第二届“强网”拟态防御国际精英挑战赛落幕，29支国内外精英队伍未能突破拟态防御，赛宁网安靶场平台完美支撑BWM新赛制.

原创

李飞cc 于 2019-06-04 16:11:22 发布 356 收藏

5月22至23日，由赛宁网安技术支持的第二届“强网”拟态防御国际精英挑战赛在南京江宁圆满落幕!该赛事吸引了网络安全领域及社会各界的广泛关注，本届大赛由中国工程院、中国网络空间安全协会、南京市人民政府、网络通信与安全紫金山实验室主办，拟态技术与产业创新联盟、江宁区人民政府、南京江宁经济技术开发区管委会承办。

来自俄罗斯、美国、乌克兰、日本、波兰和中国十个国家的29支国内外精英团队参赛，挑战由邬江兴院士创立的网络空间拟态防御技术理论。本次大赛中，全球DEF CON CTF大赛排名前15的10支国际队伍悉数到场，XCTF国际联赛前十二强中的国内队伍以及七支国内著名网络安全企业战队也开赴赛场，参赛战队的阵容可谓国内、国际少有。

本届大赛采用了由邬院士提出的一种“人机对抗”的新型网络安全竞赛模式，改变传统“人人对抗”的CTF竞赛模式，并将其应用于新型技术产品的安全众测。这一对抗模式，邬院士称之为“BWM”，包括黑盒（Black-box）测试、白盒（White-Box）测试、巅峰（Mountain）对决三个环节，既挑战选手的技术水准，又考验选手的策略能力。

经过两天近20个小时的艰苦鏖战，29支国内外精英战队对拟态设备实施了超过290余万次的高强度攻击测试，最终均未能突破或者逃逸拟态防御，冠军队伍因成功无望，在附加赛巅峰对决中直接放弃挑战拟态防御实际应用场景的机会，拟态防御这一我国独创理论的安全属性再次得到了充分验证。

福州大学 ROIS战队凭借比赛结束前十分钟在拟态防火墙造成执行体扰动的黑盒测试得分，最终反超知道创宇“老坛酸菜鱼”战队，夺得冠军和25万元奖金，“老坛酸菜鱼”战队及Nu1L联队分获亚军和季军。来自波兰的p4战队，来自日本的TokyoWestern战队、来自乌克兰的dcua战队、来自韩国的CyKor战队和来自北邮的天枢战队获得二等奖。来自绿盟的M01N等10支队伍获得三等奖。

第二届拟态赛应用的BWM赛制规则

在常规赛阶段，参赛队伍针对六款拟态设备采用服务共享模式进行黑盒测试，在未获取拟态设备相关信息的情况下，从外部进行全程的攻击测试；同时参赛队伍对其中四款拟态设备进行四轮次的白盒测试，采用分时独享方式，每款设备在同一时刻只由一支队伍注入后门进行执行体扰动和拟态逃逸攻击。

在黑盒测试环节，如参赛队伍造成执行体扰动触发拟态设备裁决器报警，便可获得该设备的黑盒执行体扰动动态分值，初始分值为1万分，根据参赛队伍通过挖掘利用执行体漏洞造成判决器针对指定目标有异常报警的队伍数量次序递减，前三名分别获得动态分值5%、3%、1%的奖励分；为鼓励参赛队伍针对同一拟态设备尝试攻击不同执行体造成扰动，还设置了成功攻击两个执行体进行两倍分奖励，成功攻击三个执行体进行三倍分奖励的加分机制。而参赛队伍如能完全突破裁决机制造成指定目标的逃逸状态，修改其中的指定目标数据持续（3分钟）通过裁决，则能得到黑盒拟态设备突破的动态分值，其初始分为10万分，分值根据突破队伍数量按次序递减，前三名分别获得动态分值5%、3%、1%的奖励分。

在白盒测试环节中，如参赛队伍干扰执行体输出异常造成裁决器报警，造成执行体扰动，则便可获得该设备的白盒执行体扰动动态分值，初始分值为5000分，动态分值根据造成同一执行体扰动参赛队伍的数量递减，为鼓励参赛队伍针对同一拟态设备尝试攻击不同执行体造成扰动，也设置了成功攻击两个执行体进行两倍分奖励，成功攻击三个执行体进行三倍分奖励的加分机制。而一旦参赛队伍能对拟态设备进行注入逃逸，造成指定目标的逃逸状态，控制拟态设备修改其中的指定目标数据并持续（3分钟）通过裁决，则获得该设备的白盒逃逸动态分值，初始分值为5万分，动态分值根据造成同一设备逃逸参赛队伍的数量而递减。白盒测试因为不同参赛队伍挑战次序不同，因此不设前三名的奖励分。

由于白盒测试分四轮次进行，每轮次又更具时长限制，选择特定数量队伍按序选择目标设备和时间进行白盒测试挑战，因此本次大赛额外引入了排位赛，采用6个未拟态环境下的执行体漏洞挖掘利用挑战题，每道挑战题初始分值为1000分，根据解出队伍数量其动态分值在100-1000分区间中递减，前三个解出挑战题的队伍获得动态分值5%、3%、1%的奖励分。在每个轮次白盒测试结束后，会依照当前的排位赛积分榜排名，选择排名靠前的队伍进入下一轮次的白盒测试环节。

附加赛则是巅峰对决环节，由常规赛冠军队伍挑战最高安全等级的拟态防御实际应用网络场景。

第二届拟态赛赛况回顾

5月22日赛事第一天9:30分，第一轮白盒测试中，来自南京本地的东南大学SUS战队造成白盒拟态域名服务器执行体扰动获得5000分，拿下正常赛事的一血。

经过第一天密集的三轮白盒测试，以及贯穿全天的排位赛及黑盒测试环节，来自中国的Nu1L战队以三轮白盒测试均成功得分排名并列第一，排位赛AK排名第二的优秀成绩，暂时领跑总分排行榜；而来自波兰的P4战队，来自日本的TokyoWestern，以及来自乌克兰的dcua战队在白盒测试榜上排名均并列第一，仅以排位赛得分的微弱差距暂时落后Nu1L战队，来自福州大学的ROIS战队，以及来自韩国的CyKor战队则因一轮白盒测试失败位列第五及第六位。

5月23日第二天比赛上午刚开始不久，来自知道创宇的老坛酸菜鱼战队开始发力，在拟态防火墙设备中通过黑盒测试造成执行体扰动，率先打破黑盒测试赛排行榜零分的尴尬局面，一举拿到10,500分，排名一下子从十名之外上升至第一名。

在第四轮白盒测试结束时，来自中国的Nu1L战队、来自波兰的p4战队、来自乌克兰的dcua战队、以及来自日本的TokyoWestern战队在第四轮的白盒测试中均造成了植入后门执行体的扰动，在白盒测试环节得分并列靠前。但因白盒测试造成执行体扰动比起黑盒测试模式要容易，得分也较少，而战队们试图逃逸拟态防御获得五万分的白盒逃逸高分均以失败告终，因此始终无法反超领跑的老坛酸菜鱼战队。

于是现场所有战队均瞄准了被老坛酸菜鱼战队黑盒测试发现漏洞攻击造成执行体扰动得分的拟态防火墙，进行“集火”攻击，然而直到当天中午仍未有队伍再次在黑盒测试中得分。当现场观众们都认为老坛酸菜鱼战队将最终夺冠时，在黑盒测试即将结束的13:50分左右，来自福州大学的ROIS战队准确找出了拟态防火墙设备执行体中的同样漏洞进行攻击，并造成裁决器扰动报警，获得黑盒测试得分。ROIS凭借其白盒测试中较老坛酸菜鱼战队的比分优势，超越其位列常规赛排行榜第一名。

最终经过激烈的角逐， 5月23日下午15点20分常规赛正式结束！ROIS战队以总分18039.78的成绩获得第二届“强网”拟态防御国际精英挑战赛总分榜第一名！

第二届拟态赛技术统计分析

第二届“强网”拟态防御国际精英挑战赛分为常规赛、附加赛两个阶段，常规赛具有黑盒测试、白盒测试和排位赛三个并行进行的环节。

在技术挑战难度最高得分最多的黑盒测试环节，需要参赛队伍在比赛过程中通过远程外部测试发现商用拟态设备产品的0day漏洞并进行利用，如造成执行体扰动即可得分，如能进一步同时控制所有执行体的输出，使得修改后的指定目标数据持续3分钟通过裁决器裁决，则成功突破拟态防御。

在现场比赛中，仅知道创宇“老坛酸菜鱼”和福州大学 ROIS战队在拟态防火墙上通过黑盒测试造成执行体扰动得分，在拟态防火墙执行体挖掘并利用了Web应用层0day安全漏洞，造成拟态裁决器报警，但未突破拟态防御。知道创宇“老坛酸菜鱼”获得黑盒测试一血10500分之后，几乎所有队伍均“集火”攻击防火墙，而只有ROIS战队成功发现了一条新的漏洞利用链并成功触发了执行体扰动效果。。在黑盒测试积分榜上，“老坛酸菜鱼”以一血奖励分优势获得9859.51分，而ROIS获得9671.71分。两队均未能进一步造成其他执行体扰动，更无法突破拟态防御造成修改数据持续通过裁决。

关于知道创宇“老坛酸菜鱼”的拟态防火墙WP可参看：

https://paper.seebug.org/932/?from=singlemessage

白盒安全测试在第一轮、第四轮全部参赛队伍均有机会参加挑战，而在第二轮、第三轮则只有在排位赛积分榜前十六的队伍才能参加，引入这种“抢机会”的比赛规则设置一是为了解决让所有队伍参加四轮白盒测试时间过长的尴尬局面，二是希望能引入未拟态环境挑战题在提高队伍排名区分度的同时又不至于吸引队伍过多的精力，从而避免出现类似第一届赛事时较多队伍在面对难度过高的拟态防御挑战时几乎将全部精力投入传统CTF模式的非拟态环境挑战题的局面。

在现场比赛中，通过排位赛，11支队伍获得四次白盒测试机会，10支队伍获得三次机会，8支队伍获得两次机会，平均每支队伍获得3.1次白盒测试机会。来自乌克兰dcua、来自波兰p4、来自中国Nu1L和来自日本的TokyoWestern四支战队在四轮白盒测试中均成功得分，在白盒测试排行榜上以8490.49分并列第一。拟态域名服务器和拟态Web服务器的解题率均为69%，而拟态路由器解题率仅24.1%，拟态文件存储服务系统解题率为27.6%。此外参赛队伍共计提交了19分白盒测试报告，但未有任何队伍能完成对植入后门意外执行体的扰动，更无法完全逃逸拟态防御造成修改目标数据持续通过裁决。

在排位赛环节中，共计有14支参赛队伍完成6道非拟态环境挑战题的AK，而来自韩国的CyKor战队以1129.42分在排位赛中名列第一位。

第二届“强网”拟态防御国际精英挑战赛常规赛的最终成绩为黑盒测试、白盒测试和排位赛的得分综合，最终ROIS战队凭借比赛结束前十分钟黑盒测试得分以及先前在白盒测试及排位赛的不错表现，以18039的高分，领先第二名近5000分的优势捧得冠军奖杯；知道创宇“老坛酸菜鱼”获得亚军，第一天夺冠呼声很高的Nu1L战队则因为黑盒测试未能成功跟进拟态防火墙执行体扰动得分，而痛失冠军机会，但也获得季军的好名次，帮助中国战队包揽了前三名。

参赛队伍赛后反馈

赛后技术支持方和波兰p4，韩国CyKor，美国Shellphish，新加坡HATS SG等战队进行了沟通交流。国际战队总体上对这届拟态赛还是挺满意的，p4的“乔布斯”大哥说“much better than last year”，这种结合黑盒测试高风险拿大分，白盒测试看速度拿中分，排位赛低风险长时间开放拿小分并争取白盒测试机会的赛制很有意思，竞争性和不确定性也比传统夺旗赛更高，他们对通过开放的NEST预先了解测试拟态设备很感兴趣。韩国Cykor建议能给更多次数和时间的白盒测试机会，以便更加针对性的了解和熟悉拟态防御的深层技术原理，期望能找出应对之策。美国Shellphish认为拟态赛虽然比传统夺旗赛少一些乐趣，但是能结合真实产品的测试更具挑战性和不确定性。新加坡HATS SG战队对比赛支持方能够在一个多月的时间内完全定制开发与拟态设备进行交互的比赛竞赛平台和挑战题目，并组织起这么高规格的国际性赛事表示非常惊讶和钦佩。各支战队均表示了有机会再来参赛挑战的意向。

夺得冠军的ROIS战队认为：“本次赛事赛制新颖，黑盒和白盒模式是传统CTF中从来没见到过的赛制，对选手的综合能力有一定的要求。多线并行赛制有效地提升了比赛的趣味性，不过倒是挺容易拉大分差，导致赢家通吃”，并希望增加白盒测试的时间以及在黑盒测试中增加应用层业务逻辑的漏洞，“相信如果给予几倍的时间，我们就能想办法突破白盒。黑盒上，希望能为应用层业务逻辑上增加一些漏洞，以便能更深入地尝试突破拟态机制” 。夺得亚军的知道创宇“老坛酸菜鱼”战队表示：“这次引入的比赛模式我觉得还蛮有趣的，排位赛的排名决定你是不是能挑战白盒拟态，这样的多线并行挑战考验的除了你的实际水平，也给比赛本身平添了一些有趣的色彩”。获得季军的Nu1L战队认为：“赛制新颖，对选手的综合能力有一定的要求，但过于复杂，难以快速理解。多线并行赛制有效地提升了比赛的趣味性。

赛宁网安CP-CR靶场竞赛平台全程流畅支撑

赛宁网安CP-CR靶场平台在本场竞赛中作为核心竞赛平台进行了全程流畅的支撑。在赛前，通过赛宁靶场平台所提供的虚实结合能力，主办方在靶场平台中部署了用于大赛黑盒测试的六款拟态设备，用于白盒测试的四款拟态设备，并通过靶场平台所提供的定制化事件采集接口，无缝对接拟态设备裁决器对于攻击测试所产生的扰动报警等事件以及攻击流量等统计数据。此外赛宁靶场平台基于虚拟化和容器技术为所有参赛队伍进行排位赛提供了六个稳定运行的非拟态挑战题环境。参赛队伍在赛宁靶场平台上针对不同环节目标的攻击测试和得分情况均通过Flag验证、攻击事件采集、队伍WP提交和审核等方式，进行及时高效地处理，最终保障了本场竞赛的全程流畅运行。

为了让前来观赛的现场观众们能更加直观的理解拟态防御内生安全结构，以及了解实时赛况，赛宁网安在现有靶场平台产品已提供的网络拓扑场景仿真、星际战争两套3D态势展示的基础上，专门为本次大赛定制开发了“人类队伍 PK 拟态机器章鱼”的3D特效态势展示大屏。

在比赛现场展示的赛况态势大屏中，将黑白盒测试的各个拟态设备设计为“拟态机器章鱼”的样式，按黑盒白盒测试目标为组分列两旁，中间红蓝绿三道光柱代表国际战队、国内战队、企业团队三个不同阵营，各个阵营按照赛事规则对“拟态机器章鱼”发起攻击！而不同的攻击方式各有不同的展示效果。

如上图有一绿色侦察兵托枪走近白盒拟态域名服务器“侦查”后，返回企业战队阵营，头顶并标有九州攻防实验室名称及其战队LOGO，实际就是九州攻防实验室战队人员正在准备挑战拟态域名服务器的白盒测试。

而下图国际战队阵营出动大量人类战士，并对黑盒阵营中拟态路由器实施攻击，表示为国际战队的人员正在尝试对拟态路由器实施黑盒攻击，如若扰动成功，“拟态机器章鱼”的触角将会脱落一只，然而由于拟态防御具有的特性，脱落的触角将会重生，从而恢复完整拟态章鱼的形态。

在此图中，来自国内CTF战队阵营的Whitzard等战队在白盒测试中对拟态Web服务器、拟态域名服务器、拟态文件存储系统分别实施攻击并成功造成执行体扰动，表示为三组国内战队的人员正在尝试对三款拟态设备实施白盒攻击，扰动成功后，三个“拟态机器章鱼”的触角均会脱落一只并重生。

中国工程院院士、国家数字交换系统工程技术研究中心主任邬江兴院士也莅临赛场与大家探讨拟态防御及创新赛制，并充分肯定了赛宁网安靶场平台的完善功能及炫酷展示。

总结

第二届“强网”拟态防御国际精英挑战赛的成功举办，是国内赛事历史上的又一次创新！邬院士提出的“BWM”赛制受到参赛团队和业界的充分认可，成为对先进技术及产品进行线下共测的最佳赛制选择。同时也标志着网络安全竞赛的发展进入到新的“以赛促建，以赛为用”阶段。

目前国内网络安全体系还不够完善，尤其是缺乏内在自生的安全体系。正如在拟态防御挑战赛现场，中国工程院邬江兴院士所说，传统安全都是依靠于已发生的经验，依靠外在的软硬件来保护自己，缺乏一种内在自生的安全体系。通过两届拟态防御国际精英挑战赛数十支国内外精英队伍数百万攻击测试验证拟态防御技术理论，从实践上证明了网络安全性能是可以通过科学的方法进行度量的，拟态防御这一颠覆性技术将迅速扭转我国网络空间安全易攻难守的被动局面。

另一方面，我们通过市场调研发现，各地网信办、相关行业管理机构对于网络安全的实战竞赛都有不同程度的思考，出于实际情况以及行业特点的考虑，虽然大家不谋而合，但还是“不敢贸然行动”。“强网”拟态防御国际精英挑战赛作为国内最具关注点的赛事，具有战略意义。主要表现在以下几个方面：

1、网络安全赛事进入实战阶段

“以赛代练、以赛带学”是网络安全领域一个比较普遍的说法，核心目的是推动网络安全人才的培养。拟态防御挑战赛是这一理念的成果检验，更是“以赛促建，以赛为用”的一次重要实践，将竞赛从传统的安全人才培养推动到对实体安全技术的挑战和检测。比赛已经不再是游戏，不再仅仅是发现锻炼培养人才，而且具有了产品安全测试的作用，竞赛正在为产业发展服务。

2、以国际化视角来检验自身安全能力

在央视对强网国际精英挑战赛的访问中提到，邀请全球强队来检测国内的网络安全理念和体系，这是一个大胆的想法和尝试。邬江兴院士表示再好的理论和技术不通过实践检验都难以提升。关起门来说自己伟大不是一个科学家应有的作为。通过这样(邀请全球战队)的活动来丰富理论，完善技术非常有价值。

敢于摆下国际擂台、敢于设置“白盒测试”，这就是一种自信，一种对创新技术的自信，一种使用技术的方式解决网络空间发展安全天花板、网络安全“顽疾”的自信，一种敢于更加开放、更加坚定地推进国际化的自信，一种坚定不移构建网络空间人类命运共同体的自信。

拟态防御挑战赛作为一项标杆性的赛事，赛宁网安通过XCTF国际联赛平台邀请了十支排名靠前的国际精英战队参与挑战拟态防御，以国际化视角来检验自身网络安全技术，这对于国内的网络安全自身建设来说是一种开放态度的引领。

3、从赛事体现出国内人才培养的成长

在首届“强网”拟态防御国际精英挑战赛的比赛过程中，国际战队一直处于领先的排名上，最终俄罗斯和日本战队分获冠亚军。而今年第二届拟态赛中，国内的企业战队、高校战队和社区联队均表现出了非凡的自信以及长足的技术进步，社区联队Nu1L在排位赛面对较高难度的非拟态挑战环境时，其应对能力和响应速度已经和韩国CyKor、日本TokyoWestern、波兰p4等国际级强队不相上下；而企业战队知道创宇“老坛酸菜鱼”战队能在全场29支战队中首个发现拟态防火墙执行体中的0day漏洞成功在黑盒测试中造成执行体扰动，体现出了国内网络安全企业对于实际产品真实漏洞挖掘的敏锐嗅觉和高超技艺；通过XCTF联赛中磨练出的高校战队代表ROIS在全场针对拟态防火墙的集火攻击中能快速定位出新的漏洞链，并采取了十分优雅的利用方式稳定触发执行体扰动，也反映出高校战队在过去一两年CTF命题趋向于真实世界场景的趋势下网络安全实战能力的快速提升。

第二届“强网”拟态防御国际精英挑战赛，以拟态防御体系为真实场景，以“BWM”形式为赛事创新，以开放态度打造国际舞台，不仅再次验证拟态防御理论的安全可行，并且推动网络安全赛事进入新的发展阶段，为网络安全行业理论发展、技术应用、人才培养起到巨大推动作用。