



中华人民共和国公共安全行业标准

GA/T 1485—2018

信息安全技术 工业控制系统 入侵检测产品安全技术要求

Information security technology—Security technical requirements for
industrial control system intrusion detection products

2018-05-07 发布

2018-05-07 实施

中华人民共和国公安部 发布

目 次

| | |
|----------------------|----|
| 前言 | I |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语和定义 | 1 |
| 4 总体说明 | 1 |
| 4.1 安全技术要求分类 | 1 |
| 4.2 安全等级划分 | 1 |
| 5 安全功能要求 | 2 |
| 5.1 数据探测功能 | 2 |
| 5.2 入侵分析功能 | 2 |
| 5.3 入侵响应功能 | 3 |
| 5.4 管理控制功能 | 3 |
| 5.5 检测结果处理 | 4 |
| 5.6 标识与鉴别 | 4 |
| 5.7 管理安全 | 4 |
| 5.8 安全审计 | 5 |
| 5.9 产品自身安全 | 5 |
| 6 安全保障要求 | 6 |
| 6.1 开发 | 6 |
| 6.2 指导性文档 | 7 |
| 6.3 生命周期支持 | 7 |
| 6.4 测试 | 8 |
| 6.5 脆弱性评定 | 8 |
| 7 安全等级划分要求 | 8 |
| 7.1 概述 | 8 |
| 7.2 安全功能要求等级划分 | 9 |
| 7.3 安全保障要求等级划分 | 10 |

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部信息系统安全产品质量监督检验中心、公安部第三研究所、北京神州绿盟科技有限公司、启明星辰信息技术集团股份有限公司。

本标准主要起草人：沈清泓、邹春明、顾健、张笑笑、俞优、邱梓华、王晓鹏、景晓晖。

信息安全技术 工业控制系统 入侵检测产品安全技术要求

1 范围

本标准规定了工业控制系统入侵检测产品的安全功能要求、安全保障要求和安全等级划分要求。本标准适用于工业控制系统入侵检测产品的设计、开发及测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件

GB/T 25069—2010 信息安全技术 术语

GB/T 30976.1—2014 工业控制系统信息安全 第1部分:评估规范

GB/T 30976.2—2014 工业控制系统信息安全 第2部分:验收规范

3 术语和定义

GB/T 18336.3—2015、GB/T 25069—2010、GB/T 30976.1—2014 和 GB/T 30976.2—2014 界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统入侵检测产品 industrial control system intrusion detection product

面向工业控制系统,旁路部署在工业控制网络中,以工业控制网络上的数据包作为数据源,监听所保护工业控制网络内的所有数据包并进行分析,从而发现异常行为的入侵检测产品。

4 总体说明

4.1 安全技术要求分类

本标准将工业控制系统入侵检测产品安全技术要求分为安全功能要求和安全保障要求两大类。其中,安全功能要求对工业控制系统入侵检测产品应具备的安全功能提出具体要求,包括数据探测、入侵分析、入侵响应、管理控制、检测结果处理、标识与鉴别、管理安全、安全审计、产品自身安全等;安全保障要求针对工业控制系统入侵检测产品的生命周期过程提出具体要求,例如开发、指导性文档、生命周期支持和测试等。

4.2 安全等级划分

本标准按照工业控制系统入侵检测产品安全功能的强度划分安全功能要求的级别,参照 GB/T 18336.3—2015 划分安全保障要求的级别。安全等级突出安全特性,分为基本级和增强级,安全功能要求强弱和安全保障要求高低是等级划分的具体依据。

5 安全功能要求

5.1 数据探测功能

5.1.1 数据收集

应具有实时获取受保护网段内的数据包的能力。

5.1.2 协议识别

至少应识别基于以下协议的事件：

- a) 网络层协议：TCP/IP；
- b) 应用层协议：ModBus TCP、OPC、S7 等。

5.1.3 行为监测

至少应监视以下行为：端口扫描、工程师站组态变更、操作站数据与操作指令变更，以及资产变更、通信行为等。

5.1.4 流量监测

应监视整个网络或者某一特定协议、地址、端口的报文流量和字节流量，特别是异常流量的监测。

5.1.5 协议定义

除支持默认的工控协议集外，支持基于应用的协议自动识别，还应允许授权管理员定义新的协议，或对协议的端口进行重新定位。

5.2 入侵分析功能

5.2.1 数据分析

应对收集的数据包进行分析，发现攻击事件。

5.2.2 分析方式

应以模式匹配、协议分析等一种或多种方式进行入侵分析。

5.2.3 参数分析

应具备过程状态参数、控制信号的阈值检查功能。

5.2.4 恶意代码识别

应支持恶意代码识别的功能，如对木马、蠕虫等的识别。

5.2.5 防躲避能力

应能发现躲避或欺骗检测的行为，如 TCP 流重组、协议端口重定位等。

5.2.6 事件合并

应具有对高频度发生的相同安全事件进行合并告警的功能。

5.2.7 事件关联

应具有将不同的事件关联起来,发现低危害事件中隐含的高危害攻击的能力。

5.3 入侵响应功能

5.3.1 安全告警

当检测到入侵时,应自动采取相应动作以发出安全告警。

5.3.2 告警方式

告警方式可以采取界面实时提示、声音告警等方式中一种或多种方式。

5.3.3 报文留存

在监测到网络上的攻击行为时,应具有自动保存攻击报文的能力。

5.3.4 排除响应

应允许管理员定义对被检测网段中指定的主机或特定的事件不予告警。

5.3.5 定制响应

应允许管理员对被检测网段中指定的主机或特定的事件定制不同的响应方式,以对特定的事件突出告警。

5.4 管理控制功能

5.4.1 事件数据库

应提供事件数据库,包括事件定义和分析、详细的漏洞修补方案、可采取的对策等。

5.4.2 事件分级

应按照事件的严重程度将事件分级,以使授权管理员能从大量信息中捕捉到危险的事件。

5.4.3 策略配置

应提供安全策略配置功能,并支持:

- a) 对安全策略进行添加、删除、修改和分发;
- b) 对安全策略进行的导入和导出。

5.4.4 产品升级

应具有及时更新、升级产品和事件库的能力,支持离线升级并保证升级安全。

5.4.5 分布式部署

应具有本地或异地分布式部署、远程管理的能力。

5.4.6 端口分离

探测器应配备不同的端口分别用于产品管理和网络数据监听。

5.5 检测结果处理

5.5.1 事件记录

应记录并保存检测到的入侵事件。入侵事件信息应至少包含以下内容：事件发生时间、源地址、目的地址、危害等级等。

5.5.2 报告生成

应能生成检测结果报告。报告应至少包含事件详细描述、解决方案建议等。

5.5.3 报告模板定制

应具有自定义报告模板的功能。

5.5.4 报告查阅

应具有查询检测结果报告的功能。

5.5.5 报告导出

应具有支持检测结果报告导出的功能。

5.6 标识与鉴别

5.6.1 唯一性标识

应为用户提供唯一标识,并能将标识与其所有可审计事件相关联。

5.6.2 基本鉴别

应在执行任何与安全功能相关的操作前鉴别用户身份。

5.6.3 多重鉴别

应为用户提供两种或两种以上的鉴别机制。

5.6.4 超时机制

应提供超时重新鉴别机制,如果用户停止操作的时间超过一定时限,应对用户身份重新进行鉴别。时限仅由授权管理员进行设置。

5.6.5 鉴别数据保护

应保护鉴别数据不被未经授权查阅和修改。

5.6.6 鉴别失败处理

当对用户身份鉴别失败的次数达到设定值后,应能终止用户的访问。

5.7 管理安全

5.7.1 安全角色管理

应能对授权管理员设置不同的管理角色,并赋予不同的管理权限。

5.7.2 数据保护

5.7.2.1 数据存储保护

应能对存储的重要数据进行保护,以免被非授权访问。这些重要数据至少包括:

- a) 用户的鉴别信息;
- b) 产品的审计日志、安全配置和安全策略等。

5.7.2.2 数据传输保护

应采取安全措施保护重要数据在传输过程中不被泄露和窃取。这些重要数据至少包括:

- a) 用户的鉴别信息;
- b) 产品的安全配置和安全策略等。

5.8 安全审计

5.8.1 审计日志生成

应对与自身安全相关的下列事件生成审计日志:

- a) 用户登录成功和失败;
- b) 对安全策略进行更改;
- c) 对用户进行增加、删除和属性修改;
- d) 因鉴别失败的次数超出设定值而导致的会话连接终止;
- e) 对事件记录、审计日志的操作。

5.8.2 审计日志内容

审计日志至少应包括事件发生的日期、时间、用户标识、事件描述和结果等。若采用远程登录方式对产品进行管理,还应记录管理主机的地址。

5.8.3 审计日志查阅

应支持按照一定条件对审计日志进行查阅。

5.8.4 审计日志存储

审计日志应存储于掉电非易失性存储介质中,并满足以下要求:

- a) 当审计日志存储空间超过阈值时,应能通知用户;
- b) 当审计日志存储空间将要耗尽时,应采取相应的防止审计数据丢失的技术措施。

5.9 产品自身安全

5.9.1 自我隐藏

应采取隐藏探测器 IP 地址等措施使产品自身在网络上不可见,以降低被攻击的可能性。

5.9.2 自我监测

在启动和正常工作时,应周期性地、或者按照授权管理员的要求执行自检,以验证产品自身执行的正确性。

6 安全保障要求

6.1 开发

6.1.1 安全架构

开发者应提供产品安全功能的安全架构描述。安全架构描述应满足以下要求：

- a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
- b) 描述与安全功能要求一致的产品安全功能的安全域；
- c) 描述产品安全功能初始化过程为何是安全的；
- d) 证实产品安全功能能够防止被破坏；
- e) 证实产品安全功能能够防止安全特性被旁路。

6.1.2 功能规范

开发者应提供完备的功能规范说明。功能规范说明应满足以下要求：

- a) 完全描述产品的安全功能；
- b) 描述所有安全功能接口的目的与使用方法；
- c) 标识和描述每个安全功能接口相关的所有参数；
- d) 描述安全功能接口相关的安全功能实施行为；
- e) 描述由安全功能实施行为处理而引起的直接错误消息；
- f) 证实安全功能要求到安全功能接口的追溯；
- g) 描述安全功能实施过程中，与安全功能接口相关的所有行为；
- h) 描述可能由安全功能接口的调用而引起的所有直接错误消息。

6.1.3 实现表示

开发者应提供全部安全功能的实现表示。实现表示应满足以下要求：

- a) 提供产品设计描述与实现表示实例间的映射，并证明其一致性；
- b) 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的水平；
- c) 以开发人员使用的形式提供。

6.1.4 产品设计

开发者应提供产品设计文档。产品设计文档应满足以下要求：

- a) 根据子系统描述产品结构；
- b) 标识和描述产品安全功能的所有子系统；
- c) 描述安全功能所有子系统间的相互作用；
- d) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
- e) 根据模块描述安全功能；
- f) 提供安全功能子系统到模块间的映射关系；
- g) 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
- h) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
- i) 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

6.2 指导性文档

6.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南,操作用户指南与为评估而提供的其他所有文档保持一致。对每一种用户角色的描述应满足以下要求:

- a) 描述在安全处理环境中被控制的用户可访问的功能和特权,包含适当的警示信息;
- b) 描述如何以安全的方式使用产品提供的可用接口;
- c) 描述可用功能和接口,尤其是受用户控制的所有安全参数,适当时指明安全值;
- d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件,包括改变安全功能所控制实体的安全特性;
- e) 标识产品运行的所有可能状态(包括操作导致的失败或者操作性错误),以及它们与维持安全运行之间的因果关系和联系;
- f) 充分实现安全目的所必须执行的安全策略。

6.2.2 准备程序

开发者应提供产品及其准备程序,准备程序描述应满足以下要求:

- a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤;
- b) 描述安全安装产品及其运行环境必需的所有步骤。

6.3 生命周期支持

6.3.1 配置管理能力

开发者的配置管理能力应满足以下要求:

- a) 为产品的不同版本提供唯一的标识。
- b) 使用配置管理系统对组成产品的所有配置项进行维护,并唯一标识配置项。
- c) 提供配置管理文档,配置管理文档描述用于唯一标识配置项的方法。
- d) 配置管理系统提供一种自动方式来支持产品的生成,通过该方式确保只能对产品的实现表示进行已授权的改变。
- e) 配置管理文档包括一个配置管理计划,配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致。
- f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

6.3.2 配置管理范围

开发者应提供产品配置项列表,并说明配置项的开发者。配置项列表应包含以下内容:

- a) 产品、安全保障要求的评估证据和产品的组成部分;
- b) 实现表示、安全缺陷报告及其解决状态。

6.3.3 交付程序

开发者应按照一定的交付程序交付产品,并将交付程序文档化。在给用户方交付产品的各版本时,交付文档应描述为维护安全所必需的所有程序。

6.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中,为保护产品设计和实现

的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

6.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制,并提供生命周期定义文档,描述用于开发和维护产品的模型。

6.3.6 工具和技术

开发者应明确定义用于开发产品的工具,并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

6.4 测试

6.4.1 测试覆盖

开发者应提供测试覆盖文档。测试覆盖描述应满足以下要求:

- a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性;
- b) 表明上述对应性是完备的,并证实功能规范中的所有安全功能接口都进行了测试。

6.4.2 测试深度

开发者应提供测试深度分析。测试深度分析描述应满足以下要求:

- a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块间的一致性;
- b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

6.4.3 功能测试

开发者应测试产品安全功能,将结果文档化并提供测试文档。测试文档应包括以下内容:

- a) 测试计划,标识要执行的测试,并描述执行每个测试的方案,这些方案包括对于其他测试结果的任何顺序依赖性;
- b) 预期的测试结果,表明测试成功后的预期输出;
- c) 实际测试结果和预期的测试结果的一致性。

6.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源,以用于安全功能的抽样测试。

6.5 脆弱性评定

基于已标识的潜在脆弱性,产品能够抵抗以下攻击行为:

- a) 具有基本攻击潜力的攻击者的攻击;
- b) 具有增强型基本攻击潜力的攻击者的攻击。

7 安全等级划分要求

7.1 概述

本标准将工业控制系统入侵检测产品的安全技术要求划分成基本级和增强级。

基本级规定了工业控制系统入侵检测产品的最低安全要求。通过简单的管理员标识和鉴别来限制对产品的功能配置和数据访问的控制,使管理员具备自主安全保护的能力,阻止非授权管理员危害系

统,保护产品的正常运行。

增强级划分了安全管理角色,以细化对工业控制系统入侵检测产品的管理。通过访问控制、产品的自身保护等要求,对工业控制系统入侵检测产品的正常运行提供更强的保护。本级还要求产品具有协议定义、参数分析、恶意代码识别、防躲避能力、事件合并、事件关联、报文留存、排除响应、定制响应、分布式部署、端口分离、报告模板定制、多重鉴别、超时机制、鉴别数据保护、鉴别失败处理、审计日志存储、自我监测等功能。同时,还增加了管理安全、产品自身安全运行的措施,要求产品具有较强的抗攻击能力。

7.2 安全功能要求等级划分

工业控制系统入侵检测产品的安全功能要求等级划分如表 1 所示。

表 1 工业控制系统入侵检测产品安全功能要求等级划分

| 安全功能要求 | | 基本级 | 增强级 |
|--------|--------|-------|-------|
| 数据探测功能 | 数据收集 | 5.1.1 | 5.1.1 |
| | 协议识别 | 5.1.2 | 5.1.2 |
| | 行为监测 | 5.1.3 | 5.1.3 |
| | 流量监测 | 5.1.4 | 5.1.4 |
| | 协议定义 | — | 5.1.5 |
| 入侵分析功能 | 数据分析 | 5.2.1 | 5.2.1 |
| | 分析方式 | 5.2.2 | 5.2.2 |
| | 参数分析 | — | 5.2.3 |
| | 恶意代码识别 | — | 5.2.4 |
| | 防躲避能力 | — | 5.2.5 |
| | 事件合并 | — | 5.2.6 |
| | 事件关联 | — | 5.2.7 |
| 入侵响应功能 | 安全告警 | 5.3.1 | 5.3.1 |
| | 告警方式 | 5.3.2 | 5.3.2 |
| | 报文留存 | — | 5.3.3 |
| | 排除响应 | — | 5.3.4 |
| | 定制响应 | — | 5.3.5 |
| 管理控制功能 | 事件数据库 | 5.4.1 | 5.4.1 |
| | 事件分级 | 5.4.2 | 5.4.2 |
| | 策略配置 | 5.4.3 | 5.4.3 |
| | 产品升级 | 5.4.4 | 5.4.4 |
| | 分布式部署 | — | 5.4.5 |
| | 端口分离 | — | 5.4.6 |

表 1 (续)

| 安全功能要求 | | 基本级 | 增强级 |
|--------|--------|--------------------|-------|
| 检测结果处理 | 事件记录 | 5.5.1 | 5.5.1 |
| | 报告生成 | 5.5.2 | 5.5.2 |
| | 报告模板定制 | — | 5.5.3 |
| | 报告查阅 | 5.5.4 | 5.5.4 |
| | 报告导出 | 5.5.5 | 5.5.5 |
| 标识与鉴别 | 唯一性标识 | 5.6.1 | 5.6.1 |
| | 基本鉴别 | 5.6.2 | 5.6.2 |
| | 多重鉴别 | — | 5.6.3 |
| | 超时机制 | — | 5.6.4 |
| | 鉴别数据保护 | — | 5.6.5 |
| | 鉴别失败处理 | — | 5.6.6 |
| 管理安全 | 安全角色管理 | — | 5.7.1 |
| | 数据保护 | 数据存储保护 | 5.7.2 |
| | | 数据传输保护 | 5.7.3 |
| 安全审计 | 审计日志生成 | 5.8.1 a) ~5.8.1 c) | 5.8.1 |
| | 审计日志内容 | 5.8.2 | 5.8.2 |
| | 审计日志查阅 | 5.8.3 | 5.8.3 |
| | 审计日志存储 | — | 5.8.4 |
| 产品自身安全 | 自我隐藏 | 5.9.1 | 5.9.1 |
| | 自我监测 | — | 5.9.2 |

7.3 安全保障要求等级划分

工业控制系统入侵检测产品的安全保障要求等级划分如表 2 所示。

表 2 工业控制系统入侵检测产品安全保障要求等级划分

| 安全保障要求 | | 基本级 | 增强级 |
|--------|--------|--------------------|-------|
| 开发 | 安全架构 | 6.1.1 | 6.1.1 |
| | 功能规范 | 6.1.2 a) ~6.1.2 f) | 6.1.2 |
| | 实现表示 | — | 6.1.3 |
| | 产品设计 | 6.1.4 a) ~6.1.4 d) | 6.1.4 |
| 指导性文档 | 操作用户指南 | 6.2.1 | 6.2.1 |
| | 准备程序 | 6.2.2 | 6.2.2 |

表 2 (续)

| 安全保障要求 | | 基本级 | 增强级 |
|--------|--------|--------------------|--------|
| 生命周期支持 | 配置管理能力 | 6.3.1 a) ~6.3.1 c) | 6.3.1 |
| | 配置管理范围 | 6.3.2 a) | 6.3.2 |
| | 交付程序 | 6.3.3 | 6.3.3 |
| | 开发安全 | — | 6.3.4 |
| | 生命周期定义 | — | 6.3.5 |
| | 工具和技术 | — | 6.3.6 |
| 测试 | 测试覆盖 | 6.4.1 a) | 6.4.1 |
| | 测试深度 | — | 6.4.2 |
| | 功能测试 | 6.4.3 | 6.4.3 |
| | 独立测试 | 6.4.4 | 6.4.4 |
| 安全保障要求 | | 基本级 | 增强级 |
| 脆弱性评定 | | 6.5 a) | 6.5 b) |
