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