白皮书

理解白盒密码技术

密码学的常规手段无法提供一个刀枪不入的解决方案，用以完全解决不同场景对其固有弱点的攻击。

介绍

传统意义上，加密技术提供了除信息接收者之外别人难以理解的传输敏感（秘密、机密或私有）信息的一种手段。密码技术，在古圣经时代就被使用，提供了其中文本被手工替换为隐藏其原始内容的一种技术。多年以后的二战期间，密码技术被广泛应用于机电设备（如臭名昭著的恩尼格玛密码机）。如今，密码技术越来越无处不在地主要依赖于有坚实的数学基础支持的计算机上。

加密技术，顾名思义，试图使用各种方法来隐藏文本部分不被恶意的眼睛所查看。理论上来讲，概念听起来很完美，但现实世界的经验证明，多种因素和环境问题发生作用对密钥强度产生负面的影响。常规手段无法提供一个刀枪不入的解决方案，以全面解决多种不同的利用密码学固有弱点的攻击场景。

Peter G. Neumann 教授，计算机系统和网络可信度和可靠性，被引述说“如果您认为解密技术解决了您的问题，那您还不清楚问题所在。”1

本文在讨论传统技术的同时，专注于白盒加密技术的实现。

近观加密技术

典型的 DRM（数字版权管理）中实现的加密算法采用公知的、依靠密钥保密性的强大算法作为安全解决方案的一部分。多数情况下，这是非常不妥的，这是因为很多这些应用程序执行在具有潜在敌意的最终用户所控制的平台上。

用于加密技术的传统前提是一个黑盒装置，其假定攻击者无法访问所述密钥，只能控制加密输入（明文），并能够访问结果输出（密文）。长期以来这已被假定为真实的，如同智能卡之类的硬件设备，但恶意攻击利用从黑盒“泄漏”信息的技术已经开发出来了（如差分功耗分析攻击，也被称为 DPA），这能让黑客推导出黑盒内部使用的密钥。黑客已有效地使用该方法对黑盒进行攻击，并将其实现成“灰色阴影”而非黑色。2

流行的行业标准加密算法如 AES 并没有设计在可以查看到它们执行的环境中运行。

事实上，标准的加密算法模型假设如终端、电脑和硬件保护令牌等都是可被信任的。

1. Peter G. Neumann，源引自纽约时报，2001 年 2 月 20 日.

2. Amitabh Saxena，Brecht Wyseur 和 Bart Preneel，白盒加密技术的安全观

白盒加密技术的必要性

流行的行业标准加密算法如 AES 并没有设计在可以查看到它们执行的环境中运行。事实上，标准的加密算法模型假设如终端、电脑和硬件保护令牌等都是可被信任的。如果这些终端存在于具有潜在敌意的环境中，当应用程序试图从内存中提取嵌入的或生成的密钥时，攻击者正在监控应用程序的执行，则密钥对于攻击者来说直接可见。对于运行在 PC、IPTV 机顶盒及其他要实施 DRM 的数字设备上的基于软件的应用程序，这是个普遍的问题。通过主动监控标准的加密算法 API 或内存转储，黑客就能够在使用时提取密钥。

一个成功的基于内存的密钥提取攻击的实例就是使用工具 BackupHDDVD 来复制被保护的 DVD 的内容，并从 Windows 受保护的媒体内容中删除 DRM。

白盒的挑战

在完全透明的环境中工作时，让有价值的信息如授权和其他商业机密保持隐藏，该理念带来了各种挑战：

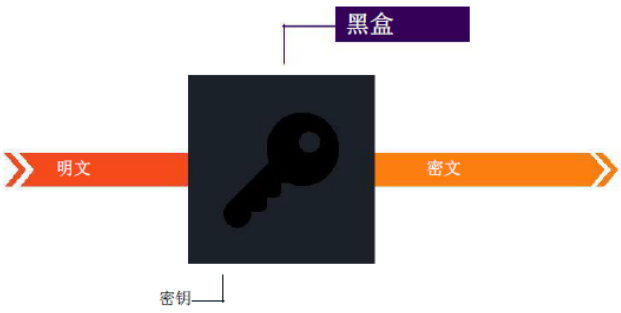
> 如何加密或解密内容而无需直接暴露密钥和/或数据的任何部分？

> 如何执行强大的加密机制，以在执行时知晓黑客在查看和/或变更代码？

各种加密模式

黑盒（传统）加密技术

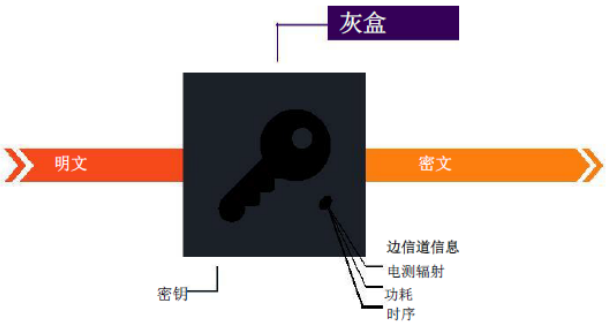
作为一个传统模式，黑盒加密假定攻击者无法物理访问密钥（执行加密或解密算法）或任何内部运作，而只能观察外部信息和行为。该信息包括系统的明文（输入）或密文（输出），同时假设零可见代码的执行和动态加密操作。



灰盒加密技术

灰盒的场景是假设攻击者可以部分物理访问密钥或者说是“泄漏”所谓的边信道信息。边信道分析攻击（SCA）利用从物理实现的加密系统中泄漏的信息。通过时序信息、功耗、电磁辐射等被动式地观察该泄漏。防护边信道攻击非常重要，这是由于该种攻击能够快速且低成本地实现。公开可用的边信道信息能够让黑客发现部分密钥，从而大大降低其功效并降低整体保护能力。[3]

灰盒加密技术实际上是传统黑盒实现的副产物。实践已经证明，即使是智能卡，被认为能够提供强大的安全性，其内部执行的加密事实上也会向外界泄漏信息。很显然假定为黑盒的场景在现实中仅为灰色阴影。



3. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, DRM 应用程序的白盒 DES 实现

白盒加密技术的概念

白盒加密技术与上述传统的安全模型针锋相对。相对于以前的实现下，攻击者只给出一个黑盒子，即获取输入和输出，并受到攻击的加密算法，并假设零可视性内部运作，白盒提供了充分的可见性来代替。与之前给黑客提供一个黑盒的实现（如访问输入、输出、攻击下的加密算法以及假设零可见内部工作）有所不同，白盒提供充分的可见性。

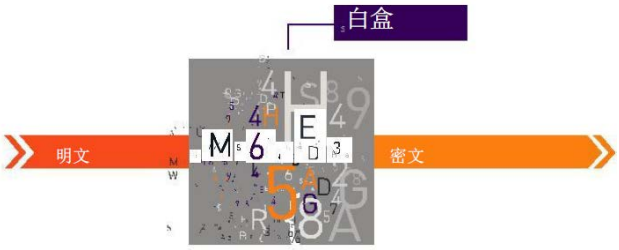
白盒加密技术旨在保护软件实施加密算法以对抗密钥的还原，即使攻击者完全控制机器执行加密 – 这在 DRM 领域特别有效。

白盒加密技术

白盒的场景与前面所述的情况恰恰相反，处理更为严重的威胁，同时假设黑客能够完全可视和控制整个操作。黑客可以自由地观察动态代码的执行（使用实例化的密钥），并且完全可见和改变内部算法的细节。尽管有这种完全透明的方法论，白盒加密技术整合密文的方式不会暴露密钥。

因此很显然，对于黑盒和灰盒模式的内置算法在面临不可信主机上操作时是不切实际的。不难理解的是，黑客不会只用黑盒和灰盒的场景下可用的手段来破解密文，而是观察到使用未受保护的密钥时 - 直接窃取它。

暴露在白盒场景下的传统加密算法，假设该密钥作为实施的一部分而存在。



白盒场景下，白盒加密算法受到保护，这是由于密钥不在内存中，无法被提取 - 即使动态地。

因此选择最合适、最安全的加密模式是抵御恶意威胁的唯一出路 – 这恰恰是白盒加密技术要实现的。

实现白盒加密技术幕后的方法论

在假设可以全面监控并更改每条指令的前提下，如何能够在可执行代码中安全地“隐藏”密钥？

抽象地说，这是通过使用一个数学运算来实现的，结合安全密钥的功效和一些实施的特定数据，以确保该运算事实上不可反转。4

举个例子，通过一个简单的乘法运算到大数字使得 RSA 算法的固有强度成立，但这是将结果分解为其素因数的数学难题。

另外，同样重要的是，白盒加密算法的实现完全能够加密或解密。

如前所述的实现方式是基于数学运算的，非常难以反转。

这事实上能够构建一个类似完整公钥/私钥方案的系统，但在性能水平方面，却更接近一个标准的对称式加密算法。

4. Amitabh Saxena，Brecht Wyseur 和 Bart Preneel，白盒加密技术的安全观

解密功能可在分布式应用程序内实现，但密钥无法被提取并且解密如同加密操作一样无法反向。攻击者没有任何手段来创建正确的加密过的数据，将其解密回所需的值。

这种特定的方法尤为适用于保障硬件设备保护的通信通道，例如硬件保护令牌。攻击者无法提取用于安全通信通道的密钥，因此无法解密通过该通道的数据，也无法将数据注入到该通道，同时他也没有正确加密它的手段。

解决该挑战

尽管白盒场景被认为不适于安全相关的任务，但白盒加密技术打乱所有牌，并提供了运行在完全透明环境中执行加密的一个高度安全的方法。尽管完全透明，加密和解密操作能够不泄露密钥或数据本身的任何部分，以保护敏感数据。此外，明知有恶意的双眼在执行过程中有可能观察代码的执行，白盒加密技术可使强大的加密机制执行（与其他技术相结合）。

金雅拓安全措施的一个组成部分

金雅拓的 Sentinel 产品所提供的安全通信通道确保被保护的应用程序和硬件令牌之间的通信被加密且无法重放。与以往旨在隐藏加密密钥的措施不同，新的措施围绕着白盒加密技术，其假定攻击者可以跟踪被保护的应用程序及其运行环境来寻找加密密钥。随着该前提作为设计的一部分，算法和加密密钥被替换为执行相同加密的特定的供应商专用 API 库，将加密密钥嵌入为算法的一部分，这样就确保其不会出现在内存中，因此无法被提取。供应商专用库的生成是在金雅拓的服务器上利用一些商业机密 来执行的。此外，为每个特定软件供应商单独生成与混淆每个应用程序库 – 通用的破解几乎不可能。

真正的突破性解决方案

金雅拓是提供白盒加密技术作为其 Sentinel 产品系列软件授权解决方案的首个也是唯一的供应商。该新技术能够时时保护加密密钥，而不会在某个时间段分解并暴露它。从安全角度来看，这确保了密钥的保护免遭黑客攻击，因此在潜在的攻击过程中不易重建。

白盒加密技术是一个重要组成部分，使得开发人员能够保护他们的应用程序以应对逆向工程、篡改和自动攻击。金雅拓的白盒加密方法集成到软件设计过程中，能够将多一层的保护直接嵌入到源代码级，从而提供一个高效的软件保护方法。

结论

被保护的应用程序的整体安全性高度依赖于实施本身，即如果没有在其设计的环境中使用，仅仅采取强大的加密算法并不提供任何安全 - 不在白盒设置中使用白盒加密技术大大地帮助黑客反向工程所保护的软件。最常见的攻击都试图利用软件的安全漏洞，而非加密算法的弱点 - 但最近攻击者已经意识到开放的 PC 环境中经典加密算法的弱点。

除了继续增强产品生命周期和新版本的发布外，在设计和实施阶段也要特别注意软件的保护。除了白盒加密技术外，应当使用更多互补的安全措施，以进一步加强整体保护方案。

安全带来一定的成本，直接的结果，无法密不透风。因此，关键是要正确地评估应用程序本身所需要的安全级别，即需要保护的价值结合忽略潜在风险所遭受的损失。

其他出版物

更多信息和详细的技术出版物可在以下的链接中找到：

1. Towards Security Notions for White box Cryptography
http://www.cosic.esat.kuleuven.be/publications/ article-1260.pdf

2. White box Cryptography: Formal Notions and (Im) possibility Results http://eprint.iacr.org/2008/273.pdf

3. White box (software engineering) on Wikipedia
http://en.wikipedia.org/wiki/White_box_(software_ engineering)

4. What is a white-box implementation of a cryptographic algorithm?
http://crypto.stackexchange.com/questions/241/what-is-a-white-box-implementation-of-a-cryptographic-algorithm

5. Portable Executable Automatic Protection, Wikipedia
http://en.wikipedia.org/wiki/Portable_Executable_ Automatic_Protection

关于 Gemalto 的 Sentinel 软件货币化解决方案

金雅拓公司，通过收购 SafeNet 公司，是为预置、嵌入式和基于云计算软件厂商提供软件许可和授权管理解决方案的市场领先供应商。金雅拓的 Sentinel 是软件行业中最值得信赖的品牌，提供安全、灵活、面向未来的软件货币化解决方案。

软件货币化的其他资源

要了解更多有关如何更好地盈利您的软件，请访问 Gemalto’s on-demand resource library。

访问中文活动在线中心 http://china.safenet-inc.com

联系我们：Marketing-China@safenet-inc.com

欢迎加入我们的对话

- > Facebook
- > LinkedIn
- > Twitter
- > Google+
- > Sentinel Video Cloud
- > Blog
- > Sentinel Customer Community

gemalto
security to be free