-Pointer Integrity
OSDI 2014
https://www.usenix.org/system/files/conference/osdi14/osdi14-paper-kuznetsov.pdf

12. DOP 攻击
Data-Oriented Programming: On the Expressiveness of Non-Control Data Attacks
S&P 2016
https://www.cc.gatech.edu/~hhu86/papers/dop.pdf

13. Spectre:
Spectre Attacks: Exploiting Speculative Execution
https://spectreattack.com/spectre.pdf

14. Meltdown:
Meltdown: Reading Kernel Memory from User Space
https://meltdownattack.com/meltdown.pdf

15. Tagged Memory
Protecting the Stack with Metadata Policies and Tagged Hardware
http://ic.ese.upenn.edu/pdf/stack_ieeesp2018.pdf

16. Moving target
Morpheus: A Vulnerability-Tolerant Secure Architecture Based on Ensembles of Moving Target Defenses with Churn
https://dl.acm.org/doi/10.1145/3297858.3304037

17. A2
A2: Analog Malicious Hardware
https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf

18. Port contention
Port contention for fun and profit
https://eprint.iacr.org/2018/1060.pdf