白盒安全通道技术有效保护密钥

软件保护需要加密，加密需要算法，算法需要密钥，密钥需要白盒来保护。

软件破解的威胁:加密狗仿真

仿真器是软件组件

目的是代替加密狗——重放与加密狗的通讯或模拟它的行为

两种类型的仿真器：

部分仿真（重放仿真）——与真实加密狗之间的通讯被记录（中间人攻击），然后在加密狗不存在时进行重放

完全仿真——仿真器能够解析调用并模拟功能，比如说内存的读写，许可的验证，在某些情况下甚至是加密功能

安全通道的重要性

在应用程序和加密狗之间传递的数据是加密的——使用一个加密密钥和一个随机的会话 ID

这使得记录通过安全通道传递的数据变得不可能——会话之间的数据不能被重放

包计数器——保证在相同的会话中不能重放数据

多数加密狗通过实施在被保护的应用程序和加密狗之间的安全通讯来规避仿真器

常见的安全通道弱点

如果安全通道被打破，破解者就能够创建一个可工作的仿真器。

纯仿真——突破安全通道（找到加密密钥）就足以使破解者构建一个仿真器，通过它可以看到通过通道的明文数据，使得它能够支持多个版本并处理动态/随机数据。被保护的二进制可以保持不变。

仿真+可执行的补丁——当加密密钥不能被抽取时需要。通过对随机的会话 ID 打补丁能够突破特定的版本。不能提供对随机和动态数据的通用版本。需要破解者花费更多的精力。

专注信息安全 共享安全策略 服务专享：400 600 9103 ©2015 SafePloy.com All rights reserved.

白盒安全通道介绍

以前的软件保护技术中，安全算法通常会在攻击者的眼皮底下执行，程序产生密钥，没有黑盒保护密钥，因此应用程序的执行可一步一步地监视，所有访问过的数据均为可见。为了更好地保护密钥不受损害，我们需要采用一种不同的方法--白盒技术。白盒解决方案假定攻击者拥有完全的可见性，用专门的应用程序库取代了暴露的算法和软件保护密钥，可尽量减少攻击面。这种方法保证受到保护的密钥保持隐蔽，以免受到黑客攻击，并在攻击期间比较不容易被重建。

根据动态安全性的理念，在设计保护的时候，要考虑到安全保护有可能被破解掉，需要考破解掉以后的策略，就要对软件的生命周期进行监督观察，发现攻击行为后采取一定手段，在短时间内使得软件恢复保护，使得加密安全性更新，商业版权模式才能得以继续，ISV 的合法权益受到有效保护，因此新的白盒技术正是建立在密钥保护基础上，将密钥进行打散，也使得 USB 无驱成为可能。

无驱是调用系统的 HID。USB HID 类设备属于人机交互操作的设备，用于控制计算机操作的一些方面，如 USB 鼠标、USB 键盘、USB 游戏操纵杆、USB 触摸板、USB 轨迹球、电话拨号设备、VCR 遥控等等设备。另外，使用 HID 设备的一个好处就是，操作系统自带了 HID 类的驱动程序，而用户无需去开发很麻烦的驱动程序，只要直接使用 API 调用即可完成通信。目前，超级狗支持无驱，LDK7.0 也支持，不过需要先进行无驱写入操作。

上层应用程序和加密锁进行通讯，黑客去监听加密锁通讯，用来返回加密值，破解加解密的密钥，从而得到数据，整个安全体系出现风险，黑客破解的主要手段采用仿真器技术。仿真器是软件组件，目的是代替加密狗，以重放与加密狗的通讯或模拟它的行为。两种类型的仿真器：部分仿真（重放仿真），与真实加密狗之间的通讯被记录（中间人攻击），然后的加密狗不存在时进行重放。完全仿真：仿真其能够解析调用并模拟功能，比如说内存的读写，许可的验证，在某些情况下甚至是加密功能。

专注信息安全 共享安全策略 服务专享：400 600 9103 ©2015 SafePloy.com All rights reserved.

软件和底层数据库沟通，会用到一些加密信息，进行数据加密。举个例子：聊天软件的记录通过加密存放在本地，这个过程包含软件本身，黑客破解了加密、解密的过程，能拿到整个聊天数据。如何保证软件算法的安全？在应用软件和加密锁之间建立安全通道的方法，通过随机混发密钥和一个独立混发密钥来保护，会有随机性，使得每一次传递不一样，很难产生一个密码表，得到真正的数据。

安全通道机制是通过实施在被保护的应用程序和加密狗之间的安全通讯来规避仿真器。在应用程序和加密狗之间传递的数据是加密的，使用一个加密密钥和一个随机的会话 ID，这使得记录通过安全通道传递的数据变得不可能，会话之间的数据不能被重放。包计数器，也保证在相同的会话中不能重放数据。

如果安全通道被打破，破解者就能够创建一个可工作的仿真器。一旦黑客有机会得到密钥，还是有机会获取相关信息。纯仿真，突破安全通道（找到加密密钥）就足以使破解者构建一个仿真器，通过它可以看到通过通道的明文数据，使得它能够支持多个版本并处理动态/随机数据。仿真加可执行的补丁，当加密密钥不能被抽取时需要。通过对随机的会话 ID 打补丁能够突破特定的版本，不能提供对随机和动态数据的通用版本。

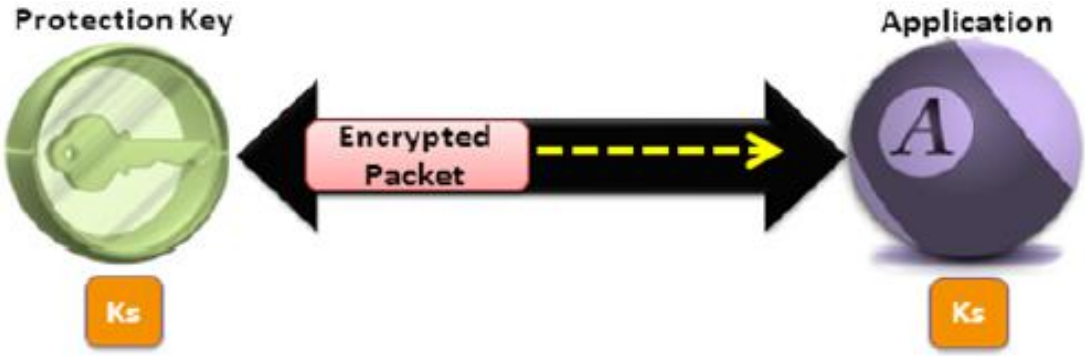
安全通道的实施过程：

密钥 Kh 在制造过程中被编程至加密狗，密钥 Ka 被安全地嵌入至应用程序的 API 库。为了使每个会话都有区别，使用一个随机的会话 ID(RND)，应用程序设置 RND 同时使用它+Ka 来认证加密狗并对会话密钥 Ks 达成一致。

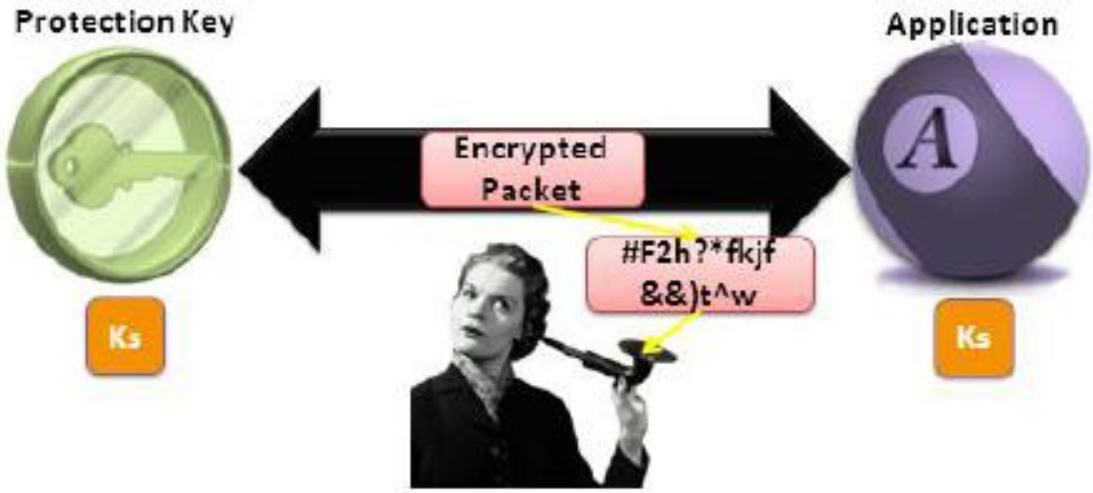
现在应用程序和加密狗都知道会话密钥 Ks.

专注信息安全 共享安全策略 服务专享：400 600 9103 ©2015 SafePloy.com All rights reserved.

双方使用这个信息来加密传输的数据包。



企图偷听安全通道中的通讯是没有意义的，数据是被完全加密的，从而对抗中间人攻击（MITM）。



如果攻击者从应用程序中提取 Ks 密钥，黑客找到 Ks 密钥那么就可以反向解析，得到明文，在上层程序要考虑这个问题。如果密钥不被泄露，那么整个安全体系就是安全的。我们要做的事情是密钥隐藏，存在加密锁里，整个加解密都在加密锁里完成，那么就实现安全性。

专注信息安全 共享安全策略 服务专享：400 600 9103 ©2015 SafePloy.com All rights reserved.

对于密码技术，在典型的 DRM（数字版权保护）应用中，加密算法安全解决方案的一部分采用的就是知名的强力算法，主要依赖于密钥的隐蔽性。在大多数情况下，这非常不合适，因为很多应用程序平台容易被潜在恶意终端用户所控制，黑客能够在你的执行过程中观察，监听相关的通讯。

传统密码学是假设建立一个黑盒方案，假定攻击者无法获得密钥，只能控制加密输入（明文），获取加密输出（密文）。很长时间以来人们误认为这是正确的，这包括了智能卡这样的硬件设备。黑盒方案认为攻击者并未实质性地接触到密钥（执行加密或者解密的算法）或者任何内部操作，仅仅能观察到一些外部信息或者操作。这些信息包括系统内的明文（输入）或者密文（输出），并且认为代码执行以及动态加密不可被观察。

但是，利用从黑盒（例如差分功耗分析 Differential Power Analysis 攻击，也称为 DPA）中泄露的信息进行恶意攻击的方法已经获得长足发展，黑客们可以计算出黑盒中使用的密钥。这种方法可使黑客们进行有效的非黑盒攻击，结果是将这些应用变为“灰色的阴影”，而不再是“黑色”。

事实上，一些标准密码模式假设终点、PC、硬件保护令牌等是可以信任的。如果这些终点存在于一个潜在的恶意环境中，那么当黑客们能够直接监测应用程序运行、尝试从内存中提取内置的或由应用程序生成的密钥时，密钥对黑客们来说就是透明可见的了。这对在 PC、IPTV 机顶盒及其它数据使用设备上运行的、采用 DRM 的基于软件的应用程序来说是非常常见的问题。通过主动监测标准密码的应用程序或者内存，一些黑客就能随时提取密钥。举一个加密失败的案例：一次基于内存的密码提取攻击，使 Backup HD DVD 工具复制了一个受保护 DVD 里面的内容，并将 DRM 从受保护的 Windows 媒介内容中删除。

白盒密码技术充分考虑其应用环境会被控制被观察这一因素，能够在一个完全透明的环境中运行，同时将一些有价值的信息如许可证以及其它商业秘密隐藏起来，而不直接暴露任何密钥或数据的情况下加密或解密内容，即使在黑客能够

专注信息安全 共享安全策略 服务专享：400 600 9103 ©2015 SafePloy.com All rights reserved.

在你的执行过程中观察或者更改代码时仍执行强力加密机制，这就是白盒密码技术带来更高的安全性，值得注意的是，在设计密钥时要将密钥保存在加密锁里来实现。

关于 SafePloy：

安策科技（上海）有限公司（SafePloy）是一家专注于信息安全领域的企业，其是由旺财信息、闪电信息合并而成，在北京、青岛、南京、深圳、香港均有分支结构。公司致力成为**软件商品化解决方案、身份认证及访问控制解决方案以及企业数据加密解决方案**等专业领域的安全服务提供商。经过 10 多年的努力与发展，安策科技已在许多行业获得了信息安全策略部署经验，从企业的信息化应用需求入手，到实际问题的解决部署，再到使用过程中的数据维护保全，以及持续使用风险预测等各个环节都有一支专业、合规的团队提供服务。

公司目前与国际知名信息安全厂商 Gemalto-SafeNet 达成战略合作，是其国内总代理及总服务承包商。

关于 SafePloy 软件保护服务：

安策科技专业的软件保护服务团队可以帮助您规划和实施符合您需要的软件保护策略、许可授权管理和权限管理解决方案，让您能够在最优时间范围内充分实现软件业务安全需求，充分让您的软件产品货币化，保障软件产品在各生命周期中能构建完整的保护解决方案。

安策科技融合常用的硬件加密锁，软锁，云授权等加密产品，为本地及虚拟化的软件提供定制或者专门的授权管理，确保您的软件中内嵌的算法、商业机密和专门知识不被黑客获取。

安策科技与国际知名信息安全厂商 Gemalto-SafeNet 建立了战略合作，是其在中国地区总服务商。

市场联系：

陈汀 女士
商务 经理
电话：021 5464 0133 - 809
传真：021 3363 4530
手机：136 2185 6110
Email：chen.ting@safeploy.com

张亦鹏 先生
技术 经理
电话：021 5464 0133 - 806
传真：021 3363 4530
手机：139 1744 7500
Email：zhang.yipeng@safeploy.com

 ©2015 SafePloy.com All rights reserved.

更多软件保护资源服务请访问：http://www.safeploy.com/Class/softmonization/

专注信息安全 共享安全策略 服务专享：400 600 9103 ©2015 SafePloy.com All rights reserved.