

“开源”与“安全”并不冲突

“开源”这个词曾经代表商业软件的掘墓人、代表着 free、代表着全新的软件销售模式，好像在其光辉下，软件行业进入了一个全新的时代，一起以软件为中心的项目都应该向“开源”看齐，仿佛所有与之冲突的软件项目都会被淹没在“开源”浪潮中。那么作为软件业中的信息安全业，是否也要向开源看齐呢？是否也会被淹没在“开源”的洪流中呢？作为信息安全业的佼佼者飞天诚信公司并不这么认为。因为从宏观来讲“经济利益”才是一切商业活动的最终目的，当然软件业也必须遵守这个游戏规则。而信息安全行业的最终目的是保证商家和用户最终的“经济利益”，所以“开源”与“安全”并不冲突。

纵观软件发展史，borland 的崛起与没落、微软的辉煌、SUN 的如日中天，我们不难发现所有的软件销售模式都是围绕利润旋转的。“开源”也只是软件销售模式中一个必然的阶段，但是“安全”却是直接和利润挂钩的。软件最终是要转化为经济利益的，但是在这之前，依然需要“安全”这个环节来保证其最终利益。也就是说，“开源”不等于“免费”，安全问题也不会因为开源而消失。

横向比较国内的几个支柱产业，我们不难发现，随着 IT 技术在中国的发展，已经有了使用开源产品完成政府、金融项目的先例（例如电子政务）。虽然软件开源了，但是这些政府机关和金融机构是不会“开源”的，在完成这些项目的同时依然要考虑安全问题。举例来说，现在很多项目都是基于 JAVA EE 的，JAVA EE 是一个开源产品，但是应用到实际中依然要考虑安全问题，尤其像政府和金融业这种对安全很敏感的机构，他们对安全的要求更高。他们在使用开源产品做项目的同时也用 USBKEY（一种证书的硬件载体，提供了各种公开算法并且防止非法用户访问）来进行安全保护。由此可见，“开源”与“安全”并不冲突。

也许电子政务离我们的生活稍微远了一些，下面讲一个比较贴近生活的例子。众所周知网络支付是一个比较新型的经济模式，网络支付中一个重要环节就是通过网络银行进行支付操作。网络支付的服务程序中很大一部分是采用开源产品进行开发的，并且网络银行就服务程序而言，也有一部分是采用开源产品进行开发的。由于支付过程是直接牵扯经济利益的，所以对通讯安全性的要求相对较高，因而网络银行通常是采用 USBKEY 来进行网络支付的。由于在交易过程中有硬件的参与，使得安全系数大大提高，不仅保证了银行的利益，更主要的是保证了买卖双方的经济利益。而且 USBKEY 非常方便携带，用户无须再向 PC 机上安装麻烦的程序，从而提高了产品易用性。这个事例已经说明了“开源”与“安全”所处的位置不同，因此根本不会有直接的冲突。

以上实例表明“开源”与“安全”并不冲突，因为开源只是降低了开发成本，而最终转化为经济利益的时候依然需要安全的支持。并且在某些方面“开源”会间接的刺激安全产品的销量（如前面提到的网络支付）。但是新的事务总是有两面的，“开源”软件对某些安全产品还是有间接的负面影响。

比如风靡一时的加密锁（一种软件安全硬件，用于防止盗版、保护程序源代码），在“开源”软件的冲击下销量的确有些减少。因为开源软件的价格优势使得很多商业软件不得不做出让步，从而导致加密锁的销量减少，像这种直接以销售为目的的软件的确受到了“开源”的冲击。但是某些商业软件还是加密锁的核心支柱，比如建筑业、医疗业等行业软件是不可能“开源”的，所以加密锁的生存空间还是很广阔的。

总而言之，“开源”与“安全”并不冲突，“开源”只会间接的影响“安全”，但总的来说是向好的方向发展的。