阿里安全IoT安全研究团队Leader谢君：如何黑掉无人机

原创

csdn业界要闻 于 2017-12-01 16:54:38 发布 1215 收藏 1
文章标签： 阿里 谢君 看雪安全开发者峰会 安全

本文链接：https://blog.csdn.net/csdn_bang/article/details/80133060

11月18号，2017看雪安全开发者峰会在北京悠唐皇冠假日酒店举行。来自全国各地的开发人员、网络安全爱好者及相应领域顶尖专家，在2017看雪安全开发者峰会汇聚一堂，只为这场“安全与开发”的技术盛宴。

最近两年越来越多的安全人员开始投入到IoT设备的研究热中，常见的研究方向包括路由器、摄像头、汽车等。阿里安全IoT安全研究团队Leader谢君在主题演讲中为我们带来的如何黑掉无人机的技术解析。他介绍了某品牌无人机的架构体系、功能模块、传感器等，包括各个组件的攻击面、安全防护体系、软硬件反调技术及其绕过方法，并深度解读无线宽带通信等。

此外，在峰会现场谢君还介绍了一个不需要通过软件漏洞就能Root无人机的方法，并演示了如何远程劫持一台无人机。其中就涉及了诸如飞控系统等专业领域的研究。而从最初的设备拆解到各个芯片子系统的深入剖析，都展现了他求索与收获的一段心路历程，相信现场很多听众对于这种钻研态度都是由衷的钦佩，再考虑到目前国内外这方面的公开资料都很少，其中的难度可想而知。

阿里安全IoT安全研究团队Leader 谢君

> 谢君，阿里安全IoT安全研究团队Leader，资深安全专家，12年安全领域工作经验。现专注于IoT安全研究与 提供解决方案。2016年发现小米整个智能硬件生态高危远程漏洞，在XPwn2016展示其漏洞利用并协助修复；2016年发现美的智能生态远程高危漏洞，并协助修复；2015年发现Broadlink整个智能硬件生态高危远程利用漏洞，在GeekPwn2015展示其漏洞利用；2014年发现美国奔驰高危远程漏洞，并控制超过50辆奔驰汽车。此前并发现过惠普，富士施乐打印机远程漏洞和微软高危漏洞；2011年发现迅雷网络多个高危漏洞，并且验证利用迅雷网络发起大规模DDOS攻击。

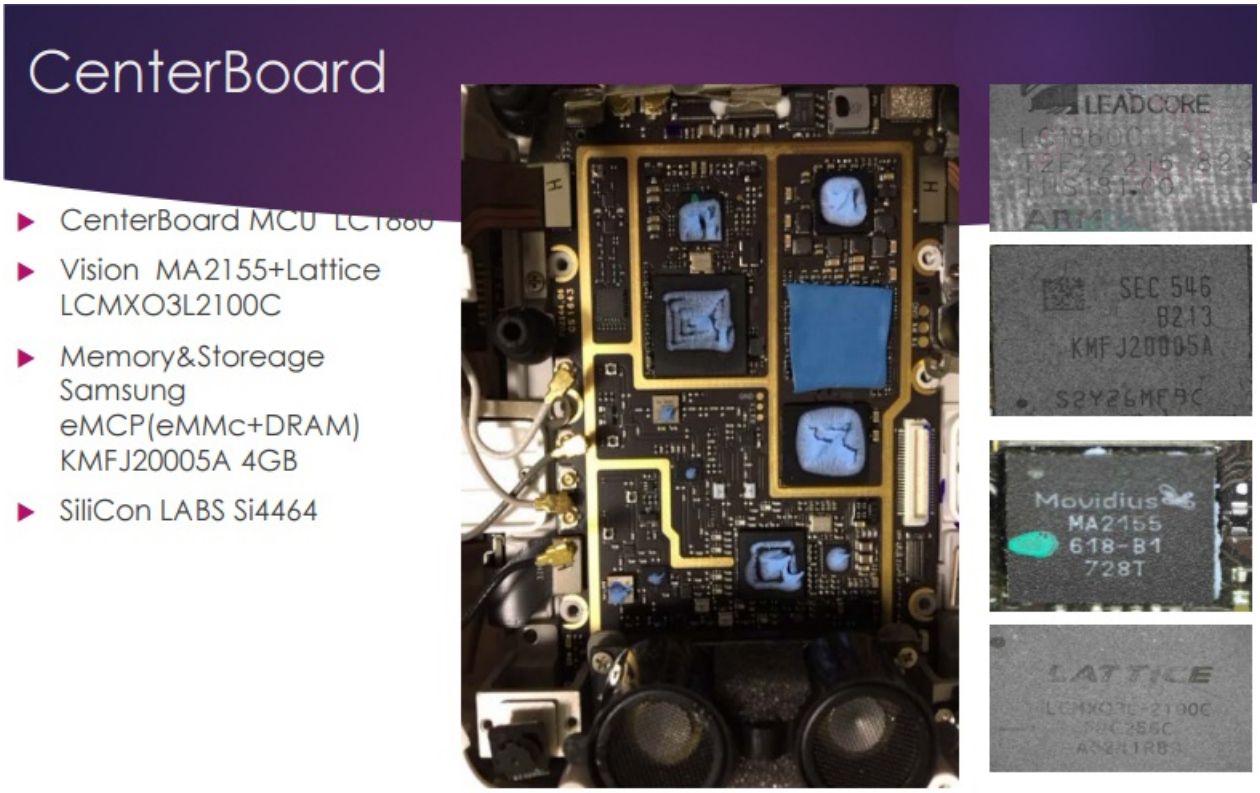
以下为演讲速记：

谢君：今天我分享的议题是如何黑掉某品牌的无人机。我在研究无人机的过程中从物理接触和非物理接触两个方面对整个无人机进行系统化的研究，研究的过程中其实也是一个学习的过程，所以今天我想跟大家分享一下我在这个研究过程中的一些收获和所学到的一些东西。

无人机是个复杂的系统工程

自我介绍一下，我现在是在阿里安全负责IoT安全攻防研究以及安全解决方案，在安全领域也折腾了十几年。现在专注于互联网安全这一块的研究，无人机对于我来讲是一个比较新的东西，我接触的时间也比较晚了，才有一年的时间。我在整个研究和学习的过程中，总结了无人机的一些功能，无人机系统一个复杂的系统工程，里面涉及到领域实在是太多了、太复杂了，里面涉及到结构工程、自动化控制，空气动力学，计算机视觉处理以及各种传感器、无线通讯，并且涉及到人工智能相关的深度学习。
对它有整体的感官，我整个系统全部拆开，发现里面应用了哪些硬件，哪些传感器，哪些芯片。无人机这一块涉及到不同的传感器以及控制系统，很多嵌入式芯片没有这个OS的概念，所有代码是直接上位机执行，通过实时中断以及计时器和IO的控制来完成整个系统的实时操作。

我的分析是基于某品牌的无人机进行分析，包括无线通讯、飞行控制，以及微机电传感器、机器视觉处理，这些微控制芯片来自各个不同厂商。这么多的传感器芯片之间进行通讯，必须满足相应的通信规范，大家才能协同自如，所以产商设计了一套无人机各个模块之间的通信协议，整个协议满足它整个全系列消费级无人机的产品，定义最多不超过32个硬件功能模块，硬件功能模块下面可以定义子功能模块，比如说我们的飞控系统用03来表示，06表示飞控系统下面这个子控制功能，比如下面支持的飞机起降功能等。我们可以看到摄像头采集系统是用01的来编号的，云台控制系统是用04来编号的，而在传输过程中，这些编号将会通过算法来编码。这些不同的传感器之间通讯链路有多种，这里面通讯协议按照他自己的一些划分，有本地的，通过串口的，区域网络等等，在里面用的最多的通讯协议是两个，一个logic以及是V1，logic像进程间通讯的方式，V1指远程不同硬件之间进行通讯的一种协议方式。模块间通信也做了一些相应的隔离，非常像现在的汽车系统，汽车有不同ECU各个模块，各个模块通讯也有一定的通讯协议和格式，也有一些网关隔离某一些子系统是不允许公共访问的。像无人机里面GPS模块的话，只允许飞控系统访问，其他应用系统是不允许访问，整个无人机的通讯的结构，类似于这张图一样，所有的不同的传感器之间通讯是有一定的路径，而且也有一定的限制。这是无人机通讯格式，就是说他们有一定的规范比如说他的头部一定是55开头的，它的每一个包的长度不能超过多少个字节，它的控制命令设置还有一些校验位。并且，对于每一个子系统的编码通过一定的算法来计算的。

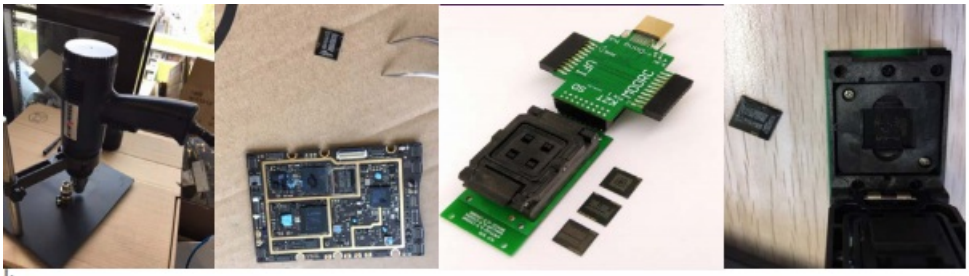


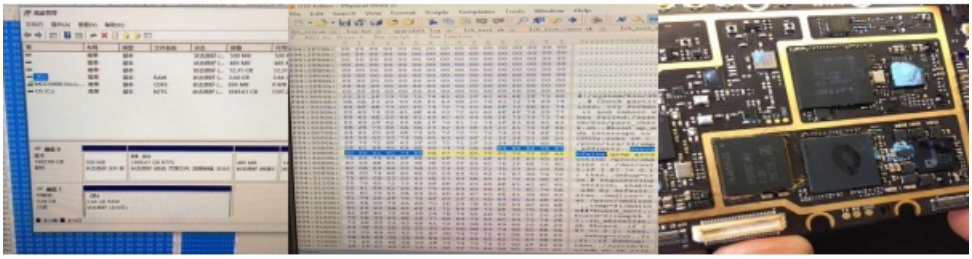
无人机的核心中心桥的控制板，主要是基于LC1860SoC外加图像识别芯片，双目避障，无线收发器，无线基带，LightBridge，它的主要功能是整个系统的协调以及固件更新和摄像内容数据编码和图象深度学习，ROI检测之类的。这个LC1860芯片运行的是嵌入式Linux系统，下面是三星的EMCP，是集LPDDR和eMMc于一体的存储芯片，操作系统就存放在这个芯片里面。下面这一块芯片intel Movidus MA2155，这是英特尔图像深度学习芯片，因为无人机不能联网，无人机需要做实时的机器视觉分析，需要用到大量的矢量运行，这个时候这个芯片的优势就体现出来了，这个芯片在这个无人机上面的应用有视觉测距，障碍物识别，还有ROI，比如说你的飞机进行跟随飞行的时候，跟随一个人飞行的时候，通过CNN建立好的深度学习模型，来精确判断。LATTICE的这块FPGA芯片，主要是用于双目避障功能，通过可见光反射回来检测障碍物的存在。

root无人机

我们在研究IOT设备的时候说的最多一个词就是能否root这台设备，root掉设备意味着我们可以获得系统很高的控制权。我们为什么要root无人机，我们root无人机目的是扩大它的攻击面，更好研究无人机。我们在研究的过程中发现要root无人机，最好的办法就是利用一个合适的漏洞，执行打开Adb这个接口功能，就能得系统的root shell了。如果你要是没有漏洞的话，这个时候怎么办。这个时候我们在研究过程中发现有意思的办法：可以不利用漏洞也可以root无人机。其实这个办法也可以运用到很多的领域。像一些路由器。研究的过程中发现启动脚本里面有一个变量是控制adb功能打开与否的，默认出出厂是这个ADB是不打开的，ADB功能接口在安卓手机应用广泛，怎么打开这个adb功能，一种是利用漏洞执行ADB_en.sh的脚本，另外一种就是方法就是直接修改这个启动脚本的变量。

我们不通过漏洞的方式来root无人机，因为安卓系统是存在三星EMCP里面，是集内存和存储于一体的EMCP的芯片，如果我们可以修改这个芯片里面的内容，我们就可以直接root无人机了。



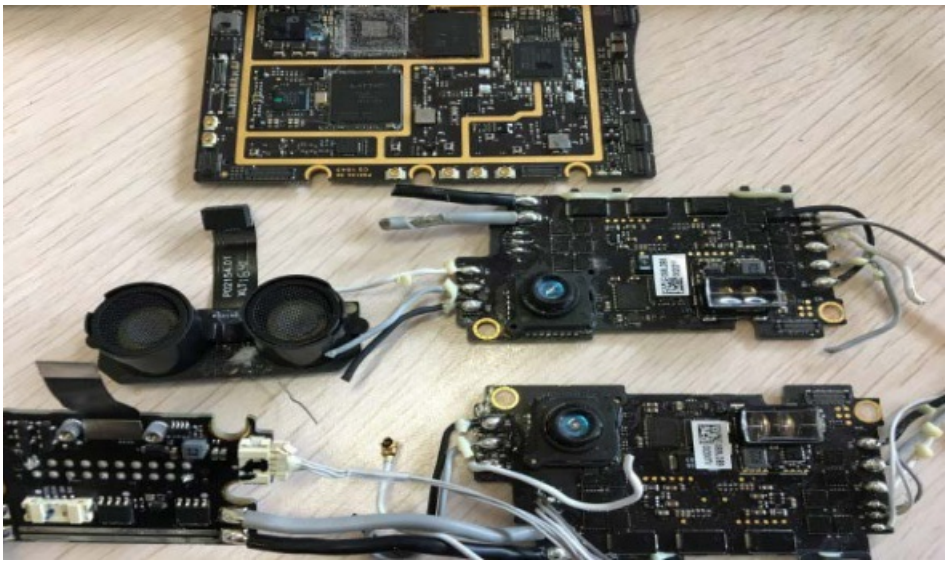


操作步骤是这样子：首先找到这一块存储芯片的位置，把它电热风枪吹下来，需要EMMC的读书卡，把这个内容读取出来，这个时候我们就找到了EMMC的读卡器，把这个EMMC插到电脑上，这个时候可以看到有一个弹出，用存储器里面的空间和内容，找到那个设置调试的变量的地方，修改了之后，再写到EMCP里面焊回来。这个里面有一个小细节，因为这个存储器里面的内容是有一些分区，我们需要把这些系统分区直接挂在到电脑上面，用EXT4的方式挂在，修改完了以后再保存，再剪辑切回去EMCP的芯片里面，后续我们需要把它焊回去。再运行直接ADB打开，就可以得到root的权限，成功后可以看到它的系统信息和进程。这里面涉及到很复杂的问题，要手工脱焊和焊接的过程，这个芯片是BGA封装，引脚多，引脚间距小，而且这个芯片底座里面人为灌了一些黑胶，对于操作过程带来很大的不便，而且操作不当，很容易使这个芯片废掉了。手工操作的难度是非常高的。

飞控系统

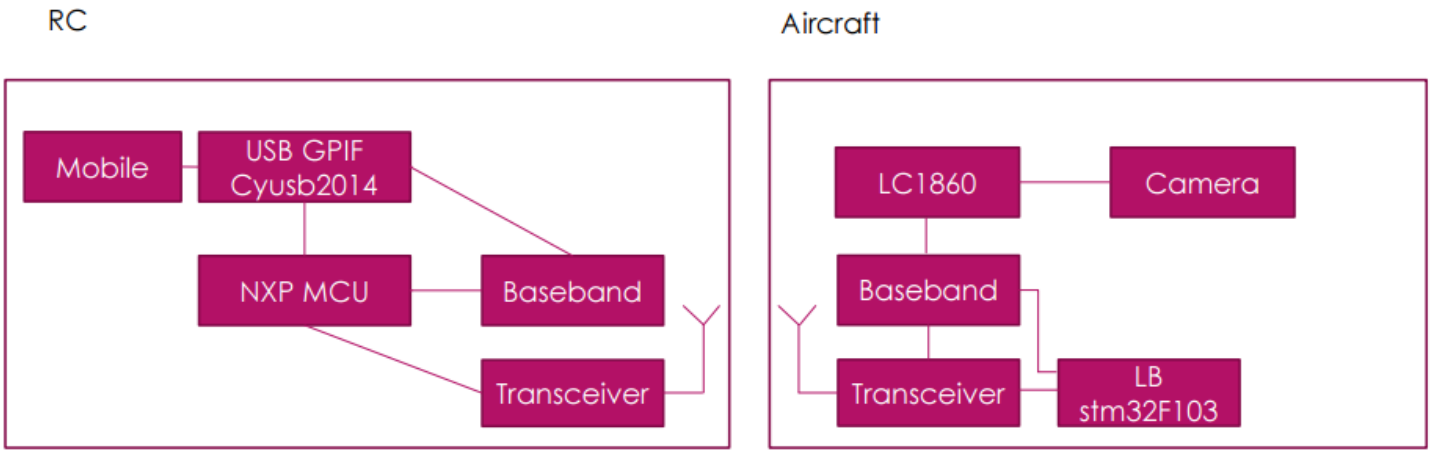
飞控系统是无人机里面的核心。因为会搜集到很多的无人机的各个传感器模块的一系数据，通过一些综合的算法来判断飞控系统应该如何操作，飞控系统核心芯片用的ATSAME70Q21，这个不需要外置存储器存储它的部件以及算法，与之相关有两块IMU陀螺仪以及加速度计，检测这个飞机处于什么状态。气压计，主要为了检测这个飞机的高度，作为一个飞机高度的判断因素。UbloxGPS模块，这一个可编程的模块，因为飞控和GPS通讯是有一个协议交互，并不是说任何一个GPS模块可以替换它，可以做一些欺骗GPS的事情。因为之前说用于替换GPS模块做GPS的切换。指南针模块，主要用于方向的定位。智能电源，智能电源是用德州仪器MSP430G2755 16位的微控制芯片，它主要是收集了电源现在状态，保持了我什么时候放电，什么时候通过飞控系统说我的电量还剩多少的时候应该返航。电调芯片，因为无人机有四个螺旋桨，四个马达，每一个马达需要一个电调的芯片控制转速，控制不同的马达的转速和相位，来达到控制飞行姿态以及速度的操作。

视觉系统



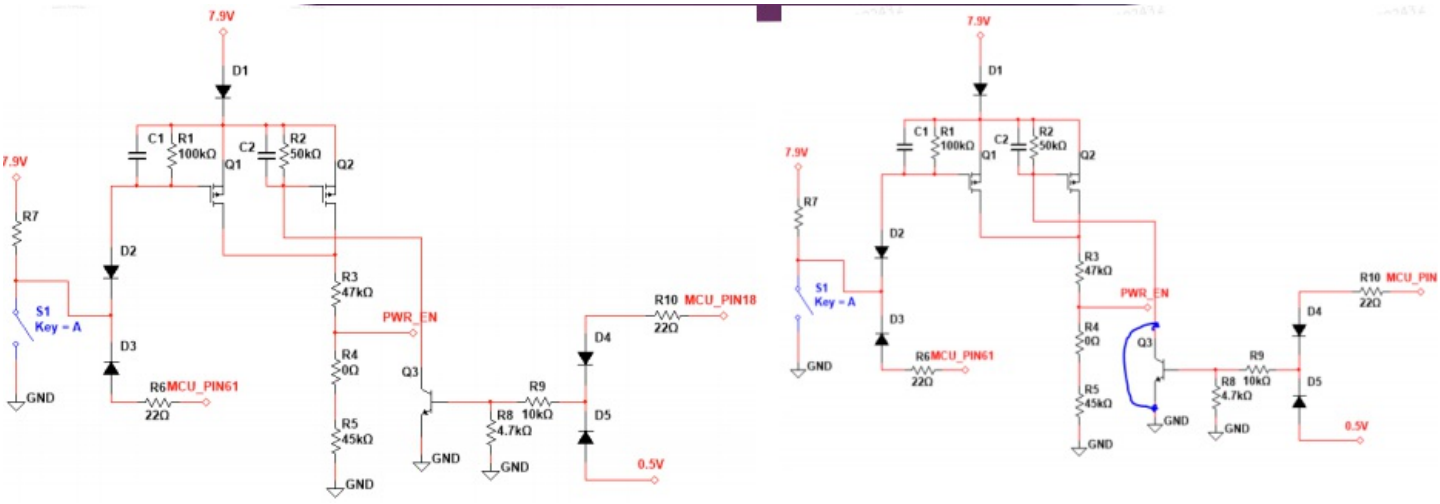
视觉系统是无人机里面非常重要的功能，这里面核心的一个处理芯片是用的英特尔的MA2155深度学习的处理芯片，飞机搭载摄像头首先是可以进行视频的录制、拍照，图像内容输出给视觉处理芯片来完成视觉识别的一些特点功能，这里面有一个功能叫做飞行跟随，这个飞行跟随就是在手机屏幕上选点跟随飞行的目标，无人机就可以跟着他/它飞行了，这个时候就利用了这一块芯片的强大深度学习的能力，感兴趣的区域进行识别，人物、姿态，再有一个功能就是测距，通过MA2155这块深度学习芯片来完成视觉测距的功能，飞机前面以及后面障碍物的距离我是通过这个图象识别的方式来识别出来的。还有一个是双目避障，这是观测倾斜度70度是否有障碍物，是有两个，一个接收端一个发射端，发射出去的光，通过反射回来，我要判断右下角是否有障碍物。超声波检测下方障碍物以及检测地面的功能。无线通讯，是无人机里面最核心的一块功能，也是最复杂的一块功能。因为里面涉及到控制系统和图象传输。基本上的原理就是前端的收发器收到信号，通过基带系统解调，解码以后通过遥控器的LPC1549芯片处理进而通过Cypress的USB芯片反馈到手机上。无线通讯的特点，通过OFDM方式进行图传以及数控的传输，它的特点就是控制通道数据通过遥控器通过1Mhz带宽的跳频发送，飞机回传的图象和控制通道回传数据是通过10Mhz带宽进行定频传输。为了保证数控通道及时性，采取定时跳频的方式。因为有可能信号会被干扰，在某一个特定的频点的时候会被干扰到，如果被干扰了的话，飞机有可能收不到遥控器的一些数据，这个时候我们就需要切换不同的频点，找信噪比高的地方，保证它的可靠性。它在FCCID通信管理局申请的5G频段的频宽执照在5727-5821Mhz，但是实际上，它的操作已经超过了它的通讯管理局规定的频段，滥用这个频段的资源，在我们的研究过程中发现已经到了5845Mhz。遥控器跟飞机怎么样进行识别，这需要一个配对以及连接的过程。配对的唯一信息是来自于遥控器，所有信息都是遥控发给无人机，配对成功以后接下来的过程可以在操作的过程中识别到哪个是我控制无人机，而且这些控制的配对信息都是通过摇控器的芯片LPC1549的序列号来生成的。

无线通信系统架构



首先是遥控器先初始化的芯片，初始化基带系统各个寄存器，寄存器里面存入了唯一可以配对码的信息。这个配对码是有五个字节，写入到寄存器里面，真正用到只有三个字节，所以在未来需要无线劫持这个无人机，就有了可能。无线通讯传输的过程其实是非对称的传输，无人机遥控器发的信息是跳频传输给飞机，接收端也是跳频接收，但是图传和下行的通道是由飞机是一个定频的方式来发到，而且这些跳频算法都是通过代码来实现的。旁边这张图就是遥控器用于检测飞机是否配对上的算法检测基带芯片SPI地址0xE4、0xE5、0xE6进行比较。所以劫持一台无人机，其实我们是通过可以暴力破解的方式，用所有的密钥空间进行离线的破解，找到配对码，去控制这个无人机，在空中的时候就可以动态改掉这个配对码，然后这个无人机就属于你了。

无人机反调对抗技术



我们也发现了一些硬件的反调技术和软件的反调技术，比如说用atmel芯片的安全位置1，可以阻止外置硬件仿真器的挂载调试，遥控器的LPC1549通过ADC的粒度检测来检测调试器，LightBridge用的stm32F103芯片通过remap SWDIO来使用swd调试接口失效，通过遥控器的硬件开关电路来阻止LPC1549芯片硬件仿真调试。
最后还有很多工作还没有来得及做，未来会更加深入的研究各个硬件模块的功能hacking与未来一些想法的验证工作。

谢谢大家。

> 注：本文根据大会主办方提供的速记整理而成，不代表CSDN观点。

2017看雪安全开发者峰会更多精彩内容：

- 2017看雪安全开发者峰会在京召开 共商网络安全保障之策
- 中国信息安全测评中心总工程师王军：用技术实现国家的网络强国梦
- 兴华永恒公司CSO仙果：Flash之殇—漏洞之王Flash Player的末路
- 中国婚博会PHP高级工程师、安全顾问汤青松：浅析Web安全编程
- 威胁猎人产品总监彭巍：业务安全发展趋势及对安全研发的挑战
- 启明星辰ADLab西南团队负责人王东：智能化的安全——设备&应用&ICS
- 自由Android安全研究员陈愉鑫：移动App灰色产业案例分析与防范
- 腾讯反病毒实验室安全研究员杨经宇：开启IoT设备的上帝模式
- 绿盟科技应急响应中心安全研究员邓永凯：那些年，你怎么写总会出现的漏洞
- 腾讯游戏安全高级工程师胡和君：定制化对抗——游戏反外挂的安全实践
- 绿盟科技网络安全攻防实验室安全研究员廖新喜：Java JSON 反序列化之殇