(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 108234400 B
(45)授权公告日 2021.01.22

(21)申请号 201611158794.X
(22)申请日 2016.12.15
(65)同一申请的已公布的文献号
申请公布号 CN 108234400 A
(43)申请公布日 2018.06.29
(73)专利权人 北京金山云网络技术有限公司
地址 100085 北京市海淀区小营西路33号3F02室
专利权人 北京金山云科技有限公司
(72)发明人 邱雁杰
(74)专利代理机构 北京柏杉松知识产权代理事务所(普通合伙) 11413
代理人 马敬 项京
(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 105376245 A,2016.03.02
CN 105553957 A,2016.05.04
CN 104426881 A,2015.03.18
US 2016269423 A1,2016.09.15

审查员 丁彬

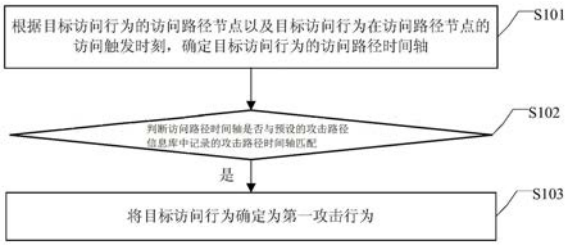
权利要求书4页 说明书13页 附图3页

(54)发明名称

一种攻击行为确定方法、装置及态势感知系统

(57)摘要

本发明实施例公开了一种攻击行为确定方法、装置及态势感知系统，该方法包括：根据目标访问行为的访问路径节点以及目标访问行为在访问路径节点的访问触发时刻，确定目标访问行为的访问路径时间轴；判断访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配，其中攻击路径时间轴为：根据攻击行为的攻击路径节点以及攻击行为在攻击路径节点的攻击触发时刻确定的；如果是，将目标访问行为确定为第一攻击行为。应用本发明实施例提供的方案，能够全面准确的感知攻击行为。



CN 108234400 B

1.一种攻击行为确定方法,其特征在于,所述方法包括:

根据目标访问行为的访问路径节点以及所述目标访问行为在所述访问路径节点的访问触发时刻,确定所述目标访问行为的访问路径时间轴;

判断所述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配,其中,所述攻击路径时间轴为:根据攻击行为的攻击路径节点以及所述攻击行为在所述攻击路径节点的攻击触发时刻确定的;所述判断所述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配为:将所述访问路径时间轴与预设的攻击路径信息库中记录的攻击路径时间轴逐一进行比对;

如果是,将所述目标访问行为确定为第一攻击行为。

2.根据权利要求1所述的方法,其特征在于,所述目标访问行为存在于业务系统中。

3.根据权利要求1所述的方法,其特征在于,所述预设的攻击路径信息库按照以下方式生成:

获取预设的蜜罐系统中的蜜罐日志;

确定所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴;

根据所确定的第二攻击行为的攻击路径时间轴,生成所述预设的攻击路径信息库。

4.根据权利要求3所述的方法,其特征在于,所述蜜罐系统为:根据业务系统中的服务搭建的。

5.根据权利要求3所述的方法,其特征在于,所述确定所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴,包括:

根据预设的攻击行为特征,确定所述蜜罐日志所对应的第二攻击行为;

根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻,确定所述第二攻击行为的攻击路径时间轴。

6.根据权利要求5所述的方法,其特征在于,所述根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻,确定所述第二攻击行为的攻击路径时间轴,包括:

根据所述蜜罐系统中的流量,确定所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻;

根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻,确定所述第二攻击行为的攻击路径时间轴。

7.根据权利要求3-6中任一项所述的方法,其特征在于,所述蜜罐日志为:

通过应用层替换bash记录的bash操作日志;和/或

通过内核模块补丁记录的键盘操作日志。

8.一种攻击行为确定装置,其特征在于,所述装置包括:

第一确定模块,用于根据目标访问行为的访问路径节点以及所述目标访问行为在所述访问路径节点的访问触发时刻,确定所述目标访问行为的访问路径时间轴;

判断模块,用于判断所述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配,其中,所述攻击路径时间轴为:根据攻击行为的攻击路径节点以及所述攻击行为在所述攻击路径节点的攻击触发时刻确定的;所述判断所述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配为:将所述访问路径时间轴与预设的

攻击路径信息库中记录的攻击路径时间轴逐一进行比对；

第二确定模块，用于在所述判断模块判断出所述访问路径时间轴与预设的攻击路径信息库中记录的攻击路径时间轴匹配时，将所述目标访问行为确定为第一攻击行为。

9.根据权利要求8所述的装置，其特征在于，所述目标访问行为存在于业务系统中。

10.根据权利要求8所述的装置，其特征在于，所述装置还包括：

生成模块，用于生成所述预设的攻击路径信息库；

其中，所述生成模块，包括：

获取子模块，用于获取预设的蜜罐系统中的蜜罐日志；

确定子模块，用于确定所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴；

生成子模块，用于根据所确定的第二攻击行为的攻击路径时间轴，生成所述预设的攻击路径信息库。

11.根据权利要求10所述的装置，其特征在于，所述蜜罐系统为：根据业务系统中的服务搭建的。

12.根据权利要求10所述的装置，其特征在于，所述确定子模块，包括：

第一确定单元，用于根据预设的攻击行为特征，确定所述蜜罐日志所对应的第二攻击行为；

第二确定单元，用于根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

13.根据权利要求12所述的装置，其特征在于，所述第二确定单元，包括：

第一确定子单元，用于根据所述蜜罐系统中的流量，确定所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻；

第二确定子单元，用于根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

14.根据权利要求10-13任一项所述的装置，其特征在于，所述蜜罐日志为：

通过应用层替换bash记录的bash操作日志；和/或

通过内核模块补丁记录的键盘操作日志。

15.一种态势感知系统，其特征在于，所述系统包括：态势感知分析平台、业务系统、蜜罐系统，其中：

所述业务系统，用于向所述态势感知分析平台反馈自身的目标访问行为；

所述态势感知分析平台，用于接收所述业务系统反馈的目标访问行为；根据所述目标访问行为的访问路径节点以及所述目标访问行为在所述访问路径节点的访问触发时刻，确定所述目标访问行为的访问路径时间轴；判断所述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配，其中，所述攻击路径时间轴为：根据攻击行为的攻击路径节点以及所述攻击行为在所述攻击路径节点的攻击触发时刻确定的；所述判断所述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配为：将所述访问路径时间轴与预设的攻击路径信息库中记录的攻击路径时间轴逐一进行比对；如果是，将所述目标访问行为确定为第一攻击行为；

所述蜜罐系统，用于向所述态势感知分析平台反馈自身的蜜罐日志；

所述态势感知分析平台，还用于接收所述蜜罐系统反馈的蜜罐日志；确定所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴；根据所确定的第二攻击行为的攻击路径时间轴，生成所述预设的攻击路径信息库。

16.根据权利要求15所述的系统，其特征在于，所述蜜罐系统为：根据所述业务系统中的服务搭建的。

17.根据权利要求15所述的系统，其特征在于，

所述态势感知分析平台，具体用于根据预设的攻击行为特征，确定所述蜜罐日志所对应的第二攻击行为；根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

18.根据权利要求17所述的系统，其特征在于，

所述态势感知分析平台，具体用于根据所述蜜罐系统中的流量，确定所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻；根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

19.根据权利要求15-18任一项所述的系统，其特征在于，所述蜜罐日志为：

通过应用层替换bash记录的bash操作日志；和/或

通过内核模块补丁记录的键盘操作日志。

20.根据权利要求15所述的系统，其特征在于，所述蜜罐系统包括：

蜜罐控制服务器、日志服务器蜜罐、应用数据库蜜罐、应用服务器蜜罐；

其中，所述应用数据库蜜罐，用于提供数据库服务，生成针对数据库服务的日志，并向所述日志服务器蜜罐发送所生成的日志；

所述应用服务器蜜罐，用于提供应用服务，生成针对应用服务的日志，并向所述日志服务器蜜罐发送所生成的日志；

所述日志服务器蜜罐，用于接收并存储所述应用数据库蜜罐和所述应用服务器蜜罐发送的日志；

所述蜜罐控制服务器，用于获取所述日志服务器蜜罐中存储的蜜罐日志，并向所述态势感知分析平台反馈所获取的蜜罐日志。

21.根据权利要求20所述的系统，其特征在于，

所述蜜罐控制服务器，用于对所述日志服务器蜜罐、应用数据库蜜罐、应用服务器蜜罐中的流量进行备份；并将备份的流量反馈给所述态势感知分析平台；

所述态势感知分析平台，具体用于根据备份的流量，确定所述第二攻击行为的攻击路径节点以及所述第二攻击行为在所述攻击路径节点的攻击触发时刻；根据所确定的所述第二攻击行为的攻击路径节点以及所述第二攻击行为在所述攻击路径节点的攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

22.根据权利要求20所述的系统，其特征在于，

所述业务系统，还用于对其中的业务数据进行脱密处理，并将脱密处理后的业务数据发送至所述应用数据库蜜罐；

所述应用数据库蜜罐，还用于接收并存储所述业务系统发送的经过脱密处理的业务数

据。

23.根据权利要求20所述的系统，其特征在于，

所述业务系统，还用于对其中的业务日志进行脱密处理，并将脱密处理后的业务日志发送至所述日志服务器蜜罐；

所述日志服务器蜜罐，还用于接收并存储所述业务系统发送的经过脱密处理的业务日志。

一种攻击行为确定方法、装置及态势感知系统

技术领域

[0001] 本发明涉及网络安全技术领域，特别涉及一种攻击行为确定方法、装置及态势感知系统。

背景技术

[0002] 随着计算机网络的迅速普及和各种网络新业务的不断兴起，网络安全问题已经逐渐渗透到社会生活的各个领域，并且变得越来越严峻。为了更好地保证网络安全，阻止破坏资源完整性、可用性和保密性等的攻击行为，及时发现攻击行为并采取相应的抵御措施来避免进一步的攻击，减少攻击造成的危害，已成为目前网络安全研究的热点。

[0003] 网络态势是指各种网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和变化趋势，网络态势感知是指在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。对于网络安全的态势感知，现有技术是基于业务日志来进行分析的，从业务日志中分析出攻击行为，并根据分析出的攻击行为对业务系统进行态势感知，业务日志为业务系统实际运行时产生的日志。

[0004] 由于现有的业务系统在层层防御体系之后，业务日志中的攻击日志更多是较浅层面的泛扫描攻击行为，因而从业务日志中并不能捕获到足够多的数据来确定深入的攻击路径，进而也就无法了解攻击者对业务的关注度和深度攻击手法，及攻击者意图窃取的关键业务数据。也就是说，现有技术中的态势感知方法不能全面准确的感知攻击者的攻击行为。

发明内容

[0005] 本发明实施例的目的在于提供一种攻击行为确定方法、装置及态势感知系 统，以全面准确的感知攻击行为。具体技术方案如下：

[0006] 为达到上述目的，本发明实施例公开了一种攻击行为确定方法，所述方法 包括：

[0007] 根据目标访问行为的访问路径节点以及所述目标访问行为在所述访问路径 节点的访问触发时刻，确定所述目标访问行为的访问路径时间轴；

[0008] 判断所述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径 时间轴匹配，其中，所述攻击路径时间轴为：根据攻击行为的攻击路径节点以 及所述攻击行为在所述攻击路径节点的攻击触发时刻确定的；

[0009] 如果是，将所述目标访问行为确定为第一攻击行为。

[0010] 可选的，所述目标访问行为存在于业务系统中。

[0011] 可选的，所述预设的攻击路径信息库按照以下方式生成：

[0012] 获取预设的蜜罐系统中的蜜罐日志；

[0013] 确定所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴；

[0014] 根据所确定的攻击路径时间轴，生成所述预设的攻击路径信息库。

[0015] 可选的，所述蜜罐系统为：根据所述业务系统中的服务搭建的。

[0016] 可选的，所述确定所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴， 包

括：

[0017] 根据预设的攻击行为特征，确定所述蜜罐日志所对应的第二攻击行为；

[0018] 根据所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述 目标攻击路径节点的目标攻击触发时刻，确定所述第二攻击行为的攻击路径时 间轴。

[0019] 可选的，所述根据所述第二攻击行为的目标攻击路径节点以及所述第二攻 击行为在所述目标攻击路径节点的目标攻击触发时刻，确定所述第二攻击行为 的攻击路径时间轴，包括：

[0020] 根据所述蜜罐系统中的流量，确定所述第二攻击行为的目标攻击路径节点 以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻；

[0021] 根据所述目标攻击路径节点以及所述目标攻击触发时刻，确定所述第二攻 击行为的攻击路径时间轴。

[0022] 可选的，所述蜜罐日志为：

[0023] 通过应用层替换bash记录的bash操作日志；和/或

[0024] 通过内核模块补丁记录的键盘操作日志。

[0025] 为达到上述目的，本发明实施例还公开了一种攻击行为确定装置，所述装 置包括：

[0026] 第一确定模块，用于根据目标访问行为的访问路径节点以及所述目标访问 行为在所述访问路径节点的访问触发时刻，确定所述目标访问行为的访问路径 时间轴；

[0027] 判断模块，用于判断所述访问路径时间轴是否与预设的攻击路径信息库中 记录的攻击路径时间轴匹配，其中，所述攻击路径时间轴为：根据攻击行为的 攻击路径节点以及所述攻击行为在所述攻击路径节点的攻击触发时刻确定的；

[0028] 第二确定模块，用于在所述判断模块判断出所述访问路径时间轴与预设的 攻击路径信息库中记录的攻击路径时间轴匹配时，将所述目标访问行为确定为 第一攻击行为。

[0029] 可选的，所述目标访问行为存在于业务系统中。

[0030] 可选的，所述装置还包括：

[0031] 生成模块，用于生成所述预设的攻击路径信息库；

[0032] 其中，所述生成模块，包括：

[0033] 获取子模块，用于获取预设的蜜罐系统中的蜜罐日志，其中，所述蜜罐系 统为：根据所述业务系统中的服务搭建的；

[0034] 确定子模块，用于确定所述蜜罐日志所对应的第二攻击行为的攻击路径时 间轴；

[0035] 生成子模块，用于根据所确定的攻击路径时间轴，生成所述预设的攻击路 径信息库。

[0036] 可选的，所述蜜罐系统为：根据所述业务系统中的服务搭建的。

[0037] 可选的，所述确定子模块，包括：

[0038] 第一确定单元，用于根据预设的攻击行为特征，确定所述蜜罐日志所对应 的第二攻击行为；

[0039] 第二确定单元，用于根据所述第二攻击行为的目标攻击路径节点以及所述 第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻，确定所述第二攻 击行为的攻击路径时间轴。

[0040] 可选的，所述第二确定单元，包括：

[0041] 第一确定子单元，用于根据所述蜜罐系统中的流量，确定所述第二攻击行 为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标 攻击触发时刻；

[0042] 第二确定子单元，用于根据所述目标攻击路径节点以及所述目标攻击触发 时刻，确定所述第二攻击行为的攻击路径时间轴。

[0043] 可选的，所述蜜罐日志为：

[0044] 通过应用层替换bash记录的bash操作日志；和/或

[0045] 通过内核模块补丁记录的键盘操作日志。

[0046] 为达到上述目的，本发明实施例还公开了一种态势感知系统，所述系统包 括：态势感知分析平台、业务系统、蜜罐系统，其中：

[0047] 所述业务系统，用于向所述态势感知分析平台反馈自身的目标访问行为；

[0048] 所述态势感知分析平台，用于接收所述业务系统反馈的目标访问行为；根 据所述目标访问行为的访问路径节点以及所述目标访问行为在所述访问路径节 点的访问触发时刻，确定所述目标访问行为的访问路径时间轴；判断所述访问 路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配，其中， 所述攻击路径时间轴为：根据攻击行为的攻击路径节点以及所述攻击行为在所 述攻击路径节点的攻击触发时刻确定的；如果是，将所述目标访问行为确定为 第一攻击行为；

[0049] 所述蜜罐系统，用于向所述态势感知分析平台反馈自身的蜜罐日志；

[0050] 所述态势感知分析平台，还用于接收所述蜜罐系统反馈的蜜罐日志；确定 所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴；根据所确定的攻击路 径时间轴，生成所述预设的攻击路径信息库。

[0051] 可选的，所述蜜罐系统为：根据所述业务系统中的服务搭建的。

[0052] 可选的，所述态势感知分析平台，具体用于根据预设的攻击行为特征，确 定所述蜜罐日志所对应的第二攻击行为；根据所述第二攻击行为的目标攻击路 径节点以及所述第二攻击行为在所述目标攻击路径节点的目标访问触发时刻， 确定所述第二攻击行为的攻击路径时间轴。

[0053] 可选的，所述态势感知分析平台，具体用于根据所述蜜罐系统中的流量， 确定所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标 攻击路径节点的目标攻击触发时刻；根据所述目标攻击路径节点以及所述目标 攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

[0054] 可选的，所述蜜罐日志为：

[0055] 通过应用层替换bash记录的bash操作日志；和/或

[0056] 通过内核模块补丁记录的键盘操作日志。

[0057] 可选的，所述蜜罐系统包括：

[0058] 蜜罐控制服务器、日志服务器蜜罐、应用数据库蜜罐、应用服务器蜜罐；

[0059] 其中，所述应用数据库蜜罐，用于提供数据库服务，生成针对数据库服务 的日志，并向所述日志服务器蜜罐发送所生成的日志；

[0060] 所述应用服务器蜜罐，用于提供应用服务，生成针对应用服务的日志，并 向所述日志服务器蜜罐发送所生成的日志；

[0061] 所述日志服务器蜜罐，用于接收并存储所述应用数据库蜜罐和所述应用服 务器蜜罐发送的日志；

[0062] 所述蜜罐控制服务器，用于获取所述日志服务器蜜罐中存储的蜜罐日志，并向所述态势感知分析平台反馈所获取的蜜罐日志。

[0063] 可选的，所述蜜罐控制服务器，用于对所述日志服务器蜜罐、应用数据库 蜜罐、应用服务器蜜罐中的流量进行备份；并将备份的流量反馈给所述态势感 知分析平台；

[0064] 所述态势感知分析平台，具体用于根据备份的流量，确定所述第二攻击行 为的攻击路径节点以及所述第二攻击行为在所述攻击路径节点的攻击触发时 刻；根据所确定的所述第二攻击行为的攻击路径节点以及所述第二攻击行为在 所述攻击路径节点的攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

[0065] 可选的，所述业务系统，还用于对其中的业务数据进行脱密处理，并将脱 密处理后的业务数据发送至所述应用数据库蜜罐；

[0066] 所述应用数据库蜜罐，还用于接收并存储所述业务系统发送的经过脱密处 理的业务数据。

[0067] 可选的，所述业务系统，还用于对其中的业务日志进行脱密处理，并将脱 密处理后的业务数据发送至所述日志服务器蜜罐；

[0068] 所述日志服务器蜜罐，还用于接收并存储所述业务系统发送的经过脱密处 理的业务日志。

[0069] 由以上可知，本发明实施例所提供的方案中，根据目标访问行为的访问路 径节点以及目标访问行为在访问路径节点的访问触发时刻，确定目标访问行为 的访问路径时间轴；判断访问路径时间轴是否与预设的攻击路径信息库中记录 的攻击路径时间轴匹配，其中，攻击路径时间轴为：根据攻击行为的攻击路径 节点以及攻击行为在攻击路径节点的攻击触发时刻确定的；如果是，将目标访 问行为确定为攻击行为。与现有技术相比，本发明实施例提供的方案中，通过 建立攻击路径时间轴的方式来生成攻击路径信息库，而攻击路径时间轴能够准 确的反映攻击行为的攻击路径和攻击手法，因此本发明实施例的方案能够全面 准确的感知攻击行为。

附图说明

[0070] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施 例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述 中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付 出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0071] 图1为本发明实施例提供的一种攻击行为确定方法的流程示意图；

[0072] 图2为本发明实施例提供的一种攻击路径信息库生成方法的流程示意图；

[0073] 图3为本发明实施例提供的一种攻击行为确定装置的结构示意图；

[0074] 图4为本发明实施例提供的另一种攻击行为确定装置的结构示意图；

[0075] 图5为本发明实施例提供的一种攻击路径信息库生成装置的结构示意图；

[0076] 图6为本发明实施例提供的一种态势感知系统的结构示意图；

[0077] 图7为本发明实施例提供的另一种态势感知系统的结构示意图；

[0078] 图8为本发明实施例提供的一个具体实施例的示意图。

具体实施方式

[0079] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清 楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是 全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造 性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0080] 为解决现有技术问题，本发明实施例提供了一种攻击行为确定方法及装置。下面首先对本发明实施例所提供的一种攻击行为确定方法进行详细说明。

[0081] 图1为本发明实施例提供的一种攻击行为方法的流程示意图，该方法包括：

[0082] S101，根据目标访问行为的访问路径节点以及目标访问行为在访问路径节 点的访问触发时刻，确定目标访问行为的访问路径时间轴。

[0083] 其中，目标访问行为可以是业务系统中的访问行为。具体的，目标访问行 为的信息可以是从业务系统中的业务日志中获得的，也可以是实时从业务系统 中获得的，本实施例对此不做限定。上述目标访问行为的信息可以包括：目标 访问行为的访问路径节点、目标访问行为在访问路径节点的访问触发时刻等信 息。

[0084] 用户从进入业务系统开始访问到离开业务系统，为一次访问行为。在一次 访问行为中，用户会访问业务系统中不同的节点，如业务服务器、数据库服务 器等，这些节点按照访问的先后顺序可以构成一次访问行为中的访问路径。因 此，可以根据业务系统中访问行为的访问路径节点以及访问行为在访问路径节 点的访问触发时刻，来确定访问行为的访问路径时间轴。

[0085] 示例性的，用户访问业务系统时，业务系统可以记录此次访问行为的用户 标识如IP地址、所访问的服务的标识、以及访问该服务的时刻等信息，根据所记 录的信息，可以确定该访问行为的访问路径时间轴，例如，所确定的访问路径 时间轴可以为：IP地址为36.7.72.139的用户于2015年11月30日10点10分20秒访问 服务A、又于10点15分40秒访问服务B、又于10点16分40秒到18分50秒之间连续5 次访问服务B。

[0086] 当然，访问触发时刻可以使用上述实际发生的时刻表示，还可以以第一个 节点对应的访问触发时刻为起始时刻，根据各个节点之间的访问触发时刻的相 对差值的方式来表示。例如，上述访问路径时间轴还可以表示为：IP地址为 36.7.72.139的用户于2015年11月30日10点10分20秒访问服务A、又于5分20秒后 访问服务B、又于1分钟后在2分10秒内连续5次访问服务B。

[0087] S102，判断访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路 径时间轴匹配。

[0088] 其中，攻击路径时间轴为：根据攻击行为的攻击路径节点以及攻击行为在 攻击路径节点的攻击触发时刻确定的。

[0089] 预设的攻击路径信息库用于记录蜜罐系统中的攻击行为的攻击路径时间 轴，攻击路径信息库的具体生成过程可以参见图2所示实施例，这里暂不详述。

[0090] 判断访问路径时间轴与攻击路径时间轴是否匹配，可以将访问路径时间轴 与攻击路径信息库中记录的攻击路径时间轴逐一进行比对，根据时间轴所记录 的信息是否一

致来判断，也可以预先设置相似度阈值，当访问路径时间轴与攻 击路径时间轴的相似度达到阈值时，判定访问路径时间轴与攻击路径时间轴匹 配，也可以根据其他方式进行判断，本实施例对此不做限定。

[0091] 示例性的，若访问路径时间轴A中的各个访问路径节点与某一攻击路径时间 轴A’中的各个攻击路径节点均相同，只是各个节点所对应的相对触发时刻略有 不同，比如，访问路径时间轴A显示访问节点M与访问节点N的访问触发时刻的 相对差值为10分钟，而攻击路径时间轴A’显示攻击节点M’与攻击节点N’的 攻击触发时刻的相对差值为8分钟，可见，A和A’的相似度较高，则可以判定 访问路径时间轴A与攻击路径时间轴A’匹配。

[0092] S103，如果是，将目标访问行为确定为第一攻击行为。

[0093] 由以上可知，本实施例所提供的方案中，根据目标访问行为的访问路径节 点以及目标访问行为在访问路径节点的访问触发时刻，确定目标访问行为的访 问路径时间轴；判断访问路径时间轴是否与预设的攻击路径信息库中记录的攻 击路径时间轴匹配，其中，攻击路径时间轴为：根据攻击行为的攻击路径节点 以及攻击行为在攻击路径节点的攻击触发时刻确定的；如果是，将目标访问行 为确定为攻击行为。与现有技术相比，本实施例提供的方案中，通过建立攻击 路径时间轴的方式来生成攻击路径信息库，而攻击路径时间轴能够准确的反映 攻击行为的攻击路径和攻击手法，因此本实施例的方案能够全面准确的感知攻 击行为。

[0094] 下面通过具体实施例详细介绍前面涉及到的预设的攻击路径信息库。

[0095] 图2为本发明实施例提供的一种攻击路径信息库生成方法的流程示意图， 该方法包括：

[0096] S201，获取预设的蜜罐系统中的蜜罐日志。

[0097] 其中，蜜罐系统可以为：根据业务系统中的服务搭建的。这是为了达到模 拟真实业务系统、最大程度的迷惑攻击者的目的，蜜罐系统与业务系统相一致， 包含了与业务系统同样的机器设备，并且在机器设备上部署同样的应用服务， 例如，在蜜罐系统中部署与业务系统相同的服务器，并且服务器所包含的服务 程序也相同。

[0098] 其中，蜜罐日志可以为：

[0099] 通过应用层替换bash记录的bash操作日志；和/或

[0100] 通过内核模块补丁记录的键盘操作日志。

[0101] 为保证蜜罐日志的可记录性，通过应用层替换bash，记录蜜罐系统中的访问 者的bash操作日志，应用层bash为操作系统自带的执行shell的应用程序，替换bash 是使用修改的bash替换系统自带的shell执行程序，修改的bash的主要功能是：在 bash执行命令的时候，可以将所执行命令记录到系统日志syslog中，在蜜罐系统 中系统日志syslog是蜜罐日志的一部分。bash是一个为GNU计划编写的Unix shell，是大多数Linux系统以及Mac OS X v10.4默认的shell，它能运行于大多数 Unix风格的操作系统之上，甚至被移植到了Microsoft Windows上的Cygwin系统 中，以实现windows的POSIX虚拟接口。

[0102] 还可以通过内核模块补丁，例如ttyrpld，进行键盘记录，避免由于上述应用 层记录缺失导致蜜罐日志记录不完整。

[0103] S202，确定蜜罐日志所对应的第二攻击行为的攻击路径时间轴。

[0104] 具体的，确定蜜罐日志所对应的第二攻击行为的攻击路径时间轴，可以包 括：

[0105] 根据预设的攻击行为特征，确定蜜罐日志所对应的第二攻击行为；

[0106] 根据第二攻击行为的目标攻击路径节点以及第二攻击行为在目标攻击路径 节点的目标攻击触发时刻，确定第二攻击行为的攻击路径时间轴。

[0107] 由于蜜罐系统也有可能会被网络爬虫爬取到，因此蜜罐日志中记录的访问 行为不全是攻击者的攻击行为。这种情况下，还需要根据预设的攻击行为特征， 确定蜜罐日志对应的攻击行为。例如，预设的攻击行为特征可以为攻击行为短 时间内多次访问特定服务、攻击行为意图调取用户数据，等等，当然，攻击行 为特征还可以设置为其他类型的异常访问的行为特征，本实施例对此不做限定。

[0108] 攻击者从进入蜜罐系统开始攻击到离开蜜罐系统，为一次攻击行为。在一 次攻击行为中，攻击者会攻击蜜罐系统中不同的节点，如业务服务器蜜罐、数 据库服务器蜜罐等，这些节点按照攻击的先后顺序可以构成一次攻击行为中的 攻击路径。因此，可以根据业攻击行为的攻击路径节点以及攻击行为在攻击路 径节点的攻击触发时刻，来确定攻击行为的攻击路径时间轴。

[0109] 示例性的，攻击者访问蜜罐系统时，蜜罐系统可以通过蜜罐日志记录此次 攻击行为的用户标识如IP地址、所攻击的服务的标识、以及攻击该服务的时刻等 信息，根据所记录的信息，可以确定该攻击行为的攻击路径时间轴，例如，所 确定的攻击路径时间轴可以为：IP地址为36.7.72.139的攻击者于2015年11月30日 10点10分20秒访问服务A、又于10点15分40秒访问服务B、再于10点16分40秒到 18分50秒之间连续5次访问服务B。

[0110] 当然，攻击触发时刻可以使用上述实际发生的时刻表示，还可以以第一个 节点对应的攻击触发时刻为起始时刻，根据各个节点之间的攻击触发时刻的相 对差值的方式来表示。例如，上述攻击路径时间轴还可以表示为：IP地址为 36.7.72.139的攻击者于2015年11月30日10点10分20秒攻击服务A、又于5分20秒 后攻击服务B、又于1分钟后在2分10秒内连续5次攻击服务B。

[0111] 进一步的，由于蜜罐日志中记录的攻击行为的信息有限，比如攻击者成功 入侵蜜罐系统后，在蜜罐系统中种植木马程序以及向木马控制端建立的连接， 或者对蜜罐系统发送的恶意流量攻击，这些都需要通过蜜罐系统的流量来查看， 蜜罐日志一般没有记录。因此，还可以实时对蜜罐系统中的流量进行保存，以 便于后续根据流量来更深入的了解攻击行为。

[0112] 因此，可以根据蜜罐系统中的流量，确定第二攻击行为的目标攻击路径节 点以及第二攻击行为在目标攻击路径节点的目标攻击触发时刻；根据目标攻击 路径节点以及目标攻击触发时刻，确定第二攻击行为的攻击路径时间轴。

[0113] 以上述攻击行为为例，如果根据蜜罐系统中的流量，发现IP地址为 36.7.72.139的攻击者还于10点20分10秒在服务B中种植了木马程序X，此时，还 可以将该信息添加到该攻击行为的攻击路径时间轴上。

[0114] S203，根据所确定的攻击路径时间轴，生成预设的攻击路径信息库。

[0115] 可以理解的，由于不断会有攻击者进入蜜罐系统进行攻击行为，所以蜜罐 日志中的第二攻击行为是不断更新和增加的，因此，需不断更新上述预设的攻 击路径信息库，例如，可以是按照固定的时间间隔更新上述预设的攻击路径信 息库，如，一天更新一次、一周更新一次等等。

[0116] 需要说明的是，攻击者在蜜罐系统中的活动可以由蜜罐日志进行记录，由 于蜜罐系统可以吸引或者迷惑更多的攻击者在其中进行攻击活动，因此相对于 业务日志，蜜罐日志可以记录攻击者更多深入的攻击行为，进而帮助业务人员 了解攻击者对业务的关注度和深度攻击手法，及攻击者意图窃取的关键业务数 据。基于蜜罐日志分析出的攻击路径时间轴对业务系统中的访问行为进行态势 感知分析，可以提升对业务系统中的攻击态势的感知发现能力。

[0117] 由以上可知，本实施例所提供的方案中，搭建与业务系统中的服务相同的 蜜罐系统，根据蜜罐系统中的蜜罐日志，确定蜜罐系统中的攻击行为的攻击路 径时间轴，并建立攻击路径信息库以记录攻击路径时间轴。当业务系统中的访 问行为的访问路径时间轴与攻击路径信息库中的攻击路径时间轴相匹配时，将 该访问行为确定为攻击行为。与现有技术相比，本实施例利用了与业务系统相 同的蜜罐系统，从蜜罐日志中能够获得足够多的数据来分析更多深入的攻击路 径，并建立攻击路径信息库，因此本实施例的方案能够全面准确的感知攻击行 为。

[0118] 与上述的攻击行为确定方法相对应，本发明实施例还提供了一种攻击行为 确定装置。

[0119] 与图1所示的方法实施例相对应，图3为本发明实施例提供的一种攻击行 为确定装置的结构示意图，该装置可以包括：

[0120] 第一确定模块301，用于根据目标访问行为的访问路径节点以及所述目标访 问行为在所述访问路径节点的访问触发时刻，确定所述目标访问行为的访问路 径时间轴；

[0121] 判断模块302，用于判断所述访问路径时间轴是否与预设的攻击路径信息库 中记录的攻击路径时间轴匹配，其中，所述攻击路径时间轴为：根据攻击行为 的攻击路径节点以及所述攻击行为在所述攻击路径节点的攻击触发时刻确定 的；

[0122] 第二确定模块303，用于在所述判断模块302判断出所述访问路径时间轴与 预设的攻击路径信息库中记录的攻击路径时间轴匹配时，将所述目标访问行为 确定为第一攻击行为。

[0123] 具体的，所述目标访问行为可以存在于业务系统中。

[0124] 由以上可知，本实施例所提供的方案中，根据目标访问行为的访问路径节 点以及目标访问行为在访问路径节点的访问触发时刻，确定目标访问行为的访 问路径时间轴；判断访问路径时间轴是否与预设的攻击路径信息库中记录的攻 击路径时间轴匹配，其中，攻击路径时间轴为：根据攻击行为的攻击路径节点 以及攻击行为在攻击路径节点的攻击触发时刻确定的；如果是，将目标访问行 为确定为攻击行为。与现有技术相比，本实施例提供的方案中，通过建立攻击 路径时间轴的方式来生成攻击路径信息库，而攻击路径时间轴能够准确的反映 攻击行为的攻击路径和攻击手法，因此本实施例的方案能够全面准确的感知攻 击行为。

[0125] 在一种优选的实施方式中，如图4所示，在图3所示实施例的基础上，该攻 击行为确定装置还可以包括：生成模块304，用于生成所述预设的攻击路径信息 库。

[0126] 下面通过具体实施例详细介绍前面涉及到的预设的攻击路径信息库。

[0127] 与图2所示的方法实施例相对应，图5为本发明实施例提供的一种攻击路径 信息库生成装置的结构示意图，该装置为生成模块304的一种具体装置，包括：

[0128] 获取子模块3041，用于获取预设的蜜罐系统中的蜜罐日志；

[0129] 确定子模块3042，用于确定所述蜜罐日志所对应的第二攻击行为的攻击路 径时间轴；

[0130] 生成子模块3043，用于根据所确定的攻击路径时间轴，生成所述预设的攻 击路径信息库。

[0131] 具体的，所述蜜罐系统可以为：根据所述业务系统中的服务搭建的。

[0132] 具体的，所述确定子模块3042，可以包括：

[0133] 第一确定单元(图中未示出)，用于根据预设的攻击行为特征，确定所述蜜 罐日志所对应的第二攻击行为；

[0134] 第二确定单元(图中未示出)，用于根据所述第二攻击行为的目标攻击路径 节点以及所述第二攻击行为在所述目标攻击路径节点的目标攻击触发时刻，确 定所述第二攻击行为的攻击路径时间轴。

[0135] 具体的，所述第二确定单元，可以包括：

[0136] 第一确定子单元(图中未示出)，用于根据所述蜜罐系统中的流量，确定所 述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标攻击路 径节点的目标攻击触发时刻；

[0137] 第二确定子单元(图中未示出)，用于根据所述目标攻击路径节点以及所述 目标攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

[0138] 具体的，所述蜜罐日志可以为：

[0139] 通过应用层替换bash记录的bash操作日志；和/或

[0140] 通过内核模块补丁记录的键盘操作日志。

[0141] 由以上可知，本实施例所提供的方案中，搭建与业务系统中的服务相同的 蜜罐系统，根据蜜罐系统中的蜜罐日志，确定蜜罐系统中的攻击行为的攻击路 径时间轴，并建立攻击路径信息库以记录攻击路径时间轴。当业务系统中的访 问行为的访问路径时间轴与攻击路径信息库中的攻击路径时间轴相匹配时，将 该访问行为确定为攻击行为。与现有技术相比，本实施例利用了与业务系统相 同的蜜罐系统，从蜜罐日志中能够获得足够多的数据来分析更多深入的攻击路 径，并建立攻击路径信息库，因此本实施例的方案能够全面准确的感知攻击行 为。

[0142] 与上述的攻击行为确定方法、装置相对应，本发明实施例还提供了一种态 势感知系统。

[0143] 图6为本发明实施例提供的一种态势感知系统的结构示意图，该系统可以包 括：态势感知分析平台601、业务系统602、蜜罐系统603，其中：

[0144] 所述业务系统602，用于向所述态势感知分析平台601反馈自身的目标访问 行为；

[0145] 所述态势感知分析平台601，用于接收所述业务系统602反馈的目标访问行 为；根据所述目标访问行为的访问路径节点以及所述目标访问行为在所述访问 路径节点的访问触发时刻，确定所述目标访问行为的访问路径时间轴；判断所 述访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹 配，其中，所述攻击路径时间轴为：根据攻击行为的攻击路径节点以及所述攻 击行为在所述攻击路径节点的攻击触发时刻确定的；如果是，将所述目标访问 行为确定为第一攻击行为；

[0146] 所述蜜罐系统603，用于向所述态势感知分析平台601反馈自身的蜜罐日志；

[0147] 所述态势感知分析平台601，还用于接收所述蜜罐系统603反馈的蜜罐日志；确定所述蜜罐日志所对应的第二攻击行为的攻击路径时间轴；根据所确定的攻 击路径时间轴，生成所述预设的攻击路径信息库。

[0148] 具体的，所述蜜罐系统可以为：根据所述业务系统602中的服务搭建的。

[0149] 可以理解的是，预设的攻击路径信息库也可以由蜜罐系统根据蜜罐日志按 照上述方法生成并反馈给态势感知分析平台的，以使态势感知分析平台根据攻 击路径信息库对业务系统的业务日志进行态势感知分析。

[0150] 具体的，所述态势感知分析平台601，具体用于根据预设的攻击行为特征，确定所述蜜罐日志所对应的第二攻击行为；根据所述第二攻击行为的目标攻击 路径节点以及所述第二攻击行为在所述目标攻击路径节点的目标访问触发时 刻，确定所述第二攻击行为的攻击路径时间轴。

[0151] 具体的，所述态势感知分析平台601，具体用于根据所述蜜罐系统中的流量，确定所述第二攻击行为的目标攻击路径节点以及所述第二攻击行为在所述目标 攻击路径节点的目标攻击触发时刻；根据所述目标攻击路径节点以及所述目标 攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

[0152] 具体的，所述蜜罐日志为：

[0153] 通过应用层替换bash记录的bash操作日志；和/或

[0154] 通过内核模块补丁记录的键盘操作日志。

[0155] 图7为本发明实施例提供的另一种态势感知系统的结构示意图，在图6所示 实施例的基础上，所述蜜罐系统603可以包括：

[0156] 蜜罐控制服务器6031、日志服务器蜜罐6032、应用数据库蜜罐6033、应用 服务器蜜罐6034；

[0157] 其中，所述应用数据库蜜罐6033，用于提供数据库服务，生成针对数据库 服务的日志，并向所述日志服务器蜜罐6032发送所生成的日志；

[0158] 所述应用服务器蜜罐6034，用于提供应用服务，生成针对应用服务的日志，并向所述日志服务器蜜罐6032发送所生成的日志；

[0159] 所述日志服务器蜜罐6032，用于接收并存储所述应用数据库蜜罐6033和所 述应用服务器蜜罐6034发送的日志；

[0160] 所述蜜罐控制服务器6031，用于获取所述日志服务器蜜罐6032中存储的蜜 罐日志，并向所述态势感知分析平台601反馈所获取的蜜罐日志。

[0161] 可以理解的，业务系统中可以是由应用数据库、应用服务器、日志服务器 等组成，为了搭建与业务系统一致的蜜罐系统，在蜜罐系统中可以设置与业务 系统相同的应用数据库蜜罐、应用服务器蜜罐、日志服务器蜜罐。另外，还可 以在蜜罐系统中设置蜜罐控制服务器，来对各个日志服务器蜜罐、应用数据库 蜜罐、应用服务器蜜罐进行统一管理和控制。

[0162] 并且，在应用数据库蜜罐和应用服务器蜜罐可以设置可控数量和类型的安 全漏洞，以便于攻击者能够较为容易地进入蜜罐系统访问其中的数据。

[0163] 具体的，所述蜜罐控制服务器6031，用于对所述日志服务器蜜罐6032、应 用数据库蜜罐6033、应用服务器蜜罐6034中的流量进行备份；并将备份的流量 反馈给所述态势感

知分析平台601；

[0164] 所述态势感知分析平台601，具体用于根据备份的流量，确定所述第二攻击 行为的攻击路径节点以及所述第二攻击行为在所述攻击路径节点的攻击触发时 刻；根据所确定的所述第二攻击行为的攻击路径节点以及所述第二攻击行为在 所述攻击路径节点的攻击触发时刻，确定所述第二攻击行为的攻击路径时间轴。

[0165] 具体的，所述业务系统602，还用于对其中的业务数据进行脱密处理，并将 脱密处理后的业务数据发送至所述应用数据库蜜罐6033；

[0166] 所述应用数据库蜜罐6033，还用于接收并存储所述业务系统602发送的经过 脱密处理的业务数据。

[0167] 业务数据可以理解为业务系统中与用户有关的数据，例如用户的基本信息， 用户的历史访问信息等。为保证蜜罐系统的真实性，可以将业务系统中的业务 数据进行脱密处理并导入到应用数据库蜜罐中，达到既不泄露用户信息、又使 蜜罐中的数据看起来合理、进而迷惑攻击者的目的，脱密处理是指对某些敏感 信息进行数据的变形，实现敏感隐私数据的可靠保护。

[0168] 具体的，所述业务系统602，还用于对其中的业务日志进行脱密处理，并将脱密处理后的业务日志发送至所述日志服务器蜜罐6032；

[0169] 所述日志服务器蜜罐6032，还用于接收并存储所述业务系统602发送的经过脱密处理的业务日志。

[0170] 可以理解的，为保证蜜罐系统真实性，还可以定期或实时将业务系统中的 脱密处理过的业务日志导入到日志服务器蜜罐中，并定期对导入到的业务日志 进行备份及删除操作，以保持蜜罐系统活跃性，使其更接近真实的业务系统， 从而能够吸引攻击者进入蜜罐系统，并且不容易被攻击者发现自身进入的是蜜 罐系统。

[0171] 攻击者在蜜罐系统中的活动可以由蜜罐日志进行记录，由于蜜罐系统可以 吸引或者迷惑更多的攻击者在其中进行攻击活动，因此相对于业务日志，蜜罐 日志可以记录攻击者更多深入的攻击行为，进而帮助业务人员了解攻击者对业 务的关注度和深度攻击手法，及攻击者意图窃取的关键业务数据。

[0172] 由以上可知，本实施例所提供的方案中，搭建与业务系统中的服务相同的 蜜罐系统，根据蜜罐系统中的蜜罐日志，确定蜜罐系统中的攻击行为的攻击路 径时间轴，并建立攻击路径信息库以记录攻击路径时间轴。当业务系统中的访 问行为的访问路径时间轴与攻击路径信息库中的攻击路径时间轴相匹配时，将 该访问行为确定为攻击行为。与现有技术相比，本实施例利用了与业务系统相 同的蜜罐系统，从蜜罐日志中能够获得足够多的数据来分析更多深入的攻击路 径，并建立攻击路径信息库，因此本实施例的方案能够全面准确的感知攻击行 为。

[0173] 下面以一个具体实施例对本发明实施例提供的态势感知系统进行详细说 明。

[0174] 如图8所示的基于蜜罐的态势感知系统的示意图。将关键业务组成业务系 统，包括业务系统的应用服务器、业务系统的数据库服务器、业务系统的日志 服务器，业务系统在图8中未示出。搭建与业务系统一致的蜜罐系统，蜜罐系 统包括：与业务系统的应用服务器相对应的应用服务器蜜罐(即蜜罐B)、与业 务系统的数据库服务器相对应的应用数据库蜜罐(即蜜罐A)、与业务系统的日 志服务器相对应的日志服务器蜜罐，以及用于对各个日

志服务器蜜罐、应用数 据库蜜罐、应用服务器蜜罐进行统一管理和控制的蜜罐控制服务器。

[0175] 其中，蜜罐A所模拟的是应用数据库，可在蜜罐A中设置可控数量和类型 的安全漏洞，蜜罐B所模拟的是应用服务，同样可在蜜罐B中设置可控数量和 类型的安全漏洞，以便于攻击者能够较为容易地进入对应的蜜罐访问其中的数 据。

[0176] 日志服务器蜜罐用于存储蜜罐A中的数据库日志和蜜罐B中的登录日志。当攻击者攻击蜜罐B时，蜜罐B可以以日志的形式记录攻击者的攻击行为，并 将日志传输给日志服务器蜜罐；当攻击者攻击蜜罐A时，蜜罐A同样可以以日 志的形式记录攻击者的攻击行为，并将日志传输给日志服务器蜜罐。

[0177] 蜜罐控制服务器可以获取日志服务器蜜罐中存储的蜜罐日志，并向态势感 知分析平台反馈所获取的蜜罐日志。同样的，业务系统也可以将自身的业务日 志反馈给态势感知分析系统。

[0178] 态势感知分析系统根据蜜罐日志分析出其中的攻击行为，建立每个攻击行 为对应的攻击路径时间轴，并组成攻击路径信息库；将攻击路径信息库中的攻 击路径时间轴作为特征因子，对业务日志进行态势感知分析，确定出业务日志 中的攻击行为。使用蜜罐系统中的蜜罐日志对业务系统中业务日志进行态势感 知分析，可以提高态势感知分析系统对业务系统中的攻击行为的发现能力。

[0179] 为保证蜜罐系统的真实性，可以将真实的业务数据经过脱密处理后存储在 模拟业务系统应用数据库服务器的蜜罐A中。在日志服务器蜜罐也需要定期输 入真实的脱密实际业务应用日志，并定期对业务日志进行备份及删除操作。

[0180] 为保证蜜罐日志的可记录性，可以通过应用层替换bash记录攻击者的bash 操作日志，以及通过内核模块补丁(ttyrpld)进行键盘记录，避免由于应用层记 录导致的缺失。还可以对蜜罐系统的流量进行旁路备份，存储蜜罐系统中流量， 用于分析攻击行为的攻击路径时间轴。

[0181] 由以上可知，本具体实施例中，在态势感知系统中搭建与业务系统的服务 相同的蜜罐系统，根据蜜罐系统中的蜜罐日志，确定蜜罐系统中的攻击行为的 攻击路径时间轴，并建立攻击路径信息库以记录攻击路径时间轴。可见，本具 体实施例利用了与业务系统相同的蜜罐系统，从蜜罐日志中能够获得足够多的 数据来分析更多深入的攻击路径，并建立攻击路径信息库，因此本具体实施例 的方案能够全面准确的感知攻击行为。

[0182] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将 一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些 实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包 含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素 的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的 其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在 没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包 括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0183] 本说明书中的各个实施例均采用相关的方式描述，各个实施例之间相同相 似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置和系统实施例而言，由于其基本相似于方法实施例，所以描述 的比较简单，相关之处参

见方法实施例的部分说明即可。

[0184] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均包含在 本发明的保护范围内。

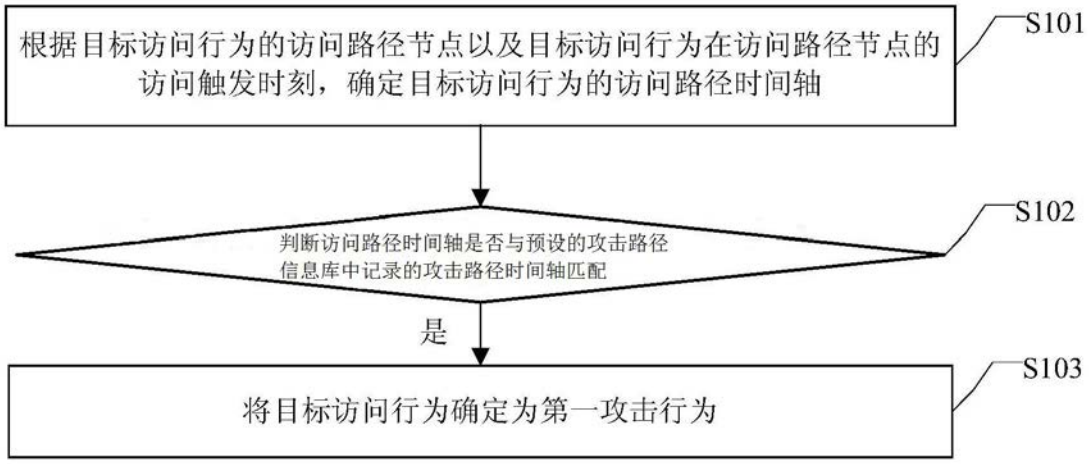

根据目标访问行为的访问路径节点以及目标访问行为在访问路径节点的访问触发时刻，确定目标访问行为的访问路径时间轴
S101
判断访问路径时间轴是否与预设的攻击路径信息库中记录的攻击路径时间轴匹配
S102
是
将目标访问行为确定为第一攻击行为
S103

图1

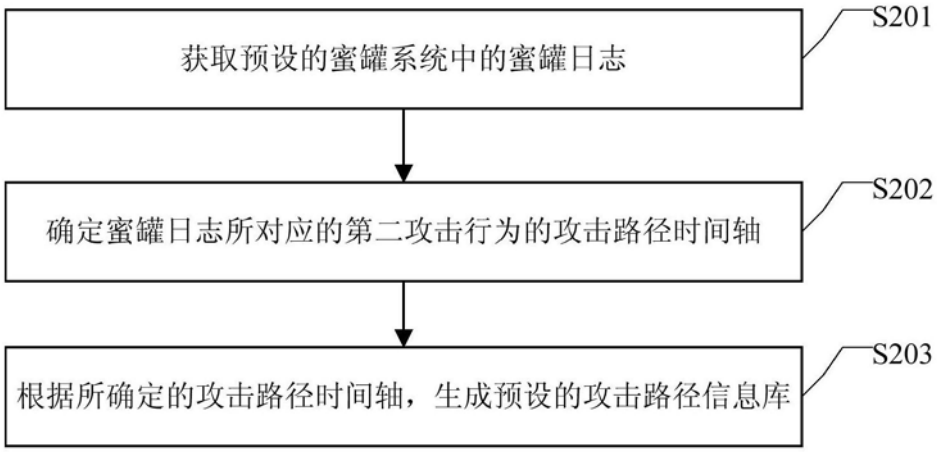

获取预设的蜜罐系统中的蜜罐日志
S201
确定蜜罐日志所对应的第二攻击行为的攻击路径时间轴
S202
根据所确定的攻击路径时间轴，生成预设的攻击路径信息库
S203

图2

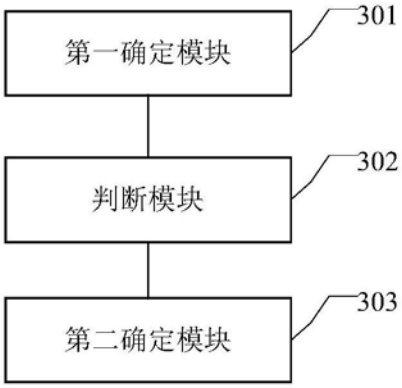

第一确定模块
301
判断模块
302
第二确定模块
303

图3

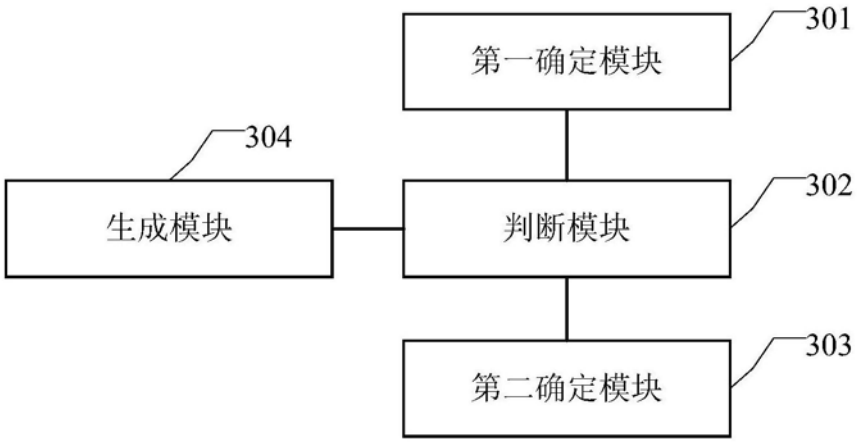

第一确定模块
301
304
生成模块
判断模块
302
第二确定模块
303

图4

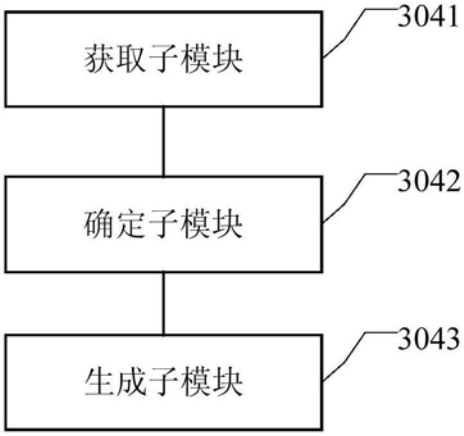

获取子模块
3041
确定子模块
3042
生成子模块
3043

图5

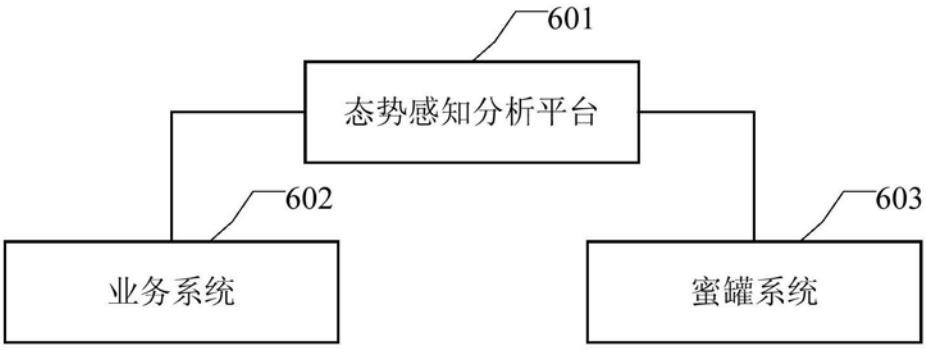

601
态势感知分析平台
602
603
业务系统
蜜罐系统

图6

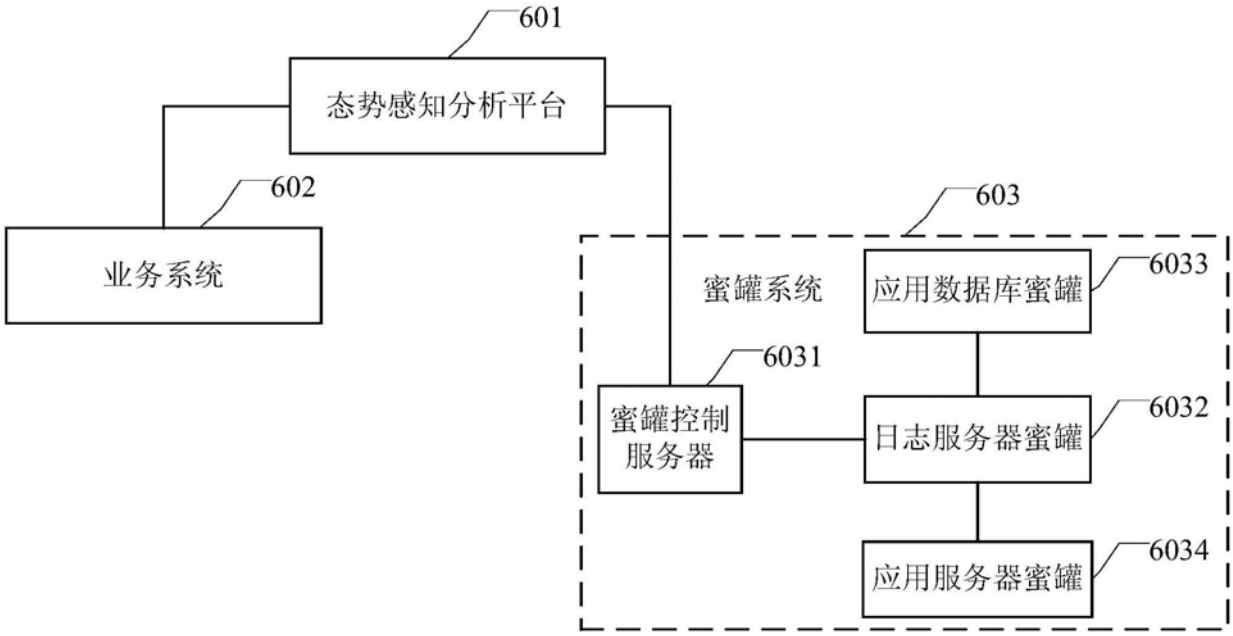

601
态势感知分析平台
602
业务系统
603
蜜罐系统
应用数据库蜜罐
6033
6031
蜜罐控制服务器
日志服务器蜜罐
6032
应用服务器蜜罐
6034

图7

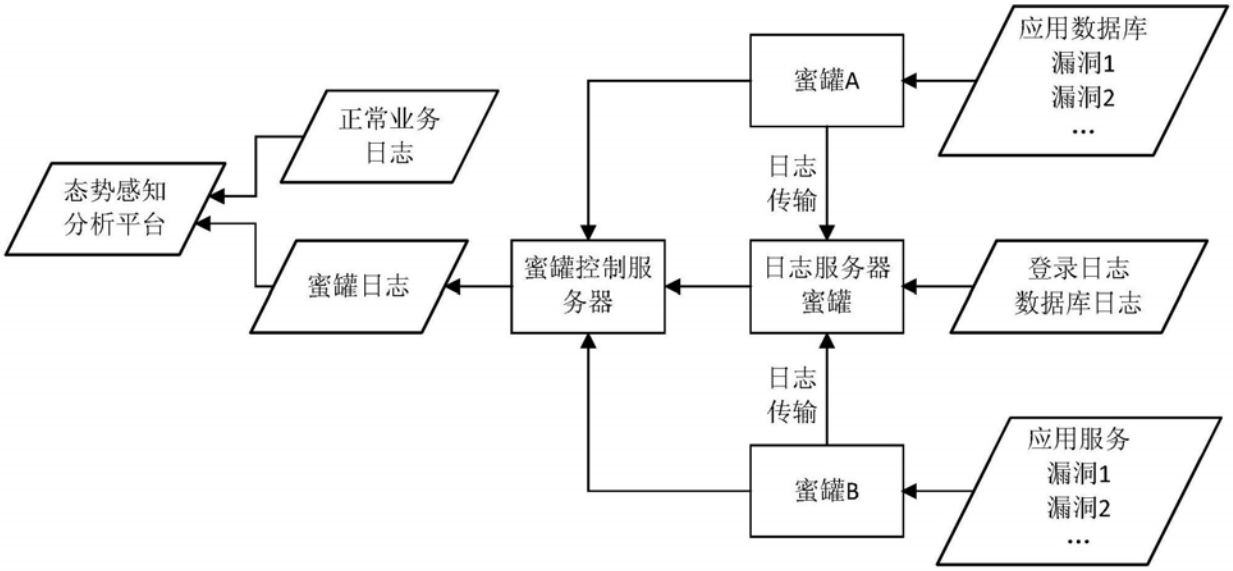

应用数据库
漏洞1
漏洞2
…
蜜罐A
正常业务日志
日志传输
态势感知分析平台
蜜罐日志
蜜罐控制服务器
日志服务器蜜罐
登录日志
数据库日志
日志传输
应用服务
漏洞1
漏洞2
…
蜜罐B

图8