揭开加密解密未来的神秘面纱——看雪软件安全网站创始人段钢谈加密解密技术的发展趋势...

转载

weixin_34194359 于 2009-02-06 10:36:07 发布 39 收藏
文章标签： 运维
原文链接：http://blog.51cto.com/broadviewsec/128890

软件的加密与解密是矛与盾的关系，是互为因果的辩证统一，它们是在不断的对抗中发展和进步的。软件加解密技术，同样也是逆向工程和反逆向工程技术的争斗。软件“逆向工程”在什么情况下合法、什么情况下非法，国内外尚无定论，我国尚无明确的法律规定。一般认为，作为个人学习研究，而不将自己的成果公开或应用于商业用途，与我国现行法律或行政法规不冲突。技术的较量，是永无止境的，正是这个特点，才促成了技术的不断进步。因而，研究软件加密与解密技术，对大家来说，都是会从中受益的。

未来的安全技术发展，必定是多重安全措施的综合应用。对于解释性语言或平台，如VB、VFP等，主要是防止反编译。谈到解释语言，不得不关注一下微软的.NET平台。由于.NET的架构和设计理念，反编译.NET程序很容易获得源码，而.NET是微软的一个重要战略步骤，越来越多的企业已经在.NET平台上开发自己的产品，因此，摆在企业和.NET程序员面前一个迫切需要解决的问题，就是.NET安全性！

对于本地编译的程序，如VC、DELPHI等，一般人大都认为不容易被逆向，其实不然，现在逆向技术较前几年更普及，逆向工具和水平都有个质的提高。现在一位技术熟练的逆向人员，对VC编译的程序，一天就能还原C源代码几百行，更况且现有的一些工具可以完全将C转换成源码（虽可读性还需要加强）。这样的现实，已经让一些软件商的核心技术被他人成功借鉴。针对逆向技术的发展，软件保护技术也从最初的简单反跟踪，发展到变形技术和虚拟机保护，其核心思想就是将每条汇编指令变形或用虚拟机代码来实现，这样最大可能地防止被反编译或提高对手反编译的时间成本。

看雪安全网站是2000年创建的。那段时间，软件安全是技术人员很关注的一个主题，我本人对这个主题很感兴趣。但当时苦于网上缺少这方面的交流空间，所以就自己动手建立了这个站点。这些年来，我和一些志同道合的朋友一直在努力坚持网站的纯技术发展方向和非商业化模式。我们认为，大家在一起，有机会做自己感兴趣的事，才是最快乐的。

本文主要内容整理自看雪软件安全网站创始人段钢先生在 **2008中国软件安全峰会** 上的演讲。