(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103973679 B
(45)授权公告日 2017.02.15

(21)申请号 201410177570.8

(22)申请日 2014.04.29

(65)同一申请的已公布的文献号
申请公布号 CN 103973679 A

(43)申请公布日 2014.08.06

(73)专利权人 重庆邮电大学
地址 400065 重庆市南岸区黄桷垭崇文路2号

(72)发明人 魏旻 王平 王维 王浩 洪承镐 屈洪春 陈豪

(74)专利代理机构 重庆市恒信知识产权代理有限公司 50102
代理人 刘小红

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)

(56)对比文件
CN 101951414 A,2011.01.19,
CN 102625312 A,2012.08.01,
CN 102333307 A,2012.01.25,
US 2007283001 A1,2007.12.06,
US 2007233881 A1,2007.10.04,
US 2009097397 A1,2009.04.16,

审查员 王相君

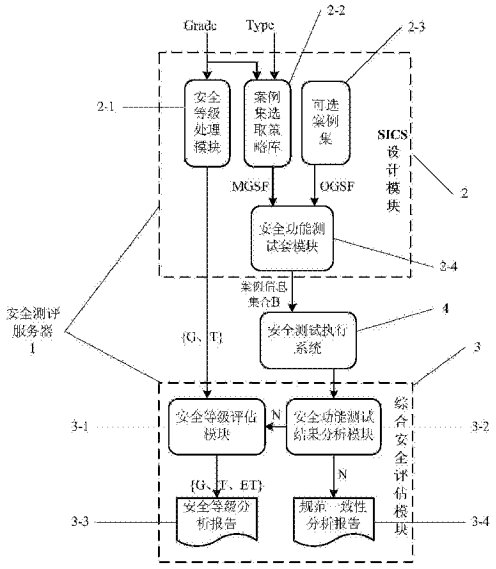
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种基于安全等级的传感网安全测评系统

(57)摘要

本发明公开了一种基于安全等级的传感网安全测评系统，用于测评设备的安全性，评估设备符合的安全等级，同时对系统的安全性能进行评估。本发明系统包括SICS设计模块、安全测评执行模块和综合安全评估模块。测试端作为安全等级和功能设备类型选择接口，安全测评服务器根据安全等级和设备类型自动生成安全功能测试套，并接收系统执行测试后的结果。服务器对功能测试结果进行分析并生成规范一致性测试报告，同时结合功能测试结果和安全等级强度要求，生成安全等级分析报告。本发明系统的测评结果能反映设备安全功能的实现是否与规范一致，特别是能将等级结果与事先声明的等级对比，分析设备的安全性，同时为设备的安全功能改善提供参考依据。



CN 103973679 B

1.一种基于安全等级的传感网安全测评系统，其特征在于包括：安全测评服务器(1)和设置于待测传感网络端的安全测试执行系统(4)，所述安全测评服务器(1)包括SICS安全实现一致性声明设计模块(2)和综合安全评估模块(3)；

所述SICS安全实现一致性声明设计模块(2)包括安全等级处理模块(2-1)、案例集选取策略库(2-2)、可选案例集(2-3)和安全功能测试套模块(2-4)；

所述综合安全评估模块(3)包括安全等级评估模块(3-1)、安全功能测试结果分析模块(3-2)、安全等级分析报告模块(3-3)和规范一致性分析报告模块(3-4)；

当测试待测传感网时，测试端一边将设备的安全等级Grade传输给安全等级处理模块(2-1)及案例集选取策略库(2-2)，另一边测试端将设备的设备类型Type传输给案例集选取策略库(2-2)；其中所述安全等级处理模块(2-1)用于根据安全等级Grade得到安全等级划分要素集合G和标准等级强度集合T，然后将得到的安全等级划分要素集合G和标准等级强度集合T发送给综合安全评估模块(3)的安全等级评估模块(3-1)；

所述案例集选取策略库(2-2)中存储有策略结构图，所述案例集选取策略库(2-2)用于根据收到测试端发送来的安全等级Grade和设备类型Type根据策略结构图构造必测案集合MGSF，并将必测案集合MGSF发送给安全功能测试套模块(2-4)；所述安全功能测试套模块(2-4)根据可选案例集库(2-3)的可选案例集OGSF和案例集选取策略库(2-2)发送的必测案集合MGSF构造测试案例集合S，其中S＝{MGSF+OGSF}，然后将测试案例集合S转化为案例信息集合B，其中B＝{M_1,M_2...M_n}，MGSF表示必测案集合，OGSF表示可选案例集，M_1,M_2...M_n表示从1-n编号的案例信息，可选案例集并将所述案例信息集合B发送给安全测试执行系统(4)，所述安全测试执行系统(4)根据案例信息集合B对设备进行测试得到设备的测试响应集合，并将设备的测试响应集合转发给安全功能测试结果分析模块(3-2)进行分析，形成测试结果集合N，所述安全等级评估模块(3-1)模块以安全等级处理模块(2-1)发送来的安全等级划分要素集合G、标准等级强度集合T和安全功能测试结果分析模块(3-2)的输出集合N作为输入，根据安全功能测试套的对应关系将集合N中案例的测试结果分别对应到集合G中的G_i，由此对G_i的案例结果进行量化并计算出测试等级强度集合ET_i，并将安全等级划分要素集合G、标准等级强度集合T和测试等级强度集合ET发送给安全等级分析报告模块(3-3)生成设备安全等级报告，所述设备安全等级报告包括设备安全等级的测试值；所述安全功能测试结果分析模块(3-2)还将测试结果集合N发送给规范一致性分析报告模块(3-4)，当测试结果集合N的测试结果为1时表示测试成功，则符合一致性规范，若测试结果为0时表示测试失败，则不符合一致性规范。

2.根据权利要求1所述的基于安全等级的传感网安全测评系统，其特征在于：所述安全功能测试套模块(2-4)包括必测案例集MGSF和可选案例集OGSF，其中必测案例集MGSF包括测试组G_0和安全等级划分要素对应的测试组G_1-G_{10}，用测试案例GSF来表示必测案例集MGSF和可选案例集OGSF，GSF_n代表第n个测试案例号，每个测试案例对应一个测试命令CMD_n和测试期望响应RP_n，则每个测试案例对应的信息集合有M_n＝{GSF_n,CMD_n,RP_n}。

3.根据权利要求1所述的基于安全等级的传感网安全测评系统，其特征在于：所述安全等级划分要素集合G＝{G_1,G_2...G_{10}}，对应安全等级划分要素G_i，其中1≤i≤10且为整数，标准等级强度集合T，T＝{T_1,T_2...T_{10}}，T_i为安全等级，安全划分要素G_i需要满足的强度，0≤T_i≤5，T_i为整数。

4.根据权利要求1所述的基于安全等级的传感网安全测评系统，其特征在于：所述设备类型Type包括网关Gateway、路由器Router、终端设备End Device。

5.根据权利要求1所述的基于安全等级的传感网安全测评系统，其特征在于：所述安全等级划分要素集合G包括数据完整性G_1、数据保密性G_2、数据新鲜性G_3、密钥管理G_4、数据鉴别G_5、敏感标记G_6、自主访问控制G_7、强制访问控制G_8、用户身份鉴别G_9及节点鉴别G_{10}。

一种基于安全等级的传感网安全测评系统

技术领域

[0001] 本发明涉及传感网安全技术和传感网安全测评领域，具体地说，涉及一种基于安全等级的传感网安全测评系统。

背景技术

[0002] 随着社会的发展，网络安全越来越引起人们的关注。传感网中加入网络的设备对整个网络的运行有着至关重要的影响，如果非安全设备加入网络，不仅影响网络的运行，还会严重影响网络的安全性，所以，设备自身的安全性必须有一定的要求。传统的安全测评系统是从网络的整体角度考虑安全性，对在网设备自身的安全性没有做定性的评估，不能保证设备的加入是否会影响网络的安全运行。如果具有一定安全性的设备加入网络，不但可以提高设备运行的安全性，也能提高整个网络的安全性。

[0003] 因此，本专利发明了一种基于安全等级的传感网安全测评系统，从设备的功能测试结果和安全等级的角度评估设备的安全性，同时对系统的安全性做出评价。

发明内容

[0004] 针对以上现有技术中的不足，本发明的目的在于提供一种减小设备对系统造成的不安全影响，还可以提高系统的整体安全的基于安全等级的传感网安全测评系统，本发明的技术方案如下：一种基于安全等级的传感网安全测评系统，其包括：安全测评服务器和设置于待测传感网络端的安全测试执行系统，所述安全测评服务器包括SICS安全实现一致性声明设计模块和综合安全评估模块；

[0005] 所述SICS安全实现一致性声明设计模块包括安全等级处理模块、案例集选取策略库、可选案例集和安全功能测试套模块；

[0006] 所述综合安全评估模块包括安全等级评估模块、安全功能测试结果分析模块、安全等级分析报告和规范一致性分析报告；

[0007] 当测试待测传感网时，测试端一边将设备的安全等级Grade传输给安全等级处理模块及案例集选取策略库，另一边测试端将设备的设备类型Type传输给案例集选取策略库；其中所述安全等级处理模块(2-1)用于根据安全等级Grade得到安全等级划分要素集合G和标准等级强度集合T，然后将得到的安全等级划分要素集合G和标准等级强度集合T发送给综合安全评估模块(3)的安全等级评估模块；

[0008] 所述案例集选取策略库中存储有策略结构图，所述案例集选取策略库用于根据收到测试端发送来的安全等级Grade和设备类型Type根据策略结构图构造必测案集合MGSF，并将必测案集合MGSF发送给安全功能测试套模块；所述安全功能测试套模块根据可选案例集库的可选案例集OGSF和案例集选取策略库发送的必测案集合MGSF构造测试案例集合S，其中S＝{MGSF+OGSF}，然后将测试案例集合S转化为案例信息集合B，其中B＝{M_1,M_2...M_n}，并将所述案例信息集合B发送给安全测试执行系统(4)，所述安全测试执行系统(4)根据案例信息集合B对设备进行测试得到设备的测试响应集合，并将设备的测试响应集合转发给

安全功能测试结果分析模块(3-2)进行分析，形成测试结果集合N，所述安全等级评估模块以安全等级处理模块发送来的安全等级划分要素集合G、标准等级强度集合T和安全功能测试结果分析模块的输出集合N作为输入，根据安全功能测试套的对应关系将集合N中案例的测试结果分别对应到集合G中的G_i，由此对G_i的案例结果进行量化并计算出测试等级强度集合ET_i，计算出测试等级强度集合ET，并将安全等级划分要素集合G、标准等级强度集合T和测试等级强度集合ET发送给安全等级分析报告模块(3-3)生成设备安全等级报告，所述设备安全等级报告包括设备安全等级的测试值；所述安全功能测试结果分析模块还将测试结果集合N发送给规范一致性分析报告模块，当测试结果集合N的测试结果为1时表示测试成功，则符合一致性规范，若测试结果为0时表示测试失败，则不符合一致性规范。

[0009] 进一步的，所述安全功能测试套模块包括必测案例集MGSF和可选案例集OGSF，其中必测案例集MGSF包括测试组G_0和安全等级划分要素对应的测试组G_1-G_{10}，用测试案例GSF来表示必测案例集MGSF和可选案例集OGSF，GSF_n代表第n个测试案例号，每个测试案例对应一个测试命令CMD_n和测试期望响应RP_n，则每个测试案例对应的信息集合有$M_n=\{GSF_n, CMD_n, RP_n\}$。

[0010] 进一步的，所述安全等级划分要素集合$G=\{G_1, G_2 \ldots G_{10}\}$，对应安全等级划分要素$G_i$，其中$1\leqslant i\leqslant 10$且为整数，标准等级强度集合T，$T=\{T_1, T_2 \ldots T_{10}\}$，$T_i$为安全等级，安全划分要素$G_i$需要满足的强度，$0\leqslant T_i\leqslant 5$，$T_i$为整数。

[0011] 进一步的，所述设备类型Type包括网关Gateway、路由器Router、终端设备End Device，

[0012] 进一步的，所述安全等级划分要素集合G包括数据完整性G_1、数据保密性G_2、数据新鲜性G_3、密钥管理G_4、数据鉴别G_5、敏感标记G_6、自主访问控制G_7、强制访问控制G_8、用户身份鉴别G_9及节点鉴别G_{10}。

[0013] 本发明的优点及有益效果如下：

[0014] 本发明从两方面对设备自身安全性进行评估：一方面评估设备安全功能的实现与规范一致；另一方面，从安全等级角度评估设备所符合的安全等级。保证设备具有一定的安全性，不仅可以减小设备对系统造成的不安全影响，还可以提高系统的整体安全，同时，本发明的测试报告还为设备的改善提供了参考依据。

附图说明

[0015] 图1为安全测试系统结构图；

[0016] 图2安全功能测试套结构图；

[0017] 图3安全测试系统案例选取策略结构图；

[0018] 图4测试系统示意图。

具体实施方式

[0019] 下面结合附图给出一个非限定性的实施例对本发明作进一步的阐述。

[0020] 参照图1-图4所示，本发明基于安全等级的传感网安全测评系统包括SICS(Security Implementation Conformance Statement)设计模块、安全测试执行系统和综合安全评估模块，其中，SICS设计模块和综合安全评估模块均执行于安全测评服务器，而安

全测试执行系统独立于测评服务器。SICS设计模块包括安全等级处理模块、安全功能测试套模块、可选案例集和案例集选取策略库。综合安全评估模块包括安全功能测试结果分析模块、安全等级评估模块、规范一致性分析报告和安全等级分析报告。

[0021] 表1安全等级表

[0022]

安全等级划分要素	第一级	第二级	第三级	第四级	第五级
数据完整性 G_1	+	++	++	+++	+++
数据保密性 G_2	+	++	++	+++	+++
数据新鲜性 G_3	×	+	+	++	++
密钥管理 G_4	×	+	++	+++	++++
数据鉴别 G_5	×	×	+	++	++
敏感标记 G_6	×	×	+	+	+
自主访问控制 G_7	+	++	++	++	+++
强制访问控制 G_8	×	×	+	+	+
用户身份鉴别 G_9	+	++	+++	++++	+++++
节点鉴别 G_{10}		+	++	+++	++++

[0023]

注：“+”表示对安全功能要素的要求，“+”数量的增加表示安全功能要素强度的提高；“×”表示无要求。

[0024] 本发明系统按照《传感器网络信息安全通用技术规范》的安全要求，将系统安全分为五个等级，分别为：第一级、第二级、第三级、第四级和第五级，级别越高表示安全性能越好，所以不同等级对安全等级划分要素的强度要求不同，如表1所示。遵循上述等级要求，本发明系统形成一种安全功能测试套，如图2所示，测试套包括多个测试组，测试组G_1到G_{10}与

安全等级划分要素对应，测试组G_0为必测案例集，其他测试组为可选案例集，用以评估设备和系统的安全性。其中，GSF表示测试案例，GSF_n代表第n个测试案例号，每个测试案例对应一个测试命令CMD_n和测试期望响应RP_n，则每个测试案例对应的信息集合有$M_n=\{GSF_n,CMD_n,RP_n\}$。

[0025] 所述安全等级处理模块根据测试端提交的安全等级Grade，分析该等级下安全等级划分要素集合G和标准等级强度集合T，并作为该模块的输出。

[0026] 安全等级划分要素集合G，$G=\{G_1,G_2...G_{10}\}$，对应于表1的安全等级划分要素G_i，其中$1\leqslant i\leqslant 10$且为整数。

[0027] 标准等级强度集合T，$T=\{T_1,T_2...T_{10}\}$，T_i为符合某一个安全等级，安全划分要素G_i需要满足的强度，$0\leqslant T_i\leqslant 5$，$T_i$为整数，由系统给出。将表1中的“+”进行量化，规定“+”为一个单位，取值为1，“++”表示2，以此类推，“×”表示不作要求，取值为0。

[0028] 设备进行安全测试前，测试端需声明被测设备的安全等级及设备类型，设备类型Type包括网关(Gateway)、路由器(Router)、终端设备(End Device)。该声明是本发明测评系统的基础条件，也是系统的先决条件。

[0029] 所述可选案例集为系统提供扩展接口，用户可通过测试端增加新案例信息，系统提供的可选案例有GSF_{27}、GSF_{28}、GSF_{29}、GSF_{30}，如图2中虚线所示，则有可选案例集$OGSF=\{GSF_{27},GSF_{28},GSF_{29},GSF_{30}\}$。其中，安全测评服务器在整个查询和生成测试命令集过程中均使用测试案例编号进行识别，编号对照如表2所示。

[0030] 表2案例编号对照表

[0031]

编号	案例名称	编号	案例名称	编号	案例名称
GSF_1	安全入网认	GSF_{11}	分对称运算	GSF_{21}	标识数据
GSF_2	密钥分发服	GSF_{12}	32位MIC码	GSF_{22}	用户等级
GSF_3	密钥建立服	GSF_{13}	64位MIC码	GSF_{23}	节点资源等级
GSF_4	密钥更新服	GSF_{14}	128位MIC	GSF_{24}	数据资源访问
GSF_5	密钥撤销	GSF_{15}	关键数据传	GSF_{25}	节点资源访问
GSF_6	序列号机制	GSF_{16}	所有数据传	GSF_{26}	鉴别用户身份
GSF_7	时间戳机制	GSF_{17}	所有数据存	GSF_{27}	路由鉴别
GSF_8	异或运算鉴	GSF_{18}	标识网络设	GSF_{28}	网络层路由交换
GSF_9	哈希运算鉴	GSF_{19}	对访问者身	GSF_{29}	协调器解析融合
GSF_{10}	分组密码鉴	GSF_{20}	访问控制表	GSF_{30}	安全路由数据融

[0032] 所述案例集选取策略库为整个系统提供必测案例集MGSF。策略库根据Grade和Type自动选择案例形成被测设备的MGSF，然后发送给安全功能测试套模块，策略库中的案例集选取规则如图3所示。图3是由表1和图2训练生成的基于等级的案例选取规则，最终生成的案例集能够从等级角度反映设备的安全性能。每一个等级和设备类型的组合都对应不同的安全功能案例集，等级越高，对安全划分要素的强度要求越高，所需的案例越多。

[0033] 所述的安全功能测试套模块将集合MGSF和OGSF整合为一个新的测试案例集合S，有$S=\{MGSF+OGSF\}$，根据集合中每个测试案例对应的测试命令和期望响应将集合S转化为案例信息集合B，即$B=\{M_1,M_2...M_n\}$。

[0034] 所述的安全测试执行系统解析集合B中测试命令并对被测设备进行测试，测试完后将测试响应发送到安全功能测试结果分析模块，此处的测试执行方法已在专利“一种传感网安全测试方法和系统”，专利号：201310654199.5中描述。，此处不再赘述。

[0035] 所述的安全功能测试结果分析模块对安全测试执行系统输出的测试响应集合进行分析，并形成测试结果集合N，结果N提供给安全等级评估模块和规范一致性分析报告模块。结果分析模块主要是分析每个案例的期望响应和测试响应。若符合测试结果为“成功”，否则为“失败”。模块的输出为集合N，$N=\{N_1,N_2...N_n\}$，$N_n=\{GSF_n,RT_n\}$，N_n代表GSF_n的结果信息集，RT_n为案例GSF_n的测试结果。

[0036] 所述的规范一致性分析报告模块分析安全功能的实现是否与规范一致，该模块接收安全功能测试结果分析模块的集合N，统计已完成测试的案例和结果，若测试结果为成功，则安全功能的实现符合规范，相反，则不符合。

[0037] 所述安全等级评估模块以安全等级处理模块的集合G、T和安全功能测试结果分析模块的输出集合N作为输入，根据计算方法计算出期望G_i对应的测试等级强度ET_i。

[0038] 计算方法：案例测试成功则表示强度值为1，反之则表示强度值为0，最后将G_i中每一个案例的强度值相加，即为ET_i，$0\leqslant ET_i\leqslant 5$，$ET_i$为整数，$G_i$包含的案例是从N中筛选出的对应案例。

[0039] 所述安全等级分析报告将等级评估模块的结果导入，比较声明安全等级的标准等级强度集合T和测试执行后统计的安全等级强度集合ET，计算强度差值的平均值∂，根据∂分析强度出现差异的原因并加以说明，并对整个系统的安全性进行分析。

[0040] 实际测试中，案例全部测试成功是难以实现的，但个别案例的测试失败也不能说明设备不符合该安全等级，需衡量等级中的安全等级划分要素G_i，所以通过强度差值的平均值∂来评估设备是否符合该安全等级，公式为：

[0041] $$\partial=\frac{\sum D_i\times P_i}{n}$$

[0042] 其中，P_i表示G_i的标准等级强度与测试等级强度的差值，即$P_i=T_i-ET_i$，$0\leqslant P_i\leqslant 5$，$P_i$的值为整数。

[0043] D_i表示G_i的加权系数，其值与安全要素对整个网络的影响程度和测试执行的先后顺序有关，如下表所示：

[0044]

G_i	1	2	3	4	5	6	7	8	9	10
D_i	0.3	0.3	0.2	0.4	0.1	0.1	0.2	0.2	0.2	0.1

[0045] n为执行测试的安全等级划分要素个数，即G_i至少拥有一个已执行测试的案例。用户可以根据具体情况事先设定一个参考阈值，∂大于阈值，说明测试结果不符合声明的安全等级，小于阈值则表示该设备基本符合事先声明的安全等级，若∂值越小，说明符合度越高。

[0046] 报告的结论部分，根据∂的大小判定被测设备是否符合声明的安全等级，并给出测试结果失败的案例，分析系统的安全性，并为用户提供设备改善的参考依据。

[0047] 以下将结合附图，对本发明的具体实施进行详细的描述。

[0048] 本发明一种基于安全等级的传感网安全测评系统，系统包括SICS设计模块、安全测试执行系统和综合安全评估模块，实现对设备的安全性测试，测试系统示意图如4所示，

具体实施过程如下：

[0049] Step1：测试端选择声明的设备安全等级、设备类型和可选案例集，假设当前选择的安全等级Grade＝{第三级}，Type＝{Router}，可选案例为OGSF＝{M_{27},M_{29}}。Step2：安全测评服务器对Step1的信息进行解析，将Grade分别发送给安全等级处理模块和案例集选取策略库，Type发送给案例集选取策略库，OGSF发送给安全功能测试套模块。

[0050] 安全等级处理模块根据表1确定Grade＝{“第三级”}的安全等级划分要素G_i，安全等级划分要素集合

[0051] G＝{G_1,G_2,G_3,G_4,G_5,G_6,G_7,G_8,G_9,G_{10}}

[0052] 标准等级强度集合T＝{T_1,T_2,T_3,T_4,T_5,T_6,T_7,T_8,T_9,T_{10}}＝{2,2,1,2,1,1,2,1,3,2}

[0053] 该模块将G和T发送给安全等级评估模块；

[0054] Step3：案例集选取策略库根据Grade和Type对照策略结构图构造必测案集合MGSF，MGSF＝{GSF_1,GSF_2,GSF_3,GSF_6,GSF_{12},GSF_{13},GSF_{15},GSF_{16}}，案例编号从小到大，代表测试执行的顺序。

[0055] Step4：安全功能测试套模块接收案例集选择策略库的集合MGSF后，构造案例集合S，

[0056] S＝{OGSF+MGSF}

[0057] 将案例集合S中每个案例对应的信息构成所有案例的信息集合

[0058] BB＝{M_1,M_2,M_3,M_6,M_{12},M_{13},M_{15},M_{16},M_{27},M_{29}}

[0059] 其中，M_n＝{GSF_n,CMD_n,RP_n}。

[0060] Step5：服务器将Step4的集合B发送给测试执行系统，系统根据B中的CMD激发设备执行测试，并将执行后的测试响应反馈给服务器的安全功能测试结果分析模块。

[0061] Step6：安全功能测试结果分析模块对比每个案例的测试响应和期望响应，即案例的测试结果RT_n等于“失败”或者“成功”。构建测试结果集合N，N＝{N_1,N_2,N_3,N_6,N_{12},N_{13},N_{15},N_{16},N_{27},N_{29}}，N_n＝{GSF_n,RT_n} n∈{1,2,3,6,12,13,15,16,27,29}。

[0062] Step7：规范一致性分析报告接收Step6的集合N，服务器将N导入规范一致性分析报告，并存储在数据库中，供测试端查看。

[0063] Step8：安全等级评估模块接收Step6的案例测试结果集合N，模块根据Step2接收的安全等级划分要素集合G在集合N中选取期望G_i包含的案例并计算对应的测试等级强度ET_i，对照图2可知：

[0064] $G_1 \supseteq \{GSF_{12}, GSF_{13}\}, G_2 \supseteq \{GSF_{15}, GSF_{16}\}, G_3 \supseteq \{GSF_6\}$

[0065] $G_4 \supseteq \{GSF_2, GSF_3\}, G_5 \supseteq \{GSF_{12}, GSF_{13}\}$

[0066] 根据集合G选取案例，可以直接筛选掉N中的可选案例和不属于安全等级划分要素的必测案例，直接获得集合G中G_i包含的案例。案例选取完成后计算G_i对应的测试等级强度集合

[0067] ET＝{ET_1,ET_2,ET_3,ET_4,ET_5}

[0068] 计算ET_i时，从N中调取属于G_i的案例的测试结果，“成功”则值为1，“失败”则为0，然后将案例测试结果的值相加即为G_i对应的测试等级强度ET_i。

[0069] 若系统结果如下表所示：

[0070]

GSF1	成功
GSF2	成功
GSF3	成功
GSF6	成功
GSF12	成功
GSF13	失败
GSF15	成功
GSF16	成功
GSF27	成功
GSF29	成功

[0071] 因$G_1 \supseteq \{GSF_{12}, GSF_{13}\}$，其中$GSF_{12}$的测试结果为成功，$GSF_{13}$为失败，则$ET_1=0+1=1$，类似可推知：$ET_2=2, ET_3=1, ET_4=2, ET_5=1$

[0072] 即：$ET=\{1,2,1,2,1\}$。

[0073] Step9：安全等级分析报告接收Step8的测试等级强度集合ET、安全等级划分要素集合G、和标准等级强度集合T，服务器计算强度差值的平均值∂，通过∂值判定等级评估的结果。

[0074] 由Step2可知$T'=\{T_1,T_2,T_3,T_4,T_5\}=\{2,2,1,2,1\}$，则有：

[0075] $P=\{P_1,P_2,P_3,P_4,P_5\}$

[0076] $=\{T_1-ET_1, T_2-ET_2, T_3-ET_3, T_4-ET_4, T_5-ET_5\}$

[0077] $=\{2-1,2-2,1-1,2-2,1-1\}$

[0078] $=\{1,0,0,0,0\}$

[0079] 根据公式计算∂值：

$$\partial=\frac{\sum D_i\times P_i}{n}$$

[0080] $$=\frac{\sum(0.3*1+0.3*0+0.2*0+0.4*0+0.1*0)}{5}$$

$$=0.06$$

[0081] 其中，$n=5$，Step8中有5个G_i包含至少一个以上的案例。

[0082] 安全等级评估报告表格格式为：

[0083]

安全等级划分要素 G	标准等级强度 T	测试等级强度 ET	说明

[0084] 除了以上信息，报告还包括测试时间、测试单位、被测单位、声明等级、被测设备类型、参考标准和评估结论。

[0085] 假设用户设定的参考阈值为0.15，则有以下结论：$\partial<0.15$，其值相对于阈值偏离度较大，说明设备的安全等级较好的满足测试前声明的等级要求；

[0086] Step10:结合Step9的等级评估结果,提取Step6中测试失败的案例,同时根据测试结果分析系统的安全性,并将信息导入等级评估报告的结论部分存储于服务器的数据库中,供测试端查看,同时为设备的完善提供参考的依据。

[0087] 以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后,技术人员可以对本发明作各种改动或修改,这些等效变化和修饰同样落入本发明方法权利要求所限定的范围。

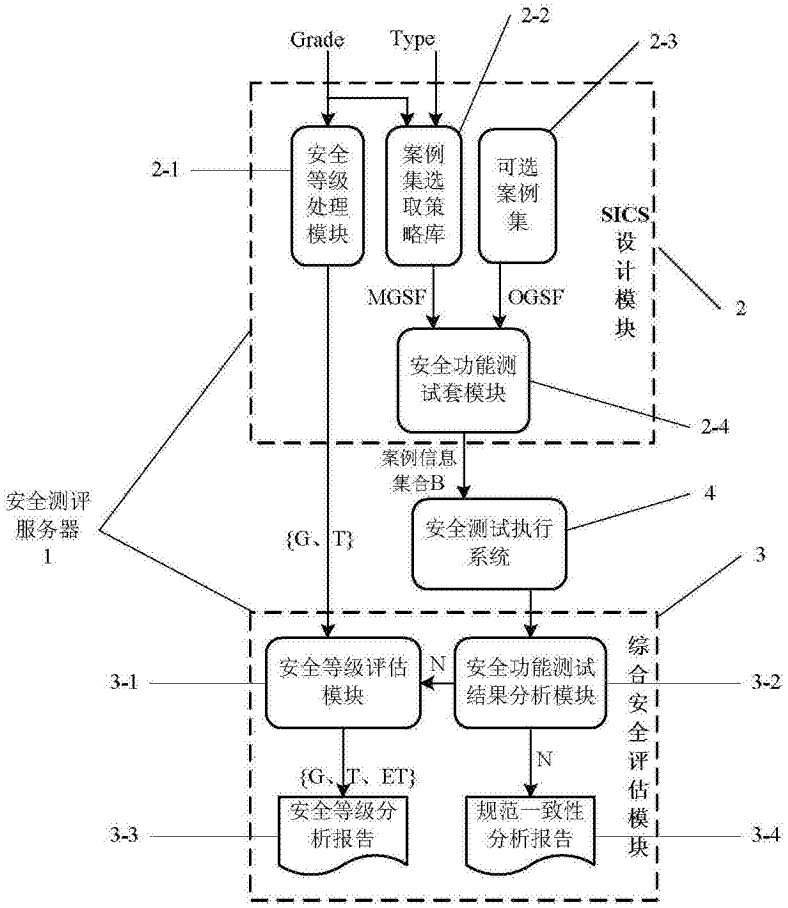

Grade
Type
2-2
2-3
2-1
安全等级处理模块
案例集选取策略库
可选案例集
SICS设计模块
2
MGSF
OGSF
安全功能测试套模块
2-4
案例信息集合B
4
安全测评服务器1
{G、T}
安全测试执行系统
3
安全等级评估模块
N
安全功能测试结果分析模块
综合安全评估模块
3-1
3-2
{G、T、ET}
N
安全等级分析报告
规范一致性分析报告
3-3
3-4

图1

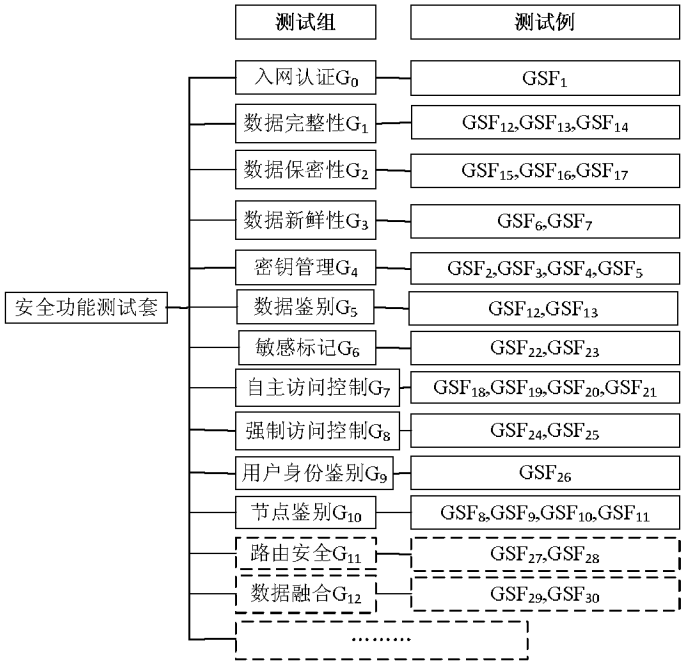

测试组
测试例
安全功能测试套
入网认证G_0
GSF_1
数据完整性G_1
GSF_{12},GSF_{13},GSF_{14}
数据保密性G_2
GSF_{15},GSF_{16},GSF_{17}
数据新鲜性G_3
GSF_6,GSF_7
密钥管理G_4
GSF_2,GSF_3,GSF_4,GSF_5
数据鉴别G_5
GSF_{12},GSF_{13}
敏感标记G_6
GSF_{22},GSF_{23}
自主访问控制G_7
GSF_{18},GSF_{19},GSF_{20},GSF_{21}
强制访问控制G_8
GSF_{24},GSF_{25}
用户身份鉴别G_9
GSF_{26}
节点鉴别G_{10}
GSF_8,GSF_9,GSF_{10},GSF_{11}
路由安全G_{11}
GSF_{27},GSF_{28}
数据融合G_{12}
GSF_{29},GSF_{30}
……

图2

	网关	路由器	终端设备	
第一级	{GSF18,GSF19,GSF26}	{GSF1,GSF12,GSF15}	{GSF1,GSF12,GSF15}	
第二级	第一级{GSFn}+{GSF20}	第一级{GSFn}+{GSF2,GSF13,GSF16,GSF6}	第一级{GSFn}+{GSF2,GSF13,GSF16,GSF6}	GSF8
第三级	第二级{GSFn}+{GSF22,GSF23,GSF24,GSF25}	第二级{GSFn}+GSF3	第一级{GSFn}+{GSF3,GSF2,GSF13,GSF16,GSF6}	GSF9
第四级	第三级{GSFn}	第一级{GSFn}+{GSF2,GSF13,GSF16,GSF7,GSF3,GSF4,GSF14,GSF17}	第一级{GSFn}+{GSF2,GSF13,GSF16,GSF7,GSF3,GSF4,GSF14,GSF17,GSF6}	GSF10
第五级	第四级{GSFn}+GSF21	第四级{GSFn}+GSF5	第一级{GSFn}+{GSF2,GSF13,GSF16,GSF7,GSF3,GSF4,GSF14,GSF17,GSF6,GSF5}	GSF11

图3

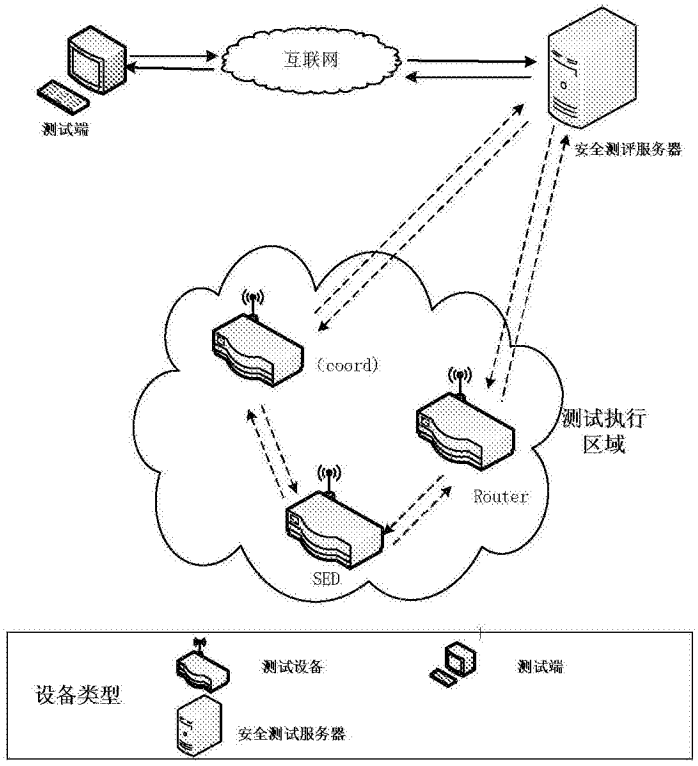


图4