(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111970272 A
(43)申请公布日 2020.11.20

(21)申请号 202010819967.8

(22)申请日 2020.08.14

(71)申请人 上海境领信息科技有限公司
地址 200000 上海市浦东新区中国(上海)自由贸易试验区芳春路400号1幢3层

(72)发明人 施勇 傅烨文 刘宁 何翔

(74)专利代理机构 广州越华专利代理事务所(普通合伙) 44523
代理人 陈岑

(51)Int.Cl.
H04L 29/06(2006.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

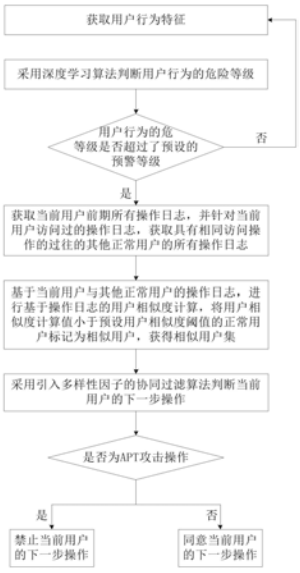
权利要求书3页 说明书9页 附图1页

(54)发明名称

一种APT攻击操作识别方法

(57)摘要

本发明公开了一种APT攻击操作识别方法，包括步骤：一、获取用户行为特征；二、判断用户行为的危险等级；三、判断用户行为的危险等级，当用户行为的危险等级超过了预警等级时，执行四，否则，返回一；四、获取当前用户前期所有操作日志，并获取具有相同访问操作的正常用户的所有操作日志；五、进行基于操作日志的用户相似度计算，获得相似用户集；六、判断当前用户的下一步操作是否为APT攻击操作，当该操作是APT攻击操作时，执行七；否则，执行八；七、禁止下一步操作；八、同意下一步操作。本发明能够快速高效且准确地识别出APT攻击，能够避免将正常用户判断为非正常用户，实用性强。



CN 111970272 A

1.一种APT攻击操作识别方法,其特征在于,该方法包括以下步骤:

步骤一、获取用户行为特征;

步骤二、采用深度学习算法判断用户行为的危险等级;

步骤三、判断用户行为的危险等级是否超过了预设的预警等级,当用户行为的危险等级超过了预警等级时,执行步骤四,否则,返回步骤一;

步骤四、获取当前用户前期所有操作日志,并针对当前用户访问过的操作日志,获取具有相同访问操作的过往的其他正常用户的所有操作日志;

步骤五、基于当前用户与其他正常用户的操作日志,进行基于操作日志的用户相似度计算,将用户相似度计算值小于预设用户相似度阈值的正常用户标记为相似用户,获得相似用户集;

步骤六,采用引入多样性因子的协同过滤算法判断当前用户的下一步操作,并判断该操作是否为APT攻击操作,当该操作是APT攻击操作时,执行步骤七;否则,当该操作不是APT攻击操作时,执行步骤八;

步骤七、禁止当前用户的下一步操作;

步骤八、同意当前用户的下一步操作。

2.按照权利要求1所述的一种APT攻击操作识别方法,其特征在于:步骤一中所述获取用户行为特征是对用户行为进行操作影响文件数、是否系统文件、是否保密文件、是否修改权限进行one-hot词向量的特征提取。

3.按照权利要求1或2所述的一种APT攻击操作识别方法,其特征在于:步骤二中所述采用深度学习算法判断用户行为的危险等级,是将步骤一中的用户行为特征进行归一化处理后,进行数据格式转换,使其适应需要的深度学习网络模型输入格式,再输入到预先训练好的的深度学习网络模型中,获得深度学习网络模型的输出,所述深度学习网络模型的输出为用户行为的危险等级。

4.按照权利要求3所述的一种APT攻击操作识别方法,其特征在于:步骤二中所述将步骤一中的用户行为特征进行归一化处理时,采用feature_normalize函数进行归一化处理;

步骤二中对所述深度学习网络模型进行训练时,采用pytorch框架里面的torch.nn.RNN类,通过调用RNN循环神经网络模型进行训练,训练样本为用户操作的历史数据N条,每条历史数据中均包括操作影响文件数、是否系统文件、是否保密文件、是否修改权限和危险等级。

5.按照权利要求3所述的一种APT攻击操作识别方法,其特征在于:步骤二中对所述深度学习网络模型进行训练时,采用Mask Rcnn神经网络模型,具体训练过程为:

步骤201、构建训练样本:选取用户操作的历史数据N条,每条历史数据中均包括操作影响文件数、是否系统文件、是否保密文件、是否修改权限和危险等级;

步骤202、训练Mask Rcnn神经网络模型,具体过程为:

步骤2021、构建Mask-RCNN网络,所述Mask-RCNN由ResNet网络、FPN网络、RPN卷积神经网络、ROIAlign层、全连接层和输出层构成;输出层对应于危险等级;

步骤2022、将ResNet网络和FPN网络作为主干网络,将训练样本中的危险等级作为Mask-RCNN网络模型的识别目标,将训练样本中的用户行为特征进行归一化处理后,进行数据格式转换,再输入主干网络来训练主干网络,调整ResNet网络和FPN网络的参数,使损失

函数最小,通过主干网络获取到危险等级;

步骤2023、对RPN卷积神经网络进行初始化,用不同的小随机数初始化网络中待训练参数;

步骤2024、使用反向传播BP算法,调整RPN卷积神经网络参数,使损失函数值最小;训练好RPN卷积神经网络模型;

步骤2025、RoIAlign层调整参数,以便后续全连接操作;

步骤2026、对训练样本进行全连接操作,使损失函数最小,得到训练好的Mask-RCNN网络模型。

6.按照权利要求1所述的一种APT攻击操作识别方法,其特征在于:步骤四中所述所有操作日志包括用户系统操作日志,文件访问日志和网络访问日志。

7.按照权利要求6所述的一种APT攻击操作识别方法,其特征在于:所述网络访问日志的获取是采用用于对网络日志进行处理的数据处理模块完成的,所述文件访问日志的获取是将文件的访问路径转化为网络路径后采用与网络访问日志同样的方法完成的;所述数据处理模块包括数据清洗子模块、格式转换子模块、访问用户识别子模块和访问路径树的生成子模块,具体为:

所述数据清洗子模块用于对网络日志中的噪音异常进行处理,以及对链接进行补全、去除爬虫日志和去除空白错误日志;所述噪音异常包括爬虫数据、被动请求链接和异常IP访问数据;

所述格式转换子模块用于对访问来源的referer与当前请求request字段,进行格式转化并进行响应的分类;

所述访问用户识别子模块用于识别真实的用户,以及评判用户是否是同一个用户;

所述访问路径树的生成子模块用于将处理完成的数据转化为访问路径树,存储到数据库中。

8.按照权利要求1所述的一种APT攻击操作识别方法,其特征在于:步骤五中所述进行基于操作日志的用户相似度计算时采用的计算公式为:

$$d(x,y_j)=\sqrt{\sum_{i=1}^{n}(x_i-y_{ji})^2}$$

其中,表示当前用户与第个正常用户的用户相似度,用户相似度的计算值越小,表示两个用于越接近;表示当前用户,表示正常用户中的第个正常用户,的取值为1～J的自然数,J为正常用户的总数量;表示当前用户操作日志中的第个操作日志,表示其他正常用户中的第个用户的操作日志中的第个操作日志,的取值为1～n的自然数,n为选取进行用户相似度计算的当前用户操作日志的数量。

9.按照权利要求8所述的一种APT攻击操作识别方法,其特征在于:步骤六中所述采用引入多样性因子的协同过滤算法判断当前用户的下一步操作,并判断该操作是否为APT攻击操作的具体过程为:

步骤601、找到相似用户集中的用户可能会操作的,而当前用户还没有操作过的操作步骤,推荐给当前用户,当推荐的操作内容,没有包含在当前用户的下一步操作内容时,将当前用户的下一步操作判断为可能是APT攻击操作;

步骤602、根据计算公式 $diversity = 1 - \frac{\sum_{p \in R(u)} \sum_{q \in R(u), q \neq p} S(I[p], I[q])}{\frac{1}{2}|R(u)|(|R(u)|-1)}$ 计算多样性因子的值，并将多样性因子的值与预设的多样性因子阈值进行比较，当多样性因子的值小于预设的多样性因子阈值时，增大预设用户相似度阈值后返回执行步骤五，增大步骤五中确定的相似用户集中用户的数量，并再次执行步骤601和步骤602，直到多样性因子的值等于或大于预设的多样性因子阈值，此时，将步骤601中判断出的可能是APT攻击操作确定为APT攻击操作；其中，表示用户，表示长度为M的推荐列表，表示推荐列表中的第条推荐操作步骤，表示推荐列表中的第条推荐操作步骤，表示推荐列表中的第条推荐操作步骤和第条推荐操作步骤的相似度。

10.按照权利要求9所述的一种APT攻击操作识别方法，其特征在于：步骤602中所述多样性因子阈值为不少于100次的试验得到的多样性因子值的平均值。

一种APT攻击操作识别方法

技术领域

[0001] 本发明属于计算机网络安全技术领域，具体涉及一种APT攻击操作识别方法。

背景技术

[0002] 高级持续性威胁(Advanced Persistent Threat，APT)，是黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为，是一种蓄谋已久的“恶意商业间谍威胁”。这种行为往往经过长期的经营与策划，并具备高度的隐蔽性。APT的攻击手法，在于隐匿自己，针对特定对象，长期、有计划性和组织性地窃取数据，这种发生在数字空间的偷窃资料、搜集情报的行为，就是一种“网络间谍”的行为。

[0003] 基于机器学习的行为分析方法，能够对攻击进行识别。但是很多时候，正常的访问跟攻击之间类似。而有些访问很重要，对其进行拦截的代价很大。但是如果遗漏了APT则也会让计算机系统带来更大的危险。因此为了避开这种误判，需要更加精确的算法来进行判断；为此，申请号为201310533433.9的中国专利公开了一种操作权限验证方法。所述方法包括：第一终端获取第二终端生成的特征码，所述特征码至少携带第二终端标识，所述特征码由所述第二终端接收到指定操作请求时生成，所述指定操作请求用于指示所述第二终端在输入账号信息和待校验信息后由服务器进行操作权限验证，在验证通过时基于所述服务器提供的权限执行指定操作。申请号为201710945921.9的中国专利公开了一种操作权限查询方法，包括：当用户对目标操作的操作权限进行查询时，获取所述用户输入的在各个维度上对于所述目标操作的操作权限的查询条件，所述目标操作的操作权限按照预设的两个以上的维度进行划分，在预设的操作权限表中查找在所述各个维度上均满足所述各个维度对应的查询条件的操作权限条目，所述操作权限表中记录了在所述各个维度上对所述目标操作的操作权限；若在所述操作权限表中查找到在所述各个维度上均满足所述各个维度对应的查询条件的操作权限条目，则将与查找到的所述操作权限条目对应的操作权限确定为查询结果。

[0004] 但是，以上方法，都无法解决权限误判问题。

发明内容

[0005] 本发明所要解决的技术问题在于针对上述现有技术中的不足，提供一种APT攻击操作识别方法，本发明能够快速高效且准确地识别出APT攻击，能够避免将正常用户判断为非正常用户，实用性强。

[0006] 为解决上述技术问题，本发明采用的技术方案是：一种APT攻击操作识别方法，该方法包括以下步骤：

步骤一、获取用户行为特征；

步骤二、采用深度学习算法判断用户行为的危险等级；

步骤三、判断用户行为的危险等级是否超过了预设的预警等级，当用户行为的危险等级超过了预警等级时，执行步骤四，否则，返回步骤一；

步骤四、获取当前用户前期所有操作日志，并针对当前用户访问过的操作日志，获取具有相同访问操作的过往的其他正常用户的所有操作日志；

步骤五、基于当前用户与其他正常用户的操作日志，进行基于操作日志的用户相似度计算，将用户相似度计算值小于预设用户相似度阈值的正常用户标记为相似用户，获得相似用户集；

步骤六，采用引入多样性因子的协同过滤算法判断当前用户的下一步操作，并判断该操作是否为APT攻击操作，当该操作是APT攻击操作时，执行步骤七；否则，当该操作不是APT攻击操作时，执行步骤八；

步骤七、禁止当前用户的下一步操作；

步骤八、同意当前用户的下一步操作。

[0007] 上述的一种APT攻击操作识别方法，步骤一中所述获取用户行为特征是对用户行为进行操作影响文件数、是否系统文件、是否保密文件、是否修改权限进行one-hot词向量的特征提取。

[0008] 上述的一种APT攻击操作识别方法，步骤二中所述采用深度学习算法判断用户行为的危险等级，是将步骤一中的用户行为特征进行归一化处理后，进行数据格式转换，使其适应需要的深度学习网络模型输入格式，再输入到预先训练好的的深度学习网络模型中，获得深度学习网络模型的输出，所述深度学习网络模型的输出为用户行为的危险等级。

[0009] 上述的一种APT攻击操作识别方法，步骤二中所述将步骤一中的用户行为特征进行归一化处理时，采用feature_normalize函数进行归一化处理；

步骤二中对所述深度学习网络模型进行训练时，采用pytorch框架里面的torch.nn.RNN类，通过调用RNN循环神经网络模型进行训练，训练样本为用户操作的历史数据N条，每条历史数据中均包括操作影响文件数、是否系统文件、是否保密文件、是否修改权限和危险等级。

[0010] 上述的一种APT攻击操作识别方法，步骤二中对所述深度学习网络模型进行训练时，采用Mask Rcnn神经网络模型，具体训练过程为：

步骤201、构建训练样本：选取用户操作的历史数据N条，每条历史数据中均包括操作影响文件数、是否系统文件、是否保密文件、是否修改权限和危险等级；

步骤202、训练Mask Rcnn神经网络模型，具体过程为：

步骤2021、构建Mask-RCNN网络，所述Mask-RCNN由ResNet网络、FPN网络、RPN卷积神经网络、ROIAlign层、全连接层和输出层构成；输出层对应于危险等级；

步骤2022、将ResNet网络和FPN网络作为主干网络，将训练样本中的危险等级作为Mask-RCNN网络模型的识别目标，将训练样本中的用户行为特征进行归一化处理后，进行数据格式转换，再输入主干网络来训练主干网络，调整ResNet网络和FPN网络的参数，使损失函数最小，通过主干网络获取到危险等级；

步骤2023、对RPN卷积神经网络进行初始化，用不同的小随机数初始化网络中待训练参数；

步骤2024、使用反向传播BP算法，调整RPN卷积神经网络参数，使损失函数值最小；训练好RPN卷积神经网络模型；

步骤2025、RoIAlign层调整参数，以便后续全连接操作；

步骤2026、对训练样本进行全连接操作，使损失函数最小，得到训练好的Mask-RCNN网络模型。

[0011] 上述的一种APT攻击操作识别方法，步骤四中所述所有操作日志包括用户系统操作日志，文件访问日志和网络访问日志。

[0012] 上述的一种APT攻击操作识别方法，所述网络访问日志的获取是采用用于对网络日志进行处理的数据处理模块完成的，所述文件访问日志的获取是将文件的访问路径转化为网络路径后采用与网络访问日志同样的方法完成的；所述数据处理模块包括数据清洗子模块、格式转换子模块、访问用户识别子模块和访问路径树的生成子模块，具体为：

所述数据清洗子模块用于对网络日志中的噪音异常进行处理，以及对链接进行补全、去除爬虫日志和去除空白错误日志；所述噪音异常包括爬虫数据、被动请求链接和异常IP访问数据；

所述格式转换子模块用于对访问来源的referer与当前请求request字段，进行格式转化并进行响应的分类；

所述访问用户识别子模块用于识别真实的用户，以及评判用户是否是同一个用户；

所述访问路径树的生成子模块用于将处理完成的数据转化为访问路径树，存储到数据库中。

[0013] 上述的一种APT攻击操作识别方法，步骤五中所述进行基于操作日志的用户相似度计算时采用的计算公式为：

$$d(x,y_j)=\sqrt{\sum_{i=1}^{n}(x_i-y_{j,i})^2}$$

其中，表示当前用户与第个正常用户的用户相似度，用户相似度的计算值越小，表示两个用于越接近；表示当前用户，表示正常用户中的第个正常用户，的取值为1～J的自然数，J为正常用户的总数量；表示当前用户操作日志中的第个操作日志，表示其他正常用户中的第个用户的操作日志中的第个操作日志，的取值为1～n的自然数，n为选取进行用户相似度计算的当前用户操作日志的数量。

[0014] 上述的一种APT攻击操作识别方法，步骤六中所述采用引入多样性因子的协同过滤算法判断当前用户的下一步操作，并判断该操作是否为APT攻击操作的具体过程为：

步骤601、找到相似用户集中的用户可能会操作的，而当前用户还没有操作过的操作步骤，推荐给当前用户，当推荐的操作内容，没有包含在当前用户的下一步操作内容时，将当前用户的下一步操作判断为可能是APT攻击操作；

步骤602、根据计算公式 $diversity=1-\frac{\sum_{p\in R(u)}\sum_{q\in R(u),q\neq p}S(T[p],T[q])}{\frac{1}{2}|R(u)|(|R(u)|-1)}$ 计算多样性因子的值，并将多样性因子的值与预设的多样性因子阈值进行比较，当多样性因子的值小于预设的多样性因子阈值时，增大预设用户相似度阈值后返回执行步骤五，增大步骤五中确定的相似用户集中用户的数量，并再次执行步骤601和步骤602，直到多样性因子的值等于或大于预设的多样性因子阈值，此时，将步骤601中判断出的可能是APT攻击操作确定为APT攻击操作；其中，表示用户，表示长度为M的推荐列表，表示推荐列表中的第条推荐操作步骤，表

示推荐列表中的第条推荐操作步骤，表示推荐列表中的第条推荐操作步骤和第条推荐操作步骤的相似度。

[0015] 上述的一种APT攻击操作识别方法，步骤602中所述多样性因子阈值为不少于100次的试验得到的多样性因子值的平均值。

[0016] 本发明与现有技术相比具有以下优点：

1、本发明通过获取用户特征，采用深度学习算法判断用户行为的危险等级；构建好深度学习网络模型后，能够方便地多次使用，方便快捷地识别出用户行为的危险等级。

[0017] 2、本发明加入多样性因子，采用引入多样性因子的协同过滤算法判断当前用户的下一步操作，并判断该操作是否为APT攻击操作，能够避免将正常用户判断为非正常用户。

[0018] 3、本发明基于用户行为进行APT攻击识别，在防止了误判的情况下，能够快速高效且准确地识别出APT攻击，实用性强。

[0019] 综上所述，本发明能够快速高效且准确地识别出APT攻击，能够避免将正常用户判断为非正常用户，实用性强。

[0020] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

[0021] 图1为本发明的方法流程框图。

具体实施方式

[0022] 实施例1

如图1所示，本发明的APT攻击操作识别方法，包括以下步骤：

步骤一、获取用户行为特征；

本实施例中，步骤一中所述获取用户行为特征是对用户行为进行操作影响文件数、是否系统文件、是否保密文件、是否修改权限进行one-hot词向量的特征提取。

[0023] 具体实施时，所述one-hot词向量采用128维度的词向量进行特征提取。用户的行为特征中携带有操作行为安全等级信息，操作行为安全等级信息包括操作影响文件数、是否系统文件、是否保密文件和是否修改权限，根据这些特征进行用户行为的危险等级判断。

[0024] 步骤二、采用深度学习算法判断用户行为的危险等级；

本实施例中，步骤二中所述采用深度学习算法判断用户行为的危险等级，是将步骤一中的用户行为特征进行归一化处理后，进行数据格式转换，使其适应需要的深度学习网络模型输入格式，再输入到预先训练好的的深度学习网络模型中，获得深度学习网络模型的输出，所述深度学习网络模型的输出为用户行为的危险等级。

[0025] 本实施例中，步骤二中所述将步骤一中的用户行为特征进行归一化处理时，采用feature_normalize函数进行归一化处理；

步骤二中对所述深度学习网络模型进行训练时，采用pytorch框架里面的torch.nn.RNN类，通过调用RNN循环神经网络模型进行训练，训练样本为用户操作的历史数据N条，每条历史数据中均包括操作影响文件数、是否系统文件、是否保密文件、是否修改权限和危险等级。

[0026] 具体实施时，所述N的取值为100万，100万条数据来源于用户的操作日志，是系统

自动记录的数据，这些数据只要系统被用户操作过或者网站被用户访问，就会自动记录；从100万条数据中截取的前4条数据如表1所示：

表1 深度学习网络模型训练样本数据表

操作影响文件数	是否系统文件	是否保密文件	是否修改权限	危险等级
634	是	是	否	2
12	否	是	否	4
2334	是	是	是	1
74	否	否	否	4

100万条数据中其余的数据结构都是一样的，在此不一一列出了。

[0027] 另外，具体实施时，也可以将N条历史数据分为训练样本集，和测试样本集，或者，取N条历史数据作为训练样本集，再取另外N’条历史数据作为测试样本集，训练样本集用于构建深度学习网络模型，测试样本集用于检测深度学习网络模型，并评估深度学习网络模型的准确率；通过设置训练样本集和测试样本集，能够防止深度学习网络模型的构建过度拟合，能够保证深度学习网络模型的准确性和可行性。

[0028] 步骤三、判断用户行为的危险等级是否超过了预设的预警等级，当用户行为的危险等级超过了预警等级时，执行步骤四，否则，返回步骤一；

具体实施时，将危险等级分为1～4级，将预警等级设定为3级，当用户行为的危险等级超过3级，即为4级时，执行步骤四；

步骤四、获取当前用户前期所有操作日志，并针对当前用户访问过的操作日志，获取具有相同访问操作的过往的其他正常用户的所有操作日志；

本实施例中，步骤四中所述所有操作日志包括用户系统操作日志，文件访问日志和网络访问日志。

[0029] 本实施例中，所述网络访问日志的获取是采用用于对网络日志进行处理的数据处理模块完成的，所述文件访问日志的获取是将文件的访问路径转化为网络路径后采用与网络访问日志同样的方法完成的；所述数据处理模块包括数据清洗子模块、格式转换子模块、访问用户识别子模块和访问路径树的生成子模块，具体为：

所述数据清洗子模块用于对网络日志中的噪音异常进行处理，以及对链接进行补全、去除爬虫日志和去除空白错误日志；所述噪音异常包括爬虫数据、被动请求链接和异常IP访问数据；

所述格式转换子模块用于对访问来源的referer与当前请求request字段，进行格式转化并进行响应的分类；这有利于路径树的生成并可以支持不同页面的不同粒度分析；

所述访问用户识别子模块用于识别真实的用户，以及评判用户是否是同一个用户；用

户浏览网站时无论登录与否，都能识别出其唯一的身份，通过cookie、ip进行识别；因为要精确的了解每一个用户的特征，还需要对其访问的内容做精确的路径生成；

所述访问路径树的生成子模块用于将处理完成的数据转化为访问路径树，存储到数据库中。

[0030] 具体实施时，当不同的用户通过SSH或者其他远程登录方式访问主机时，记录用户的身份，并对用户的访问生成路径树，最终存放到数据库中；设置访问用户识别子模块，能够实现对用户的监控，有利于即使APT获取了用户名密码，以正常用户登录，进行有权限的操作时，即使他操作违规，也可以被系统分析出来，进行相应的报警。

[0031] 步骤五、基于当前用户与其他正常用户的操作日志，进行基于操作日志的用户相似度计算，将用户相似度计算值小于预设用户相似度阈值的正常用户标记为相似用户，获得相似用户集；

本实施例中，步骤五中所述进行基于操作日志的用户相似度计算时采用的计算公式为：

$$d(x,y_j)=\sqrt{\sum_{i=1}^{n}(x_i-y_{j,i})^2}$$

其中，表示当前用户与第个正常用户的用户相似度，用户相似度的计算值越小，表示两个用于越接近；表示当前用户，表示正常用户中的第个正常用户，的取值为1～J的自然数，J为正常用户的总数量；表示当前用户操作日志中的第个操作日志，表示其他正常用户中的第个用户的操作日志中的第个操作日志，的取值为1～n的自然数，n为选取进行用户相似度计算的当前用户操作日志的数量。

[0032] 具体实施时，选取进行用户相似度计算的其他正常用户操作日志的数量与选取进行用户相似度计算的当前用户操作日志的数量相等，且均为n个。

[0033] 步骤六，采用引入多样性因子的协同过滤算法判断当前用户的下一步操作，并判断该操作是否为APT攻击操作，当该操作是APT攻击操作时，执行步骤七；否则，当该操作不是APT攻击操作时，执行步骤八；

本实施例中，步骤六中所述采用引入多样性因子的协同过滤算法判断当前用户的下一步操作，并判断该操作是否为APT攻击操作的具体过程为：

步骤601、找到相似用户集中的用户可能会操作的，而当前用户还没有操作过的操作步骤，推荐给当前用户，当推荐的操作内容，没有包含在当前用户的下一步操作内容时，将当前用户的下一步操作判断为可能是APT攻击操作；

例如，用户A是一个正常用户，他在两天前操作过：

‘打开过一个需写权限的加密文件’userid.doc’’，

‘以ssh账号登录服务器并将该userid.doc文件上传到IP为192.168.0.3的内部服务器。’

而当前用户B也操作过‘打开过一个需写权限的加密文件’userid.doc’’，

当需要对B进行操作安全性分析时，我们需要判断，他是否上传了userid.doc文件，以及判断上传地址是否就是正常用户A用户的举动，还是它跟相似用户有很大的行为不一样。以此来判断，当前用户的操作是否可能为异常操作。

[0034] 步骤601中采用了依据用户日志的操作协同过滤算法(UserCF),通过这个方法,可以判断,当推荐的操作内容,没有包含在用户的下一步操作内容时,那么该用户的下一步操作是具有不规范性的,有可能是一种攻击行为;但是,步骤601的判断方法,当因为相似用户稀少而导致推荐不出接下去操作的合理性时,就会导致误判。因此引入步骤602中的方法,进行进一步判断。

[0035] 步骤602、根据计算公式 $diversity = 1 - \frac{\sum_{p \in R(u)} \sum_{q \in R(u), q \neq p} S(T[p], T[q])}{\frac{1}{2}|R(u)|(|R(u)|-1)}$ 计算多样性因子的值,并将多样性因子的值与预设的多样性因子阈值进行比较,当多样性因子的值小于预设的多样性因子阈值时,增大预设用户相似度阈值后返回执行步骤五,增大步骤五中确定的相似用户集中用户的数量,并再次执行步骤601和步骤602,直到多样性因子的值等于或大于预设的多样性因子阈值,此时,将步骤601中判断出的可能是APT攻击操作确定为APT攻击操作(即将多样性满足条件时推荐的步骤还没有包含在当前用户的操作步骤中的操作确定为APT攻击操作);其中,表示用户,表示长度为M的推荐列表,表示推荐列表中的第条推荐操作步骤,表示推荐列表中的第条推荐操作步骤,表示推荐列表中的第条推荐操作步骤和第条推荐操作步骤的相似度。

[0036] 具体实施时,相似度的取值为百分数。

[0037] 例如,每个用户在服务器上或者在电脑上的操作都有很多种,系统日志上记录了所有用户的操作,例如打开一个文件、复制一个文件都就会产生一条操作记录,这些日志是以每天几万条甚至百万条的规模产生的。去到针对每一个用户,都会有很多记录。当多样性因子的值为10,即总共可以推荐给用户的操作只有10种时,那么说明,找到很少的跟当前用户相似的日志(即相似用户集中的用户可能会操作的,而当前用户还没有操作过的操作步骤很少),那么,原因可能是因为当前用户的操作太特殊,是APT攻击操作;也可能是步骤五中确定的相似用户集中用户的数量过少,推荐的操作步骤数量是不足的,需要增加相似用户集中用户的数量,而要增加相似用户集中用户的数量,就要增大预设用户相似度阈值,将更多的正常用户标记为相似用户。

[0038] 加入多样性因子,采用步骤602中的方法进行进一步判断,能够避免将正常用户判断为非正常用户。

[0039] 本实施例中,步骤602中所述多样性因子阈值为不少于100次的试验得到的多样性因子值的平均值。

[0040] 例如,当一次推荐时,推荐系统在大多数情况下,能找到10000条左右的相似操作,多样性因子值的平均值为10000,就将步骤602中所述多样性因子阈值设置为10000。当多样性因子值达到10000时,无需增加相似用户集中用户的数量;而当10000条操作数据里面都没有跟当前用户相同的操作时,说明这个操作有危险性,是APT攻击操作,应该被禁止。否则,当多样性因子值达不到10000时,需要增加相似用户集中用户的数量,来继续进行操作步骤的推荐,直到多样性因子值达到10000时,最终推荐的内容还没有包含在用户的操作命令之类,说明这个操作有危险性,是APT攻击操作,应该被禁止。

[0041] 具体实施时,为了方便步骤六的判断,步骤五之后还可以根据不同的用户操作的

日志特征建立相应的分类标签，将相似用户分为一个类别的用户。例如，采用公式 $d(y_{j'},y_j)=\sqrt{\sum_{i=1}^{n}(y_{j'i}-y_{ji})^2}$ 计算第个正常用户与第个正常用户的用户相似度，将用户相似度的计算值小于设定阈值的用户分为一个类别的用户。其中，表示正常用户中的第个正常用户，表示正常用户中的第个用户的操作日志中的第个操作日志。步骤五中将用户相似度计算值小于预设用户相似度阈值的正常用户标记为相似用户，获得相似用户集后，再将相似用户集分成多个类别的用户；进而在步骤601中，找到相似用户集中的用户可能会操作的，而当前用户还没有操作过的操作步骤，推荐给当前用户时，一个类别一个类别去找，能够加快找的速度，提高APT攻击识别效率。

[0042] 步骤七、禁止当前用户的下一步操作；

步骤八、同意当前用户的下一步操作。

[0043] 实施例2

本实施例与实施例1不同的是：步骤二中对所述深度学习网络模型进行训练时，采用Mask Rcnn神经网络模型，具体训练过程为：

步骤201、构建训练样本：选取用户操作的历史数据N条，每条历史数据中均包括操作影响文件数、是否系统文件、是否保密文件、是否修改权限和危险等级；

步骤202、训练Mask Rcnn神经网络模型，具体过程为：

步骤2021、构建Mask-RCNN网络，所述Mask-RCNN由ResNet网络(深度残差网络)、FPN网络(Feature Pyramid Networks)、RPN卷积神经网络(Region Proposal Networks)、ROIAlign层、全连接层和输出层构成；输出层对应于危险等级；

步骤2022、将ResNet网络和FPN网络作为主干网络，将训练样本中的危险等级作为Mask-RCNN网络模型的识别目标，将训练样本中的用户行为特征进行归一化处理后，进行数据格式转换，再输入主干网络来训练主干网络，调整ResNet网络和FPN网络的参数，使损失函数最小，通过主干网络获取到危险等级；

步骤2023、对RPN卷积神经网络进行初始化，用不同的小随机数初始化网络中待训练参数；

步骤2024、使用反向传播BP算法，调整RPN卷积神经网络参数，使损失函数值最小；训练好RPN卷积神经网络模型；

步骤2025、RoIAlign层调整参数，以便后续全连接操作；

步骤2026、对训练样本进行全连接操作，使损失函数最小，得到训练好的Mask-RCNN网络模型。

[0044] 其余方法均与实施例1相同。

[0045] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0046] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程

图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0047] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0048] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0049] 前述对本发明的具体示例性实施方案的描述是为了说明和例证的目的。这些描述并非想将本发明限定为所公开的精确形式，并且很显然，根据上述教导，可以进行很多改变和变化。对示例性实施例进行选择和描述的目的在于解释本发明的特定原理及其实际应用，从而使得本领域的技术人员能够实现并利用本发明的各种不同的示例性实施方案以及各种不同的选择和改变。本发明的范围意在由权利要求书及其等同形式所限定。

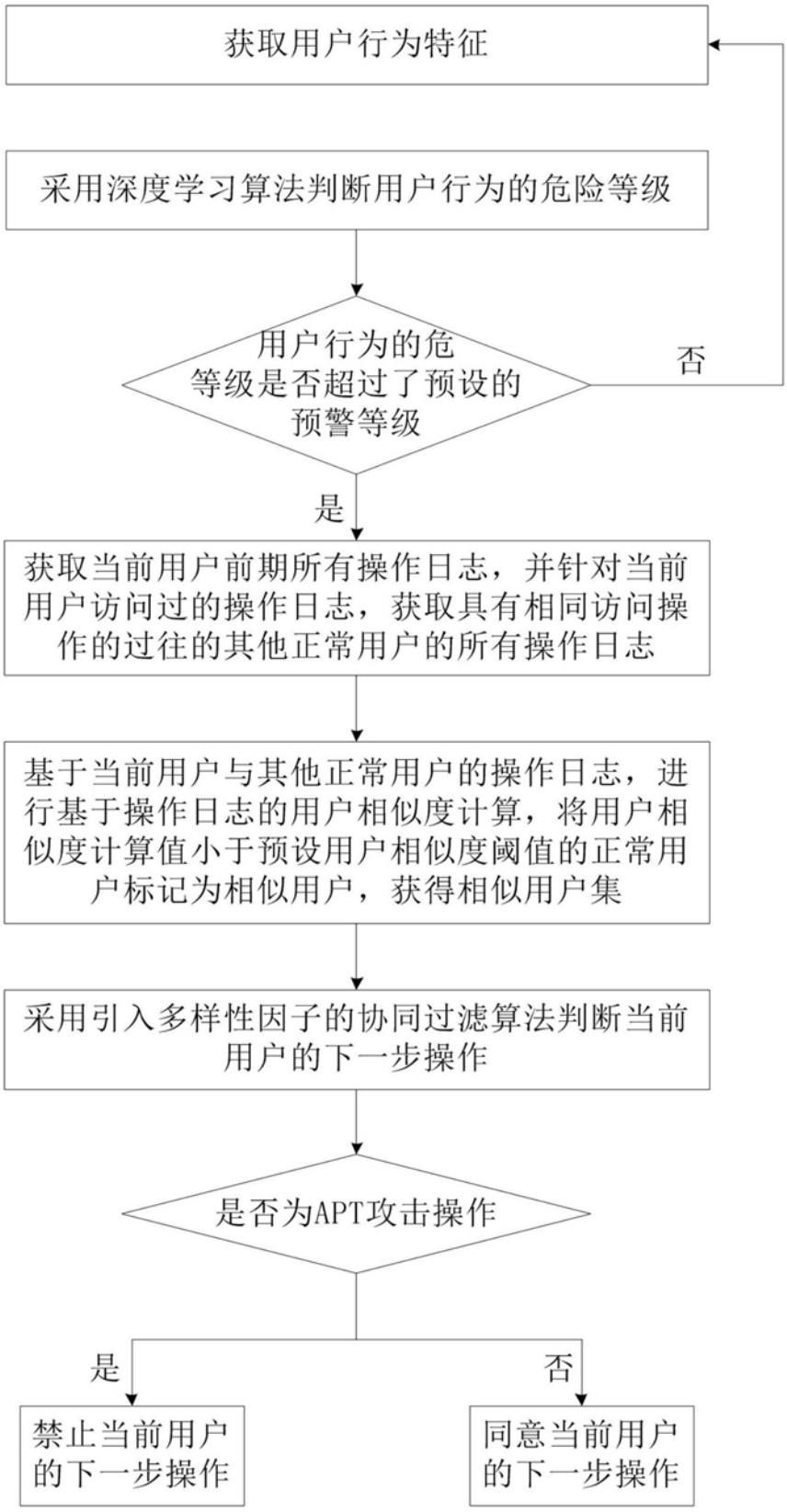

获取用户行为特征
采用深度学习算法判断用户行为的危险等级
用户行为的危等级是否超过了预设的预警等级
否
是
获取当前用户前期所有操作日志，并针对当前用户访问过的操作日志，获取具有相同访问操作的过往的其他正常用户的所有操作日志
基于当前用户与其他正常用户的操作日志，进行基于操作日志的用户相似度计算，将用户相似度计算值小于预设用户相似度阈值的正常用户标记为相似用户，获得相似用户集
采用引入多样性因子的协同过滤算法判断当前用户的下一步操作
是否为APT攻击操作
是
否
禁止当前用户的下一步操作
同意当前用户的下一步操作

图1