信息安全期刊和会议介绍

汪　定

南开大学 网络空间安全学院

2021年11月6日

目的

- **信息安全是一个日新月异的领域。**
- **信息安全是一个比较复杂的主题**，包括了传统的密码学、安全攻击等内容，同时又包括了大量和操作系统、网络、计算机体系结构、硬件、甚至金融、法律相关的内容，因此，在这些领域，同样有很多顶级学术会议值得我们关注。
- 众所周知，发表刊物的档次无法代表论文的质量，**只是在一流刊物中出现一流成果的可能性要大一些**。很多有开创性的一流成果没有发表在一流刊物 上，在一流刊物中也不并少见长像好看、但实际没什么意义的文章。无论如何，了解会议、期刊的大致水平和特点，对初学者还是很有用的。
- **计算机领域，比较重视会议**： 会议>？期刊
- **信息安全领域，非常重视会议**：会议>期刊

信息来源

- http://wangdingg.weebly.com/miscellanea.html
- http://loccs.sjtu.edu.cn/typecho/index.php/category/conf/
- http://jianying.space/conference-ranking.html
- http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm
- https://www.quora.com/What-are-the-top-computer-security-conferences
- https://wenku.baidu.com/view/7c02e66248d7c1c708a1456f.html
- https://www.ccf.org.cn/xspj/gyml/

三大A级期刊

- Journal of Cryptology
  - 影响因子： 0.437
  - 研究方向：密码学
  - 密码学顶级期刊，2018发表论文数量为32篇，2019为40篇，多收录顶级会议的某些论文的扩展版，平均命中率< 10%，很难命中
- IEEE Transactions on Dependable and Secure Computing
  - 影响因子： 6.404
  - 研究方向：安全、可靠计算等
  - 2018发表论文数量为51篇。
- IEEE Transactions on Information Forensics and Security
  - 影响因子： 6.211
  - 研究方向：网络安全、密码学、数字取证
  - 2018发表论文数量为223篇，投稿平均命中率为 20%。
  - 经验：投稿录用周期4-12个月，平均6-9个月。

B级期刊

- TOPS（ACM Transactions on Security and Privacy）
  - 影响因子: 2.591
  - 研究方向：安全和隐私
  - 2018发表论文数量为19篇。
- Computers & Security
  - 影响因子： 2.650
  - 2018发表论文数量为146篇
- International Journal of Information Security
  - 影响因子： 1.658
  - 2018发表论文数量为37篇
- IET Information Security
- IEEE Security & Privacy
- International Journal of Information Security

Big four：安全四大顶级会议

- 安全界有四大著名顶级会议，简称：S&P, CCS, Security, NDSS
  - S&P (Oakland): IEEE Symposium on Security and Privacy
  - CCS: ACM Conference on Computer and Communications Security
  - NDSS: Network and Distributed System Security Symposium
  - USENIX Security: Usenix Security Symposium （System-oriented）
  - 录用率基本都在15%左右。
- 这四个会议难分伯仲，就像非要说四个考99分，98分，98分，96分的两个学生谁更优秀一样。

注：过去41年里，中国大陆以第一作者单位发表的总数为114。

三大密码学顶级会议

- 美密会Crypto　　International Cryptology Conference
- 欧密会Eurocrypto　　European Cryptology Conference
- 亚密会Asiacrypt　　International Conference on the Theory and Application of Cryptology and Information Security

- 录用率基本都在20%左右。
- Eurocrypto和Crypto难分伯仲。Asiacrypt水平也很高，但跟前两者还有一定差距。
- 王小云院士破解MD5的论文就首发在2004年的美密会上。

注：过去39年里，中国大陆以第一作者单位发表的总数为105。

主要B级会议（7个）

- 四个安全会
  - ESORICS European Symposium on Research in Computer Security
  - ACSAC Annual Computer Security Applications Conference
  - CHES IACRWorkshop on Cryptographic Hardware and Embedded Systems
  - DSN IFIP/IEEE International Conference on Dependable Systems and Networks
  - 这4个会议目前每年的出席人数基本都稳定在200人以上，投稿量也比较大(200+)，说明大家都比较认可，有较强影响力，而且录用率也控制得很好：历年基本都在20%左右。其中ESORICS永远在欧洲开，2017年投稿数达到330篇，创历史新高。
- 如果说上面这四个会偏向安全应用的话，下面这三个会则专注安全理论，里面文章的基础性、长期影响力来看比上面四个会甚至还要好一些：
  - CSF IEEE Computer Security Foundations Symposium
  - TCC IACR Theory of Cryptography Conference
  - PKC IACR International Conference on Practice and Theory of Public-Key Cryptography 。

一个整体排名

Conference	CIF (2018)	AR (2009-2018)	PR (2009-2018)	CR (2018)
1. IEEE S&P	3.89	**12.5%** = 44.6 / 356	**9.3%** = 44.6 / 478.8	**3.9%** (129)
2. Usenix Sec	3.15	**16.7%** = 56.9 / 341	**10.3%** = 56.9 / 555	**4.7%** (106)
3. ACM CCS	2.62	**17.8%** = 102.2 / 573.8	16.4% = 102.2 / 625	**3.9%** (128)
4. Eurocrypt	2.49	22.2% = 47.2 / 212.6	**12.5%** = 47.2 / 376.1	**5.5%** (91)
5. NDSS	2.41	**17.3%** = 47 / 272.3	19.3% = 47 / 243.1	**4.9%** (103)
6. CHES	2.37	24.7% = 32.7 / 132.4	**8.4%** = 32.7 / 388.4	9.1% (55)
7. Crypto	2.34	23.1% = 58.3 / 252.7	**13.7%** = 58.3 / 425.3	6.0% (84)
8. ACSAC	2.00	**19.8%** = 45 / 227.4	19.0% = 45 / 236.3	11.1% (45)
9. Asiacrypt	1.90	21.1% = 53 / 251.5	21.8% = 53 / 243.3	9.8% (51)
10. PETS	1.87	21.5% = 25.1 / 116.5	17.3% = 25.1 / 144.8	14.7% (34)
11. FC	1.74	26.8% = 30 / 111.9	23.9% = 30 / 125.4	6.8% (74)
12. RAID	1.68	25.2% = 22.5 / 89.4	19.5% = 22.5 / 115.4	14.7% (34)
13. IEEE/IFIP DSN	1.67	23.4% = 55.1 / 235.9	25.2% = 55.1 / 218.6	11.4% (44)
14. FSE	1.58	31.7% = 30.8 / 97.2	20.6% = 30.8 / 149.2	10.9% (46)
15. ESORICS	1.543	20.0% = 50 / 249.9	34.2% = 50 / 146.3	10.6% (47)
16. PKC	1.54	24.9% = 34.7 / 139.6	30.5% = 34.7 / 113.6	9.6% (52)
17. ACNS	1.435	20.2% = 33.4 / 165.1	35.2% = 33.4 / 95	14.3% (35)
18. ACM AsiaCCS	1.43	23.4% = 57.4 / 244.8	36.8% = 57.4 / 156	9.6% (52)
19. CT-RSA	1.372	29.4% = 25.9 / 88	28.3% = 25.9 / 91.5	15.2% (33)
20. ACM WiSec	1.37	28.2% = 23.7 / 83.9	30.2% = 23.7 / 78.5	14.7% (34)
21. IEEE CSF	1.33	30.2% = 26.2 / 86.7	27.9% = 26.2 / 94	17.2% (29)
22. TCC	1.31	34.2% = 41.3 / 120.7	34.2% = 41.3 / 120.9	7.9% (63)

- http://jianying.space/conference-ranking.html

同学们加油

- 本科生也大有可为

Walls Have Ears! Opportunistically Communicating Secret Messages Over the Wiretap Channel: from Theory to Practice

Qian Wang, Kui Ren, Guancheng Li, Chengbo Xia, Zhibo Wang, and Qin Zou

CCS 2015

上周，武汉大学“十大珞珈风云学子”揭晓，一位被学子称为“冠神”的本科生，因破解40年未解学术难题，被万余名武大(微博)学子评为“十大珞珈风云学子”。

“冠神”名叫李冠成，是武大计算机学院弘毅班12级本科生，大三时，他加入武汉大学网络信息安全与隐私实验室，跟着国家“青年千人计划”引进人才王骞教授做学问。

大三时，李冠成在信息安全领域顶级会议——第22届ACM计算机与通信安全国际会议上发表论文《隔墙有耳！无线窃听信道中的秘密消息传输：从理论到实践》，去年7月曾被邀请赴美做大会报告，此前只有包括图灵奖得主在内的7位中国大陆学者撰写的论文，被该大会接受。

这篇论文在评审阶段被评委们高度赞誉，被认为“破解了困扰学术界40年的难题”。

“窃听信道”下的安全信息传输可行理论提出40年来，还没有人能在实践上证明。直到2015年，李冠成和同学在王骞教授指导下，设计并实现了基于窃听信道的一个安全、高效、

编辑：白杨

欢迎各位同学交流指正！