(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 101771582 B
(45)授权公告日 2011.12.14

(21)申请号 200910243576.X

(22)申请日 2009.12.28

(73)专利权人 北京神州泰岳软件股份有限公司
地址 100089 北京市海淀区万泉庄路 28 号万柳新贵大厦 5 层

(72)发明人 王雪飞 苏砫 郭唤斌 张志雄 黄理 方腾飞 依鹏涛

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 胡小永

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

(56)对比文件
CN 101047542 A,2007.10.03, 全文.
US 5414833 A,1995.05.09, 全文.
CN 1447263 A,2003.10.08, 全文.

审查员 张臻贤

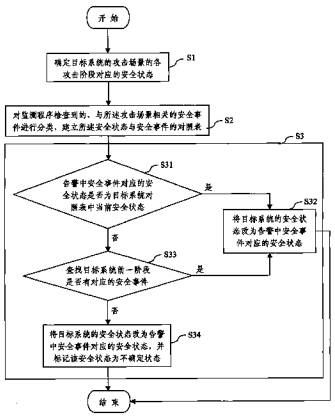
权利要求书 1 页 说明书 3 页 附图 1 页

(54)发明名称

一种基于状态机的安全监控关联分析方法及系统

(57)摘要

本发明公开了一种基于状态机的安全监控关联分析方法，包括以下步骤：确定目标系统的攻击场景的各攻击阶段对应的安全状态，所述攻击场景为相互依赖的、具有时间顺序的相互行为发生时，产生的安全事件集；对目标系统的监视程序检查到的、与所述攻击场景相关的安全事件进行分类，建立所述安全状态与安全事件的对照表；根据所述对照表检查并记录目标系统的安全状态。本发明可以在保障系统运行速度一定的情况下，对资产的安全状态存储较长时间；可以检查分布式的系统攻击；在没有定义精确攻击场景的情况下，可以确定系统的安全状态；可以分析出系统受到攻击的轨迹，为调查取证提供依据。



CN 101771582 B

1. 一种基于状态机的安全监控关联分析方法，其特征在于，包括以下步骤：

S1：确定目标系统的攻击场景的各攻击阶段对应的安全状态，所述攻击场景为相互依赖的、具有时间顺序的相互行为发生时，产生的安全事件集；

S2：对目标系统的监视程序检查到的、与所述攻击场景相关的安全事件进行分类，建立所述安全状态与安全事件的对照表；

S3：根据所述对照表检查并记录目标系统的安全状态，具体包括：

当目标系统收到监视程序的告警时，查看所述目标系统的对照表中的安全状态是否为满足所述告警中安全事件对应安全状态的前一状态，若满足，则将所述目标系统的安全状态改为告警中安全事件对应的安全状态，否则查找目标系统前一阶段是否有对应的安全事件，如果找到，则将所述目标系统的安全状态改为告警中安全事件对应的安全状态，否则将目标系统的安全状态改为告警中安全事件对应的安全状态，并标记该安全状态为不确定状态。

2. 如权利要求 1 所述的基于状态机的安全监控关联分析方法，其特征在于，所述安全状态包括：目标系统信息被收集、权限被获取、被置入后门和日志被清理。

3. 一种基于状态机的安全监控关联分析系统，其特征在于，包括：

攻击场景确定模块，用于确定目标系统的攻击场景的各攻击阶段对应的安全状态，所述攻击场景为相互依赖的、具有时间顺序的相互行为发生时，产生的安全事件集；

对照表建立模块，用于对目标系统的监视程序检查到的、与所述攻击场景相关的安全事件进行分类，建立所述安全状态与安全事件的对照表；

安全状态记录模块，用于根据所述对照表检查并记录目标系统的安全状态，具体包括：

前一状态判断模块，用于当目标系统收到监视程序的告警时，查看所述目标系统的对照表中的安全状态是否为满足所述告警中安全事件对应安全状态的前一状态，若满足，则执行当前安全状态设置模块，否则执行前一阶段查找模块；

当前安全状态设置模块，用于将所述目标系统的安全状态改为告警中安全事件对应的安全状态；

前一阶段查找模块，用于查找目标系统前一阶段是否有对应的安全事件，如果找到，则执行当前安全状态设置模块，否则执行不确定安全状态设置模块；

不确定安全状态设置模块，用于将目标系统的安全状态改为告警中安全事件对应的安全状态，并标记该安全状态为不确定状态。

一种基于状态机的安全监控关联分析方法及系统

技术领域

[0001] 本发明涉及网络安全技术领域，特别涉及一种基于状态机的安全监控关联分析方法及系统。

背景技术

[0002] 传统的解决多步攻击的攻击场景重构的方法中，主要使用时序关联的方法。

[0003] 传统的攻击场景重构主要的实现过程如下：

[0004] (1) 自定义攻击场景，把需要检查的攻击过程用规则的进行表示。

[0005] (2) 对检查到得安全事件与规则进行匹配，如果符合规则则产生告警。

[0006] 现有技术一的缺点：

[0007] (1) 需要准确的定义的攻击场景。

[0008] (2) 当定义过多的安全攻击场景时，需对安全事件进行各个攻击场景匹配，导致系统的检查效率明显下降。

[0009] (3) 当攻击者进行协同攻击时，需保持过多的安全状态，导致系统的检查效率降低。

发明内容

[0010] （一）发明目的

[0011] 本发明的目的是提供一种基于状态机的安全监控关联分析方法，解决由多步骤组成事件的检查、利用多源数据来判断系统的状态和网络协同攻击的问题。

[0012] （二）发明内容

[0013] 一种基于状态机的安全监控关联分析方法，包括以下步骤：

[0014] S1：确定目标系统的攻击场景的各攻击阶段对应的安全状态，所述攻击场景为相互依赖的、具有时间顺序的相互行为发生时，产生的安全事件集；

[0015] S2：对目标系统的监视程序检查到的、与所述攻击场景相关的安全事件进行分类，建立所述安全状态与安全事件的对照表；

[0016] S3：根据所述对照表检查并记录目标系统的安全状态。

[0017] 其中，所述步骤 S3 包括：

[0018] 当目标系统收到监视程序的告警时，查看所述目标系统的对照表中的安全状态是否为满足所述告警中安全事件对应安全状态的前一状态，若满足，则将所述目标系统的安全状态改为告警中安全事件对应的安全状态，否则查找目标系统前一阶段是否有对应的安全事件，如果找到，则将所述目标系统的安全状态改为告警中安全事件对应的安全状态，否则将目标系统的安全状态改为告警中安全事件对应的安全状态，并标记该安全状态为不确定状态。

[0019] 其中，所述安全状态包括：目标系统信息被收集、权限被获取、被置入后门和日志被清理。

[0020] 一种基于状态机的安全监控关联分析系统，包括：

[0021] 攻击场景确定模块，用于确定目标系统的攻击场景的各攻击阶段对应的安全状态，所述攻击场景为相互依赖的、具有时间顺序的相互行为发生时，产生的安全事件集；

[0022] 对照表建立模块，用于对目标系统的监视程序检查到的、与所述攻击场景相关的安全事件进行分类，建立所述安全状态与安全事件的对照表；

[0023] 安全状态记录模块，用于根据所述对照表检查并记录目标系统的安全状态。

[0024] 其中，所述安全状态记录模块包括：

[0025] 前一状态判断模块，用于当目标系统收到监视程序的告警时，查看所述目标系统的对照表中的安全状态是否为满足所述告警中安全事件对应安全状态的前一状态，若满足，则执行当前安全状态设置模块，否则执行前一阶段查找模块；

[0026] 当前安全状态设置模块，用于将所述目标系统的安全状态改为告警中安全事件对应的安全状态；

[0027] 前一阶段查找模块，用于查找目标系统前一阶段是否有对应的安全事件，如果找到，则执行当前安全状态设置模块，否则执行不确定安全状态设置模块；

[0028] 不确定安全状态设置模块，用于将目标系统的安全状态改为告警中安全事件对应的安全状态，并标记该安全状态为不确定状态。

[0029] （三）有益效果

[0030] 本发明的基于状态机的安全监控关联分析方法具有如下有益效果：

[0031] (1) 可以在保障系统运行速度一定的情况下，对资产的安全状态存储较长时间；

[0032] (2) 可以检查分布式的系统攻击；

[0033] (3) 在没有定义精确攻击场景的情况下，可以确定系统的安全状态；

[0034] (4) 可以分析出系统受到攻击的轨迹，为调查取证提供依据。

附图说明

[0035] 图 1 是根据本发明的基于状态机的安全监控关联分析方法的流程图。

具体实施方式

[0036] 本发明提出的基于状态机的安全监控关联分析方法，结合附图和实施例说明如下。

[0037] 如图 1 所示，步骤 S1 确定目标系统的攻击场景的各攻击阶段对应的安全状态，其中攻击场景是指相互依赖的、具有时间顺序的相互行为发生时，产生的安全事件集，通过规则构建攻击场景可以识别真正的攻击事件、预测攻击的下一步动作，安全状态通常包括目标系统信息被收集、权限被获取、被置入后门和日志被清理等。

[0038] 步骤 S2 中对各监视程序检查到的、与所述攻击场景相关的安全事件进行分类，建立安全状态与安全事件的对照表，即各攻击阶段与安全事件的对照表，如表 1 所示：

[0039] 表 1 各攻击阶段与安全事件的对照表

[0040]

各攻击阶段	收集系统信息	获取权限	放置后门	清理日志
安全事件	主机扫描 端口扫描 服务扫描 漏洞扫描	溢出攻击 漏洞利用 目录遍历	配置更改 安装恶意程序	删除日志

[0041] 表中的攻击各阶段对应于各个安全状态，安全事件为导致达到某个安全状态时所发生的事件。

[0042] 步骤S3根据上述对照表检查并记录资产所在目标系统的安全状态。具体地，当系统收到监视程序的一个告警Alert_new时，步骤S31中查看目标系统的对照表中的安全状态是否为满足所述告警Alert_new中安全事件对应安全状态的前一状态，若满足，则将目标系统的安全状态改为对应状态，即步骤S32，然后结束，例如：收到一个告警Alert_new，该警告中安全事件（如：溢出攻击）对应的安全状态为“获取权限”，则检查对应系统对照表的安全状态是否已经被标为“系统信息被收集”状态，如果是则把该系统的安全状态改为“权限被获取”的状态；若不满足，则在步骤S33中查找目标系统前一阶段是否有对应的安全事件，若找到，则将目标系统的安全状态改为告警Alert_new中安全事件对应的安全状态，然后结束；否则将该系统的安全状态改为告警中安全事件对应的安全状态，并标记该安全状态为不确定状态。

[0043] 一种基于状态机的安全监控关联分析系统，包括：

[0044] 攻击场景确定模块，用于确定目标系统的攻击场景的各攻击阶段对应的安全状态，所述攻击场景为相互依赖的、具有时间顺序的相互行为发生时，产生的安全事件集；对照表建立模块，用于对目标系统的监视程序检查到的、与所述攻击场景相关的安全事件进行分类，建立所述安全状态与安全事件的对照表；安全状态记录模块，用于根据所述对照表检查并记录目标系统的安全状态。

[0045] 其中，所述安全状态记录模块包括：

[0046] 前一状态判断模块，用于当目标系统收到监视程序的告警时，查看所述目标系统的对照表中的安全状态是否为满足所述告警中安全事件对应安全状态的前一状态，若满足，则执行当前安全状态设置模块，否则执行前一阶段查找模块；当前安全状态设置模块，用于将所述目标系统的安全状态改为告警中安全事件对应的安全状态；前一阶段查找模块，用于查找目标系统前一阶段是否有对应的安全事件，如果找到，则执行当前安全状态设置模块，否则执行不确定安全状态设置模块；不确定安全状态设置模块，用于将目标系统的安全状态改为告警中安全事件对应的安全状态，并标记该安全状态为不确定状态。

[0047] 以上实施方式仅用于说明本发明，而并非对本发明的限制，有关技术领域的普通技术人员，在不脱离本发明的精神和范围的情况下，还可以做出各种变化和变型，因此所有等同的技术方案也属于本发明的范畴，本发明的专利保护范围应由权利要求限定。

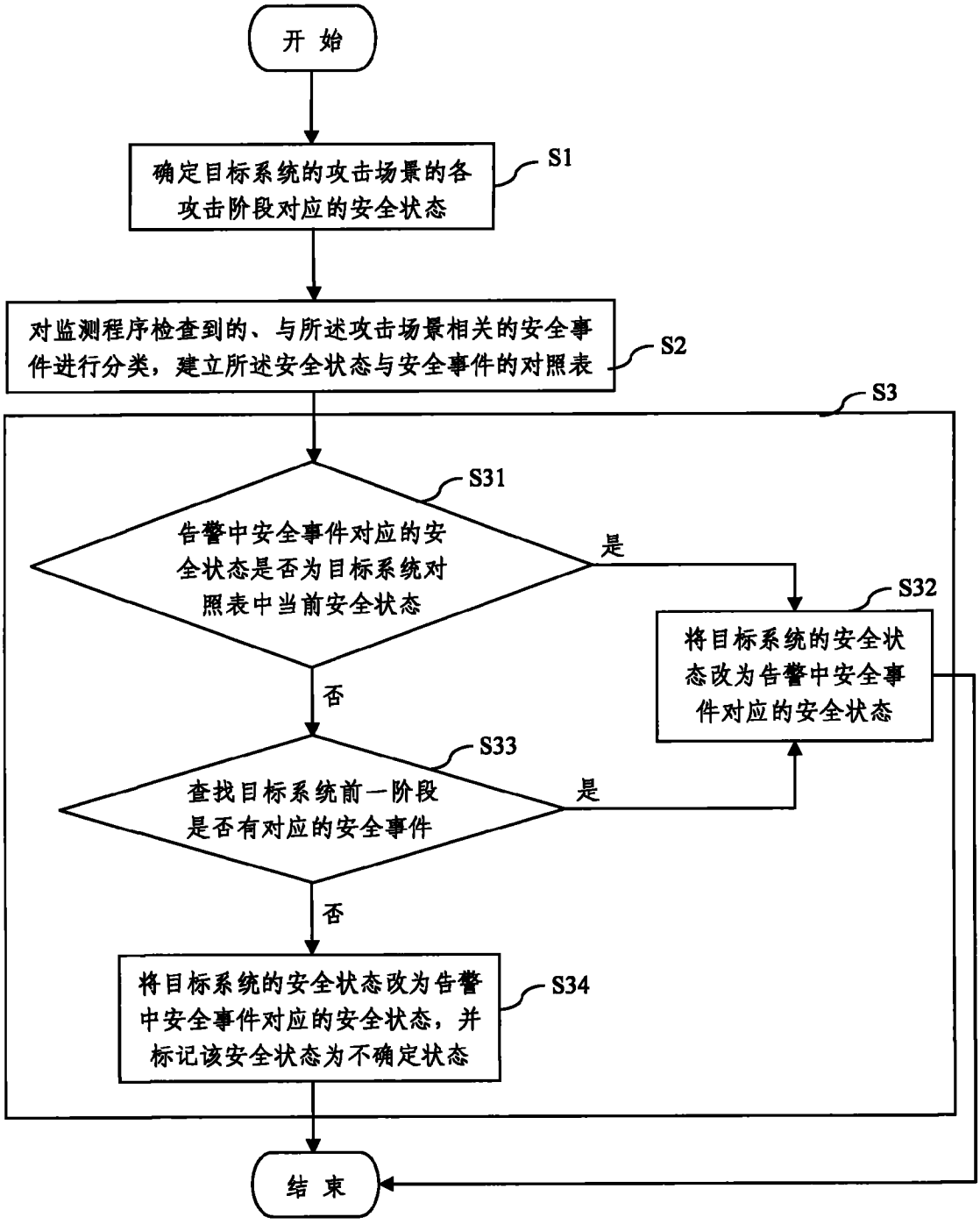

开 始
确定目标系统的攻击场景的各攻击阶段对应的安全状态
S1
对监测程序检查到的、与所述攻击场景相关的安全事件进行分类，建立所述安全状态与安全事件的对照表
S2
S3
S31
告警中安全事件对应的安全状态是否为目标系统对照表中当前安全状态
是
S32
将目标系统的安全状态改为告警中安全事件对应的安全状态
否
S33
查找目标系统前一阶段是否有对应的安全事件
是
否
将目标系统的安全状态改为告警中安全事件对应的安全状态，并标记该安全状态为不确定状态
S34
结 束

图 1