

可持续的设备安全性： 利用软件安全性摧毁黑客的商业模式

引言

本白皮书适用于那些其设备可播放优质内容的手机和消费电子产品制造商以及与之相关的参考设计供应商。

一个有效的智能手机安全保护解决方案应具备可集成性、抗攻击性以及缓解攻击的能力，这三者是构成设备的持续安全性和摧毁黑客商业模式的基本要素。任何形式的安全性，无论是硬件所具有的安全性还是软件所具有的安全性，都会最终被破解。仅只依赖防篡改型硬件所构成的安全性或许能在最初阶段提供强大的抗攻击能力，但对于降低那些不可避免的成功破解所带来的不利影响无济于事。

但软件安全性解决方案却不同，其所具有的多样性和可更新性不仅能够增强在最初阶段的抗攻击能力，而且还能将一次成功破解所造成的影响范围和持续时间控制在最小程度。多样性和可更新性的结合使用不仅能够打击黑客的积极性，同时也能够最小化黑客对智能手机所造成的影响。也只有基于灵活的软件安全性，制造商才能在快速地将新产品推向市场的同时获得可持续的设备安全性。

来自于黑客的威胁

随着数字内容的应用日益普及，确保设备的安全性就显得越来越重要。越来越多的个人信息、企业保密信息、商业机密以及优质的付费内容都必须予以安全保护以防止其被窃取和篡改。

通过设备处理、储存和传输有价值的数字信息的需求目前已经并将持续呈现出爆炸性的增长。这些设备通常在广泛应用的硬件平台上运行着标准的操作系统。这些被大家所熟知的操作系统和硬件平台使设备暴露在大范围的攻击工具和黑客的面前，设备安全性被危及的可能性也随之显著提高。

只有当优质（或付费）的内容能够安全地向用户进行分发、被用户存储和播放时，才能够确保内容产业的良性发展。而黑客的攻击和盗版每年给媒体产业带来数百万美元的损失。因此，设备制造商的任务就是要制造出能够满足反盗版要求的安全设备。如果某种设备不具备足够的内容安全保护能力，那么通过该设备播放优质内容的功能就会被废止。

为了打击此类攻击并避免设备被召回的风险，设备制造商正在寻求一种功能强大的技术解决方案以对其收入，客户以及品牌进行保护。本白皮书对设备制造商如何以较低的成本获得可持续的设备安全性进行了阐述。

摧毁黑客的商业模式

商业黑客的存在是因为盗版能给他们带来经济效益：一次成功的破解所带来的利益远远超过他们实施攻击所投入的成本。

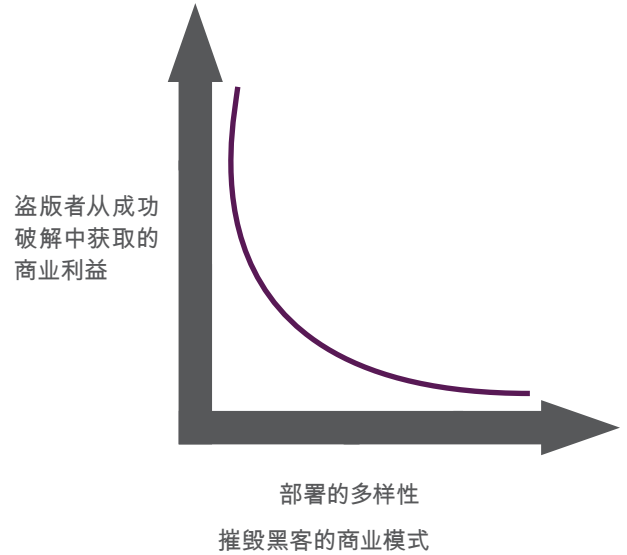
如果设备制造商能够增加黑客将盗版形成一个可持续性商业行为的难度，那么大多数黑客都会把精力集中到其它地方，如其它的设备。摧毁黑客的商业模式有以下几种办法：

- 使破解过程变得更加困难而且需要投入大量的时间
- 将一次成功破解所造成的影响范围控制到整批设备的一小部分当中
- 控制一次成功破解所造成影响的持续时间

我们通常采用的一种有效的确保硬件和软件安全性的方法是使成功破解的成本变得越来越高。但是，相比之下，使黑客很难从盗版行为中获取暴利的做法更为有效。Cloakware认为，只有具备了上述三个要素的解决方案才能在打击黑客的战役中赢得胜利。归根结底，不可能有十全十美的安全解决方案，只能是让盗版无利可图。

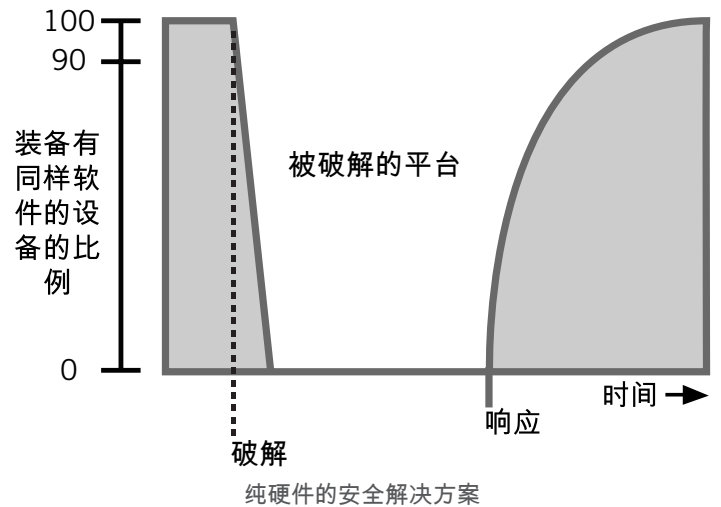
基于硬件的安全性往往在最初阶段显示出极强的抗攻击能力，但一旦被成功破解，整批同类设备就会很容易受到攻击，而要想进行设备的修复，就需要花费大量的时间和金钱。总而言之，基于硬件的安全性有可能造成“全军覆没”的后果，这是因为基于硬件的安全性并不能解决上述第二点和第三点中提及的问题。

Cloakware软件安全保护技术能自动地使软件在结构上具有多样性(1)摧毁黑客的商业模式。软件的多样性确保了自动攻击（如，有效地攻击）只能在小范围内进行。这种多样性的部署可以通过多种方式得以实现：在用户之间、设备之间、软件版本之间和在最终用户之间。上述这些办法均能够控制盗版者从一次成功破解中所获得的利益。破解某个系统的动机会随多样性的增加而显著降低，如图1所示。



基于软件的安全解决方案能通过对软件进行快速升级的方法对一次成功的破解做出快速响应。软件的升级也应具有多样性。否则，这些升级后的软件就会被后续的攻击所轻松解析和击溃。

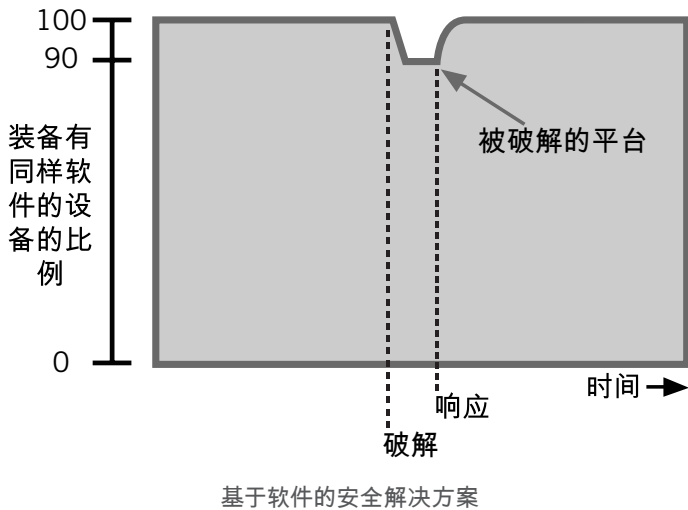
软件的多样性（在时间和空间上）以及软件的可更新性解决了上述后两点所提及的问题，这是基于硬件的安全解决方案所不具备的。这两点限制了一次破解所造成的影响范围和时间长度（范围和持续时间），从而摧毁了黑客的商业模式，削弱了黑客对该设备进行攻击的企图（2）纯硬件的安全解决方案。



利用多样性可避免硬件安全性带来的全军覆没的风险。图2和图3显示了纯硬件安全解决方案与基于软件多样性的软件安全解决方案的区别。

在仅基于硬件安全性的情形下(如图2所示),一旦出现一次成功的破解,破解工具就会在设备间进行快速扩散。此种破解极有可能在很短的时间内波及所有已安装的设备。当针对该破解的补丁开发出来时,补救的过程又需要花费大量的时间进行部署,通常这种办法无法应用到已安装的设备当中。

在基于软件安全性的情形下(如图3所示)基于软件的安全解决方案,设备制造商利用软件的多样性可以确保只有10%的已安装设备装备有同样的软件(如,每台已安装设备只是十种不同软件映像的其中之一)。当一次成功破解发生时,只会影响到装有同样软件映像的设备。同时,由于软件具有可轻松升级的特性,打补丁的时间会更短,补救措施可以通过软件升级/更新过程快速实现。



可持续安全性的要求

数字媒体设备由硬件和软件两大组件构成。功能性硬件需要在系统构架的某个位置与操作系统和设备驱动器接口。这些接口点通常是整个安全性基础构架中的薄弱环节,需要有基于软件的安全性机制加以保护。随着设备复杂化程度的提高和功能性的全面发展,毫无疑问,敏感软件将最终实现对有价值数据的操控。

设备安全性的发展历史告诉我们,绝大多数的平台最终都将被破解,只要有足够的时间和资源,无论是硬件还是软件,都会被黑客成功的破解。有经验的设备制造商都清楚的知道,安全性是否能被黑客破解不是“可不可能”的问题,而是“何时会被破解”的问题。因此,为了创建一种可持续的安全模式,我们可以将安全性的要求分为以下三个阶段,如图4所示 设备安全性的需求。



1. 可集成性: 一个理想的安全解决方案应具备轻松集成的能力并能够实现产品组合的相互兼容从而将开发成本控制到最小化。
2. 抗攻击性: 一个理想的安全解决方案应能在最初阶段提供强大的抗攻击能力,并可进行更新以防范后来出现的盗版威胁。
3. 对盗版攻击的缓解能力: 如果发生一次成功破解,应具备缓解该破解

所带来的影响以及快速修复的机制。这一点至关重要,因为一次成功的破解会导致设备DRM许可证的无效,从而给业务收入带来损失,以及给品牌的声誉带来不利影响。

第1阶段:可集成性

一个理想的安全解决方案应具备轻松集成的能力并能够实现产品组合的相互兼容从而将开发成本控制到最小化。

集成速度和工作量

要想采用基于硬件的安全解决方案,安全软件设计者在使用相关硬件之前必须先熟悉应用程序接口(API)和驱动程序。同时,设计者还必须开发/修改软件来适应整个安全构架。这就需要做大量的工作,花费大量的时间,而且还有可能会出错。例如,基于Symbian 9.1的设备需要修改应用程序以便利用平台的安全特性;Texas Instruments的安全模式在智能手机市场中也面临着同样的问题。而基于软件的安全解决方案通常能自我适配,无需重建,因此能够实现快速简便的部署。

与自我适配的安全软件相比,基于硬件的安全解决方案通常要求多方协同工作。这种工作环境本身就会带来一些新的盗版威胁。测试证书以及仿真程序都可用来当作破解工具使用。即使整个开发过程完全可信,但终端设备的安全性还是取决于您的供应商以及被许可人的安全性。

即使已经具有了一个全面的基于硬件和平台的安全解决方案,也很难将所有的敏感代码植入到安全环境当中。虽然现在有一些内容安全保护系统正在向标准密码系统迈进(基于RSA和AES标准),但还是有许多系统目前没有这么做(例如,DTCP、CPRM、CSS)。这些非标准的内容安全保护系统要求软件具备保护密钥和算法的能力,同时还应符合“鲁棒性规则”。这就要求有静态保护,同时还需能抵抗动态攻击,例如针对缓冲区和堆溢出的攻击。

最终的结果将是,部分解决方案总是依赖于软件的安全性。

平台独立

用户希望在完全不同的设备上共享自己的信息,这些设备包括个人电脑、媒体播放器或手机等。许多原始设备制造商(OME)和独立软件提供商(ISV)目前都具备支持多个平台的能力,每一个平台都有自己的安全性特征并互有细微差别。基于软件的安全解决方案其主要部分具有硬件独立的特征,并在整个产品组合中具备使用上的一致性。这种一致性提高了安全性、降低了开发成本、避免了受供应商的钳制、缩短了产品上市的时间、减少了未来为满足用户需求带来的支持成本。便携式软件结合了软件的安全性,是目前最为实用且最具可扩展性的解决方案。

向前/向后的兼容能力

一个理想的安全解决方案必须具有成本效益,并可同时支持新设备和现有的已安装设备。基于软件的安全解决方案可同时应用于高端和低端设备,还可对现有的已安装设备进行升级。

新硬件进入市场的部署是一项耗时的工程。市场对安全性和性能的要求随时处于变化之中。有经验的制造商能够认识到软件与一种通用处理器进行组合后所带来的、能够实现将高收益的创新设备快速推向市场的灵活性。这种灵活性对基于软件的安全解决方案是迫切需要的,它同时也是在未来验证制造商新设备的一个要素。

第2阶段:抗攻击性

一个理想的安全解决方案应能在最初阶段提供强大的抗攻击能力,并可进行更新以防范后来出现的盗版威胁。

最初阶段的抗攻击能力

基于软件的安全解决方案使用一种多层级保护方式来实现最大化的抗攻击能力。代码转换可以与加密、完整性验证和反调试技术相结合以实现高级别的防盗版攻击能力。(3)

如果说基于硬件的安全解决方案在最初阶段的抗攻击能力比基于软件的安全解决方案要高,我们更要认识到硬件本身并不构成一个安全的解决方案。其安全性实施的强度取决于硬件如何与其它硬件和系统软件进行集成。集成后的最终系统有一个很宽的攻击面,而安全性的整体水平与平台相关。

开发基于硬件的安全解决方案并将其推向市场需要花费更多的时间。当一台设备真正推向市场时,其具有的功能特性可能已存在了若干年。而设备还必须在市场上存续三至六年。对于原设计者来说,他们很难预测到未来的盗版威胁,也无法创建安全解决方案来弥补新发现的漏洞。同时,他们也很难预期到未来市场的需求。能够在未来消费电子市场上发展壮大公司将会是那些采用了基于软件安全性解决方案、能够快速应对市场变化、具有高度灵活性的公司。

可升级性

软件的升级和更新常见于网络连接设备。以下三点构成软件升级和更新的原因:

- 缺陷修复
- 新性能部署
- 安全性增强

随着时间的推移,盗版攻击的方式和破解工具所采用的技术也会不断发生变化。一个理想的安全解决方案应该可以主动进行升级以应对现在和将来可能出现的攻击威胁。因为基于软件的安全解决方案具有相对的独立性,可以在不给其它系统软件带来重大影响的情况下轻松升级。

可更新性缩短了一次成功破解的寿命和持续时间。通过对该次破解所持续的有效时间进行限制,可进一步抑制黑客从中获得的商业利益。通过时间的验证,我们会发现,具有可更新性,尤其是和多样性结合使用时,基于软件的安全解决方案比基于硬件的系统更为安全。

混合式支持

基于软件的安全解决方案可结合基于硬件的安全解决方案共同使用。硬件可用来向软件安全解决方案提供密钥和其它机密信息,进而扩展到整个信任链。现实情况是,软件与硬件在安全性功能的执行上互为依赖。基于硬件的解决方案其本身并不构成是一套完整的安全解决方案,因为在某些点上,硬件需要与操作系统或其它软件组件进行接口。目前正在开发的最为先进的安全解决方案系统均同时兼顾了硬件的物理特性以及软件的快速响应和低分发成本的优势。

第3阶段:对盗版攻击的缓解能力

如果发生一次成功的破解,应该具备缓解该破解所带来的影响以及快速应对破解的机制。

多样性降低了破解所造成的影响

硬件所具有安全性可以在最初阶段提供强大的抗攻击能力。但是,一旦系统被破解,也即意味着整个系统的安全性被破解。与基于软件的安全解决方案不同,由于已经安装的设备都是相类似的,同样的攻击对整个系统都有效。要从一次成功破解中进行修复通常是一件困难、

昂贵和耗时的工程。同时,设备有可能面临着被召回的风险,而业务和利润也将受到不利的影

响。当软件多样性同时在时间(不同软件版本之间)和空间上(同一批次的设备之间)具备时,能对一次成功破解造成影响和范围起到削弱的作用。

可更新性

当出现一次成功破解事件时,最快的应对方式是通过发布下一个软件版本或发布升级软件的办法来对软件进行升级换代。可用的修复机制取决于硬件缺陷的类型。当硬件发生缺陷时,其对缺陷的修复会到硬件下一版本发布时得以实现。对于ASIC来说,也许需要二年的时间。即使有了可用的新硬件,部署给用户还需要一些时间。

而基于软件的安全性解决方案可以快速且经济的进行升级和更新。回顾在设备领域以及基于硬件的安全性解决方案(如智能卡)中获得的经验教训,我们就会发现,软件升级是安全性不可或缺的最基本的组成元素。聪明的原始设备制造商都会从一开始就采用软件升级技术。

结束语

基于硬件的安全解决方案除了在最初阶段对盗版攻击有着强有力的抵抗能力之外,在整个产品使用周期为产品所能提供的安全保护微乎其微,此外还会消耗大量的成本,如下表所示。

设备安全性发展的历史表明,无论是基于硬件还是基于软件的安全解决方案都会被黑客攻击,从而最终导致终端设备被破坏。基于硬件的安全解决方案旨在提供最初阶段的抗攻击能力,但无助于削弱一次成功破解的影响范围和持续时间。如下表所列,基于软件的安全解决方案在整个安全周期内的每一阶段都可为安全性赋予额外的价值。

基于软件的安全解决方案所具备的灵活性一方面减少了系统集成的工作量,另一方面最大化了软件的兼容性。而安全技术可升级性和广泛的安全技术又能形成对首次攻击的强大抵抗能力。最后,也是最重要的一点,软件多样性与快速响应机制的结合会对一次成功破解的影响范围和持续时间起到削弱和抑制作用。为了避免内容安全保护产业中设备被召回的风险,基于软件的安全解决方案是那些希望保护其业务收入和品牌的设备制造商必须采用的安全解决方案。

| | | 软件 | 硬件 |
|------------|------------|------------|----|
| 第一阶段:可集成性 | 集成速度和工作量 | ● | |
| | 平台独立 | ● | |
| | 向前/向后的兼容能力 | ● | |
| 抗攻击性 | 最初阶段的抗攻击能力 | 取决于最初安装的选择 | |
| | 可升级性 | ● | ● |
| | 混合式支持 | ● | |
| 对盗版攻击的缓解能力 | 多样性 | ● | |
| | 可更新性 | ● | |

参考资料

“通过代码转换所获得的多样性：应用于NGNA的可更新的安全性解决方案，”作者：YongXin Zhou和Alec Main。资料来源：2006 NCTA技术白皮书

“利用多样性以防止软件的盗版”。作者：Bertrand Anckaert, Bjorn De Sutter, 和Koen De Bosschere。资料来源：2004年第4届ACM数字版权管理研讨会

“应用程序的安全性：为软件提供安全保护，”作者：Alec Main；资料来源：<http://www.stsc.hill.af.mil/crosstalk/2005/10/0510Main.html>

“最完美计划：给开发人员的警示，”作者：Lauren Weinstein；资料来源：<http://www.csl.sri.com/users/neumann/insiderisks05.html#184>

This document and the information contained herein is the subject of copyright and intellectual property rights under international convention. All rights reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical or optical, in whole or in part, without the prior written permission of Irdeto. All non-Irdeto company names, product names, and service names mentioned are used for identification purposes only and may be the registered trademarks, trademarks, or service marks of their respective owners. All information is without participation, authorization, or endorsement of the other party.

