



|                   |   |
|-------------------|---|
|                   | 陈广瑞                      易方达  |
| 时间                | 2022年5月27日 15:00  |
| 地点                | 进门财经电话会议  |
| 上市公司接待<br>人员姓名    | 公司投资者关系负责人及车联网安全团队成员  |
| 投资者关系活动<br>主要内容介绍 | <p style="text-align: center;"><b>三六零对汽车安全的愿景</b></p> <p><b>Sky-go 团队介绍：</b></p> <p>360 车联网安全研究院（360 Sky-Go）成立于 2014 年，成立八年来，曾全球首个发现特斯拉汽车安全漏洞，协助奔驰、宝马等知名厂商修复汽车信息安全漏洞，累计发现智能网联的汽车漏洞超过 500 个，接入整个智能网联汽车安全运营平台的车辆已经超过 180 万，累计保护车辆超过 2000 万。</p> <p><b>在课题研究方面</b>，研究院承接了很多标杆性的课题，都是偏向于汽车专业领域的国内首例。同时课题落地于车企，为车企的安全合规产品落地奠定基础。</p> <p><b>在标准研究方面</b>，Sky-go 是国内最早牵头，代表中国发布国际上首个汽车信息安全标准的机构，目前也在积极参与国内的准入标准的制定。</p> <p><b>在试点项目方面</b>，Sky-go 建立了国内首个车企汽车信息安全实验室，为现今车检机构对联网汽车的产品准入能力以及安全检测能力奠定了基础。在跟车企客户的合作中，我们都是基于整车设计的角度，致力于从完整性方面为车企赋能，更好保证所有新车上路前都经过安全检测，新车上路后都能提供一套安全运营机制和安全响应机制。</p> <p>今年完成了车检机构唯一标杆案例，同时我们跟高校、车检机构等成立了很多实验室，获得很多客户感谢</p> |

信。总体来说，团队8年来沉淀了很多产品，行业内几乎所有大的头部客户包括一汽、东风、广汽、长安、北汽等都与360有深度合作关系。

**提问环节：**

**Q1：车的安全是性命攸关的问题，车联网会不会是一个非常好的契机，来促使国内以车联网为代表的网络安全市场彻底转向需求导向型？**

A:前几年研究相对比较滞后，那时网联化定义相对比较泛，如OBD联网、车机互联、手机互联等。目前广义上来说，车联网更多面向协同，包括：车路通信、车车通信、车人通信；狭义上来说，车联网更多是单车联网的状态。

目前车企所发布新车的网联化与智能化的程度越来越高，面临的安全问题也越来越严峻。与传统的网络安全不太一样。车联网安全某种意义上说涉及国计民生安全，如它会直接面向人身安全，智能化网联化之后存在隐私泄露风险，产生社会的一些负面影响等，电影中黑客攻击汽车信息的场景实际上在技术层面很容易实现。

车企在做车联网投入时，不同车型开发的功能也不一样，但在车辆自动化、网联化程度越来越强的趋势下，车联网安全问题可能会慢慢演变成社会问题。从车联网路线攻击的角度上说，我们前期在以最低成本做破解的时候，可以从汽车后市场拿到很多车的智能零件，技术上可以对其进行破解和攻击。这可能会导致企业丢失大量的数据，也可能面临更多潜伏性的黑客攻击。

在国家政策法规还没有完全标准化时，车企无形中承担着车联网运营平台基础设施建设的责任，车联网安全还可能上升到国家安全。比如说车企可能有某个重要

任务的出行数据、地理测绘数据、军事数据等涉密信息。有些央企级别的车企对数据的定义为核心商业秘密，一些涉密数据他们也有自己的涉密网。

总之，车联网安全面临的问题有4类：人身安全、社会影响、经济损失、国家安全。面对目前野蛮生长的汽车市场，车联网安全标准的加速落地符合整个十四五规划和科技之路的发展进程。

**Q2：如何看待车辆安全与数据合规安全的关系？车联网安全的整个市场规模以及公司业务布局情况？**

A：三六零与其他传统安全公司不同，很早就将安全定位于数据安全，不管业务形态如何发展，根本上是源于数据，数据效应也会让公司更好的发展。同时，数据也是一个武器。数据是网络安全的攻击武器，三六零17年来积累的安全大数据形成了一套安全能力框架，再加上8年来车联网关于样本漏洞的研究，可以让我们在新的数字化转型更好地使用这把武器来解决汽车数据安全问题。

三六零的核心定位为数字安全，整个车联网安全业务板块的产品形态包括：流量监测、异常分析、威胁情报等。车联网在整个安全能力框架下更多的可以解决很多车联网场景下数据安全面临的四大场景的车联网问题，更好的从监管、从客户角度发挥本身的数据的作用。

在整个行业层面，国内最开始还没有相关法律法规约束数据采集，或存在车主被动将摄像头等信息传输给车企来训练自动驾驶模型等情况。目前国家陆续发布相关法律法规对此加以约束，网信办对数据收集、存储、使用、加工、传输、提供、公开等提出要求，其中也针

对车企和供应商规定了应该建立怎样的数据安全管理体系，从而保障信息安全。最开始并没有太多法规，可能也是为了智能网联汽车能快速发展，在国际上实现弯道超车，目前正在逐步规范化管理。国外相对会比较早，如欧盟的 GDPR、新加坡网络安全法。

国家层面虽然提了很多相关管理规定，但还缺乏实际落地的指导性建议。360 结合自身数据安全的优势和攻防能力，在标准层面会提到具体技术怎么去做，将其输出给包括汽车 oem，汽车厂商，告诉他们数据安全这块怎么做，对汽车行业来说，不管数据安全还是网络安全都是比较新的东西，所以需要 360 这样既懂数据安全、网络安全同时了解汽车行业特性的企业，可以把这三者结合起来放到标准中，可以更好帮助法规落地实施。网络安全+数据安全+汽车行业理解，360 将自身优势融合到标准制定中，可以助力车联网安全更好更快的发展。

**Q3: 现在汽车总是说五大域，公司面向各个域或者整车提供的具体产品形态是软件还是软硬件一体的解决方案？比如，面向座舱车机这块，公司是提供防火墙、车机软件管家么？公司怎么向主机厂收费的？市场空间有多大？公司能占有怎样的份额？**

**A:** 针对域的划分目前没有统一定论，现在主流的上市车型还是普通的总线架构，特斯拉可能在这一块的早期规划更为先进。

**产品形态:** 主要针对汽车联网部件进行安全管理，目前主要集中在车身 T-BOX 联网终端、IVI、车机中控系统、网关系统等。在云端可以对所部署探针的终端进行统一安全监测和管理，包括数据采集、分析、报警、

应急响应等流程。目前我们针对 SOA 的平台架构做技术研发，这是下一步规划的重点。在平台上会重点去做攻击的，我们把从 2014 年开始积累的攻击经验陆续落在平台里面，使其能够精准识别车辆的攻击行为，从而支撑整个车厂的安全运营工作。

**市场空间：**国内针对这一块的主流玩家还有一些传统的安全厂商和新兴创业企业。整体从每年的新销售乘用车数量来看，大概是千万级别。从每个车企去做网络安全的环境来看，整个市场空间目前没有相关机构的调研数据。

**收费模式：**目前我们团队整个监车数量可以说在国内处于领先水平。在国家标准出来前，车企的认知还不是很高，导致我们前期项目导入是以项目制的形式运转的，但国外基本上是跟主机厂用 license 的方式来导入，大概每一台的终端收费为 3-10 美元。随着大家认知的提升，车企这一块的需求也不断强烈起来，**后面市场会更偏向于终端授权的方式**。我们会打通这种运营模式，形成订阅模式给到车企。另外，我们还会基于具体的规则、功能、汽车所需安全能力等方面进行收费。因为这还会涉及到研发期限的问题，保守来看整车架构的研发是 2 年，新能源 1.5 年。由此来看，我们产品质保期也得是 2 年，在整车架构构建时，我们的版本升级也是一个收费点。很多车企没有针对攻防这一块的安全运营团队，所以他们愿意花钱买这方面的能力。

**Q4：面向智能网联这块，我们是在 T-BOX 里面嵌入自己的软件算法实现一个甄别么？起到一个过滤保护作用？这块市场有多大？**

**A：**一辆车大概要部署 3 个 SDK，之前有机构分析一

个单点是 104 元，但我们经过客户调研发现目前这个阶段可能达不到那么高，很保守来看客户的期望大概是 20 元。随着法律法规的实施以及行业标准的落地，这个市场的供需结构会发生比较大的变化，相应价格应该也会有比较大的变化。

**Q5：我们安全芯片这一套整车大概需要多少成本？如果是基于动态防护的方案目前成本？规模量产生后对应的成本是多少？**

**A：成本：**我们跟国内一些规模较大的专业智能卡芯片或安全芯片厂商，都有战略协议。一般消费级的芯片价格大概在几块钱，而随着使用场景要求的提升，对应的芯片价格也会随之提升，如到达工业级可能就会比消费级有较大的提升，而车内安全又属于工业级里边比较高要求的层级，所以这个价格的提升在目前是比较普遍的。如果再加上供应商品牌的溢价，那价格可能会有比较大的差异。当然配置有高有低，提升幅度也有不同，但芯片作为批量的产品，价格上也有梯度。所以单纯从芯片角度上讲，我认为并不便宜。但是如果量能够起得来，这块的边际成本还是可控的。

基于动态防护方案，我们可以在 T-BOX 里面嵌入自己的软件，但也不止是 T-BOX，因为一辆智能汽车零部件会随自动化程度变高而增多，T-BOX、IOA、智能网关可能都具备联网功能，原则上说它们都可以下一个动态防护方案来进行威胁设备的监测。动态防护方案本质是一个软件，成本主要是开发成本+适配成本，不同设备在部署方案时可能还会有些设备成本，一般也不会很多。

订阅服务主要是基于我们的研究能力进行识别和转

换，我们团队每年都会产出对威胁进行监测、识别和阻断的策略，这可以与我们的动态防护的方案进行关联。同时 360 也有自己的漏洞库和样本库，能提升我们的互联网产品核心竞争力，形成上下必行的制度壁垒。

**Q6: 黑客攻击控制汽车移动我理解是建立在特斯拉这种集中式架构下，车身控制域、自驾域也联网了，才会被攻击，如果我们要提供保护，是不是需要主机厂开放一些算法给我们，这种会开放么，短期内这类产品或者解决方案是不是不会放量？**

**A:** 从智能网联汽车来说，国内和国际上都有必须具备什么安全功能的准入要求，这主要针对的是整车的监测。

**信息安全：**纵深防御。在不同级别上做防御手段，即使第一层破了，第二层也能防御住。作为一个攻击者肯定要从最外面攻击到车内，所以第一层是针对于对外连接这种设备，包括 T-BOX 或者 IVI 车载娱乐的预控。第二层是在不同域之间能转化数据的，如智能网关。第三层是最下面的执行器。目前执行计划也对车载以太网等提出安全要求，相当于整车大部分零件都需要安全功能，这是最基本的，也是纯信息安全的要求。

**数据安全：**前后端业务都会涉及到数据安全，覆盖面非常广。同时，车上涉及数据采集的零部件还又涉及 6 个阶段的全生命周期，每个阶段都可以有一个部署方案，这样一来对每辆车会提出非常多要求，而这只是基本的上市准入要求。

之后国家层面还会陆续有一系列高于法规的信息安全要求提出来，如数字空间碰撞测试就在积极推动中，从而真正抵抗黑客攻击。消费者自身也会有一定的选择



|          |   |
|----------|---|
|          | <p>倾向，如国外比较成熟的信息安全保险。所以从车企到供应商到消费者，整体算下来每辆车的量非常大。</p> <p><b>Q7：车联网产品目前有哪些合作的客户，疫情导致很多车厂停产会对我们造成影响吗？</b></p> <p>A：具体的客户信息不方便透露。在 20 年疫情状态下，我们都还是处于工作状态，一直到现在。我们的策略是产、研、销包括解决方案，我们内部是一个独立的 BU，以这种形式再进行全面的业务开展协同。</p> <p>销售：只在疫情严重地受到影响，其他城市影响不大；研究：基于多年研究设备，环境等储备，研发不受影响；需求：客户预算有一定缩小，但基于车联网安全合规标准出台，整体影响不大。</p> <p><b>Q8：渠道我们是与车机绑定还是找软硬件的 Tier 1 来拓展？</b></p> <p>A：我们对渠道的态度是共赢，希望整个车辆安全构建一个健康的生态。<b>第一</b>，我们要跟 Tier 1 更好地合作，他们有更多的硬件，我们可以从软件上跟他做集成。<b>第二</b>，我们要与合作伙伴共同解决客户的需求，发挥各自优势。<b>第三</b>，360 本身是大公司大品牌，有自己向下的渠道，能很好解决产品交付的情况。<b>第四</b>，我们自己人才资源积累雄厚，包括学生培养、博士生导师等。</p> <p>整体来说，我们的生态建立比较丰富，并不是单纯针对硬件的绑定，同时我们的产品也有自己的独特性，包括集成能力和适配能力都是多年来跟客户一起打磨的。</p> |
| 附件清单（如有） | 无   |
| 日期       | 2022 年 5 月 30 日   |