ICS 35.080
L 77

中华人民共和国国家标准

GB/T 36099—2018

基于行为声明的应用软件可信性验证

Application software trustworthiness verification based on behavior declaration

2018-03-15 发布　　2018-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:国家应用软件产品质量监督检验中心、中国电子技术标准化研究院、北京工业大学、北京数字冰雹信息技术有限公司。

本标准主要起草人:宋红波、梁勇、于学军、汪璞、李健、王坤、邓潇。

基于行为声明的应用软件可信性验证

1 范围

本标准规定了应用软件行为声明的内容要求，给出了基于行为声明的应用软件可信性验证过程。

本标准适用于对个人计算机及移动信息处理设备上的应用软件进行可信性验证。

2 术语和定义

下列术语和定义适用于本文件。

2.1

应用软件可信性 application software trustworthiness

应用软件实际行为与所声明行为的一致性。

2.2

行为声明 behavior declaration

应用软件开发者对应用软件的敏感行为作出的明示承诺文件。

2.3

敏感行为 sensitive behavior

以下一种或多种行为：可能侵犯应用软件的用户权利的行为、可能侵犯其他软件权利的行为，可能影响其他软件运行的行为，可能引发用户无法预期的软硬件环境配置改变的行为。

注：包括但不限于与设备相关、与配置相关、与数据相关、与环境相关的行为。

3 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口(Application Programming Interface)

TCP：传输控制协议(Transmission Control Protocol)

UDP：用户数据报协议(User Datagram Protocol)

XML：可扩展置标语言(Extensible Markup Language)

4 应用软件行为声明内容要求

应用软件行为声明内容要求如下：

a) 行为声明文件自身应具备完整性验证机制。行为声明文件中包括基于数字签名的自身完整性验证方法，以防止对行为声明的篡改，确保行为声明的有效性。

b) 行为声明应具备对应用软件的版本和完整性进行验证的信息。行为声明包括应用软件的版本验证机制和软件完整性验证机制，以防止对应用软件文件的篡改，同时防止将行为声明用于非预期的软件版本。

c) 行为声明应包括应用软件敏感行为清单。该清单描述应用软件运行中可能产生的敏感行为，此处所述的敏感行为是指可能侵犯其用户权利的行为、可能侵犯其他软件权利的行为、可能影

响其他软件运行的行为或者引发用户无法预期的软硬件环境配置改变的行为。包括但不限于对用户隐私数据的访问、对系统配置(例如操作系统配置数据)的访问、对网络的访问、对传感器的访问、对外设(例如摄像头)的访问,以及对于其他用户关心的操作系统资源访问。

d) 应用软件敏感行为清单中声明的每项敏感行为应包含以下各项:

1) 行为名称:给出可以简要表达行为含义的行为名称。

2) 行为标识:给出行为的唯一标识。

3) 行为触发条件:描述何种条件下会触发该行为。

4) 行为授权属性:指出所描述的行为是授权的行为(应用软件允许该行为的发生),还是禁止的行为(应用软件不准许该行为的发生)。

5) 行为技术参数:对于需要使用一个或多个参数进行描述的行为,给出相应的参数值。对于无需参数进行描述的行为,此项不适用。

6) 行为预期结果:对于需要指出行为产生的结果的行为,用于表明对结果的预期。若不需要指出行为的预期结果,此项不适用。

e) 建议使用 XML 格式编写行为声明。

5 验证过程

5.1 验证准备

应用软件在进行可信性验证前,按以下规程进行验证准备工作:

a) 验证环境准备。建立验证环境,验证环境应符合软件用户手册描述的应用软件运行环境要求,同时应具备软件行为监测手段。

b) 行为声明准备。按以下步骤准备行为声明:

1) 从开发方取得与应用软件配套的行为声明文件。

2) 确定行为声明的合理性,在满足应用软件本身必须功能的前提下,不应包含与应用软件功能无关的多余内容。

3) 确定行为声明的充分性,即行为声明描述了软件中所包含的所有敏感行为。

c) 验证方案准备。该文件包括整个验证过程的各主要步骤、相应的用例和外部数据以及结果记录要求。所包含的用例和外部数据可以引用相应的文件号。

5.2 验证执行

应在符合 5.1 的条件下,依照验证方案进行验证工作。

5.3 验证报告

验证报告应符合如下要求:

a) 应反映受检应用软件在相应验证条件下的可信性验证结果。

b) 应对行为声明中敏感行为清单所列条目给出验证结果数据记录。

c) 合格判定——针对行为声明中描述的每个项目,比较验证结果与行为声明,若一致,则判定为符合可信性要求;若不一致,则判定为不符合可信性要求。

d) 形成报告——将所有项目分析和合格判定的结果汇总,形成该应用软件的可信性验证报告。报告文本应包括下列内容:

1) 验证工作基本信息描述:被测样品的名称、版本信息、软件开发单位信息、验证依据和执行时间等信息。

2) 被测样品的验证结果综述:主要描述被测样品在磁盘访问、操作系统配置数据访问、网络

访问、API 调用等方面的验证结果。

3） 验证工具列表：工具名称、工具版本信息、工具用途等信息。

4） 验证内容列表：在内容列表中要列出验证项目、验证要求和验证结果等信息。

e） 报告文本建议提供下列内容：

1） 可信性声明文件的内容；

2） 验证工具软件的原始数据导出结果。

6 应用软件可信性验证示例

在特定环境下对于应用软件部分项目的可信性验证示例参见附录 A。

附　录　A
（资料性附录）
应用软件可信性验证示例

A.1　说明

本附录给出某种操作系统下的桌面应用软件可信性验证示例。

本附录依据第5章的要求，给出可信性验证准备环节的具体示例。验证执行环节和验证报告具有较强的灵活性，由执行方自行设计。

A.2　验证准备

A.2.1　验证环境准备

本示例的验证环境如图A.1所示。

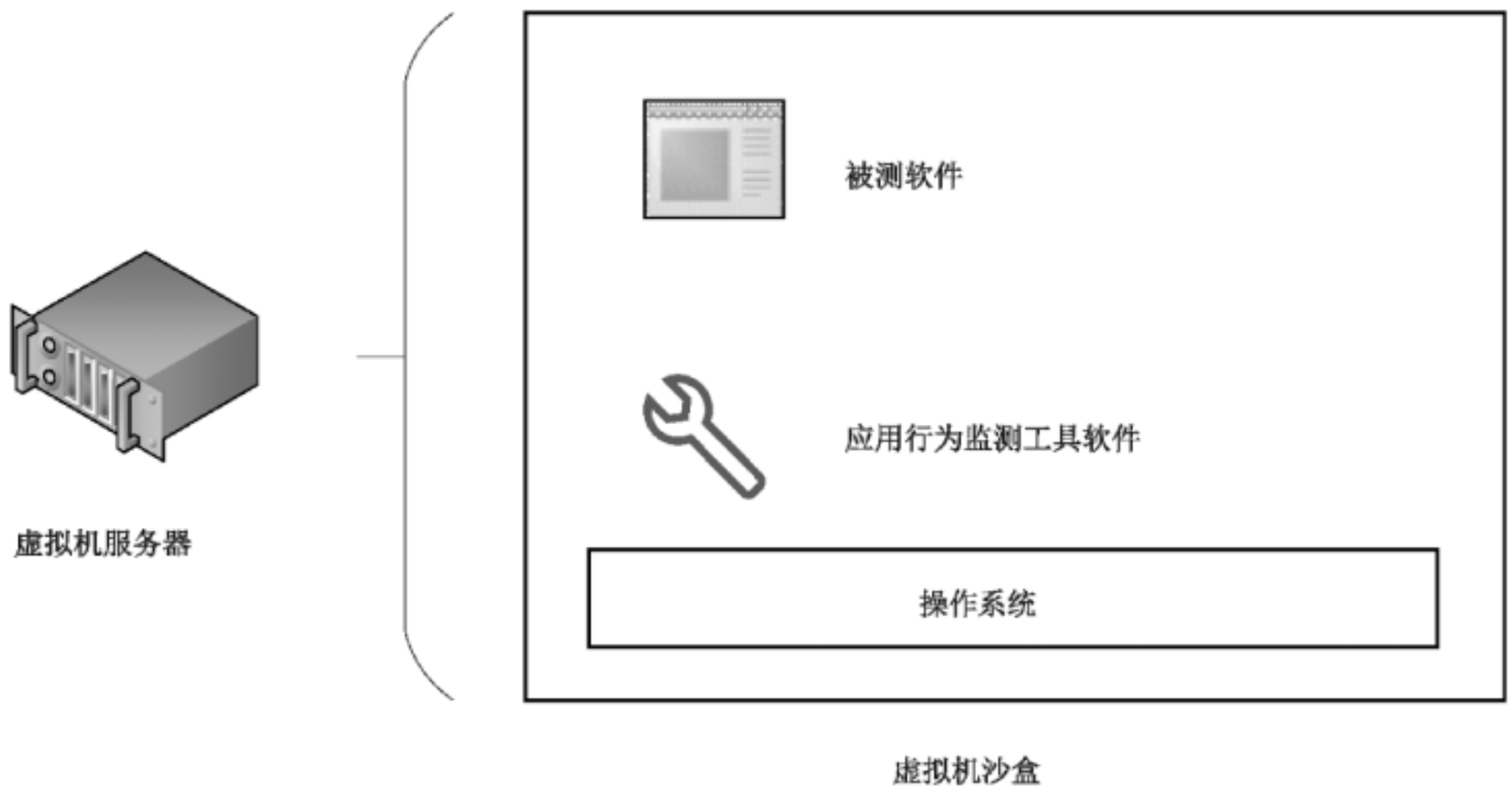

图 A.1　验证环境示意图

验证环境由一台虚拟机服务器组成，服务器内部运行一个虚拟机沙盒，沙盒内是一个带有操作系统的虚拟机环境，环境内部安装了被测软件和应用行为监测工具软件。系统配置如下：

虚拟机服务器硬件环境配置：

a）　CPU：4核8线程4.0 GHz；

b）　内存：64 G；

c）　硬盘：1T。

虚拟机服务器软件环境配置：

a）　虚机沙盒服务软件：商用虚机服务器软件。

虚拟机沙盒硬件环境配置（虚拟硬件）：

a）　CPU：4核；

b）　内存：16 G；

c）　硬盘：50 G。

虚拟机沙盒软件环境配置：

a) 操作系统：某种 32 位个人计算机桌面操作系统；

b) 应用行为监测软件：该工具使用操作系统层驱动，对应用软件运行时所发生的行为进行监测跟踪。监测内容包括：对磁盘访问的监测、对操作系统配置数据访问的监测、对网络访问的监测、对 API 调用的监测。监测工具根据软件的行为声明所要求的监测项，记录对应的软件行为结果。

A.2.2 行为声明准备

A.2.2.1 概述

本示例中，行为声明准备过程说明如下：

a) 本示例中，行为声明自身的完整性（见第 4 章要求）以及应用软件的版本验证机制和软件完整性验证机制（见第 4 章要求）在 A.2.2.2（应用软件通用信息声明）中描述。

b) 本示例中的行为声明文件描述以下几类内容：

1) 磁盘访问行为声明；

2) 操作系统配置数据访问行为声明；

3) 网络连接创建行为声明；

4) 系统 API 访问行为声明。

c) 本示例以 XML 格式编写行为声明文件。

A.2.2.2 应用软件通用信息声明

本示例中的应用软件通用信息声明描述了行为声明文件所适用的具体应用软件信息，这些信息用于确保行为声明与其所描述的应用软件之间的匹配性，从机制上确保行为声明与应用软件之间的不可分割性，以及行为声明本身的完整性。

本示例中的应用软件通用信息声明包含下列内容项：

a) 应用软件名称。

b) 版本号。

c) 编译时间。

d) 应用软件文件清单，包含文件的散列值。

e) 行为声明自身的数字签名信息。

为确保应用软件发行后的文件完整性，在应用软件中附带了发行文件清单，描述应用软件中所包含文件的文件名、路径、散列值、文件是否允许在运行过程中被修改等属性，作为应用软件完整性校验的依据。在应用软件的运行过程中，可能需要修改部分文件满足运行需求，这些文件在文件清单中进行了标示，在此情况下，这些文件的散列值仅作为初始状态的验证用途，不作为应用软件运行中的完整性验证依据。

f) 开发商公钥。

为了确保应用的来源可信性，应用所包含的动态链接库和可执行文件需要经过开发厂商的数字签名，提供开发商的数字签名公钥，用于对文件来源及完整性的验证。对于应用软件内所包含的第三方二进制组件，由第三方组件供应商确保其可信性。该公钥也被用于校验行为声明本身的来源及完整性。

应用软件通用信息声明样例如下：

＜应用行为声明＞

```
<应用软件信息>
    <应用软件名称>示例应用软件</应用软件名称>
    <版本号>1.0.2</版本号>
    <编译时间>2000.10.01 12:00:01</编译时间>
    <文件清单>
        <文件>
            <文件名>.\DEMO.exe</文件名>
            <大小>23452340</大小>
            <文件可修改性>不可修改</文件可修改性>
            <MD5> 0ca175b9c0f726a831d895e269332461</MD5>
        </文件>
        <文件>
            <文件名>.\config\DEMO.dat</文件名>
            <大小>23340</大小>
            <文件可修改性>可修改</文件可修改性>
            <MD5> 02461cac0f726a82693331d175b9895e</MD5>
        </文件>
</文件清单>
<数字签名>
  <签名算法>DSA </签名算法>
    <开发商公钥>
        <! —此处填写开发商公钥信息,略-->
    </开发商公钥>
  </数字签名>
</应用软件信息>
<敏感行为清单>
    <! —此处填写敏感行为访问规则部分的内容,略-->
</敏感行为清单>
</应用行为声明>
<! ----------数字签名内容为本行以上的部分,不含本行---------->
<数字签名值>
    KedJuTob5gtvYx9qM3k3gm7kbLBwVbEQRl26S2tmXjqNND7MRGtoew==
</数字签名值>
```

A.2.2.3 应用软件敏感行为清单

A.2.2.3.1 磁盘访问规则声明

磁盘访问规则作为行为声明中的磁盘访问行为描述,给出了应用软件在运行过程中的磁盘访问行为项,包括允许访问规则、禁止访问规则和可疑访问规则。

每条访问规则包含如下信息:

a) 规则属性:禁止访问、允许访问、可疑访问。

b) 磁盘访问指令:打开文件、读取文件、写入文件、删除文件、关闭文件、创建文件、修改文件属性、修改安全性属性、其他 I/O 操作事件。

c) 目标路径:该磁盘 I/O 操作所对应的目标磁盘路径。

d) 操作结果:成功、失败、未知。

以上规则中要求支持模糊匹配,例如磁盘访问位置可允许类似“\abc\sys * .bin”的形式。

基于 XML 的磁盘访问规则样例如下:

```
<磁盘访问规则项列表>
<磁盘访问规则项>
    <操作>IRP_MJ_CREATE</操作>
    <目标路径> * </目标路径>
    <操作结果>成功</操作结果>
    <规则属性>允许访问</规则属性>
</磁盘访问规则项>
<磁盘访问规则项>
    <操作>IRP_MJ_READ</操作>
    <目标路径>\App\ * </目标路径>
    <操作结果> * </操作结果>
    <规则属性>禁止访问</规则属性>
</磁盘访问规则项>
</磁盘访问规则项列表>
```

A.2.2.3.2 操作系统配置数据访问规则声明

操作系统配置数据访问规则作为行为声明中对于操作系统相关的配置信息访问行为的描述,给出了应用软件在运行过程中对操作系统配置信息访问行为的声明,包括允许访问规则、禁止访问规则和可疑访问规则。

每条访问规则包含如下信息:

a) 规则属性:禁止访问、允许访问、可疑访问。

b) 操作系统配置数据访问指令。

c) 目标操作系统配置数据路径:该操作所对应的目标操作系统配置数据路径,在本示例中,该路径表明配置数据库中的键路径。

d) 操作结果:成功、失败、未知。

以上规则中要求支持模糊匹配,例如操作系统配置数据访问位置可允许类似“KEY1\KEY2\ * ”的形式。

基于 XML 的操作系统配置数据访问规则样例如下:

```
<操作系统配置数据访问规则项列表>
<操作系统配置数据访问规则项>
    <操作> RegNtRenameKey</操作>
    <目标路径> SOMEKEY\ * </目标路径>
    <操作结果>成功</操作结果>
    <规则属性>允许访问</规则属性>
</操作系统配置数据访问规则项>
```

A.2.2.3.3 网络访问规则声明

网络访问规则作为行为声明中网络访问的描述,给出了应用软件在运行过程中的网络访问行为声明,包括允许访问规则、禁止访问规则和可疑访问规则。

每条访问规则包含如下信息：

a） 规则属性：禁止访问、允许访问、可疑访问。

b） 协议类型：TCP 协议或 UDP 协议。

c） 目标地址：网络访问所包含的目的地址，若目标地址不可用，可留空。

d） 目标端口：网络访问所对应的目标端口，若目标端口不可用，可留空。

e） 操作类型：创建远端连接、监听本地端口。

以上规则中要求可疑支持模糊匹配，例如目标地址许类似“192.168.*.*”的形式。

基于 XML 的网络访问规则样例如下：

```
<网络访问规则项列表>
<网络访问规则项>
    <协议类型>TCP</协议类型>
    <目标地址>10.0.0.1</目标地址>
    <目标端口>80</目标端口>
    <操作类型>建立连接</操作类型>
    <规则属性>允许访问</规则属性>
    </网络访问规则项>
    </网络访问规则项列表>
```

A.2.2.3.4 API 调用规则声明

API 调用规则作为行为声明中 API 调用的描述，给出了应用软件在运行过程中的 API 调用行为声明，包括允许访问规则、禁止访问规则和可疑访问规则。

每条访问规则包含如下信息：

a） 规则属性：禁止访问、允许访问、可疑访问。

b） API 名称：API 函数名。

c） API 参数集合：API 调用所包含的参数堆栈缓冲区，用 16 进制表示。

d） 返回值：API 调用的返回值，用 16 进制描述。

e） API 所属模块：本 API 所在的 DLL 模块。

以上规则中要求支持模糊匹配，例如 API 名称允许类似“GetText?”的形式，用于匹配 GetTextA 和 GetTextW。

基于 XML 的 API 调用规则样例如下：

```
<API 调用控制规则列表>
    <API 调用规则>
        <API 名称> GetText? </API 名称>
        <API 参数集合> * </API 参数集合>
        <返回值> * </返回值>
        <API 所属模块> test.dll</API 所属模块>
        <规则属性>允许访问</规则属性>
    </API 调用规则>
</API 调用控制规则列表>
```

A.2.3 验证方案准备

本示例中的验证方案包括以下内容：

a） 验证环境：见 A.2.1。

b） 参考文件：《软件用户手册》《软件需求说明书》。

c） 验证计划：包括执行本次验证的时间进度及参与人员安排，见表 A.1。

表 A.1 验证计划表

序号	工作任务	时间	开始日期	结束日期	参与人
1	分析软件使用流程	0.5 工作日			
2	制订验证方案	0.5 工作日			
3	制订验证用例	2 工作日			
4	执行验证测试	2 工作日			
5	编写验证报告	2 工作日			

d） 验证用例：通过软件需求说明书和软件用户手册描述的软件功能和使用方法制订验证用例，使得用例覆盖软件的全部使用流程。用例范例见表 A.2。

表 A.2 验证用例表

<table>
<tr><td>软件名称及版本</td><td colspan="2">示例软件 V1.0</td><td>验证项标识</td><td colspan="2">DLRJ_GN</td></tr>
<tr><td>用例名称</td><td colspan="2">打开文件_01</td><td>验证用例标识</td><td colspan="2">SLRJ_DKWJ_01</td></tr>
<tr><td>验证说明</td><td colspan="5">验证打开文件时软件的行为是否符合行为声明</td></tr>
<tr><td>前置条件</td><td colspan="5"></td></tr>
<tr><td colspan="6">用例输入及输出</td></tr>
<tr><td>序号</td><td>输入步骤</td><td>测试数据</td><td colspan="2">预期结果</td><td>实际结果</td></tr>
<tr><td>1</td><td>启动软件</td><td></td><td colspan="2">无违规行为</td><td></td></tr>
<tr><td>2</td><td>打开数据文件</td><td>文件 1.txt</td><td colspan="2">无违规行为</td><td></td></tr>
<tr><td>3</td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">设计人员</td><td colspan="2">张三</td><td>设计日期</td><td>2014.01.01</td></tr>
<tr><td colspan="2">验证结论</td><td colspan="4">□ 通过 □ 未通过 □_____</td></tr>
<tr><td colspan="2">问题标识</td><td colspan="4"></td></tr>
<tr><td colspan="2">执行人员</td><td colspan="2"></td><td>执行
日期</td><td></td></tr>
</table>

e） 结果记录：分为用例执行结果判定记录和原始验证数据记录。

1） 原始验证数据记录是指由应用行为监测工具软件产生的原始数据记录。此部分记录作为原始数据留存。

2） 用例执行结果判定记录是指由验证执行人员通过比对原始数据和行为声明，判定得出的用例执行的实际结果，记载至表 A.3 中“实际结果”一列。示例如下：

表 A.3　验证用例判定结果表

<table>
<tr><td>软件名称及版本</td><td colspan="2">示例软件 V1.0</td><td>验证项标识</td><td>DLRJ_GN</td></tr>
<tr><td>用例名称</td><td colspan="2">打开文件_01</td><td>验证用例标识</td><td>SLRJ_DKWJ_01</td></tr>
<tr><td>验证说明</td><td colspan="4">验证打开文件时软件的行为是否符合行为声明</td></tr>
<tr><td>前置条件</td><td colspan="4"></td></tr>
<tr><td colspan="5">用例输入及输出</td></tr>
<tr><td>序号</td><td>输入步骤</td><td>测试数据</td><td>预期结果</td><td>实际结果</td></tr>
<tr><td>1</td><td>启动软件</td><td></td><td>无违规行为</td><td>无违规行为</td></tr>
<tr><td>2</td><td>打开数据文件</td><td>文件 1.txt</td><td>无违规行为</td><td>API 违规</td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td></tr>
<tr><td>设计人员</td><td colspan="2">张三</td><td>设计日期</td><td>2014.01.01</td></tr>
<tr><td>验证结论</td><td colspan="4">□ 通过　　☑未通过　　□_____</td></tr>
<tr><td>问题描述</td><td colspan="4">应用程序执行本用例步骤 2 时，出现行为声明中未声明的敏感行为：权限提升调用</td></tr>
<tr><td>执行人员</td><td colspan="2">张三</td><td>执行日期</td><td>2014.01.01</td></tr>
</table>

中 华 人 民 共 和 国
国 家 标 准
基于行为声明的应用软件可信性验证
GB/T 36099—2018
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018 年 3 月第一版
*
书号:155066·1-59758

GB/T 36099-2018