新闻热线：010—58884062
E-mail:kbjdsm@126.com
■责编 段佳
科技日报 2016年8月15日 星期一

■今日头条

智能耳机将推行业增长

文·毛启盈

据GFK报告显示，智能手机全球市场上，华为、三星以及苹果三大巨头占据了53.7%市场份额。有数百家厂商出货量不足100万，处在亏损倒闭的边缘。

一些手机厂商开始从红海中“自救”，纷纷转型耳机、手机代工以及家电等市场。在这些转型过程中，最具有潜力的市场当数耳机市场。美国知名市场调研GrandView Research发布智能耳机穿戴行业报告，预言智能耳机市场将在未来7年迎来全球爆发性增长，并估计2022年相关行业年收入将达到74.8亿美元。消费者新需求演变将刺激耳机类产品向着无线化和智能化的方向发展。未来，在传统巨头和智能耳机等创新企业激烈竞争之后，全球耳机市场将呈现全新格局。

最新消息，苹果将推一款带有对讲机功能的耳机，可以在本地无线ad hoc网络环境下与相似设备进行连接，然后再把用户发出的语音传输至其他设备。苹果相关文件暗示，耳机是通过Lighting又或者是标准耳机插孔与移动设备进行连接的，连接方式有Wi-Fi、蓝牙又或者是蜂窝网络。

三星今年5月宣布，向中国市场全面推出其耳机产品，覆盖耳塞、耳机、耳麦等多种类型，从高端的监听级头戴式耳机到时尚小巧的耳挂式耳塞。

华为早在2015年6月份就开始进军耳机市场，其中华为TalkBand B2可穿戴设备产品将蓝牙耳机功能集成其中，并且它带来了Jawbone UP健康数据服务。2015年岁末，华为荣耀在其两周年庆典上推出首款圈铁耳机，直接进入中国高端耳机市场。

有分析认为，对于苹果、LG、三星、索尼、华为这些巨头们来说，对耳机的研发与实验性发展投入是放在首位的。因为制造商需要不断尝试开发突破性的技术，以满足不断发展的对于艺术产品的消费需求。

而这些传统巨头绝非智能耳机市场仅有玩家，越来越多的创新者正在涉足这一领域。这些新玩家研发在耳机中加入人工智能解决方案的新产品，譬如综合应用传感体系、智能语音交互和智能推荐算法等。

目前，国内耳机市场中除了华为、三星、索尼外，fiil、小米、锤子、一加纷纷进军耳机市场，而比较有意思的是，他们都步调一致地做高端耳机。

海外知名市场调研机构FMI将全球耳机市场分类为个性化、游戏、媒体、娱乐、企业和体育等标签之下。在个性化这个关键词之下，耳机需求最高，体现了耳机最重要的是“自用”的需求。

根据预测，包括防水、降噪和高保真在内新增功能，预计在未来几年将推动该行业增长。在未来七年内，越来越多的耳机产品将集成音乐播放器和无线设备，这种做法将成为推动市场增长的关键因素。一些产品还将具备针对用户个性听音需求进行定制的功能。

可视化网络安全技术“看透”黑客

文·本报记者 付丽丽

“为什么下一代防火墙防不住下一代威胁?”日前，在“2016可视化网络安全技术论坛”上，论坛承办方、北京安博通科技股份有限公司CEO苏长君的问题一抛出，立刻吸引了与会者的目光。

传统的网络安全一般是基于策略或者是特征，然而特征并不等于行为，用户可以使用合法的账户通过合法的行为而做一些非法的事情，例如已辞职员工使用其原来的账户通过VPN远程登录进公司内部的系统并盗取企业的业务敏感数据。

“下一代防火墙并不一定能防住下一代的威胁，只有通过对用户行为的学习，并利用动态的策略来匹配用户的行为，进行细粒度的响应，才能保证用户业务的连续性。所以现在安博通要做的，正是通过策略、行为和流量的可视，利用动态的策略配置、用户行为的分析和深度识别，以及敏捷响应来做到真正的‘看’透安全。”苏长君说。

让不懂安全的人看懂安全

“安全的本质就是风险控制体系，让各个层面的人都可以理解、执行安全，让每个使用网络的人有‘安全感’，我们的目标就是让不懂安全的人看懂安全。”苏长君说。

苏长君表示，需要明确的是，可视化网络安全技术并非是把界面做好，也不是就搞个大屏幕做一些飞来飞去的炫图，其最主要的是要整合各个层面的需求，实现动态的安全管理，在一个基于安全视角的平台上根据需要叠加各种各样的安全防御技术。

以乘客进站为例，一般普通乘客关心的过程是买票、取票、进站、上车，但对于车站的安全管控就不是这么简单了。需要按照管理和业务需求，划分不同的区域，在进站区域安装检测仪器，在站内区域和周边各个不同位置安装摄像头，重点区域还要有民警手动核查身份证，更核心区域还要安放武警等等。

“网络安全也是这样，而且网络访问更为复杂。”苏长君说，安全可视化的就是综合安全域、安全策略、合规基线等一系列与安全相关的因素，整合各个不同视角的安全可视化平台，在这个平台上能够根据安全的视角叠加网络探针、网络回溯、业务质量分析等功能，以满足不同角度人对于安全的不同理解，从而对安全状况有感知，动态做出快速响应，防止危害进一步扩大，并迅速弥补漏洞。

当前，传统的网络安全还大部分停留在网络边界防护、漏洞检测和特征补丁上，这些手段都相对孤立，相对静态，而且只有专业人员看得懂，客户对此很茫然。

前几年，可视化技术也广泛应用在网络设备的管理上，俗称网管或运维平台，但网管的主要目标是对网络拓扑管理和网络节点的运行，目的是网络和资产的管理与维护，不是安全的视角。“所以，在传统的技术之上谈安全动态自适应、高级威胁防御、策略合规都是在浮沙筑高台，根本站不住脚。”苏长君说。

可视化不光“看外表”还要“看内在”

让不懂安全的人看懂安全，这是苏长君心中的一个梦。但如何看？却并非一句话能够说清楚。

将网络安全可视化，背后必须要有相应的技术支撑，专业的网络分析、高性能的探针、海量存储、大数据分析等，已经对客户业务的深度理解和经验的积累才能够构建这样的安全可视化系统。

苏长君认为，网络安全是一套内外循环的“平衡”系统，需要我们将“内观”和“外察”有机地结合。他将“安全策略基线”的可视，分解为“网络、流量、业务域和身份”这四方面，并主张通过“行为可视、异常可视以及路径可视”，实现对网络安全状况的“侧写”。

“可视化作为一种更加友好直观的呈现手法与真正的可视或说可见性有着本质上的区别。”苏长君说，所谓外行看热闹，内行看门道，“可视”的价值不在于华丽的“可视化”的外表，而在于其真正对整体网络安全态势的认知和理解能力，能直观的让技术人员获得怎样的信息，只是单纯的数据流向以及攻击IP等数据的可视，不能就将其完全等价为“安全的可视”。

苏长君介绍，安博通打造的可视化网络安全技术架构，通过公网和内网部署的具有应用识别能力的探针，实现对数据中内容的提取；然后将端的数据通过安全通道传到“云”之后，在云端从用户的维度对诸如“行为、虚拟身份和访问网站”等有价值信息进行整合，并面对用户的业务进行可视化的呈现；最终通过策略、流量、用户和业务四个方面的可视，实现“可视”的安全。

“之前的可视，更多的是基于80、443等端口号和诸如DPI、post等特征码，但如果是加密流量，如果没有特征码呢？所以我们更多的是基于用户的行为，比如时间分布、报文长度、到达次序等，再通过贝叶斯、决策树等分类算法进行分类，从而实现对用户行为的分析以及学习。”苏长君说。

可视化就像在网络上安了摄像头

“可视化技术的核心理念是通过提高网络自身免疫力，让业务系统兼具自适应的防御和修复风险的能力，从而让业务安全可视、可管、可控。”苏长君说，就像人体免疫系统中涉及不计其数的细胞、特殊物质及器官之间的高度纷繁复杂的相互作用，是人体随时处于战备状态，一旦有病菌侵入身体，就会迅速发现并将其驱逐出去。

此前，苏长君曾私下和一些从事网络黑色产业的团队做过交流。他们认为这个可视化体系就像在网络各个位置安全装了摄像头，让黑客的潜伏路径更容易被发现，其网络内部的安全弱点也更容易暴露，而且入侵事后也更容易被追溯和取证。

中国工程院院士倪光南表示，信息安全必须自主可控，自主可控时，信息安全容易治理，产品和服务一般不存在恶意后门，并能不断改进或修补漏洞。因此，我国必须推进国产化战略，在对网络安全起重大作用的信息基础设施和信息关键核心技术等方面，实行国产化替代。无疑，可视化安全领域是其中一个重要方面。

延伸阅读

网络安全亟须发现攻击看见威胁

网络上制造威胁，进行攻击的人总希望自己永远不会被发现，安全防御的一方总是希望能够透视整个网络，明察秋毫，及时发现与抵御乃至消灭威胁的发生。

“因此，我们所面临的所有网络攻击都是隐藏的，未知的，不想让人发现的。而发现攻击，看见威胁，正是有效防护网络安全的基础，隐匿与发现是网络攻击与安全防御之间永恒的较量。”公安部信息安全等级保护评估中心主任张宇翔说。

张宇翔认为，如何见，见什么？是网络安全所要解决的问题。没有核心技术的网络安全其实好比在别人的墙基上砌房子，而实际情况更糟糕，好像是在别人的院子里盖房子，你的一举一动一言一行，昭昭然尽收他人眼底。

“随着新的攻击方式和手段出现，攻击常常混杂在常规的流量中，从外及内，防不胜防。发现与看见的安全能力需求迫在眉睫。”张宇翔说。

在苏长君看来，可视化网络安全技术根本在于客户的需求。“有贼我知道，但抓出来一个看看”，这是客户经常抱怨的，往往是买了一堆安全设备，可是安全事件经常发生，出了安全事件什么也找不到，其原因就是客户没有一个基于安全视角的可视化网络平台。

“再就是对国际网络安全趋势的把握。”苏长君说，在2016年网络安全RSA大会上，业界一致认为单一的静态的安全加固技术不能解决问题，需要构建一套安全自适应防御体系，而可视化技术正是这个体系中的关键点之一。

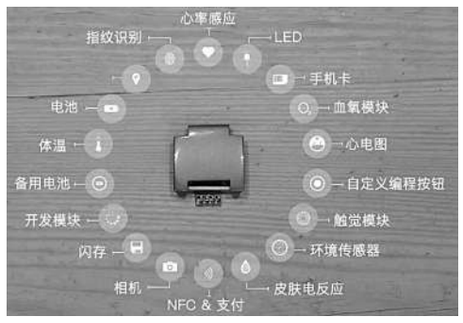
■炫技术

更直观的破窗器

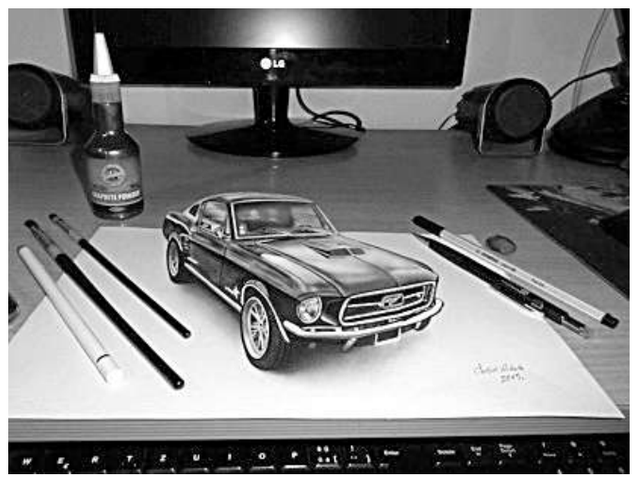
Corner Breaker是直接安装在车窗角落的一款破窗器，这里最容易产生裂痕，而且不易丢失，在关键时刻凭知觉就知道如何操作：拉起、释放即可，通过弹簧的力量破窗。直观、安全、而且无需太多的力量，老人和儿童都能操作。

模块化智能手表

Blocks模块化智能手表，需要什么功能换上去就行，不用关机支持热拔插。电不够，换个电池模块；不带手机，有SIM卡模块；骑单车，加个GPS模块；逛街，NFC模块付款；不带钥匙，无线射频识别模块开门；测血压、体温、心率的模块都有；还有手势模块，随意调节家里的家用电器。



■图片酷



绘画师Nikola创造的平面画作算是真正的跃然纸上、栩栩如生，彻底欺骗了你的眼睛。看见立体逼真的3D绘画，忍不住想要伸手去触碰一下。

■数据酷

5840亿年
无人星空游戏通关需要5840亿年

《口袋妖怪GO》是当下最火的游戏了，不过除了它以外，一款号称通关需要5840亿年的游戏也火爆网络，这款游戏的名字叫做《无人深空》(No Man's Sky)。

据了解，这款游戏由英国一个15人组成的制作团队打造，为玩家提供了一个拥有1800万的3次方个星球的广袤宇宙，没有任何玩家终其一生能够探索到其极限。

这款游戏在欧美地区的知名度可谓家喻户晓，甚至有可能将出现在美国电视节目中。这款游戏公司创始人Sean Murray表示：“如果按照每秒发现一颗行星的速度计算，游戏玩家可能需要5840亿年才能发现游戏中所有行星。每个人在游戏中都有自己独特的星球，他们将从那里开始自己独特的旅程。”

50M
美国平均宽带速率突破50M

网络测试机构Speedtest近日发布了2016年上半年美国宽带速度报告。报告显示，美国平均网速首次达到50M。

报告显示，今年上半年美国网速稳步提升，平均网速达到了54.97M，同比增长42%。上行速率更是同比增长51%，达到了18.88M。上述数据主要基于Speedtest网站及应用每日800多万次的测试。

在各服务提供商中，Comcast Xfinity的平均网速最快，达到125.53M。但Comcast Xfinity的领先优势并不明显，因为Cox的平均网速也达到了118M，而Spectrum为114M。

美国通信监管机构联邦通信委员会2015年年初以3比2的票数，将宽带定义为下行速率至少达到25M的互联网服务。相比之下，此前宽带的定义为4M。这一改变意味着，在美国家庭中，无法选择宽带服务提供商的家庭从19%增加至半数以上。

50米
大数据50米内可精确定位“伪基站”

公安部刑侦局与蚂蚁金服合作开发的“伪基站实时监控平台”已在全国各地公安机关投入使用。据蚂蚁金服公布的数据来看，其已协助警方打掉14个以通过伪基站发送含钓鱼网站短信实施银行卡盗用、欺诈犯罪的团伙。

资料显示，公安部刑侦局与蚂蚁金服于今年3月合作开发了“伪基站实时监控平台”，实现了对伪基站的实时监控。据蚂蚁金服安全部相关负责人介绍，基于蚂蚁金服及阿里巴巴的大数据模型推出的伪基站实时监控平台，能做到伪基站50米内精准定位。

通过这一平台，伪基站可被实时定位，而且能动态展示伪基站发送含钓鱼网站的动态信息，为公安机关打防伪基站相关犯罪提供协助。

蚂蚁金服表示，未来将进一步深化警企、生态伙伴合作，提升公安信息化水平、打击网络新型违法犯罪、网络“黑产”治理等应用体系建设。

300万
“月球葬”1千克骨灰300万美元

近日，私人登月公司Moon Express(月球特快)拿到了首个私人登月“执照”。随即，它们公布了自己的登月服务计划，其中将骨灰带至月球成了最抓眼球的项目。

不过，想要埋骨在月球对大多数人来说只能算梦想了，因为Moon Express创始人兼主席纳威表示，带1千克骨灰上月球就要花费300万美元，这就意味着，普通人想要在月球长眠，至少要花费500万美元。如果你长的高大些，恐怕就得花800万美元。不过，即使价格如此昂贵，需求依然很高。纳威表示：“现在已经有很多人在排队了。”

当然，作为第一个私人登月公司，Moon Express可不是来搞丧葬服务的。明年，该公司就将执行首次登月任务，到时它们将在月球上释放一台机器人探测器。这台探测器预计要在月面行驶500米并将高清视频回传到地球。

未来，Moon Express将利用自家探测器在月球挖掘一些地球上稀有的矿产资源并送回地球。