理解白盒密码技术 白皮书

传统密码技术缺少足够的防护性，面对针对其固有缺陷进行的各式攻击不能彻底应对。

介绍

传统的密码技术提供了一种敏感信息（机密或隐私信息）的传播方法，使得除了信息接受者外，其他任何人都无法理解信息的内容。在古圣经时代，密码技术提供了一种将消息中的文字进行手动替换以隐藏其原始内容的方法。很多年以后，在二次世界大战期间，密码技术广泛应用于电子机械设备（例如臭名昭著的 Enigma 密码机）。现在，密码技术比以往更加普遍，且高度依赖计算机，建立在稳定可靠的数学基础之上。

密码技术，顾名思义，就是试图通过各种方法隐藏部分文本以防止恶意的眼睛看到这些文字信息。理论上，这个概念虽然听起来非常理想，但是实际生活经验已经证明，由于受到多种因素及环境状况的影响，密钥的保护强度被削弱了。传统密码技术缺少足够的防护性，面对针对其固有缺陷进行的各式攻击不能彻底应对。

一位值得信赖的、可靠的计算机系统和网络专家——Peter G. Neumann 教授——曾经说过：“如果你认为密码技术可以解决您所面临问题，那说明你还不清楚你的问题是什么。”[1]

这篇文章对传统密码技术进行了讨论，同时重点讨论了白盒密码技术的应用。

近距离了解密码技术

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。

1. Peter G. Neumann, quoted in the *New York Times*, February 20 2001.

流行的行业标准密码如 AES，其设计目的未考虑其运行环境会被控制、被观察这一因素。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信任的。

密码术的传统假设是建立一个黑盒方案，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。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”。[2]

对白盒密码技术的需求

流行的行业标准密码如 AES，在设计上未考虑其应用环境会被控制被观察这一因素。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。一个成功的案例：一次基于内存的密码提取攻击使 BackupHDDVD 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。

白盒面临的挑战

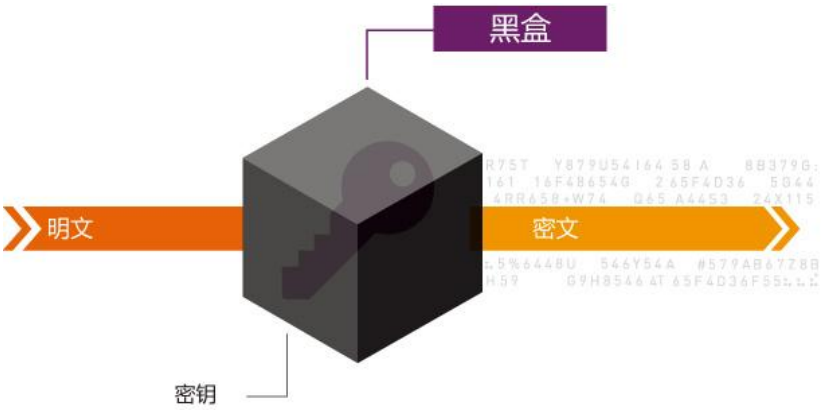
在一个完全透明的环境中运行，同时将一些有价值的信息如许可证以及其它商业秘密隐藏起来——这一想法面临多种挑战：

- 如何在不直接暴露任何密钥或数据的情况下加密或解密内容？
- 如何明知黑客能够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？

多种密码技术模型

黑盒（传统）密码技术

作为一个传统模型，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。

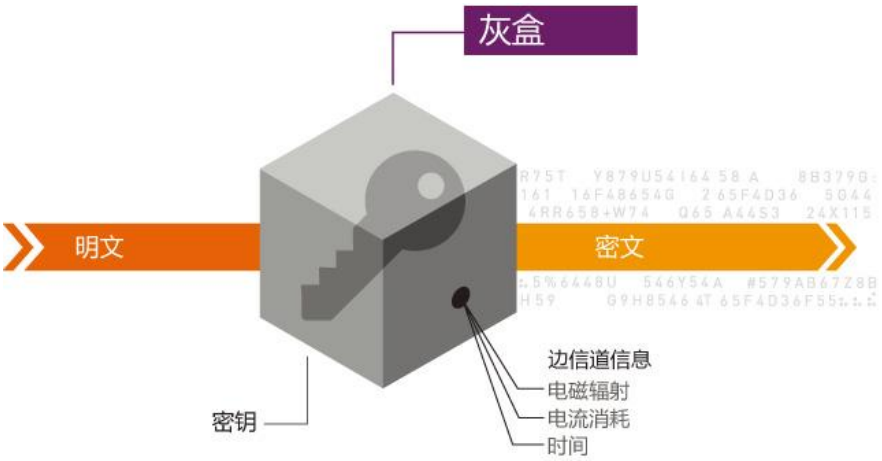


2. Amitabh Saxena, Brecht Wyseur, and Bart Preneel, *Towards Security Notions for White-Box Cryptography*

灰盒密码技术

灰盒方案认为攻击者可以实质性地接触到部分密钥或者泄露的信息（也就是所谓的边信道信息）。边信道分析攻击（Side Channel Analysis, SCA）利用了从密码系统运行过程中泄露的信息。泄露信息是通过被动观察时间信息、功率消耗、电磁辐射等而获得的。因为边信道攻击速度快且成本低，所以对边信道攻击的防护非常重要。公开的边信道信息使得黑客们可以有效地破解部分密钥以致密钥的功效大大降低，使密钥保护性能失效。

实际上，灰盒密码技术是传统黑盒应用的副产品。采用内部加密的智能卡即便是被普遍认为具有很高安全性，仍被证实能向外部泄露信息。有一点可以确定，那就是被认为是黑盒技术在实际应用中仅仅是“灰色的阴影”。



白盒密码技术的概念

白盒密码技术与上述传统安全模型完全相反。与以前的执行过程相反，以前的执行过程中攻击者仅得到一个黑盒，即在攻击下接触到明文或者密文以及加密算法，但是认为他们是看不到内部操作的，但是白盒环境里却是完全可见的。

白盒密码技术旨在保护加密算法的软件运行过程以防止密钥被重现，即便是在攻击者完全控制了正在进行加密的机器 – 这在 DRM 环境中尤为有用

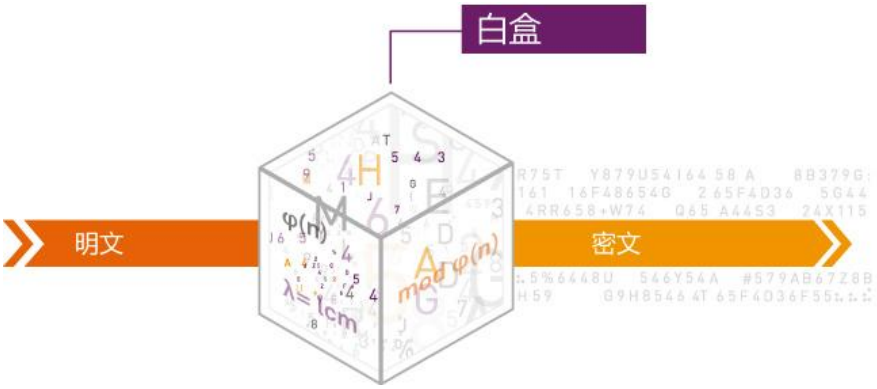
白盒密码技术

与之前描述的方案相比，白盒密码技术假定攻击者已经完全控制了整个操作过程且对此完全可见，在此情况下来处理面临的更为严重的威胁。黑客们可以自如地观察动态密码运行过程（拥有示例密钥），并且内部算法的详细内容完全可见，可随意更改。尽管白盒密码技术的方法完全透明，但是它将密码进行了组合使得密钥不容易被提取。

3. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, A White-Box DES Implementation for DRM Applications

因此可以明确的一点，在不可信任的主机上运行黑盒和灰盒模型建立的算法是不切实际的。可以理解，黑客们不会试图仅仅利用黑盒方案及灰盒方案的现有方法来破解密码，而是会观察未受保护的密钥被使用时的执行过程，而后直接窃取。

传统的加密算法，与白盒方案相反，假设密钥的出现只是执行过程的一部分。



白盒加密算法在白盒方案中会受到保护，密钥不会在内存中出现，所以不能被提取——即便是动态的。

因此，选择最合适的、最安全的密码模型是阻止恶意威胁的唯一防线——这也正是白盒密码想要实现的。

白盒应用背后的方法论

既然认为一个人可以完全监控并且修改每一个指令，那么怎样才能将密钥隐藏在执行代码中呢？

抽象地说，这是通过将密钥的作用与一些采用数学运算的运行具体数据结合起来而实现的，并且在此过程中确保该数学运算不可逆。[4]

例如，只要通过一个简单的乘法运算生成大数值就能实现足够理解的 RSA 内在强度，尽管将结果分解成因子到其素数中在数学上是一个难题。

此外，同样重要的是，白盒加密算法的应用仅仅能够加密或者解密。

如前所述，此应用基于一个很难逆转的数学运算。因此可以建立一个系统，该系统类似于完全公开或私人密钥方案，但是在性能水平上更接近于一个标准的对称密码。

解密功能可以在分布式应用程序内部执行，但是密钥不能被提取，且解密不可逆向操作来进行加密操作。攻击者没有可行的方法来创建正确的加密数据，以使逆向解密生成期望的数值。

4. Amitabh Saxena, Brecht Wyseur, and Bart Preneel, Towards Security Notions for White-Box Cryptography

当信息传输通道受到硬件设备（例如硬件保护令牌）的保护时，这一特定方法尤为有效。黑客将无法提取安全通道的密钥，因此他们既无法解密流过传输通道的数据，也无法将数据注入到传输通道中，因为黑客无法正确地对数据进行加密。

解决技术上的难题

尽管白盒方案被认为不适用于与安全相关的任务，但是白盒密码技术却对旧有技术全部重新洗牌，它提供了一种在完全透明环境中运行时高度安全的加密方法。尽管是完全透明，加密和解密程序可保护敏感数据，而不泄露哪怕是密钥或数据的任一微小部分。此外，尽管知道恶意的眼睛可能正在观察执行的代码，白盒密码技术亦能实现强力加密机制（与其它技术结合使用）。

SafeNet 安全措施的组成部分

SafeNet 圣天诺(Sentinel)产品所提供的安全通道技术可确保受保护的应用程序与硬件令牌之间的信息传播是经过加密处理的，且此过程不能重现。不象以前的应用是隐藏加密的密钥，新的应用则以白盒密码技术为核心。在白盒密码技术中是假定黑客可以跟踪受保护的应用程序及执行环境以寻找密钥的。算法和密钥以此假定作为设计的一部分，然后由特定厂商的使用相同加密技术的 API 函数库替换算法和密钥。但是作为算法的一部分，内置的密钥可确保永远不会在内存中出现，因此也就不能被提取。为软件开发商定制的函数库是在 SafeNet 服务器上结合开发商的商业机密信息生成的。此外，对特定的软件开发商来说，每一个应用程序函数库都是独立生成且经过混淆的，这使得通用的黑客入侵基本上不可能。

一个真正独创的解决方案

SafeNet 是首家且唯一一家将白盒密码技术作为其软件授权解决方案一个重要部分的厂商。这一新技术可在任何时候保护密钥，而不是将密钥分成很多小部分并一次泄露其中一份。从安全角度来看，白盒密码技术使得受保护的密钥对黑客仍然是不可见的，因此在潜在的攻击中该密钥亦不会被重建。

白盒密码技术是一个附加的基本要素，它可以使开发人员保护自己的应用程序免受逆向工程、篡改、以及自动攻击。SafeNet 的白盒密码方法集成到软件设计过程，直接在源代码级别就嵌入了额外的保护层，从而提供了一种高效的软件保护方法。

结论

一个受保护的应用程序的总体安全性高度依赖于应用本身，也就是说，当加密算法不是在其设计的环境下使用时，仅仅采用强力加密算法不能提供任何安全性——不在白盒应用中使用白盒密码技术，就会使黑客对受保护的软件进行逆向操作。大多数普通攻击都是尝试利用密码安全性的漏洞而不是加密算法的弱点——但是近来黑客们已经认识到古典密码技术在开放式 PC 环境下的易攻击特点。

毫无疑问，对软件保护在设计和应用阶段都必须特别地关注，此外在产品的整个生命周期和发布的新版本里还要持续加以强化。除了白盒密码技术之外，还应采用额外的补充安全措施来进一步加强整体保护方案。

其他出版物

如欲参看更多信息及详细技术出版物，请点击以下链接：

1. Towards Security Notions for White box Cryptography
   （了解白盒密码技术安全概念）
2. White box Cryptography: Formal Notions and (Im)possibility Results
   （白盒密码技术：正式的概念及(不可能)可能的结果）
3. White box (software engineering) on Wikipedia（维基百科上的白盒（软件工程））
4. What is a white-box implementation of a cryptographic algorithm?
   （什么是加密算法的白盒应用）
5. Portable Executable Automatic Protection, Wikipedia
   （移动式可执行的自动保护—维基百科）

SafeNet Sentinel 软件价值化解决方案

SafeNet 为全球范围内的软件及技术厂商提供创新的可靠的软件许可证及授权管理方案，SafeNet 在该行业拥有至少 25 年的经验。本公司的圣天诺(Sentinel ®)软件价值化解决方案系列，整合方便、易于使用，具有创新性且聚焦于软件功能，目的在于满足不同组织机构独特的许可证实现、执行及管理要求，不论该组织机构的规模、技术要求以及组织结构如何。

客户们只有在拥有了 SafeNet 后才能够应对如保护隐私、IP 保护、许可证实现、许可证管理等挑战，从而提升整体盈利能力、改善内部操作、维护竞争地位、加强与客户及终端用户的关系管理。在过去的时间里，SafeNet 在解决新需求、引进新技术、应对不断变化的市场条件方面的表现有目共睹。SafeNet 世界范围内的 25000 多家客户清楚地知道，选择圣天诺就意味着选择了他们今天、明天、以及未来在业务发展方面的自由。

沈阳云畅想科技有限公司
电话：024-3105 8958
网址：www.aladdin.ln.cn

©2012 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet.
All other product names are trademarks of their respective owners. WP (EN)-03.29.12