说说工业软件的安全问题

原创 邓子平 多物理场仿真技术

工业软件的安全问题其实不需要多讲，两个大家都知道的例子：

1. 海湾战争期间，美军将电脑病毒放到伊军指挥系统网络，直接干趴了伊军的指挥系统；

2. 美国与以色列的情报机构借助“震网”病毒，黑进核工厂的电脑网络，瘫痪了伊朗的核设施。

这两个例子的软件都属于工业软件中的工业控制软件，即工控软件。

另外电影《虎胆龙威4》，美剧《反恐24小时》里对工业控制软件的描述也很多。

恐怖分子可以通过黑客技术接管海底隧道交通信号灯，人为制造交通事故；通过黑客技术远程夺取核电站和天然气管道控制权，制造核泄露，爆炸，释放病毒等各种恐怖活动。

工控软件安全问题是一个国家信息安全的重中之重。我们今天讲的还是工业设计和仿真软件的安全问题，安全级别没有那么高，但是有些问题还是值得我们思考。

从Solidworks泄密事件说起

这是大概2010年发生的事情，事情一度闹到国家相关部门通知各军工企业停止使用该软件，以防止信息泄密。事情爆出来后，Solidworks在官方微博上发布声明称：“Solidworks合法授权软件不存在未经 客户许可提供机密客户数据的机制。

其实这个问题可以从好几个方面来看：

1.一般的商业软件原则上是不会窃取用户机密数据的，因为这种做法无疑是给自己挖坑：首先窃取用户机密数据非常容易被发现，随便一个安全软件都能检测出这种行为；其次软件厂商的目的是赚钱，如果被发现抓取机密数据，那几乎不会有用户再用这种软件；最后如果是军工企业泄密，那是非常严重的国家“安全事件”，国内外没有那个软件厂商有胆子干这种事。

2.软件厂商确实会抓取用户数据。这是现在很多软件做的事情，主要目的还是为了防盗版。有些软件会把软件的版本号，License相关信息通过网络传回公司分析，发现如果有盗版用户，定位盗版软件用户性质，规模等等。最有名的当属国外三维软件公司某克，其法务部有专门的团队，日常工作就是给盗版用户发律师函，然后收钱。

3.这里存在一个灰色地带，那就是如何定位用户机密数据。用户的电脑主机名，硬件配置，操作系统等等，这些信息对普通用户来讲，可能无足轻重，但是对于某些企业可能就非常敏感，比如通过电脑配置，机器运算时间，数量，就可以推断出企业规模，工作性质，甚至工作内容。

4.软件留“后门”是一种普遍现象，“后门”几乎无法被破解或找到，通过“后门”可以在用户机器上做很多事情。软件厂商给软件留“后门”在关键时刻能排上用场，不详聊。这个就好比核武器，可能永远无法使用，但必须得有。

5.普通用户如何避免“泄密”，最简单的就是不用盗版软件。首先盗版软件可能被二次加壳；再者如果使用盗版，相关信息很容易被原厂知道。另外就是物理断网或者使用沙盒，这是目前最安全的做法。

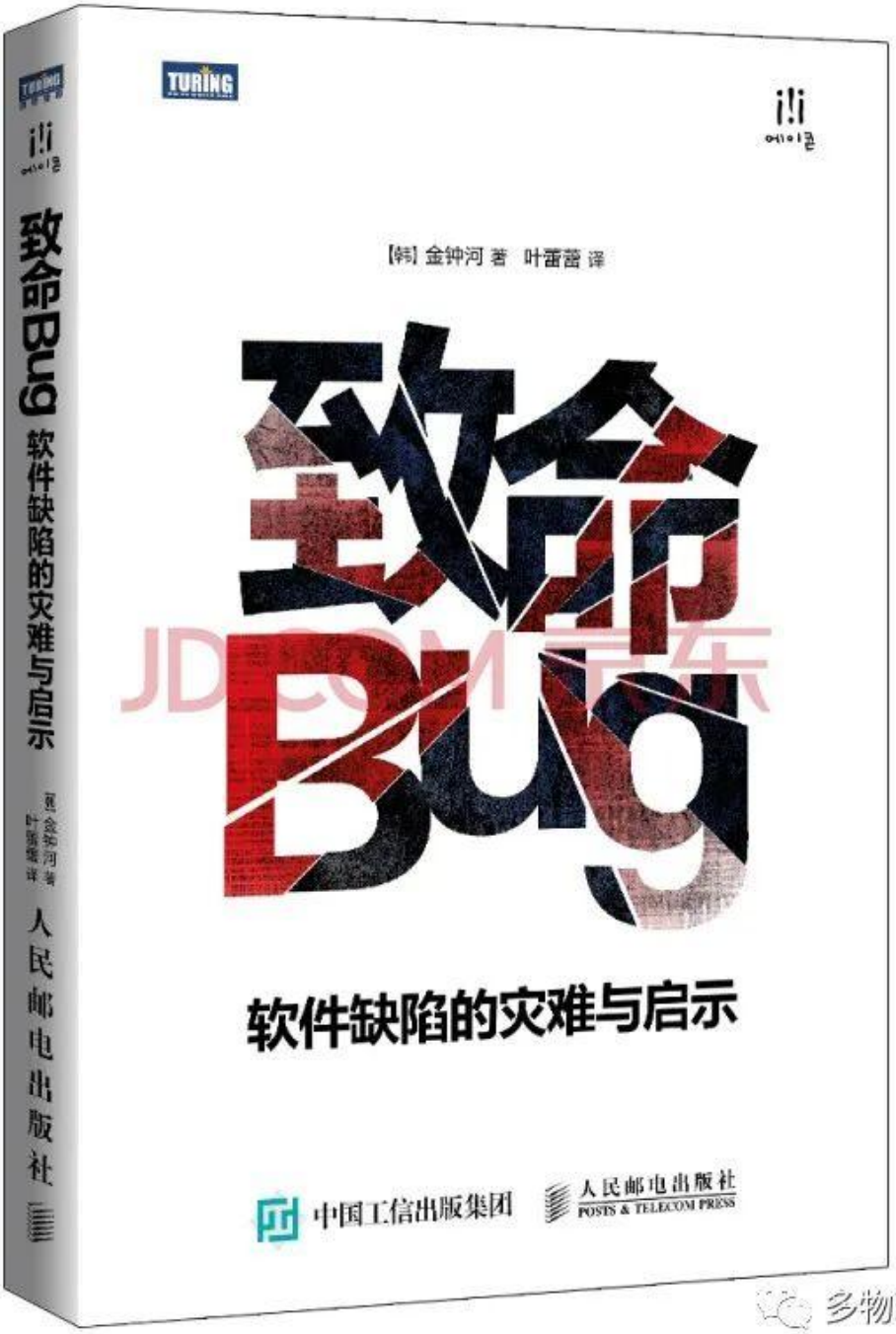
总之，从安全角度讲，工业软件，不管是工控，还是设计仿真软件，主动权还是要掌握在自己手里，因为我们不清楚别人的软件“后门”里放了什么东西，或者拿我们的信息做怎样的事情。就好比某信，今天刚电话聊完家里的电视坏了，第二天就推送电视机广告给我。

从软件开发角度看，软件的版权和使用权确实需要保护。一方面国家要加大对盗版的打击和惩罚力度，另一方面软件厂商也可以适当使用一些保护措施，但是要尽可能避免获取用户信息，最简单的做法就是使用加密狗，简单高效。虽然加密狗也可以破解，但是难度比一般的破解要大很多。

说到安全，不得不提到另外一个问题：代码安全

之前在 我所理解的“工业软件” 一文中提到了 阿丽亚娜5发射失败坠毁，阿丽亚娜4号往SRI输入的是16位整数数据，阿丽亚娜5号往SRI输入的是64位浮点数数据，数据转换时溢出。

这类安全事件可以归纳到系统工程：即在一个超大的项目里，如何保证整体上可控可靠，又要避免细节局部上的问题导致整体上的致命错误。这只能通过一系列严格的制度流程来保证，之前多有描述，后续还会就工业软件研发领域的系统工程做更多的探讨。


TURING
致命Bug
软件缺陷的灾难与启示
[韩] 金钟河 著
叶雷蕾 译
致命
Bug
软件缺陷的灾难与启示
中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS
人民邮电出版社