1.软件驱动业务模式的发展

随着硬件产品的标准化和市场竞争，不仅仅是 PC 端，一些特定领域的大型设备也开始以软件驱动产生增值利润。另外，云计算的兴起使得面向企业销售的业务软件开始被客户部署在云计算的基础设施上，这大大降低了部署的成本和维护所需要的人力。于此同时，因为软件的可复制性以及分销管理的不可控制，软件保护和授权问题也威胁着软件供应商的收益。

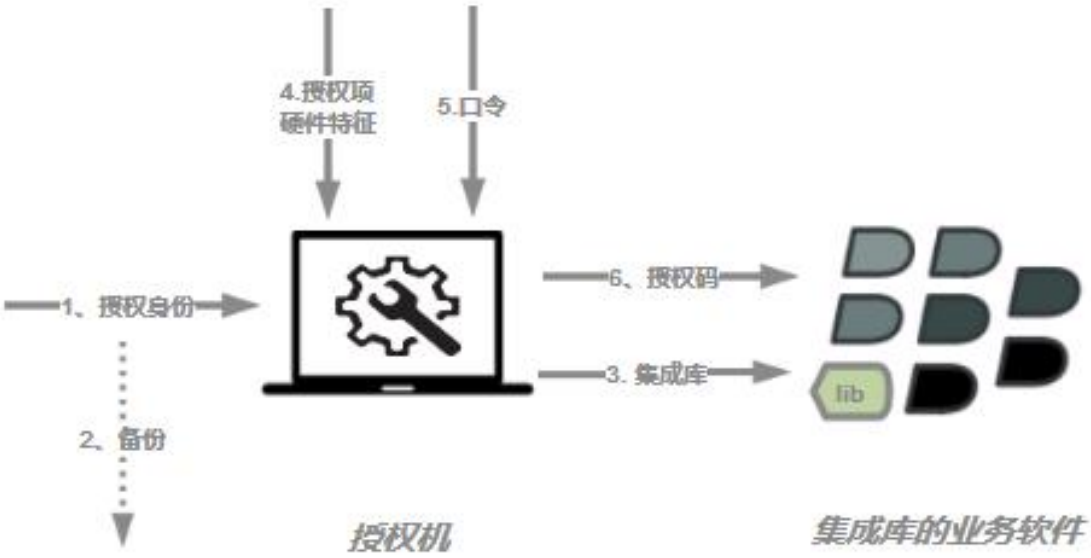
传统的软件供应商往往采购标准的授权保护套件，比如加密狗，从而可以专心聚焦于业务开发和销售。除了本身一些低价加密狗的不安全性之外，基于硬件的授权保护机制使用往往非常复杂，影响用户体验，用户希望即开即用，而无需时刻关注硬件的安装和管理。另外一方面，新的软件驱动模式并不适合硬件的授权方案，比如云端软件并没有物理接口可供部署。一些大型设备也没有通用的接口适配加密硬件产品。

2.现有的软件解决方案

一般的，软件供应商往往在业务软件上自行添加授权保护机制。实现一个抗攻击的授权机制并非如想象般简单，往往在一些著名的逆向网站上，这些软件供应商的软件都会被当做逆向工程师炫耀技术的机会。而一些高价值软件对于内部员工的作弊诱惑也在考验着组织的管理水平。市场需要一种通用灵活的软件安全机制，以便减少软件供应商的研发和管理成本，提高安全机制的健壮性。

3.NELDTV 的软件保护和授权机制

NELDTV 提供的通用软件保护和授权方案适用这些场景的高安全健壮方案。方案基于公钥机制和加密机制，且对待被集成的库和接口被进行了特殊的加固设计，以便增加逆向的难度，具有很高的安全性。



方案由授权机和集成库两部分组成。授权机是一台任意普通的电脑，上运行有跨平台的授权软件。授权软件是带 GUI 的，初次使用可以生成授权身份和集成库，被口令加密的授权身份和授权项目用于生成业务软件的授权码。没有授权码，集成库的业务软件无法正常工作。

集成库被集成到业务软件中，接口的验证被用于执行软件保护和授权机制校验。

NELDTV 的软件保护和授权机制有如下优势特征：

- 支持硬件绑定。比如连接的设备或者服务器。授权码对硬件组或者单个硬件进行绑定，比如只允许业务软件安装在指定的设备上，且只能跟指定的大型设备通信。
- 授权行为控制。只允许持有授权机上授权身份解密口令的人才可以生成授权码。当授权身份万一丢失，则需要重新生成授权身份并更新集成库。

- 可任意扩展的授权权限项目。在授权码生成上，可以写入任意自定义的授权项目，比如使用生效时间，安装台数，业务软件模块功能限制等。
- 支持 java 和 VB6 平台集成库。

4.NELDTV 软件保护和授权机制方案的安全性

任何授权方案都不是 100%安全的，黑客在充足的时间和成本下可以破解任何系统。我们方案的安全模型在如下假设前提下是安全的。

1) 程序运行逻辑无法更改，尽管逻辑可能被分析

方案可以应对反编译逻辑分析；

方案不能应对程序重打包技术，在充分逆向理解方案的前提下，可能通过重打包技术绕过业务的部分校验逻辑，尽管我们提高了逆向所需要的时间复杂度；

方案不能应对源代码泄露造成业务软件被克隆 ,如开发人员的源代码泄露无法被我们的方案保护。

2) 内存是安全的，无法更改，尽管可能被窥探

方案不能应付 OS 系统侧的部分攻击，如专门的 rootkit 系统，应用的一些调用过程尤其是业务自定义设计的权限校验过程可能被 hook 掉。

3) 安装绑定的机器设备信息无法被克隆

方案会尽可能的绑定设备信息，但无法完全避免绑定的机器特性被克隆，被克隆后克隆的机器将可以执行与原授权机器一样的权限，造成绑定设备失败

4) 高安全的代码质量

方案安全假设在校验过程中不存在安全代码 0-day 漏洞。

5.业务软件集成方案

5.1 针对小型软件供应商

对于小型软件供应商，只需要集成 NELDTV 提供的库和接口即可，授权码和集成库生成由 NELDTV 维护。客户需要向我们提交授权码申请。

5.2 针对中大型软件供应商

提供完全的透明的交钥匙服务。在 NDA 签署后，所有的代码都是开源的，并支持对授权软件使用和授权项目设计的培训，支持 1 年的服务支持和代码升级同步服务。