圣天诺 HASP(LDK) Envelope

白皮书 (外壳保护技术)

目录

软件盗版现象日益泛滥，因为难于确定其真实源头并且很难消除，使其成为全球关注的一个问题。软件发行商经常要面对互联网上对其应用程序的非法复制问题，最终导致公司收益损失。

执行摘要

在当今计算环境下，软件发行商所面临的一个复杂问题是如何避免对其软件的非法使用，同时又不会对合法购买并使用软件的客户造成不必要的障碍。在采用新技术和未许可和黑客破解副本数量之间有一个直接相关性。互联网对该现象也有显著影响，因为它提供了一个开放的平台，消除了国家界限、语言障碍和其他障碍，从而让用户可以方便地获取信息。

包括多种类型的破解软件许可/硬件许可以及未实施升级的软件盗版问题会减少收益，伤害已有的付费客户，最终会由这些客户承担非法产品使用的成本。软件盗版也会影响竞争力，导致高价但不够先进的产品，最终对整个流程造成损害。

软件盗版现象日益泛滥，因为难于确定其真实源头并且很难消除，使其成为全球关注的一个问题。软件发行商经常要面对互联网上其应用程序的非法复制问题，最终导致公司收益损失。那些使用某种许可方案提前对其软件进行保护的软件发行商往往并不能针对日益增长的破解程序而对其软件提供全面保护，这些黑客破解程序会破坏其应用程序安全定和许可机制。

本文研究了多种可用的反攻击方法，这些方法作为圣天诺 HASP Envelope 机制的一部分可以保护应用程序免遭盗版。

评估一套基于硬件的保护系统

对基于硬件的保护密钥进行破解是一件费时费力且代价高昂的事情，从潜在“投资收益”角度（例如所花费时间和收入）分析来说，破解成果与破解的者所付出的精力并不相当。黑客往往倾向于选择最容易的途径，会尽量避免长时间调试和繁琐的代码检查以生成一个完全可用的通用黑客程序。黑客常常会选择创建一个通用黑客程序——一个适用于受特定制造商硬件密钥保护的所有应用程序的通用程序。如果未能创建这样一个黑客程序的话，黑客会转向下一个可行任务，创建一个针对特定应用程序的黑客程序，例如一个只适用于单个应用程序的黑客程序。当然，他们需要对每个想要破解的应用程序重复此流程，但是这对于那些决定从该应用程序破解版本牟利的黑客来说这并不是什么阻碍。相应地，有必要对基于软件的安全功能和基于硬件的解决方案进行持续改进以确保其良好的防破解效果。

业界一个最常见的误解是一旦使用某种许可保护方式对特定应用程序进行保护和分配的话，那么就可以一劳永逸地彻底消除软件盗版问题了。独立软件供应商（ISV）有必要与许可供应商/硬件制造商合作继续更新并改进安全水平。通过整合创新的反黑客技术，软件供应商（ISV）可以一直保持在软件反盗版前沿。

圣天诺 HASP Envelope 保护方法

该系统包括一个基于加密的硬件保护密钥和支持基于软件保护的工具。只有在将硬件密钥插入到程序安装计算机后才能运行圣天诺 HASP 保护下的应用程序。

当使用圣天诺 HASP、圣天诺 HASP Run-Time API 和圣天诺 HASP Envelope 保护应用程序安全时可以选择两种保护方法。为了实现最高的安全和保护水平，建议整合使用两种方法。圣天诺 HASP Run-Time API 是一组链接到应用程序包的库，在应用程序开发阶段圣天诺 HASP 软件工具也会应用该库。通过使用 API 实现的保护要求更改源代码，允许在整个应用程序中定址对圣天诺 HASP HL 密钥的呼叫。为了实

圣天诺 Envelope 功能和益处

- 自动文件伪装 – 提供强有效保护，通过文件加密和源代码模糊处理来保护软件免受逆向工程破解。
- 重新连接应用程序和硬件 – 通过一种保护密钥方式将应用程序紧密地与硬件连接起来。
- 安全的通信渠道 – 圣天诺 HASP 可以通过在受保护应用程序和保护密钥之间提供一个安全的沟通渠道来消除中间人攻击。Java Envelope 使用此功能避免拦截通信数据从而获取保护密钥所发回的访问数据。
- 运行时间解密 – 因为圣天诺 HASP 可以在运行时间请求时（而非一次将所有.class 文件都载入到虚拟机中）对文件加密，所以它可以避免黑客重建整个应用程序。

现最高水平安全和保护，在软件开发流程之前和过程中要仔细考虑做出规划，从开始就整合圣天诺 HASP HL。与圣天诺 HASP Envelope 相比，整合圣天诺 HASP Run-Time API 是一项劳动密集型的人工操作程序，需要在整个开发阶段内做出详细规划。圣天诺 HASP Envelope 是一套开箱即用型（按钮开关）自动保护工具，可以部署在可执行文件、DLL、OCX 或其他 PE 格式的应用程序文件中，这种部署工作可以在应用程序就绪并全面测试后马上实施。

圣天诺 HASP Envelope

圣天诺 HASP Envelope 是一套自动文件伪装程序，该程序可以提供强有效的知识产权（IP）保护，通过文件加密、代码模糊处理和系统水平的反调试功能避免软件被逆向工程攻击。这可以确保软件中内置的算法、交易秘密和专业技术信息集是安全的，不会被黑客破解。软件解决方案不仅包括可执行文件和 DLL，也包括比软件应用程序本身更有价值的数据文件。在很多情况下，这些数据文件中包含高度敏感的信息和知识产权，这些都是必须要避免泄漏或丢失的重要资产。

为了保护数据文件安全，圣天诺 HASP Envelope 和 DataHASP 工具会对应用程序进行伪装，加密并控制对软件数据文件的访问，这样只有授权用户和主机托管软件才能解密并访问该文件。只需轻点一下按钮即可实现对整个产品套件的定义安全性和访问控制水平。圣天诺 HASP ToolBox 是一套基于 GUI 的应用程序，该程序可以帮你熟悉圣天诺 HASP Run-time API 并生成您软件源代码的包含代码。

圣天诺 HASP Envelope 通过添加一层保护盾来保护您应用程序的安全，该保护盾可以将应用程序与圣天诺 HASP HL 密钥结合起来，加密应用程序文件、管理并跟踪密钥中保存的许可信息，并引入多个圣天诺 HASP API 中所不能提供的盗版障碍。

载入应用程序后，Envelope 会向圣天诺 HASP HL 密钥发送一个查询信息，验证其与电脑的物理连接情况。如果专用的圣天诺 HASP HL 密钥与电脑连接在一起的话，Envelope 会使用圣天诺 HASP HL 加密引擎对应用程序文件（此前由开发人员加密）进行解密。如果未连接圣天诺 HASP HL 密钥的话，应用程序会中止并且不能运行。

一次点击的易用型解决方案

使用圣天诺 HASP Envelope 进行保护是一项只需短短几秒钟就能实现的程序（假设选择了默认保护框架）。如果采取了额外步骤和措施以使用一些或全部可用选项的话，程序时间就会稍微延长一些，为软件供应商（不能访问应用程序源代码）提供一个极其强大的平台。例如，销售不受保护软件的经销商会使用基本的默认 Envelope 设置以在其本地市场范围内保护产品，这是一个简单快速的程序。

因为使用必须在开发阶段早期完成圣天诺 HASP Run-Time API 的定址保护，Envelope 提供了一个简单的开箱即用型选择。一旦完成了开发并且应用程序可执行文件就绪后，就可以使用圣天诺 HASP Envelope 快速地应用另一个重要且极其强大的保护层，而不会对实际应用程序造成影响。

Enveloping（封装操作）组合了加密和源代码模糊处理功能，可以提供当今最强的知识产权保护水平。通过使用圣天诺 HASP Envelope 解决方案，您可以获得enveloping（封装操作）的优势，无需花时间和精力去从头开发一套解决方案。

对圣天诺 HASP 硬件密钥多个不强迫的呼叫

除了在运行时间所执行的多种任务之外，Envelope 也负责在整个软件运行时间检查圣天诺 HASP HL 密钥是否都连接到电脑上。因为 Envelope 是被使用在一个编译文件中，对圣天诺 HASP HL 密钥的呼叫不会被整合在这些应用程序代码中。会通过被添加到应用程序文件的保护代码定期执行这些操作。圣天诺 HASP HL 密钥检查的时间间隔是开发人员在保护阶段过程中完全可配置的 Envelope 参数。对密钥的每次呼叫都会使用圣天诺 HASP HL 硬件加密引擎，发送一条加密字符串。系统会对返回的解密字符串进行分析以确认密钥的存在。加密和解密机制都使用 AES128 位加密引擎，确保双路通信渠道都是完全安全的。

您知识产权和技术信息集的安全性

开发您产品所花费的时间和资源最终都要依靠提供高品质最终产品和满足市场需求来获得收益，因此必须避免产品被破解。

圣天诺 HASP Envelope 的加密特定功能是最重要的品质之一，允许对部分或整个应用程序文件进行加密，确保您的源代码不会被破解。对于那些寄希望于更改您的代码以利用您的应用程序获取个人利益的情形来说，这是非常有用的。此外，这在避免您的竞争对手了解您的专业机密和技术信息集方面也是非常有价值的。圣天诺 HASP Envelope 可以避免行业间谍刺探危害，从而保持您的竞争优势。

通过自动伪装文件并使用代码模糊处理，Envelope 提供了强有效的反逆向工程加密功能，保护您有价值的算法和专业机密。圣天诺 HASP Envelope 可以执行复杂的加密处理以隐藏您的源代码。每个用圣天诺 HASP Envelope 加密的文件都使用一个不同的随机种子进行加密，从而在保护后生成非常不同的文件，即使原始文件是相同的也会生成不同的文件。应用程序文件会被分成多个块，这些块是可以规模放缩的并且可以由开发人员在保护会话过程中预先确定。每个块都使用 128 位基于 AES 的加密引擎和不同的随机种子进行加密。

多层盾——最弱点安全性

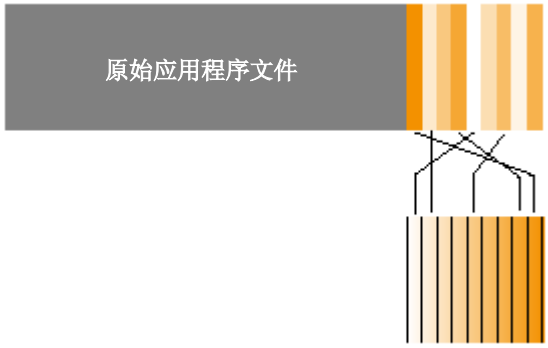
用任何伪装机制保护的应用程序的最弱点是应用程序和外部添加保护代码之间的结合处。如果这个点被废除的话，会断开与硬件密钥的链接，让应用程序完全处理未保护状态。因此，这也是多数攻击者尝试发起攻击的点。黑客会研究受保护文件，分析保护代码以及其与硬件密钥的连接方式。一旦他们理解了代码并识别了其位置，他们就可以按照下面一种方式进行操作：

- 断开特定应用程序文件保护链接——特定黑客攻击
- 如果在所有其他文件中都严格重复使用相同方法加密的话，断开由相同机制保护的所有其他文件的保护链接——通用黑客攻击

这个结合处是最脆弱的点。

因此，受保护文件和添加的保护代码之间结合点必须要进行模糊处理并且是不可跟踪的，让任何想要破解该保护的黑客都要花大量时间反复进行研究，这是非常重要的。圣天诺 HASP Envelope 最强大的功能之一就是对结合点进行保护的功能，它可以设置很多障碍以防止黑客断开保护链接。这个功能是通过提供多层保护代码而实现的，

这些代码会在保护过程中被动态添加到应用程序文件。这些层面是专门设计的代码段，一个接一个连接起来，就像火车车厢一样。在每个保护对话中，当被添加到原始应用程序文件中时，Envelope 会确保构成整个代码的多个层面都被以一种不同的顺序组织在一起，如下所示。



Envelope 保护代码

层面的动态排列在每个和每次单个的 Envelope 保护会话中都是不同的，确保每个保护后文件都是独特的。即使原始文件完全相同，保护后文件之间也没有相似之处。受保护应用程序之间从 Envelope 代码内最后指令到应用程序代码内首个指令的转换都是不同的。对于每个应用程序来说，源代码始于一个不同的位置，这让 Envelope 应用程序结合处几乎是不能跟踪到的。研究并理解受保护文件内不同的层面和布局并不能提供在另外 Envelope 会话中保护的相同文件的布局的任何暗示信息。为了让破解者更难破解，Envelope 不仅有差别地排列层面，同时也为其所保护的每个文件选择不同数量的层面。此外，层面会被加密，每个层面都被以不同的方式加密。在应用程序运行期间，每个层面负责使用随机加密密钥按顺序解密下一个层面。

是不是很复杂？还有更复杂的！每个层面内的代码都被用仿制操作码模糊处理，这些仿制操作码被插在在有效的代码指令之间。这会严重妨碍（破解者）研究代码，确保他们不能分析保护机制或破解代码。

反调试方法

圣天诺 HASP HL Envelope 的另外一个极其强大的功能是其调试程序检测机制，它会持续检测活动调试程序。通过发送误导命令和假信息来“吸引注意力”，Envelope 会误导并转移调试程序注意力。结果就是 Envelope 可以发现并控制活动的调试程序，分清敌我。

如何分清敌我？

一般来说，软件开发人员所使用的调试程序会在其应用程序开发过程中检测漏洞并跟踪问题。但是，尝试非法访问您的软件的人们会使用相同的调试器来检测并跟踪植入的保护代码，目的是更改、禁用或整体移除代码。

因为这两种人都使用相同的调试工具，Envelope 必须能够辨别合法开发人员和危害人员的调试活动。这可以通过显示一条信息来实现，该信息会说明已检测到一个调试程序并且阻止受保护应用程序载入。在此阶段开发人员会关闭调试程序以正确载入并运行应用程序。但是，如果在应用程序载入并运行后激活调试程序的话，显然这就是尝试破解软件的软件“盗版”行为，因此应用程序就会中止运行。

检测到破解行为时不同的行为

圣天诺 HASP Envelope 所采用的对付调试程序的另一项技术是名为“行为变更”的技术。圣天诺 HASP HL 密钥会使用一个复杂代码设计，该设计利用操作系统和调试程序执行应用程序的方式是不同的这一原理。当检测到破解行为时（例如，通过使用一个 checksum 程序），软件的反应行为就会被延迟，因此就会中断“原因”和“结果”之间的逻辑连接。通过混淆破解行为和软件对该特定行为的阴性反应之间的真实逻辑连接，延迟的反应也就会让软件破解程序“感到”困惑。当检测到破解行为时，诸如损害程序功能之类的行为是非常有效的。额外行为包括导致程序崩溃、重写数据文件或故意导致程序变得不精确，导致程序完全不可信赖。

如何从您的软件保护中获得更多

除了保护您的软件之外，圣天诺 HASP HL 密钥系统调用了一个先进的自动许可生成器，允许专门根据您的应用程序设定不同的许可条款，满足您不断变化的业务模式的需求。

许可管理

使用圣天诺 HASP HL 密钥许可系统可以实现诸多创新的销售模式，如租赁、订阅、演示、并行用户、按使用收费和购买前试用等。可以通过将许可参数（如计数器、到期日和并行用户数）保存在圣天诺 HASP HL 密钥内存中来实现这些模式。一旦将受保护的应用程序交付给终端用户，圣天诺 HASP Envelope 就会发挥控制力，作为许可管理程序（License Manager）负责根据预先设定的许可条款执行应用程序。这是完全自动化的。当使用 Envelope 保护您的应用程序时您只需要通过点击标记触发许可机制。

赛孚耐圣天诺：实现 Envelope 的更简单方式

圣天诺 HASP Envelope 是一套自动文件伪装程序，它可以通过文件加密和源代码模糊处理针对逆向工程为软件提供强有效的保护。圣天诺 HASP Envelope 可以确保软件中所包含的算法、交易机密和专业技术信息集信息的安全性，免遭黑客破解。圣天诺 HASP 可以通过在受保护应用程序和保护密钥之间提供一个安全的沟通渠道（用 128 位 AES 加密）来消除中间人攻击。Envelope 使用此功能避免黑客截取圣天诺 HASP HL 保护密钥发送和接受的通信数据。

结论

黑客在不断地改进黑客攻击技术，反黑客技术也随之进步，以保护软件免遭盗版。商业破解程序进一步为黑客简化了破解程序，但是 Envelope 可以提供极强的开箱即用型安全功能，在某些时候所包含的功能并不能有效地全面阻止攻击。诸如加密和模糊处理之类的技术常常会被用于拖住攻击者，但是仍然会留有漏洞点。将加密和源代码模式处理结合在一起的 Enveloping（封装）保护技术能够提供当前最强有效的保护，确保知识产权安全。通过使用圣天诺 HASP Envelope 解决方案，无需花时间和精力从头开发一套保护解决方案，您就可以获得 Enveloping（封装）保护技术的出色性能。

赛孚耐圣天诺软件货币化解决方案

赛孚耐在为全球的软件供应商就安装、嵌入和云应用程序而提供创新且稳定的软件保护、许可和管理解决方案方面拥有 25 年之多的从业经验。

公司的圣天诺®软件货币化解决方案易于整合和使用，具有创新性并且是专注于功能的，该方案设计用于满足任何公司（机构）的独特许可实施、强化和管理需求，而无论公司（机构）有怎样的规模、技术要求或组织结构，均能满足其需求。只有选择赛孚耐产品，客户才能解决其所有的反盗版、IP 保护、许可实施和许可管理难题，同时提高整体盈利性、改善内部运行、保持具有竞争力的市场位置，同时改进其与客户和终端用户的关系。赛孚耐一直以来都不断适应新要求并不断推出新技术以满足不断发展的市场需求。赛孚耐遍及全球的 25,000 多名客户都深知选择了圣天诺就等于选择了在当今和未来不断实现业务成长的自由。

欲了解有关赛孚耐的软件货币化解决方案完整产品组合的安装、内置和云应用程序的详细信息或要下载一份我们屡获奖励产品的免费评估版，请访问：
www.minghuan.com.cn

要了解更多如何针对代码操纵、逆向工程和代码偷窃对商业 J2EE 软件产品进行保护的信息请联系我们：

北京明幻畅想科技有限公司
电话：010-51292955