

数据安全与隐私保护

about class

- Access control (AC)
 - Operating system AC, mandatory AC, discretionary AC, role based AC, attribute-based AC, non-interferences, integrity protection, firewall policy languages, AC in databases, AC in mobile systems, AC in web
- Using crypto for data protection
 - Implementing crypto correctly, Authentication protocols, Homomorphic encryption, Secure Multiparty Computation
 - Using SGX and hardware security architectures
- Data privacy
 - Privacy policies, data anonymization (k-anonymity, t-closeness, l-diversity), differential privacy: concepts and algorithms, differential privacy in local setting

Workload

- Free credit - 10%
- Assignments
 - 1 literature review on HE/SMC/DP (3 pages - 30%)
 - Late policy: Five extension days to be used at your discretion
 - Must be stated explicitly in header of work being turned in
 - No fractional days
- Technical Presentation
 - Any paper on data security from big 4 security conference.
 - 中文翻译 (10%) + 15 mins presentation (50%)
 - 2 students per group

- Free credit
- Assignments
 - literature review on 同态加密/差分隐私/安全多方计算 [\(二\) 联邦学习的安](#)
[全机制 - 肖肖凯 - 博客园 \(cnblogs.com\)](#)
 - 三页, 英文
- Technical Presentation
 - 任何关于数据安全在四大安全顶会 (CCS, S&P, NDSS, USENIX) 上的 paper 就可以
 - 英文写, 中文讲

- 中文翻译10%+15min presentation 50%
- 2个同学一组

Week 1

- 数据安全形势越来越重要
- Security Goal
 - Confidentiality
 - Integrity
 - Availability