Windows XP 系统安全防御整体解决方案

2014 年 2 月

背景

从去年开始微软曾多次公开宣布在 2014 年 4 月 8 日之后,将停止对 Windows XP 系统、Office 2003 系统的技术支持与安全漏洞修复。

根据国内著名咨询机构 CNZZ 的调查统计最新统计的结果，截止 2013 年 10 月，国内仍有高达 59%的用户使用 Windows XP 系统。根据顾问 《中国企业杀毒软件产品市场调研报告》显示，Windows XP 系统在中国企业市场份保有量高达 43%，甚至在部分政府单位和大型企业中 Windows XP 系统应用比例超过了 60%。另外，很多机关和企业的信息系统应用是在 Windows XP 系统的环境下进行开发,这为系统升级迁移带了诸多问题。而通过我们对各大企事业单位的调研,由 Windows XP 系统向 Windows 更高版本系统迁移将持续 1-5 年。

受此影响，在我国政府、军队、企业中 Windows XP 系统迁移至更高版本的系统之前，这些系统都将暴漏在各种网络威胁之中，机密信息、业务的正常运行都将受到严重威胁，一旦这些威胁发生，将产生难以估量的灾难性后果。

为此，我们国家必须在 2014 年 4 月 8 日微软停止服务之前拿出切实可行的技术方案并部署到位，保障我国境内运行的 Windows XP 系统的安全性不受此次事件的影响。

需求分析

- **全面防护**

  微软停止对 Windows XP 持续服务之后，将爆漏出大量的安全漏洞，由此带来的威胁需要在各个层面和可能性上加以防护，即全面防护，具体包括：

  - ✓ **系统加固**：能够在攻击/防护原理上解决漏洞利用的问题，通过一套加固防护机制，解决各类漏洞（而非某一具体漏洞）带来的潜在安全风险
  - ✓ **漏洞修复**：对于短期内难以在原理上、机制上解决的安全问题，通过打

补丁的方式解决具体某一安全漏洞带来的安全威胁

- ✓ **操作隔离**：对于经常出现安全问题的应用，需要将其操作通过某种技术手段与 Windows XP 系统进行逻辑隔离，保证在该应用出现安全问题的情况下，对该应用的使用与操作不会对 Windows XP 系统及系统内的重要数据产生威胁
- ✓ **制度策略**：对于特别重要的组织（如：军队、金融、能源、政府），需要提供一套避免攻击程序/代码在 Windows XP 上运行的实时监控机制与策略，保证攻击程序/代码在 Windows XP 系统上无法运行、或运行起来之后每一步操作都受到严密监控

- ➢ **快速部署**

  由于距 2014 年 4 月 8 日时间已经非常紧迫，因此我们需要提供简单、快速部署的能力，解决我国企业、政府、军队、个人用户众多 Windows XP 能够在这一天到来之前快速完成部署，形成防护能力

- ➢ **稳定兼容**

  考虑到目前各大企业、政府、金融、能源、军队单位已有应用系统非常复杂，其应用系统的稳定运行对于业务来说至关重要，因此需要方案所采用的技术必须能够与这些应用系统完全兼容，不存在稳定性的问题

- ➢ **持续运行**

  对于各大企业、政府、金融、能源、军队网络中所运行的各种业务系统来说，系统运行的持续性是一个刚性要求，频繁重启业务系统无法接受，故方案采用的技术应该尽量避免重启，或者最多只允许重启一次设备，以保障业务系统运行的持续性

方案设计

设计原则：为了彻底解决微软停止 Windows XP 系统服务带来的安全威胁，根除 Windows XP 漏洞因无法修复带来的危害，同时又全面满足各大企业、金融、能源、军队中已经部署的大量应用和对应用运行稳定型、持续性的要求，我们在设

计技术方案的时候，将始终坚持、贯彻如下的设计原则

1、 **以修复操作系统自身设计机制不足带来的安全缺陷为主（加固），**力求从根本上解决操作系统自身设计缺陷导致的安全问题，以从理论上逐类解决安全问题，而不是 Case by case 地逐个封堵、修补安全漏洞为第一目标

例如：在本方中，我们采用类似于 stackguard 的技术思路禁止在操作系统栈上禁止可执行代码来解决缓冲区溢出攻击的 shellcode 执行，这会解决一大类漏洞利用的问题（包括已知漏洞和未知漏洞），而非只针对某一具体的漏洞利用才有效

2、 **以修复操作系统代码逻辑安全漏洞的热补丁为辅（修补），**目前不能排除某些漏洞的利用方法超出了我们现有已掌握的攻击手段范围，或者某个操作系统设计机制上新的缺陷被发现并利用，在这种情况下，我们通过上面提到的操作系统加固（即修复操作系统设计机制缺陷）的手段就会失效，而对加固系统的升级相对来说周期会比较长，在这段时间内，我们可以通过针对具体漏洞进行修复的方式来暂时解决安全问题，待到加固系统升级包稳定之后，再进行加固升级，从根本上解决问题，因此，我们将修复操作系统逻辑安全漏洞的热补丁作为整体解决方案的辅助技术手段

3、 **以隔离安全问题频出应用软件的执行为（隔离）补充，**通过我们以往长时间的研究发现，大量的安全漏洞主要集中在少数关键的系统应用之上，如：PDF 阅读器、Office 软件、IE 浏览器等，因此，我们在设计整体方案的一个重要原则就是，通过技术手段（比如 Sandbox）来隔离危险应用（即安全漏洞频发的应用）的执行过程，避免这些危险应用因为遭受到攻击而破坏宿主 Windows XP 操作系统和对敏感数据的访问

4、 **以非白即黑高强度的安全管控策略自动化（制度）为保障，**在大多数对安全要求非常高的环境中（如：兵器制造业、航空航天研发机构等），要求做到万无一失，针对这种情况，我们在方案中设计了“非白即黑”的文件白名单管理原则，并且将此项管理的执行自动化，满足高度安全可控的强安全需求

整体设计：根据设计原则的要求，我们采用了多层防护、标本兼治、技术与安全管理策略相结合的整体设计思路，在 Windows XP 系统之上由内到外采用了四层防护手段，包含了加固、修复、隔离、安全策略自动化等多项举措：

- 系统加固（核心手段）
- 热补丁修复
- 危险应用隔离
- “非白即黑”安全策略

图 1. 整体方案示意图

系统加固方案

解决的问题：通过系统加固解决 Windows XP 系统自身设计机制上的缺陷带来的安全隐患，切断这些缺陷导致的漏洞利用通路。

在这里，我们针对 Windows XP 系统之上已知的 12 种可带来安全隐患的设计机制进行了加固性修复，主要包括：

- Windows XP 缺乏对执行代码内存区域进行限制的缺陷
- Windows XP 对系统调用、关键函数的内存地址分配固定化的缺陷
- Windows XP 系统开启 16 位 VDM 子系统的缺陷
- Windows XP 系统远程加载 DLL 执行代码的缺陷
- Windows XP 系统通过系统调用进入操作系统内核的缺陷

- Windows XP 系统系统调用缺乏调用者、模拟执行者身份检查的缺陷
- Windows XP 系统 DEP（数据执行保护）机制默认关闭的缺陷
- Windows XP 系统 DEP、ALSR 防护机制被绕过的缺陷
- Windows XP 系统 EAF 导出表缺乏过滤检查的缺陷
- Windows XP 系统 SEHOP 安全机制被绕过的缺陷
- Windows XP 系统对零内存页缺乏防护的缺陷
- Windows XP 对 Cookie 缺乏安全防护的缺陷

通过对上述 12 种 Windows XP 系统设计机制上缺陷的安全加固，已经可以有效解决目前已知所有通过系统漏洞、应用漏洞对 Windows XP 的攻击，从根本上解决各类漏洞带来的安全威胁。系统加固方案是针对微软 Windows XP 停止服务后带来漏洞无法修复等安全威胁的最根本的解决方案，Windows XP 系统的安全问题从本质上来说是操作系统设计的过程中，缺乏对安全充分考虑导致的问题，导致黑客可以通过各种漏洞在 Windows XP 系统中大行其道，属于操作系统设计机制上的问题，因此只有从根本上解决这些 Windows XP 系统设计机制上的缺陷，才能彻底解决问题，目前微软已经清楚地认识到了这些问题的存在，并逐渐在高版本操作系统上（如：Windows7、Windows8）开始尝试加固，但不幸的是，由于 Windows XP 系统已经发布超过 10 年，因此当时微软还没来得及发现、考虑这些问题，所以这些安全加固的成果并没有体现在 Windows XP 系统之中，本方案的最大优势就在于在 Windows XP 系统之上将这些安全机制补齐，使 Windows XP 系统即使不升级到高版本 Windows 操作系统的情况下，也能拥有健全的安全防护机制

热补丁修复方案

解决的问题：通过修改替换内存中存在安全漏洞的可执行代码，清除存在漏洞的代码，在不修改二进制代码文件的情况下，实现对漏洞的热修复

热补丁方案作为辅助方案，是通过替换掉已经加载到内存中存在安全漏洞逻辑的代码完成对系统漏洞、应用漏洞的修复，其设计逻辑如下示意图：

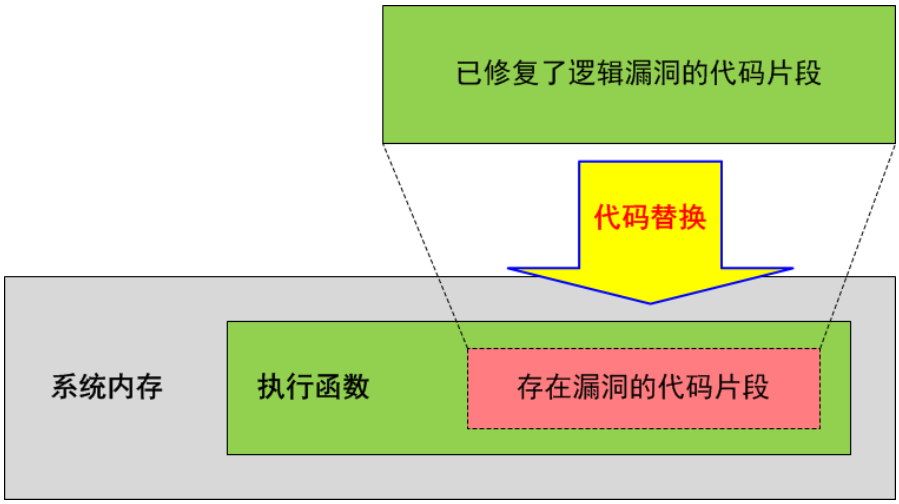

图 2. 热补丁修复过程示意图

热补丁修复是在系统内存中直接对存在安全漏洞的可执行代码进行精确的“外科手术”，替换过程与系统运行同时进行，涉及到操作同步、代码空间适配等多项复杂工作，因此精确定位存在安全漏洞代码的位置，并进行小心替换是热补丁修复成功的关键，如果替换失败，将直接导致系统崩溃或应用崩溃，因此热补丁修复技术需要有丰富的包括 Windows XP 在内的微软操作系统底层开发经验积累，同时也需要长时间 Windows 系统热补丁修复的丰富实践，在提供本方法之前，我们已经 19 次先于微软正式补丁发布向全国超过 4 亿网民提供了微软漏洞的热补丁，经过长时间的积累与实践，我们已经完全有经验、有能力在 Windows XP 上继续向系统运行稳定性要求极高的各大政府、金融、能源、企业、军队提供可修复微软 Windows XP 漏洞的热补丁

危险应用隔离方案

解决的问题：在假想系统加固与热补丁均已失效的情况下，解决危险应用（如：PDF 阅读器、Office 软件、IE 浏览器等）被漏洞利用攻击时候对 Windows XP 系统与系统敏感数据造成的威胁

危险应用隔离方案采用虚拟隔离（或称为逻辑隔离）的思想，利用沙箱（Sandbox）技术将危险应用置于沙箱中隔离运行，实现这些危险应用对于系统调用、注册表访问、文件访问、网络 IO 等涉及到安全问题的敏感操作的虚拟隔离，以此保障在这些危险应用遭受到漏洞利用攻击的情况下，也不会对其所宿主的 Windows

XP 系统及其系统资源、数据资源造成安全威胁。危险应用隔离的防护逻辑如下图所示：

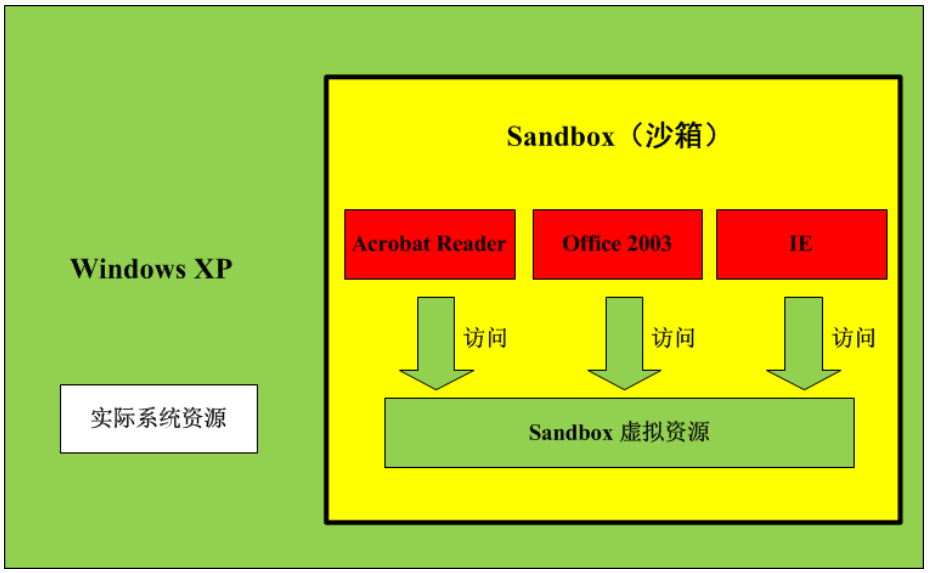

图 3. 危险应用隔离示意图

“非白即黑”策略方案（可选）

解决的问题：在假想系统加固方案、热补丁修复方案、危险应用隔离方案均失效的情况下，可以通过非白即黑的策略保证系统免受各种二进制恶意代码的攻击

“非白即黑”的安全策略采用 PE 文件白名单的机制，依托于高纯度的 PE 文件白名单库，仅允许白名单库中的文件在系统中运行（文件确认采用 MD5 的方式），而所有未在白名单库中的 PE 文件均被禁止在 Windows XP 系统上加载、运行，这就能在理论上保证所有通过 Windows XP 系统漏洞渗透进来的恶意代码均无法在 Windows XP 系统上实现攻击，其工作过程如下图所示：

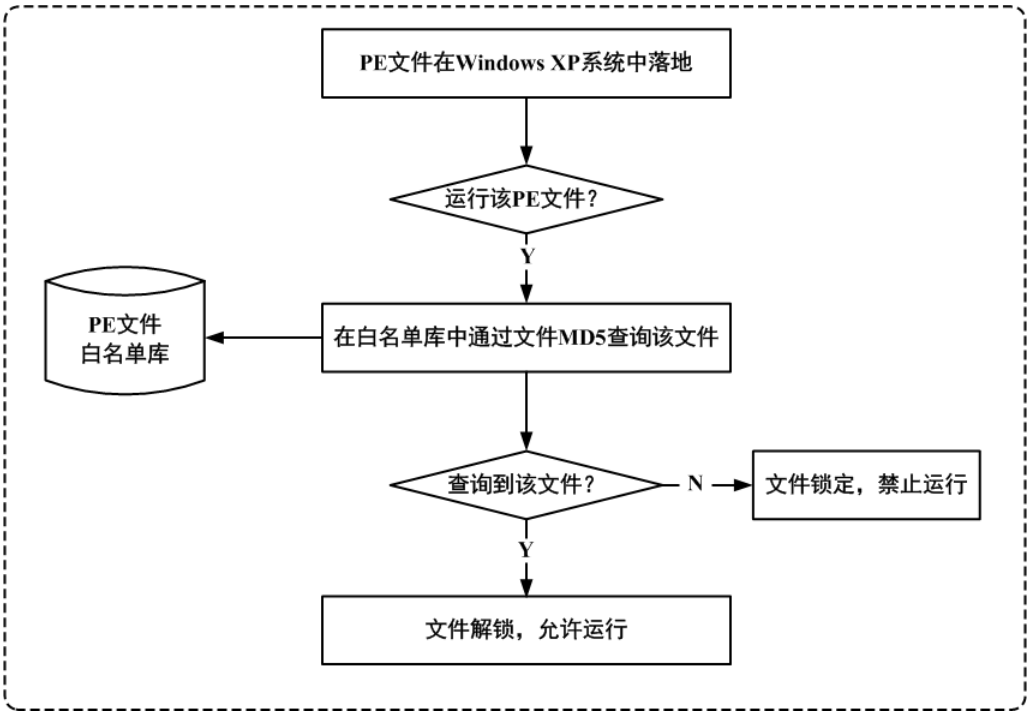

图 4. “非白即黑”策略示意图

“非白即黑”的白名单策略是美国军方、高级别政府所采用的安全防护方案，因有效防御了“火焰病毒”而受到美国政府、军队的高度重视并从此广泛部署，正因如此，为美国政府、军方提供“非白即黑”白名单策略的公司 Bit9 的产品对华禁售，因此该策略是一种已经被美国证明了行之有效的高级安全防护策略，但实施该策略需要非常高的门槛，即要对世界上出现的主要应用程序能够做到快速、全面的获取，如 Windows XP 各个版本上的所有 PE 文件，主要应用系统（如：数据库、办公软件等）各个版本的所有文件，这是一项庞大的工程，不但要求有对这些文件的快速、全面获取能力，还需要有高纯度的鉴别能力，在制定本方案之前，我们已经建立了国内最大、最快的 PE 文件获取平台，并积累了国内最大、最全、纯净度最高的 PE 文件白名单库，现在，我们的 PE 文件白名单库的规模已经接近 1 亿的白名单规模，可以保障本方案的落地

稳定性方案

由于大型政府、军队、能源、金融、企业对线上业务的高可靠性要求，无比保证系统再实施本方案之后能够持续、稳定运行。因此在提出 Windows XP 全面防护

方案的同时，需要高度关注本方案在实施、运行过程中的稳定性，在本方案的设计中，我们通过线下测试、线上回滚的方式，保障将出现问题的概率降至最低，在一旦发生故障的情况下能快速回滚到本方案实施之前的状态。

- **充分测试**

  我们的方案在发布之前，经过长期、严格的系统测试，保证能够在数亿终端上持续稳定运行一个月的前提下才会正式发布给各大企业、政府、军队等重要用户使用

- **故障回滚**

  虽然本方案在正式实施之前会经过严格、苛刻的系统测试、Beta 测试，但是并不能从理论上 100%保证不会出现故障，在此，我们采用了故障回滚的技术，在一旦发生故障的情况下能够回滚到本方案实施之前的状态，保证业务系统继续持续、稳定运行

总结：

通过本方案的全面设计，证明了采用本方案的防护手段，可以从根本上有效解决微软停止 Windows XP 服务之后带来的安全问题，并可以将由此带来的系统稳定性风险降至最低