doi :10.3969/j.issn.1671-1122.2013.10.059

基于白名单技术构建主动防御体系

章翔凌，王欢
（北京双洲科技有限公司，北京 100101）

摘 要：APT 攻击最大的特点是利用应用漏洞进行零日攻击。文章基于应用安全理论，对白名单技术进行了延展，提出了与应用相关的新的访问控制模型。由此构成对重要信息系统的主动防御体系，实现更高的安全防护要求，有效防范 APT 攻击。

关键词：白名单；应用安全；应用管控；主动防御
中图分类号：TP309 **文献标识码：**A **文章编号：**1671-1122（2013）10-0188-03

Build Active Defense System based on Whitelisting

ZHANG Xiang-ling,WANG Huan
(*Beijing Z2 Science Co., Ltd, Beijing* 100101,*China*)

Abstract: APT attack the biggest feature is used of application vulnerabilities to zero day attacks. In this paper based on application security theory, extended the whitelist technology, proposed assaciated with the application of a new access control model. Which constitutes active defense system, for important information systems, and achieve a higher level of protection, effectively preventing APT attacks.

Key words: White-List; applicaiton security;application management and control; proactive protection

网络攻击态化，APT 攻击对我国重要单位的内部网络、重要信息系统造成日益严重的威胁。我国重要信息系统实行等级保护，如何在等级保护制度下，做出何种补充，才能够有效防范 APT 攻击是本文探讨的起点。 高级持续威胁（Advanced Persistent Threat，APT ）是美国空军于 2006 年提出的概念。APT 攻击是极具针对性、多阶段、多手段组合的，具有良好定义的攻击方法，能够绕过传统安全措施。APT 攻击生命周期可分为五个阶段：1）初始攻陷，常使用零日漏洞攻击或网络钓鱼邮件；2）建立立足点，安装恶意软件或后门；3）特权升级，进行内部侦查，并主动发起对外通信；4）横向移动，维持长期存在；5）输出数据，找到窃取的目标文件后压缩归档并进行密码保护，然后使用 FTP 或后门将其输送出网络并删除归档文件。任务完成后，新的循环开始。

APT 攻击具有如下特征：1）攻击目标明确，攻击方法和工具都极具针对性；2）利用应用漏洞，进行零日漏洞攻击；3）多阶段、多手段、多层次的，攻击行为无法预测，更难以找出固定模式或特征值；4）传统安全手段无效；5）平时以窃取数据为目的，关键时刻以致瘫网络为目的。

1 基于白名单技术进行主动防御

因为 APT 攻击具有上述特点，所以最有效的防护方法就是针对目标进行主动保护。主动保护是白名单思路，与传统安全防护的黑名单思路相对。白名单思路是“枚举所有合法事项”，所有非白事项均拒绝或进行再处理。白名单不是一个新的词汇，但其含义并不明晰。目前安全技术中所提的白名单，大多是指文件、软件程序、组件、进程级白名单。

本文的白名单技术思路源于应用安全理论，基于“用户 – 应用 – 环境 – 数据”四位一体的应用安全模型建立[1]。以业务为中心，基于白名单技术构建主动防御体系，由两部分组成。一是从业务的角度，构建应用白名单，实现完整的信任传递。二是对应用进行管控，并对应用行为进行监控与防护，保证管控不被绕过，及时发现并响应异常应用行为。

2 构建主动防御体系

基于白名单技术构建的主动防御体系由两部分组成。一是从业务的角度，构建应用白名单，其核心是与应用相关的访问控制模型。通过使得应用四要素用户应用环境用户分别“变白”，并使得信任在“用户 – 应用 – 环境 – 数据”之间有效传递形成完

收稿日期：2013-09-10
作者简介：章翔凌（1963-），男，江西，硕士，主要研究方向：信息安全；王欢（1979-），女，北京，硕士，主要研究方向：信息安全管理。

整的信任链，从而实现对应用系统的主动性保护，使得应用系统变得强壮，增强应用系统自身的免疫力。

2.1 与应用相关的访问控制模型

新的访问控制模型，与传统访问控制模型相比，具有如下特点：1）主体不仅考虑用户，还考虑用户之间的关系；2）将客体拆分为应用和数据，其中应用不仅指应用程序本身，还包括应用过程；3）不仅考虑应用，还要考虑应用环境；4）在应用与数据之间添加访问控制执行点，将应用与数据隔离，对应用访问数据进行认证；5）由资产决定访问控制权限。

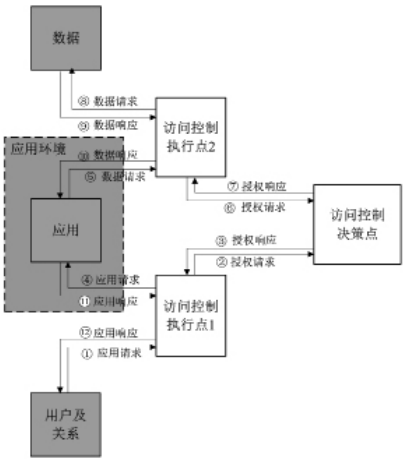

图1 与应用相关的访问控制模型

新的访问控制模型是建立应用白名单的基础。首先“用户 – 应用 – 环境 – 数据”将各个要素变白，然后使得信任在各要素之间进行有效传递，从而建立应用白名单。

1）用户“变白”。访问控制的主体不仅考虑用户，还要考虑用户之间的关系，有效防止身份假冒和特权升级攻击。一体化的访问控制。

2）应用“变白”。应用变白可在不同层次上实现。软件程序、组件级白名单，例如对于标准的、未经修改的、已知良好的软件组件、进程，进行 MD5 验证形成白名单。软件模块级白名单，对应用软件的不同功能模块进行控制，实现各个模块间的可信配合与调用。进程（线程）级白名单，通过在安全应用环境内对进程行为进行监测和管控，防止恶意代码运行。应用行为白名单，在安全应用环境内对应用行为进行管控，对新的应用或修改现有应用进行细粒度的功能 / 行为监测和管控，或者对遗留应用的输入输出行为进行监测和管控。数据访问和交换行为白名单，在数据安全网关对应用访问和交换数据的行为（包括数据的输入 / 输出、读 / 写 / 复制 / 打印 / 刻录等）进行监测和管控。

3）数据“变白”。将数据与应用隔离，建立数据安全域。在数据和应用之间，增加认证，将数据与特定应用绑定，对应用能够对数据进行的操作进行控制。

4）环境“变白”。应用环境是指特定的应用执行环境，包括硬软件平台、操作系统、定制虚拟机等。将用户与应用隔离，应用与数据隔离，将应用（或应用的功能模块）和应用环境（主要是操作系统）进行封装，构建应用安全容器。封装、隔离之后，应用在已知环境下运行，能够防止应用之间的攻击、非授权交互、应用注入攻击等。应用安全容器还可根据要求分为不同安全等级。

5）信任链在“用户 – 应用 – 环境 – 数据”间有效传递。信任链传递的难点在于信任如何“穿透应用”。通过对应用环境、应用的输入和输出进行控制，构建动态安全域，形成应用安全容器，容器的出口和入口信任一致，实现信任穿透应用。

2.2 应用监控与防护

应用不完全可信，主动防御体系需对应用进行细分，对应用行为进行更细颗粒的管控，并对应用行为进行监控与防护。

目前业界主流的应用安全防护方案在传统网络安全防护基础上，在应用安全方面做了扩展，包括网络层面的应用防火墙、Web 防火墙、邮件安全网关等；主机层面的操作系统加固、应用加固等手段；应用层面的软件白名单，以及认证、访问控制手段；数据层面的访问审计、数据防泄露系统、数据加密等手段。这些解决方案主要存在以下问题：针对特定互联网应用，最常见的是 Web 服务和 Email 服务，不具有应用普适性；各种工具分段防护，缺乏互动和连贯性；信任链不能有效传递，容易受到身份假冒和提权攻击；以黑名单技术为主，无法穷尽易被绕过；部分使用白名单技术，也仅限于文件白名单、程序和进程白名单，没有针对应用细粒度功能和组织行为的白名单；没有考虑到环境状态和时态对安全的影响。

本文的应用管控是基于应用安全理论，建立在“用户 – 应用 – 环境 – 数据”四位一体的应用安全模型基础上。应用管控可在不同层次上实现，包括软件程序（组件）级管控、软件功能模块级管控、进程（线程）级管控、应用行为管控、数据访问和交换行为管控等。应用管控实现在不同层次，亦即应用在不同层次上变白。当应用管控在进程、线程级实现时，一旦系统中隐藏的恶意软件、特殊木马等被触发，就能够被监控到。

在对应用进行细颗粒度管控的同时，对应用行为进行监控与防护。监控是指实时监控应用行为，对所有应用行为进行审计，对所有用户行为进行记录，保证管控不被绕过，及时发现并响应异常应用行为，在异常行为发生后能够追溯。保护是指建立业务模型，根据业务需要从组织行为角度对应用进行控制，建立一套的、不关联的规则，对应用访问数据的行为进行管控，如每天只能打印 5 份等，使得数据泄漏难度增加，既使数据被非法访问，也无法被窃取，实现对应用和数据进行多重保护。

3 主动防御体系的效果

对于重要信息系统，基于白名单构建主动防御体系，对应用进行管控，能够实现比等级保护更高的安全要求，能够有效防止 APT 攻击。防御效果主要体现在以下方面：

1）防止应用攻击。四位一体的应用白名单，保征在应用运行的整个过程中，不被恶意软件、特殊木马等污染或被注入攻击。

2）防止数据泄漏。当应用系统被恶意软件、特殊木马侵蚀后，通过应用管控，并以业务为中心建立保护规则，所以数据不会被泄漏到系统之外。

3）防止信息系统崩溃。当应用管控及监控到进程、线程级时，一旦恶意软件发作，就能被立即发现，保证信息系统不被破坏，防止信息系统崩溃。

4）防止 APT 攻击。在 APT 攻击的初始攻陷、建立立足点、特权升级、横向移动、数据输出的各个阶段，都进行了有针对性的防护。

4 结束语

本文设计实现了基于白名单技术构建的主动防御体系，能够增强信息系统自身的健壮性，能够有效地防范 APT 攻击。（责编 程斌）

参考文献

[1] 王欢，章翔凌．以资产为中心、自内向外的安全测评[C]．第二十二届全国信息保密学术会议（IS2012）论文集，2012:64-68.

[2] 王欢，章翔凌．基于“白名单”技术思路构建应用安全容器[J]．保密科学技术，2012,10:18-22

[3] 王欢，章翔凌．面向窃密型APT的主动安全架构——高等级内网防泄漏[C]．第二十三届全国信息保密学术会议（IS2013），2013: 32-37.

[4]BELL,D., and LAPA DULA, L. Secure computer systems: Mathematical foundations[R].MTR-2547, Volume Ⅰ, Mitre Corporation, Bedford, Massachusetts, 1973.

[5]BELL,D., and LAPA DULA, L.. Secure computer systems: A mathematical model[R].MTR-2547, Volume Ⅱ, Mitre Corporation, Bedford, Massachusetts, 1973.

[6] 王希忠，曲家兴，黄俊强等．网络数据库安全检测与管理程序设计实现[J]．信息网络安全，2012,(02):14-18.

资讯

国家网络与信息安全信息通报机制技术支持工作会议在京召开

2013 年 9 月 17 日，国家网络与信息安全信息通报机制技术支持工作会议在公安部召开，公安部十一局郭启全总工程师、新增的技术支持单位代表以及国家网络与信息安全信息通报中心有关人员共 20 余人参加会议。

会上，国家网络与信息安全信息通报中心向与会代表介绍了国家网络安全通报机制情况和近年来工作开展情况，宣布了新增的技术支持单位名单，郭启全总工程师向各单位颁发了“国家网络与信息安全信息通报机制技术支持单位”牌匾。各技术支持单位分别表态支持通报工作，介绍了本单位基本情况和技术特点，并对通报技术支持工作提出了意见建议。

郭启全总工程师在最后的讲话中，强调了国家网络安全通报机制的重要性，深入分析当前面临的网络安全形势，并对各技术支持单位提出明确工作要求，要求各技术支持单位高度重视、加强合作、充分发挥各自力量，共同维护国家网络空间安全。（记者 马珂）