内容：2014 互联网安全大会演讲

时间：2014 年 9 月 24 日

主题：IoT 时代的大数据安全

非常感谢这么多人来参加中国互联网大会，我虽然经常在台上表演节目，但今天现场有五、六千人，对我来说也是第一次。去年我们办了第一次大会，今天我们办了第二次，我希望这个会议规模能够越办越大，最好能够超过 ChinaJoy，我觉得安全也可以做得不那么严肃，也可以做得很逗比对不对。

其实前一段我干了很多和安全关系不大的事情，因为最近有很多企业都得了一种病，特别是很多传统行业的大佬们，他们都从“瞧不上互联网”变成了“互联网焦虑”，大家都觉得互联网成了一个颠覆的力量，成为了一个价值的毁灭者。所以，我就和他们沟通，讲讲如何理解互联网。最近互联网思维这个词特别热，后来很多骗子也都开始举办互联网思维的讲座，写了各种书，后来我就想要写一本真正讲互联网思维的书。

本来我想送给与会者每人一本的，但因为这本书我要刷榜的，我要把稿费捐给抗战老兵，所以希望大家自己买一本，谢谢大家。

很多人问我互联网思维是什么？如果用一个词总结是什么？**我想了想是在过去的 20 年里互联网最大的力量就是实现了“网聚人的力量”，互联网把我们很多人连接起来。**

在互联网第一代的时候是 PC 互联网，我们每个人的电脑连接起来，这时候安全问题还 OK，当时的防病毒和查杀流氓软件，以及我们很多边界和防火墙的防御技术；但到了互联网的新阶段，我们每个人都用手机了，今天手机已经变成我们每个人手上的一个器官，我们每个人有一种新的病，几分钟不看手机就觉得心里很失落，手机变成了一个新的连接点。手机打破了我们原来对边界的定义，手机更多和我们的个人隐私信息联接在一起，所以，安全的问题变得更加严重。

有一个好消息，也是一个坏消息，手机互联网之后，下一个五到十年我们的互联网将会往何处去？

其实我觉得一个最重要的时代可能要开始那就是 IoT——万物互联。

互联网不仅仅是人和人连接起来，也不仅仅是手机之间的连接，而是互联网能够把今天我们所有能看到、能想到、能碰到的各种各样的设备，大到工厂里的发电机，车床，小到家里的冰箱、插座、灯泡，甚至到每个人身上的戒指、耳环、手表、皮带……所有的东西都连接起来。

过去中国有一个和它相对的概念叫做物联网，但物联网这个概念我不是很喜欢，可能在过去几年里把它更多解释成一个叫做传感器网络，我觉得这个和 IoT 不太一样。

第一，所有的设备，它都会内置一个智能的芯片和内置的智能操作系统。所以你可以看到说所有的东西，实际上都变成了一个“手机”，只不过它的外形不是手机，它可能没有手机的屏幕。举个最简单的例子，如果各位比较喜欢拉风，你开了一辆智能汽车，在我看来您就是骑在一部有四个轮子的大手机上。

第二，所有的设备都通过 3G、4G 的网络，通过 Wi-Fi、蓝牙等各种各样的协议，与互联网、云端 7×24 小时相连，这里面就会产生真正的海量大数据，所以我说大数据时代其实刚刚开始。

过去我们用电脑的时候一天也就用几个小时，这里产生的数据量还是非常有限；手机，除了睡觉的时候，我们基本上都在使用，因此手机的使用时间比电脑时间已经长了很多，而且手机里有各种各样的传感器，大家手机里的信息基本也都被上传到云端。

但我觉得这个数据还不够大，到 IoT 时代这个数据才真正足够大。

比如说电脑，中国可能有五亿台，电脑市场已经不大幅度增长了；手机，中国人有 15 亿，好人拿一部手机就足够了，别有用心的人会拿两到三部手机，这样算下来中国可能有 20 亿部手机，我觉得手机市场也差不多是这样的一个数目。

但如果相对 IoT 来讲，一个人身上可能就有五、六部设备连接互联网，你回到家里，家里所有的智能电器，回家路上开的汽车，所有的东西都连上互联网以后，我估计未来五年内至少有 100 至 200 亿智能设备连接互联网，这个设备的数量会远超过今天我们人口的数目，会远远超过我们现在电脑和手机的数目。

甚至，这些智能设备即便在你睡觉的时候，它也无时不在工作，所以它基本上是 7×24 小时记录和产生数据，而且这些智能设备本地的存储能力一般都比较弱，因为它需要装在各种各样的微小设备里，所以，大量的数据会被传送到云端。

想像一下，比如说有人带了一个手环，这个手环现在不仅提供运动的监测，还能够提供很多参数，可能您在睡觉的时候，它也不断产生数据，所以你把这两个因素结合起来计算，你会发现这是真正的大数据时代。

此外，到了大数据时代，我觉得还有一个可能的变化。

最近美国除了 IoT 很热，还有一个概念很热，就是机器人。其实我理解机器人的背后是机器的人工智能和机器的意识。

传统的机器人工智能的方法，我们教电脑下棋和做电脑翻译，从五十年代这些问题好像一直在解决中，但从来没有找到真正革命性的解决方法。

但最近一年大家可能感觉到了，一些机器学习和智能算法的出现，包括让我们在图像识别，在机器翻译方面都取得了进展，其实它的本质不是说什么算法特别神，而是说这个算法背后实际上是利用了大数据。有了海量数据，再跟这些算法的结合，它可能产生真正的人工智能。

所以，IoT 的第三点很重要的一个概念，将来在云端可能会出现利用大数据之后产生机器的智能，或者我们所称之为的“云脑”和“机器大脑”，让它再反过来对各种设备进行反向控制。这听起来可能既是一个好消息，也可能对安全也会是一个全面的挑战。

对 IoT 来讲，我先讲讲好消息，我觉得这是一个巨大的机会。

首先，对于互联网公司，可以利用 IoT 技术把原来很多线上的设计延展到线下。举个例子，过去 360 做你的电脑卫士，之后我们做你的手机卫士，但现在我们要做路由器，为什么呢？我们要成为你的家庭卫士，因为如果你的家居网络未来被人攻占了，你的家庭局域网出现了问题，可能影响都会比较大。

比如我们利用 IoT 技术，马上会重新发售儿童手表，给每个儿童戴上一个手表，父母可以随时定位知道孩子的位置，根据环境我们可以知道孩子所处的情况，并迅速把他的位置和情况通知给父母，这就是利用 IoT 技术让 360 从过去只是做线上安全走到线下，使 360 也变成可以解决用户人身安全和家居安全的卫士。

但 IoT 更大的机会，我觉得是对中国传统产业，特别是传统制造业的一个机会。用一句俗话说，叫做“重新发明轮子的时代”到了。

人们之前以为很多东西已经走到尽头了，你再怎么发明不可能把轮子从圆的变成方的，但利用 IoT 的技术你可以把轮胎也变成智能的。

其实马航 370 事件，告诉我们，原来一个飞机也可以处在实时监控中；GE 公司过去是卖发动机，现在他们通过 IoT 不仅卖发动机，而且还可以告诉航空公司什么时候该维修，什么时候该换零件，所以，他们把一个卖东西的生意变成了长期服务的生意。

所以，很多 IoT 的技术，我们很多传统企业就不仅仅是说利用互联网来获取信息、发布信息和卖我们的东西，它可以利用 IoT 的技术，可以让自己的产品每个都变成具有互联网体验的产品，它可以让商业模式从一次性买卖的模式变成提供互联网服务的模式。

所以，某种角度意味着 IoT 可以帮助很多企业转型升级，最后所有的企业都会变成互联网企业。IoT 的好处我不多渲染了，我想提出六个问题，请我们所有安全的从业人员来思考，这在安全上对我们意味着什么样的挑战。

顺道说一下，今天我相信来的有很多人可能并不一定都是互联网行业的人，可能有很多是 CIO，其实我倒是觉得未来安全的挑战越大，包括 IoT 和互联网思维的发展，可能会让传统行业的 CIO 的角色变得越来越重要。因为过去你只是一个 Information，你只是一个 IT 的支持，你是为了你公司的核心业务提供帮助，但未来当 IoT 技术变成主导，当互联网思维变成主导之后，你会发现，因为你在单位里对互联网技术的了解、对互联网产业的了解，你可能会从一个支持的角色变成一个主导的角色。另外，随着安全的挑战进一步加大，相信我们很多单位的首席信息官或者首席技术官也会变成首席安全官，所以，我觉得这都是给我们带来巨大的机遇。

但是安全的挑战，我觉得有这么几个问题。

第一，当所有的设备都变成智能化，都接入网络以后，边界的概念将会进一步被削弱，也就是说接入点越多，可以被攻破的这种可能的入口就会越多。过去，我们很信奉“隔离”、“切断”，我们可以把电脑放在一个屋子里，我们可以把一个网络进行隔离，但今天你会发现越来越多的不起眼设备都支持 Wi-Fi 和蓝牙，这里面有太多可以被别人攻击的接入点，而且攻击点越多，对防守的挑战就会越大。

第二，过去我们很多企业可能不太重视企业的安全。我们很多时候买防火墙是为了合规，是上级要求和行业要求。但就像刚才云博士讲到的，那个防火墙究

竟有没有配置好，能起多大的作用并不太知道，可能也不太出事。过去我们企业的发展，可能把自己割裂在一个安全的孤岛上，但你要变成互联网企业之后，你不可避免要把自己的核心业务系统接入到互联网上。

举个例子，过去办银行业务就要到银行的网点和后台服务主机，它可以把所有的环节都进行保护。但今天所有的银行都要提供网上银行、网上支付和互联网金融的业务，那么它就不可能避免的。

当所有的企业都变成互联网企业之后，你的企业安全一定要提高到一个更重要的优先级上，也就是说当你的服务器或你的网络被攻破之后，可能不意味着仅仅是你内部数据的泄露，可能意味着用户数据的灾难。

比如，就是美国一家零售业遭受攻击，有五千万用户的资料丢失，中国有一个企业也发生过用户信用卡密码数据出现的丢失，这对很多企业来说意味着你在安全上的防护级别和对抗能力要前所未有的提高。

第三个问题，大数据污染。就是大数据中如果被人人为加入了这种不好的数据，人为操作和注入修改虚假信息，在数据传输存储过程中出现了问题，你根据大数据做一些行业的指导和趋势的分析，可能会出问题，这个问题今后会进一步阐释。

第四个是这种智能设备 IoT 被控制之后的灾难，这种危害或者会比电脑手机更大。

过去大家都记得，你的电脑中毒了、有问题了，大家最多觉得“今天给老板交的报告写不出来了”，所以我电脑中毒了经常成为工作完不成的一个借口。机出问题了呢，无非你们看到最近多了很多“艳照”，不小心照片上传了；然今天手机和支付系统连在一起，可能当你的通信录被盗用了，就会收到一些诈骗短信。包括前面讲到的那个木马之所以会得逞，就是因为它盗用了你的通信录的地址本，熟人发来的短信，大家都会连接。

但 IoT 是可被控制的，不是一个单纯的网络，这个被控制了带来的风险就大了。

前段时间中国人崇拜完乔布斯之后，因为中国的假乔布斯太多了，他们又开始崇拜美国另外一个人，号称钢铁侠，他造了一部汽车叫做特斯拉，他上次来中国的时候，我有幸和他们大家一起吃了晚餐。我问了一个他很恼怒的问题，我说

你的汽车会被人骇客吗？他说不会，我们所有的应用都是自己写的，我们不会安装任何第三方应用，所以不会有任何问题。我就提了两个问题，第一个你的汽车是有 Wi-Fi 和蓝牙，我可能骇客不了你的汽车，但你用手机接入的话，我可以骇客你的手机，我一样可以通过手机骇客这个汽车。自然你是一个智能汽车，它就像一个大手机一样，一定要和云端通信，所以如果有人下发了你的通信协议或者破解了你的云端的网络，我一样可以控制你的汽车。

我们后来在全国征得了很多有识之士，有人成功破解了对特斯拉的协议，成功实现了对汽车的控制。所以，中国汽车厂要生产智能汽车，我给他们说最重要的不是边开汽车边看互联网影视，最重要的是老百姓敢不敢开你的车，如果半路上突然死机了，突然蓝屏了，突然弹出一个大窗口说你必须下载一个什么玩意儿，这样的汽车不会有人开的，一旦出现问题就会非常的严重。

所以，这是我讲的在 IoT 时代一旦网络被人控制不可设想。我是一个电影迷，我家里有很多好莱坞电影，很多都是网上下的，我记得布鲁斯威利斯在《虎胆龙威》里说过，说恐怖分子控制了美国的电厂，控制了大坝，控制了交通信号灯，当时我看的时候觉得匪夷所思，他们怎么这么傻，这都是专用系统，为什么要接入互联网呢？

但到了 IoT 时代，你发现所有的设备都希望可以远端控制和智能采集数据，这些东西都可以接入互联网。举个小例子，当一个 IT 发烧友把你们家的灯泡、电视、都换成智能的，又装了一个摄像头，变成智能摄像头，如果你们家路由器被人骇客了，我就可以把你家的灯都关到，还可以装上一个摄像机，这何止艳照啊，三级片都出来了。

有很多问题我有没有答案，我只是在安全大会上提出来，我觉得这要靠我们大家共同努力去意识到这些挑战，同时我们来寻找解决的方法。

第五个问题，最近美国机器人很热，坦率说我觉得也是代表了一个趋势，**当大数据产生了人工智能之后很有可能人类技术发展会到达一个新的“奇点”**，当能够控制很多设备的时候，我觉得有两种可能，一种是我们的家庭生活会变得更加幸福，一种是骇客帝国的时代会来临。

所以下次我的 PPT 再做可以多用一些电影的剧照，大家更便于理解。

比如说你以后设想看到的机器人和智能汽车，我有一个断言，它未必是由这个设备里的智能系统单独做智能判断，它一定是和云端一个更大的智能系统相连，比如在你真正的智能驾驶，你何止需要这一部汽车的数据才能做判断，你可能需要路边很多传感器和很多其他汽车发来来的信息，你需要在云端进行高速的分析，再反馈过去。

所以，将来有一天可能不仅仅是这台车上的电脑在指挥，很有可能是云端的一个东西在指挥，所以你看到各种各样无论是专用机器人还是通用机器人，我相信在几年以后也会越来越普及，它都会和互联网相连，这样当真正云端安全出现问题以后，这些自动驾驶汽车，包括有些人觉得《说变形金刚》这个电影完全是瞎扯，我不这么看。比如，现在很多人在研究无人机，亚马逊用无人机送货，无人机加上智能传感器的判断，无人机就是“飞机人”，所以，机器智能带来的转换这是我们下一个五到十年所谓做网络安全的人需要考虑的问题。

第六方面，也是最重要的一个挑战就是对用户隐私的挑战。在这样一个 IoT 和大数据的时代，我们每个人的数据，实际上只要你使用网络服务就会被传到云端，就会被储存到各个提供互联网的企业，不一定是互联网公司，可能是所有的公司都有它的云端数据的收集，每个人会变得更加透明。

这时候我觉得法律和规则的制定是落后的，有很多问题是不清楚的，怎样在这种情况下更好的去保护我们个人的隐私，我可以举两个例子，比如对很多公司来讲，大数据时代是他们梦寐以求的最好的黄金时期，过去做广告都不知道你是谁，不知道你喜欢什么，当然所有的广告效果都很难评估；但今天有了大数据，可以 7×24 小时的不断的采集，这些在云端，当这些数据看起来是碎片，再把它汇总起来，你会发现可能我们每个人就变成了透明人，我们每个人在干什么，在想什么，这时候云端全部都知道，在这种情况下，除非你不用任何先进的设备，除非你不用网络，除非你不用手机，否则的话你怎样解决在这种情况下对个人隐私数据的保护。

比如我们推出了儿童手环，我们第一版做得不是很完美，后来我要求改版，要求他们一定要做到表袋足够短，一定成年人戴不上，因为很多妈妈听说这个消息以后，他们觉得非常兴奋，觉得终于有了保护自己家庭的利器了，他们买了两个，一个给孩子戴，一个给老公戴。

所以，在大数据时代，个人隐私的这种挑战空前大。

美国有一家公司，他说你只要给他的试管吐一口吐沫，就可以免费测出你的基因组。我相信未来测基因一定会成本很低，如果有这样一家免费测基因的公司，他就拿到了大家最隐私的数据，过了二十年以后，他就上门来找你了，说从你的基因看，你就会得老年痴呆症，所以我们给你卖药，他掌握了你很多的最隐私的信息，所有的商业模式就会建立起来，这对公司是一个黄金时代，但对我们个人来说可能每个人都会觉得自己很脆弱。

所以我提出了一个新的想法，在大数据时代，我提出了如何保护用户隐私的三原则。

第一，虽然这些信息储存在不同的服务器上，但你们觉得这些数据的拥有权究竟属于这些公司还是属于用户自己？

我的答案是这些数据应该是用户的资产，这是必须明确的。我希望将来在打很多官司的时候会提出，如同财产所有权一样，个人隐私数据也会有一个所有权，我希望立法能够考虑这个所有权应该属于用户所有，这是第一个原则。

就像当年我很爱看科幻小说，有一个小说家叫阿西诺夫，他提出机器人三原则，他幻想未来机器人遍地跑的时候，机器人如何不伤害人类和破坏人类的文明。到 IoT 时代也需要一个类似的三原则，使得用户数据都在云端的时候，这些公司能够遵循一些更好的原则，给用户提供更好隐私的保护，所以，第一个是个人信息是用户的资产，它只是暂时托管和存放在各个公司的服务器上。

第二，不仅是今天的互联网公司，更不仅仅是今天的网络安全公司，甚至包括更多要进入互联网、要利用 IoT 技术、要给用户提供信息服务的公司来讲，你要有相应的安全能力。

任何企业都需要把收集到的用户数据进行安全存储和安全的传输，这是企业的责任和义务。如果你这个企业没有足够的安全能力，收集了用户的信用卡资料，比如你是一个网店卖东西的，你拿到了用户的帐号，你这些信息的丢失，都会给整个社会带来很灾难的结果。

举个例子，一家网站被拖库，所有的用户口令都要改，因为用户在很多网站上都用一个用户名和一个口令。所以我也讲，可能未来五到十年网络安全的责任不仅仅是我们今天这些安全从业人员的责任，我觉得每一个想做互联网业务的公

司，每一个有用户资料的公司，每一个要把自己的服务摆到互联网上去的公司，都要提升自己的安全能力，提升自己的安全防护水平。你要收集用户的数据，必须要先解决安全可靠的传输存储的基础。

第三，就是使用用户的信息，一定要让用户有知情权，要让用户有选择权，所谓叫做平等交换、授权使用，你不能未经用户的授权就去采集他的信息。

比如今天在手机上有很多数据，有很多应用，它根本和短信毫无关系，它却要把你的短信记录上传到网上，这种就没有让用户有知情权；还有很多用户可以选择说，我不需要你提供这个服务，我可以把它关掉，我可以拒绝你采集我的数据，用户一定要有这种选择权。

事实上像今天，我刚才说的手环业务、智能家电业务和汽车的业务，很多时候用户没有选择，因为当你选用了这样一个智能产品，你在使用它的服务时，它这个服务先天功能的设计就不可避免的把你一些数据会上传，这里面实际上是用户用自己的数据交换了对这种服务使用的可能。这种数据被企业拿到之后，企业可以利用数据做一些对用户的推广，但一定要事先获得用户的授权。如果未经用户授权就对用户的数据泄露，甚至把这种数据卖给别人、利用这种数据牟利，我觉得将来不仅要被视作不道德的行为，而且要看成是非法的行为。

所以有了这三原则，在我们进入 IoT 时代时，我们才能让用户对下一代互联网感觉更放心，才能更好的使用。

最后的结束语也是我开头讲的，未来安全的问题不会被彻底解决掉，随着人类越来越贪婪，越来越懒惰，我们的生活越来越舒服，我们对各种先进技术的使用越来越多，带来一个负面就是对安全的挑战越来越多。

如何解决安全的挑战，需要我们每个人，也需要我们安全行业的公司，更需要我们安全企业各方面的支持。我们大家一起携手未来创造一个安全的互联网，只有安全的互联网才有美好的互联网，所以在互联网上最重要的就是安全第一。

谢谢大家。