

2019年哪些安全大会的议题值得学习？

原创

riusksk 于 2019-05-11 16:37:03 发布 580 收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/riusksk/article/details/96241748>

版权

“2019年哪些安全大会值得参加？”或者这更符合多数人心中的标题，但为何不这么写呢？

因为有些拥有好议题的大会一般都会公开PPT，尤其是国外会议，来回参会成本比较高，如果有现成的PPT供学习，自然不用每次都参加。当然，也有因作者拒绝公开的议题，这种只能现场听了。

评价安全大会的好坏，是多方面的，绝不是单纯的议题质量这一维度。但这里我主要想从技术者的角度来看评价，所以后面你发现很多知名大会未在此列，请不要惊讶。

即使是同一举办方，也无法保证每年的议题质量呈上升状态，有些会议也开始没落了，所以这里以2019年为时间点来点评。

下面来聊聊2019年哪些安全大会的议题值得学习，有些已经举办过，有些尚未开始。

推荐的安全会议

1、BlackHat



官网：<https://www.blackhat.com>

如果你不知道BlackHat，说明你不在安全圈混。

USA是主会场，议题质量和数量也是最高的，议题类型覆盖面也很广，除此之外还有欧洲和亚洲等分会场，质量相对次一些。

这次BlackHat USA的议题也陆续公开了：<https://www.blackhat.com/us-19/briefings/schedule/index.html>

早几年的议题水平参差不齐，很水的也有，打广告也有。最近几年反而议题质量提高，不少华人面孔出现，为了PR效果而竞争，促进大家都拿出干货来分享，这也是其有利的一面。

每年都有几千个议题投稿，竞争很大，但这很好地促进议题质量的提高。

每年会后，官方都会放出PPT与视频，非常开放地分享知识。

所以，首推BlackHat，自然无疑。

但如果你以为接下我会写Defcon，那我会告诉你：No!

2、OffensiveCon



官网：<https://www.offensivecon.org/>

我之前还专门写了篇文章《今年的OffensiveCon大会议题质量不错》介绍2019年大会中一些不错的议题。

虽然OffensiveCon是从2018年才开始举办的，但议题质量一直保持不错，演讲者中包括Project Zero、Google syzkaller作者、Pwn2Own与Hack2Win获奖者等等。

会后，一般是由演讲者选择是否公开ppt，多数人是在Twitter上公开的，官网上我没找到资源（<https://github.com/riusksk/SecConArchive/tree/master/OffensiveCon2019>），所以之前收集的ppt都是从twitter上扒下来的。

3、HITB (Hack In The Box)



官网：<https://conference.hitb.org/>

这几天HITB刚在荷兰阿姆斯特丹举办完，议题PPT也一并公开（<https://conference.hitb.org/hitbsecconf2019ams/materials/>）。

如果要说国内外安全会议中，哪个公开PPT最快的，一定是HITB，他们一般是现场演讲完，就直接扔官网下载。然后过一段时间，也同样发布演讲视频。

他们有时会同时搞两个演讲会场，一个是收费的主会场，议题质量高一些，一个是免费的，叫CommSec，用来提携新人，议题质量相对比较次，每个议题分享时间也比较短，最多半小时。

之前去新加坡参加过一次HITB，人数不多，场地也不大，但可以感受到与国内安全会议的区别：更注重技术交流，而非搞关系。

2018年开始，HITB也开始与京东合作，在北京举办分会场，没去过，不作评价，但国际会议本土化，总会产生一些差异的。

4、InfiltrateCon



官网：<https://infiltratecon.com>

从2011年开始举办的，已经走过8个年头。

看了今年的议题，还是有干货的，但只有4个议题ppt在twitter上公开。

以前，会后都会在官网上公开PPT和视频，但目前官方还没公开。

今年的议题涉及Chrome RCE、iOS与Android提权、Pwn TEE、浏览器JS Fuzzing等等，只能坐等官方公开PPT了。

5、Chaos Communication Congress(C3)



官网：<https://www.ccc.de/>

德国混淆黑客大会，常叫C3会议，常在C3前面加上第几届，比如今年第35届，所以叫35C3，历史非常悠久。

以前大多是聚焦在无线电安全，所以一些什么2G\3G\4G短信、电话窃听经常出自该会议。熟悉无线电安全的同学，应该都听过。2018年也有一些不错的软件安全相关的议题，这些在之前写的文章《推荐今年C3黑客大会上的几个议题》介绍过了。

除了大会议题，不得不提下他们的CTF，非常具有实战价值，比如2018年的题目，直接拿pwn2own漏洞当比赛，从safari代码执行到提权，还有VisualBox沙盒逃逸题目，需要利用到0Dday，出题者是ProjectZero的人，早就将其卖给ZDI，刷了不少VBox漏洞。这些CTF题目在网上都有相应的WriteUp可供学习。

这些议题只有演讲视频公开，没有PPT，官方会放在<https://media/ccc.de>，可在线或下载观看。

都是在每年的12月份举办，2019的还有半年呢.....

6、CanSecWest



官网：<https://cansecwest.com>

CanSecWest都是与Pwn2Own一块出现的，以前议题PPT都是放在<https://www.slideshare.net/>上分享，但从2018年开始又不搞了。

每年议题不多，但质量还是可以的，不过感觉这两年的质量略有下降。

今年3月的议题也没看到有下载，也是混Twitter找ppt的，只看了《vs com.apple.security.sandbox》这个议题，今年我感兴趣的议题没几个，大家根据自己喜好选择吧。

如果你各个议题PPT，也欢迎分享下。

7、MOSEC 移动安全技术峰会



官网：<http://mosec.org>

MOSEC是从2015年开始举办的，由盘古与韩国POC联合举办，聚集移动安全领域，包括Android、iOS、IoT以及无线电等领域。虽然起步晚，但议题干货满满的，应该是目前国内最好的安全会议了。

今年的议题也已经陆续公开了，包括iOS越狱、Android提权、LTE、基带、卫星系统等等。

官网是不公开大会的议题PPT，由演讲者选择，所以想学习的同学，可能还是得去参会。

从2015年第一届我就开始参加，本月底还会去。去年参会，早上出酒店一辆车都打不到，又不在地铁口，最后骑了1个多小时的单车到会场，不容易啊.....

8、POC



官网：<http://powerofcommunity.net/>

POC(PowerOfCommunity)起始于2006年，在韩国举办的。单从议题质量看，确实不错，大多漏洞研究领域的前沿技术，但它经常是"二手货"，也就是在其它安全会议讲过后，但去韩国观光旅游顺便讲下。

还有个意思的现象就是，每年的议题超过一半是中国人讲的。

所以，你推荐也对，你不推荐也没错。

不过，有个好处就是，POC议题PPT都是提供下载的。有时在其它会议找不到PPT时，到POC官网翻下，偶有小惊喜。

另外还有个会议叫ZeroNights，同一举办方，更多是面向老外的。

那些未提及的知名大会

1、Defcon

很多时候，Defcon议题都是BlackHat挑剩的，有的人也会直接议题双投。上面的议题质量更是参差不齐，相对BlackHat要求更低，更开放。我很少看Defcon议题，偶而网上有人发才看。

2、RSA

RSA是一个充满商业气息的大会，如果你看过官网的PPT，就会发现里面充满诸多广告，有的议题可能就几页图片，所以从技术角度来看，是没有多少学习的价值。

但是，RSA有时也反应出的安全的风向标，虽有炒作的成分，但显然PR得甚是成功。比如当年的APT、数据可视化、威胁情报等等

RSA的创新沙盒是一项不错的活动，很多创业公司把他们研发的新产品拿出来比赛，从中可以反映出一些行业发展的方向。

所以，RSA比较适合管理者、创业者以及产品运营者。

3、XCon

以前国内安全会议很少，基本唯XCon为首。以前参加都是为了跟圈内朋友相聚聊天，有时场外比场内还热闹。

但这几年开始，XCon逐渐没落了。如果你参加过XCon2018，相信会有很大的体会，会场已经没几个人，有时在场人数可能达到个位数，找个同行聊天都难，且门票还是国内同类会议最贵的。

4、KCon

KCon应该算是国内比较有自己特色的会议，2018年的议题质量也还可以，中场休息的摇滚音乐很赞，场地与音效很好。

之前几届的议题质量忽上忽下，2019年的议题还没出来，大家可以关注下先。

若是在2018年，我还是会给个推荐的。

5、BlueHat

以前微软的闭门邀请制会议，从今年开始在上海举办国内版，议题列表已经放出，感觉质量一般。但跟MOSEC时间联着，可以考虑一并参加下。

6、RECON

因为多数议题自己不感兴趣，它比较偏向于逆向工程，以及系统底层、硬件、固件等方向，对此方向感兴趣的话，依然可以看看。

7、Syscan/Syscan360

官网已经打不开了，聊啥.....

后话

评价一个会议的好坏真是很容易，但要举办一个好的会议却是不容易，影响的因素特别多，且非一人之力可以搞定。

无论最终质量如何，对于为行业提供沟通交流平台的一些会议，还是值得点赞的。



漏洞战争

长按识别二维码，关注我的公众号

 漏洞战争



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)