Journal of System Simulation

Volume 30 | Issue 10 Article 25

1-4-2019

APT-oriented Dynamic Assessment of Attack Behaviors

Jindong Wang
Information Engineering University, Zhengzhou 450001, China;

Haopu Yang
Information Engineering University, Zhengzhou 450001, China;

Hengwei Zhang
Information Engineering University, Zhengzhou 450001, China;

Li Tao
Information Engineering University, Zhengzhou 450001, China;

APT-oriented Dynamic Assessment of Attack Behaviors

Abstract

Abstract: The existing attack assessment methods cannot effectively deal with the long-term concealment in APT attack. Aiming at the accurate assessment of attack behaviors in APT attack, the APT-oriented dynamic assessment of attack behaviors which focuses on both the space dimension and the time dimension is proposed. *The attack behaviors are correlated in the causality-diversion among the whole network system to discover the attack paths. The attack paths are modified in the time-diversion to get the dynamic causal attack traces. The attack traces are quantified based on CVSS standard.* The experimental result shows that the proposed method can correctly reflect the attack status and effectively assess the attack behavior.

Keywords

APT attack, attack quantification, dynamic assessment, causal correlation

Recommended Citation

Wang Jindong, Yang Haopu, Zhang Hengwei, Li Tao. APT-oriented Dynamic Assessment of Attack Behaviors[J]. Journal of System Simulation, 2018, 30(10): 3796-3806.

第 30 卷第 10 期 系统仿真学报© Vol. 30 No. 10
2018 年 10 月 Journal of System Simulation Oct., 2018

面向 APT 攻击的攻击行为动态评估方法

王晋东，杨豪璞，张恒巍，李涛
(信息工程大学，河南 郑州 450001)

摘要：针对现有攻击评估方法大多属于静态评估、无法有效应用于 APT 攻击长期潜伏、持续渗透的特点，分别从空间、时间两个维度入手，提出了一种面向 APT 攻击的攻击行为动态评估方法。*通过对攻击行为在整个网络系统中进行因果关联，初步发现攻击痕迹；基于 APT 攻击的持续性特征，再对因果关联结果在时间层面上进行调整与修正，得到含有真实攻击信息的攻击动态因果行为链；结合 CVSS 标准对攻击行为链进行动态量化评估。*设计实验对所提方法的有效性进行证明，实验结果显示该评估方法能够较为真实的反映 APT 攻击情况，能够对攻击收益进行合理有效的评估。

关键词：APT 攻击；攻击量化；动态评估；因果关联
中图分类号：TP393.08 文献标识码：A 文章编号：1004-731X (2018) 10-3796-11
DOI: 10.16182/j.issn1004731x.joss.201810025

APT-oriented Dynamic Assessment of Attack Behaviors

Wang Jindong, Yang Haopu, Zhang Hengwei, Li Tao
(Information Engineering University, Zhengzhou 450001, China)

Abstract: The existing attack assessment methods cannot effectively deal with the long-term concealment in APT attack. Aiming at the accurate assessment of attack behaviors in APT attack, the APT-oriented dynamic assessment of attack behaviors which focuses on both the space dimension and the time dimension is proposed. *The attack behaviors are correlated in the causality-diversion among the whole network system to discover the attack paths. The attack paths are modified in the time-diversion to get the dynamic causal attack traces. The attack traces are quantified based on CVSS standard.* The experimental result shows that the proposed method can correctly reflect the attack status and effectively assess the attack behavior.

Keywords: APT attack; attack quantification; dynamic assessment; causal correlation

引言

高级可持续性威胁(Advanced Persistent Threat, APT)是近年来备受关注的网络攻击类型，不同于常规网络攻击的迅速、目标单一、特征明显等性质，APT 攻击通常是隐蔽且持久的，所造成的危害和损失也是不可估量的。因此在复杂的系统环境和多变的网络环境中及时对收集到的攻击行为进行有效的分析与评估，有利于管理者对网络系统的受威胁程度有直观的了解，调整防御的重点，并对攻击的进一步行为及时做出防护，可最大程度减小攻击所带来的损失。

现有的网络攻击评估研究已比较成熟。国内外制定了一系列与网络安全评估相关的标准，如美国国防部制定的《可信计算机系统评估准则》[1]，对

收稿日期：2016-09-08 修回日期：2016-12-19;
基金项目：国家自然科学基金(61303074, 61309013), 国家重点基础研究发展计划(2012CB315900);
作者简介：王晋东(1966-)，男，山西，教授，博导，研究方向为信息安全、云计算；杨豪璞(1993-)，女，河南，硕士，助工，研究方向为 APT 攻防、博弈论。

网络系统的安全等级进行了划分，这一标准提出得较早，为后期其他标准的制定提供很大的依据;《信息技术安全性评估通用准则》[2]是北美与欧盟联合制定的信息安全评估标准，是目前获得最广泛认可的准则之一；CVSS(Common Vulnerability Scoring System)[3-4]体系为 IT 漏洞的特征提取及风险量化提供了一个开放的计算框架，在风险评估、收益量化、脆弱性提取等多个研究方向得到广泛应用。国内的评估标准大多在国际上所认可的标准的基础之上进行修改与借鉴得到的，如《计算机信息系统安全保护等级划分准则》[5]、《信息技术、安全技术、信息技术信息安全评估准则》[6]、《信息安全技术、信息系统的风险评估规范》[7]等。网络攻击评估的方法也有大量研究成果，如基于攻击图模型的方法[8-9]、基于 Petri 网的方法[10]、基于博弈理论的方法[11-12]、基于知识推理的方法[13]等，这些方法大多基于网络系统中已知漏洞之间的关联性进行评估，通常仅对攻击事件进行独立分析，缺少对攻击事件之间的关联性研究。此外，现有的评估方法大多依赖于已知漏洞和专家经验，且大部分是对网络系统安全性的静态评估，难以对复杂多变的网络系统及攻击过程给出准确的评估。

根据美国国家标准与技术研究所 NIST 对 APT 攻击所作的定义[14]，APT 攻击是攻击策略上的先进而非攻击技术上的创新，其核心在于其攻击的“持续性”特征，攻击者在较长的周期内潜伏在目标网络系统中，不断地收集有效信息，调整攻击手段，并进一步地隐蔽自己的攻击痕迹。因此，攻击者需要躲避常规的系统安全防护设备的检测，这也就要求攻击者所采取的攻击行为在单系统节点、单时间节点上不体现攻击性，从而可以实现更加隐蔽持久的攻击。

通过上述分析可知，目前的评估方法可在一定程度上对网络攻击有所掌握，但在面对 APT 攻击时却存在很大的局限性。主要体现在以下两点：1、现有的攻击评估方法主要对攻击进行独立的分析，而 APT 攻击中的攻击行为在单系统节点、单时间节点上通常不体现攻击性；2、现有评估方法通常对攻击收益进行静态量化，而 APT 攻击的收益蕴含在动态的攻击过程之中。因此，对 APT 攻击的攻击行为进行分析与量化，需要从以下两个角度进行：首先需要对攻击数据在空间上的因果关系和时间上的动态关系两个层面进行关联分析，更加准确地发现数据中隐含的攻击信息；其次需要对关联得到的攻击信息进行动态的综合量化，对攻击的收益进行更加精准地评估。本文作为抗 APT 攻击的初步研究，可用于指导以下工作：(1)APT 攻击痕迹检测与发现。(2)APT 攻击行为预测。(3)面向 APT 攻击的主动防御策略选取。

据此，本文在现有研究基础上提出面向 APT 攻击的攻击行为动态评估方法。首先将攻击行为在整个网络系统内进行因果关联，初步识别攻击因果行为链，再对其进行时间层面的动态关联，调整并修正因果关联结果，得到攻击动态因果行为链；最后结合 CVSS 量化标准，对关联后的攻击动态因果行为链进行动态量化评估，得到攻击行为的收益。

1 APT 攻击行为动态评估基础

网络攻击评估是基于已知的攻击状态以及系统状态对网络系统所造成的影响进行衡量。APT 攻击周期长、方法多样、目标明确、范围广泛，对 APT 攻击行为进行评估，需要对 APT 攻击条件下的攻击状态、系统状态及环境信息进行描述。本节将对描述上述信息时所涉及的相关概念进行定义，并以一简单例子进行具体解释说明。

首先对描述系统状态及环境信息的要素进行定义。

定义 1 系统节点 SNode，指网络系统中可独立运行、可进行数据交互的设备，如主机、防火墙等。APT 攻击者将这些设备作为攻击的对象或者跳板来实施攻击或者渗透，因此需要对系统节点进行抽象，这也是描述系统状态的基础。本文用 3 元组(IP, Priority, Services)来表示系统节点。其中，IP 指节点的 IP 地址，在同一个网络系统中，每个 IP 地址唯一对应到一个系统节点，可作为系统节点的标识

DOI: 10.16182/j.issn1004731x.joss.201810025

第 30 卷第 10 期 系统仿真学报 Vol. 30 No. 10
2018 年 10 月 Journal of System Simulation Oct., 2018

符；Priority 指节点的权限，如管理员 admin、组 group、用户 user 等，节点权限可反映出该节点在网络系统中的重要程度，权限越大的节点越重要；Services 指节点上运行的服务集合，如 Http, SQL, POP3 等。

定义 2 系统拓扑，用于描述网络系统中各节点之间的物理连接，本文用无向图 SysTP=(SN, SE)来描述。其中，SN 是无向图中的点集合，代表网络系统中独立的系统节点；SE 是无向图中的边集合，代表系统节点之间的物理连接。

定义 3 通信拓扑，用于描述网络系统中各节点之间的通信结构，本文用有向图 CommunTP=(CN,CE)来描述。其中，CN 是有向图中的点集合，代表网络系统中独立的系统节点；CE 是有向图中的边集合，代表系统节点之间的通信关系。通常，系统管理员通过设置请问控制规则、设置节点权限等方法，控制系统内部节点与外部节点、系统内部节点与内部节点之间的通信规则。

接下来对描述攻击状态的要素进行定义。

定义 4 APT 元攻击 MetaAtk，指 APT 攻击实施过程中的单个攻击行为，该行为可能是利用节点中存在的漏洞，可能是直接对节点进行的物理操作，也可能是一些不会被安全防护设备检测、却隐含攻击痕迹的正常操作。本文根据 APT 攻击的阶段性特征，用八元组(name, phase, SrcIP, DstIP, SrcPort, DstPort, prior, p)来表示 APT 元攻击。其中，name 指名称，每个元攻击都有其固定的命名，可作为该攻击行为的标识符；phase 是指该攻击所属的攻击阶段，这是根据 APT 的阶段性特征所决定的，同一种元攻击行为在不同攻击阶段中所具有的危害性不同；SrcIP 指该攻击行为的源节点地址；DstIP 指该攻击行为的目标节点地址；SrcPort 指该攻击行为的源端口；DstPort 指该攻击行为的目标端口；prior 指实施该攻击行为所需要的最低权限；p 指攻击者采取该攻击行为的概率。通过 name, phase, p 三个参数可以对该攻击行为进行评估，其余五个参数则可以对该攻击行为进行描述。

定义 5 APT 攻击评估图，本文用一个四元组(S, T, A, R)来描述。对其中的参数解释如下：

(1) S 表示评估状态节点集合，各评估状态节点用 4 元组(N, Actions, status, ttl)来表示。其中 N 指系统节点；Actions 指该节点上可能出现的元攻击行为集合；status 有｛True, False｝2 种取值，当 status=True 时，表示该节点上出现某种攻击行为，当 status=False 时，表示该节点上未出现某种攻击行为；ttl 指某种攻击行为出现的生存时间，其初始值 T 与具体的攻击行为相关，当检测到系统节点上该攻击行为的 status=True 后，ttl 置为其初始值 T，并逐渐递减，直到 ttl 值为 0 后，丢弃该评估状态节点。

(2) T 表示评估状态转移空间，$T \subseteq (S_i, S_j)$，$S_i, S_j \in S$。其中 S_i 是 S_j 的前置节点，也可称为 S_j 的父节点，用 Pre(S_j)；S_j 是 S_i 的后续节点，也可称为 S_i 的子节点，用 Post(S_i)。对任一状态节点而言，其前置节点可有零个、一个或多个，若前置节点数为 0，则表示该状态节点为状态转移过程的起点；其后续节点也可有零个、一个或多个，若后续节点数为 0，则表示该状态节点为状态转移过程的终点。

(3) A 表示触发行为，用于描述触发评估状态进行转移时所需要的 APT 元攻击事件，可用二元组(T_i, A_i)表示，其中 $T_i \in T$，A_i 指元攻击行为。

(4) R 用于表示状态转移依赖关系，指各评估状态节点对其直接前置节点的依赖关系，用(S_i, r_i)表示。这种依赖关系可分为两种情况：若当且仅当状态节点 S_i 的全部前置节点都发生，S_i 才可能发生，此时 r_i=1，即 $r_i = 1 \Leftrightarrow \forall S_j \in Pre(S_i), S_j.status =$ True；若当状态节点 S_i 的任意前置节点发生，S_i 即可发生，此时 r_i=0，即 $r_i = 0 \Leftrightarrow \exists S_j \in Pre(S_i), S_j.status = True$。此外，若 S_i 为状态转移过程的起点，则 r_i=0。

依据上述概念的定义，即可对网络系统建立 APT 攻击评估图模型。以图 1 为例对该模型进行简单说明。节点 1、2、4 发生在主机 A，节点 3、5

出现在主机 B。节点 4 的前置节点有节点 2 和节点 3，且 $r_4=1$，则说明只有当主机 A 上的状态 2 与主机 B 上的状态 3 均已发生，主机 A 才有可能向状态 4 发生转移；节点 3 的前置节点也有 2 个，分别是节点 1 和节点 2，且 $r_3=0$，则说明只要主机 A 上出现状态 1 或者状态 2，主机 B 便有可能转移到状态 3。不同状态之间进行转移需要触发点，即某种行为或操作，如 ping, Address probe, login 等。

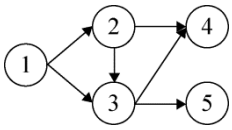

图 1 APT 攻击评估图
Fig. 1 APT Attack Assessment Graph

2 APT 攻击行为动态评估

通过在上一节对 APT 攻击行为评估过程中所必需的相关信息的描述，可将实际中复杂的网络系统及攻击过程抽象作一系列参数进行表示。本节在此基础上，对具体的评估流程与方法进行说明。

2.1 APT 攻击行为动态评估流程

APT 攻击行为动态评估的整体流程大致分为数据处理、关联发现、动态评估 3 个阶段，具体流程如下：

第一，攻击行为的数据采集与预处理。APT 攻击的数据难以获得，这是由于攻击者采取持续性攻击与隐蔽性攻击的方案，其行为通常难以被常规的安全防护设备所发现，攻击者的真实攻击意图往往隐含在较长一段时间内一系列“正常”的系统行为中。因此，APT 攻击行为数据的采集范围应在时间、空间上均进行扩展，时间上的收集范围包括实时运行数据与历史日志数据，空间上的收集范围包括防火墙数据、IDS 数据、主机数据、系统内部传递的数据甚至包括与外部网络传递的数据信息等。具体的采集方法不是本文研究的重点，在此不再赘述。将收集到的攻击行为数据进行预处理，依据本文第 2 节中所给概念，提取其中的关键要素，并整理为统一格式，便于后续分析。

第二，攻击行为的动态因果关联。APT 攻击行为通常在单系统节点、单时间节点上不会展现其攻击性，因此为发现大量数据中的攻击痕迹，需要对其进行全系统的、动态的关联。首先对攻击数据进行因果关联，依据系统节点、系统通信拓扑等信息在整个网络系统中进行攻击因果行为链的识别；其次，依据 APT 攻击阶段信息、图模型等信息，对已识别出的攻击因果行为链进行时间关系上的修正与补充，挖掘系统中的攻击痕迹。具体算法在第 3.2 小节中进行介绍。

第三，攻击行为动态评估。由于 APT 攻击存在持续性特征，基于单时间点对攻击数据进行量化无法反映攻击的整体收益，因此需要扩大分析的时间范围。攻击在一段时间内的整体收益，为该时间段内出现的所有攻击行为收益总和的叠加，借鉴数学中卷积的概念，并依据已识别出的攻击因果行为链，首先对行为链中单个攻击行为的收益进行量化，再对其进行卷积计算，从而得到行为链的整体收益。具体计算方法在 3.3 小节中进行介绍。

2.2 APT 攻击行为动态因果关联

2.2.1 攻击行为因果关联

通常攻击者需要采取一系列行为来实现某一攻击目标，且这些行为之间必然存在一定的因果关系。尤其是对 APT 攻击而言，为保证攻击隐蔽性从而达到持续攻击的目的，攻击者所采取的每一步行为都需要十分谨慎，且保证能够为后续攻击提供支持。本文参考文献[15], 选用(SrcIP, DstIP, SrcPort，DstPort, Service, priori) 6 个要素作为判断两个攻击行为是否存在因果关系的依据，其中前四个要素唯一标识了该攻击行为的前导系统节点与后续系统节点，*Service* 表示出现该攻击行为所需要的服务类型，priori 表示该攻击行为的最低权限要求。

首先对攻击过程做出相关假设。

假设一：在一次攻击中，同一系统节点上的攻

击阶段不循环且不可逆。依据文献[16-18]可知，APT 攻击周期可以按阶段进行划分的，在不同攻击阶段的主要目标不同，对攻击者的能力与掌握的信息也有不同的要求。通常在一个完整的攻击周期内，从信息收集阶段开始，直到达成攻击目的清理攻击痕迹阶段为止，攻击阶段是按顺序发生，因此本文设定在同一个系统节点上的攻击阶段是不可循环且不可逆。

假设二：在一次攻击中，攻击者在网络系统中拥有的权限水平逐渐增加且不可逆。在 APT 攻击过程中，随着攻击者在目标网络系统中潜伏的时间越长，窃取到的数据越多，攻防双方的信息不对称性越明显。由于攻击者掌握更多的信息与主动权，因此其在网络系统中能够拥有的权限越来越高，只要攻击者不被发现，这个权限增加的过程是不可逆的。

其次对攻击行为之间的因果相关性进行说明，并引入相关程度的概念，相关定义如下。

定义 6 直接因果相关，指 2 个攻击行为之间具有绝对的因果关系，其中一个行为直接导致了另一个行为的出现。

定义 7 间接因果相关，指两个攻击行为之间不具有绝对的因果关系，其中做任意一个行为无法直接导致另一行为的出现，但是可在一定程度上对其出现产生影响。

定义 8 相关程度，指间接因果相关的两个行为之间的影响程度，用符号 $Rel(e_1, e_2)$表示，且 $0<Rel(e_1, e_2)<1$。计算方法见公式(1)。

$$Rel(e_1,e_2)=\sum_{i=1}^{6}\omega_i \times F_i(e_1,e_2) / \sum_{i=1}^{6}\omega_i \qquad (1)$$

其中，本文仅选取 6 个要素作为判断 2 个行为之间是否存在因果相关性的依据，因此 $1\leqslant i\leqslant 6$，ω_i 指第 i 个要素的权重，$F_i(e_1, e_2)$指第两个攻击行为在第 i 个要素上的相关程度，权重与相关程度的取值参考文献[15]。

定义 9 因果独立行为，指与任意攻击行为之间均不存在因果相关性的攻击行为。

基于上述分析，可对任意 2 个攻击行为进行因果相关性的计算，具体过程如图 2 所示。

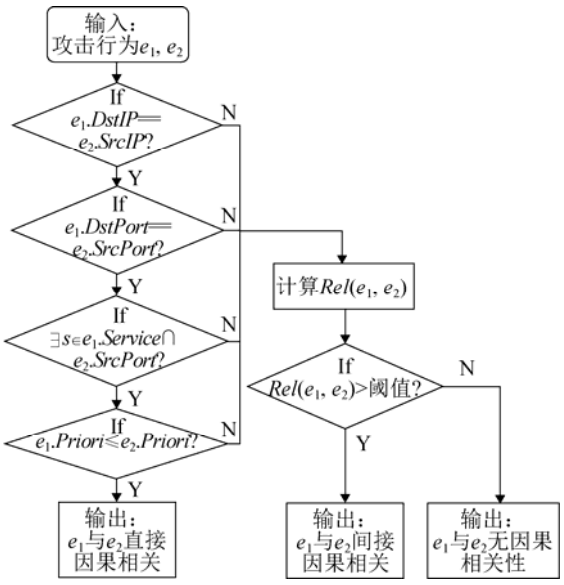

图 2 攻击行为因果关联流程

Fig. 2 Causal Correlation Process Graph of Attack Behaviors

经过对攻击数据进行因果关联，相互之间存在因果相关性的攻击行为可关联成攻击因果行为链，所有的攻击因果行为链构成因果关系库 RR，与所有因果独立行为组成的集合 RI 一起，作为下一阶段动态关联的输入。

2.2.2 攻击行为动态因果关联算法

APT 攻击的持续性特征可以理解为运用了“以时间换空间”的策略，即用更长的攻击时间为代价，减少其攻击行为的异常性，从而实现隐蔽的在更大范围内进行渗透、窃取、破坏等攻击目的。因此，为更加准确地理解攻击行为之间的相关性，需要在时间轴上对其进行动态关联。

参考 APT 攻击的阶段特征，本文选取(IP, name, phase, ttl,) 4 个要素作为动态关联的依据，其中 IP 指产生该攻击行为的系统节点；name 表示该攻击行为的名称，可用于标识攻击行为所属的类型；phase 表示该攻击行为所处的攻击阶段；ttl 表示该攻击行为的生存时间，每种攻击行为都有设定的初始生存时间 T，代表其在网络系统中能够发挥作用的有效期，一旦该行为确认发生，则生存时间被设置为其初始值 T，并随时间递减，直至 ttl=*0*，表示

该行为已失效。由于动态关联是在因果关联的基础上进行的，而因果关联的结果可能不符合时间上的合理性，因此需要首先对因果关联的结果进行修正。在此基础上，再将因果独立行为与之进行匹配，判断是否存在时间关联关系，若存在，则将该行为加入到因果关系链中；若不存在，则认为该行为是孤立节点，不含攻击信息。具体关联过程如图 3 所示。

在上述关联过程中，左侧流程是对因果行为链的修正过程，判断符合因果关系的行为判断之间是否符合时间上的相关性，前三步表示攻击行为的复制，第四步表示攻击行为的更新。右侧流程将因果无关的行为在时间轴上判断其相关性，若满足其时间上的攻击阶段递进规律，则认为其是时间上相关的，否则表示该攻击行为未含有攻击信息。需要注意的是，上述关联判断的前提条件是，所有攻击行为的是生存时间 *ttl* 均大于 0，若某攻击行为的生存时间为 0，则直接删除。

2.3 APT 攻击行为动态量化评估

由于 APT 攻击的持续性与潜伏性特征，攻击者采取的攻击行为通常会在一定时间范围内产生影响，即攻击行为的“持续有效”特征。根据上文的定义，这个范围即为攻击行为的生存时间。常规的评估方法在单个时间点对攻击行为进行静态评估，无法合理分析 APT 攻击中攻击行为的持续有效性，基于该问题，提出 APT 攻击行为动态评估方法。

经过对攻击数据进行动态因果关联，可将杂乱无章的攻击行为依据空间和时间上的相关性进行整理，形成一系列攻击动态因果行为链(简称为“动态因果链”)，将所有动态因果链组成的集合称为关联库 *R*，该关联库可在一定程度体现攻击信息，包括攻击过程、攻击路径、攻击方法、关键节点等。对攻击动态因果行为链的收益进行量化评估，可以更加直观地了解网络系统的安全性和攻击行为的有效性，从而为进一步的攻击行为预测提供指导。

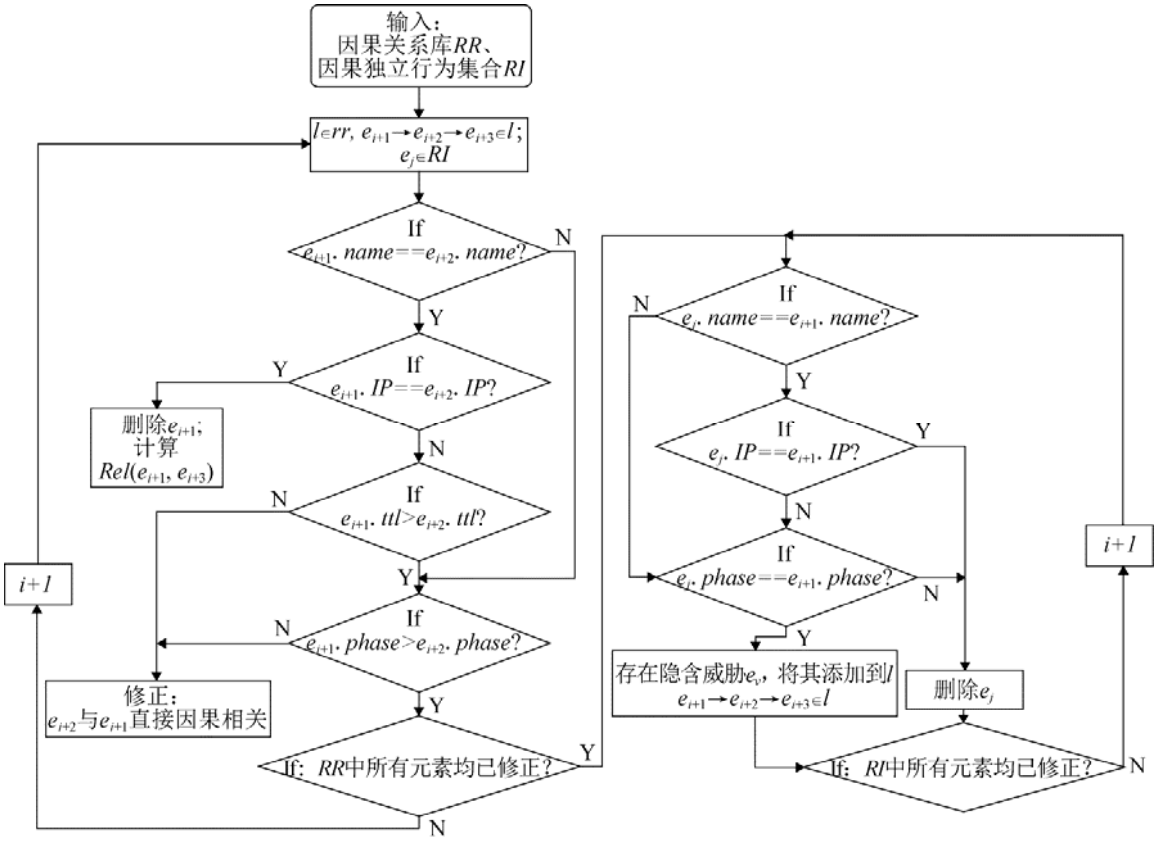

图 3 攻击行为动态因果关联流程

Fig. 3 Dynamic Causal Correlation Process Graph of Attack Behaviors

https://dc-china-simulation.researchcommons.org/journal/vol30/iss10/25
DOI: 10.16182/j.issn1004731x.joss.201810025

第 30 卷第 10 期 系统仿真学报 Vol. 30 No. 10
2018 年 10 月 Journal of System Simulation Oct., 2018

一条动态因果链上的多个攻击行为存在时间上的先后顺序，整条动态因果链的收益应该是该链上所有攻击行为收益的叠加，借鉴数学中卷积的思想，定义以下量化方法。

定义 10 攻击动态因果行为链收益，即链中所有单个攻击行为收益的卷积，具体计算方法为：

已知关联库 R，$\forall l \in R$，且 l 中包含 n 个攻击行为 $\{e_1,e_2,...,e_n\} \in l$，则

$$Payoff(l,t) = \omega_1 f_{e_1}(t-t_1) \times \omega_2 f_{e_2}(t-t_2) \times \cdots \times \omega_n f_{e_n}(t-t_n) \quad (2)$$

其中，ω_{e_i} 指攻击行为 e_i 的系数，t_i 指 e_i 的出现时刻，$f_{e_i}(t)$ 指单个攻击行为 e_i 的收益。

动态因果链中各攻击行为之间的相关程度是由关联度决定的，也可理解为由前一行为推导出下一行为的概率，因此 ω_{e_i} 可由关联度表示。

$$\omega_{e_i} = \begin{cases} 1, & i=1 \\ Rel(e_{i-1},e_i), & 1<i\leqslant n \end{cases} \quad (3)$$

t_i 指攻击行为 e_i 出现的时刻，由 e_i 的原始生存时间 T_{e_i} 与剩余生存时间 $e_i.ttl$ 决定。

$$t_i = T_{e_i} - e_i \times ttl \quad (4)$$

单个攻击行为的收益由攻击成本、攻击回报组成，成本又分为行为自身成本和行为环境成本，回报则可分为行为潜在回报和行为直接回报。参考 CVSS1.0，做出如下定义。

定义 11 攻击成本 cost(e)，执行攻击行为的综合成本，包括自身成本和环境成本两项。其中，行为自身成本 Scost(e)表示执行攻击行为的基本成本，仅与攻击行为自身的相关性质有关，如代码信息 I、代码利用率 U、攻击者能力 C，对代码信息的要求越高、对代码的重复利用率越高、攻击者能力越高，行为的自身成本则越低；行为环境成本 Ecost(e)表示执行该行为所需要的环境资源，如平台与系统 S、漏洞与权限 V。这一要素反映了在采取该攻击行为之前所需要投入的资源，通常，对攻击环境资源的要求越多，如对攻击所需平台的要求越多、所需漏洞的要求越高，则其攻击范围越小，攻击收益也越小。利用 Office 办公软件中存在的漏洞所实施的攻击，其环境成本较低，且攻击的范围广，只要安装有 Officer 的设备都可作为攻击对象，而基于数据库实施的攻击对环境的要求更高，且仅可对数据库服务器实施攻击。

定义 12 攻击回报 value(e)，执行攻击行为的综合收益，包括潜在回报和直接回报，其中，行为潜在回报 Pvalue(e)表示由于攻击行为的实施为后续攻击所带来的潜在有效价值，包括在目标网络系统中的渗透范围 P、有效信息的占有程度 O、作用效果 E，攻击能够在网络系统中的渗透范围越小、对有效信息的占有程度越低、攻击效果越微弱，则行为的潜在回报越少；行为直接回报 Dvalue(e)表示采取攻击行为可直接获得的收益，包含信息获取 L、破坏程度 D，某攻击行为可直接获取的有效信息越多、可造成的破坏越严重，则其直接回报越多。

参考 CVSS 体系[4]中的量化等级和标准，在表 1 中给出上述定义中涉及参数的详细量化值。

表 1 行为收益影响因子的分级与量化

Tab. 1 Classification and Quantitative of Attack Behaviors

参数	影响因子	分级	量化
自身成本	代码信息 I	完整/局部	0.25/0.43
Scost(e)	利用率 U	高/中/低	0.32/0.69/0.83
	攻击者能力 C	无/基础/一般/较高	1/0.77/0.46/0
环境成本	平台与系统 S	高/中/低	0.3/0.6/1
Ecost(e)	漏洞与权限 V		0.25/0.67/1
潜在回报	渗透范围 P	无/局部/较完整/完整	0/0.5/0.75/1
Pvalue(e)	信息占有 O		0/0.3/0.75/1
	攻击效果 E	无/低/中/高微弱/一般/较好/好	0.27/0.55/0.75/1
直接回报	信息获取 L	无/少/中/多	0.2/0.33/0.6/0.85
Dvalue(e)	破坏程度 D	无/一般/重要/严重	0/0.43/0.62/0.85

将上述定义中的各参数用向量表示，则自身成本 Scost(e)=(I U C)，环境成本 Ecost(e)=(S V)，攻击成本 cost(e)=[Scost(e) Ecost(e)]；潜在回报 $Pvalue(e)^T$=(P O E)^T，直接回报 $Dvalue(e)^T$=(L D)^T，攻击回报 $value(e)^T$=[$Pvalue(e)^T$ $Dvalue(e)^T$]^T。本文依据公式(5)计算单个攻击行为的收益。

$$f(e,t)=\begin{cases} cost(e)\times value(e)^{T}, & 0\leqslant t\leqslant T_e \\ 0, & otherwise \end{cases} \quad (5)$$

其中 T_e 表示行为 e 的初始生存时间。

依据上文分析，各攻击行为有其生存时间，超出生存时间范围则认为该行为不对攻击产生影响，因此在生存时间之外的攻击行为收益均为 0。

3 实验验证

本文实验验证中所用的数据集来自于 2015 年举行的第 23 届世界黑客大赛 Defcon23 CTF[19]，该数据集较为新颖，包含多种网络攻击对抗中产生的相关数据，同时，大赛的参与者均具有较高的网络攻防水平，符合本文所提方法的适用场景。比赛共进行了 3 天，本文实验采用中国蓝莲花小组比赛中第一天的数据集作为分析对象。

首先利用 TCPReplay, Snort 以及 Graphviz 3 个工具，在不改变数据集的原始状态下将数据集进行重放、检测与可视化，通过对数据集进行攻击动态因果关联，可识别出攻击动态因果行为链，如图 4 所示。图中横轴代表时间，纵轴代表主机。可以很清晰地看出共有 19 个攻击主机(IP 地址范围为 10.5.1.2 到 10.5.9.2 以及 10.5.11.2 到 10.5.20.2 中)分 6 个批次先后对目标主机(IP 地址为 10.5.10.2)发起攻击，首先采用 ICMP PING 试图连通到目标主机，再基于该主机进行 PortScan、Portsweep 等操作，逐步获取主机 RootAccess 权限，之后对 SIP 代理服务器(IP 地址为 10.5.10.12)进行 AdvancedFishing, LocalSniffer, FTPinfo_Leak, SQLinfo_Leak 等操作，最后对其进行 MessageFlooding 攻击。

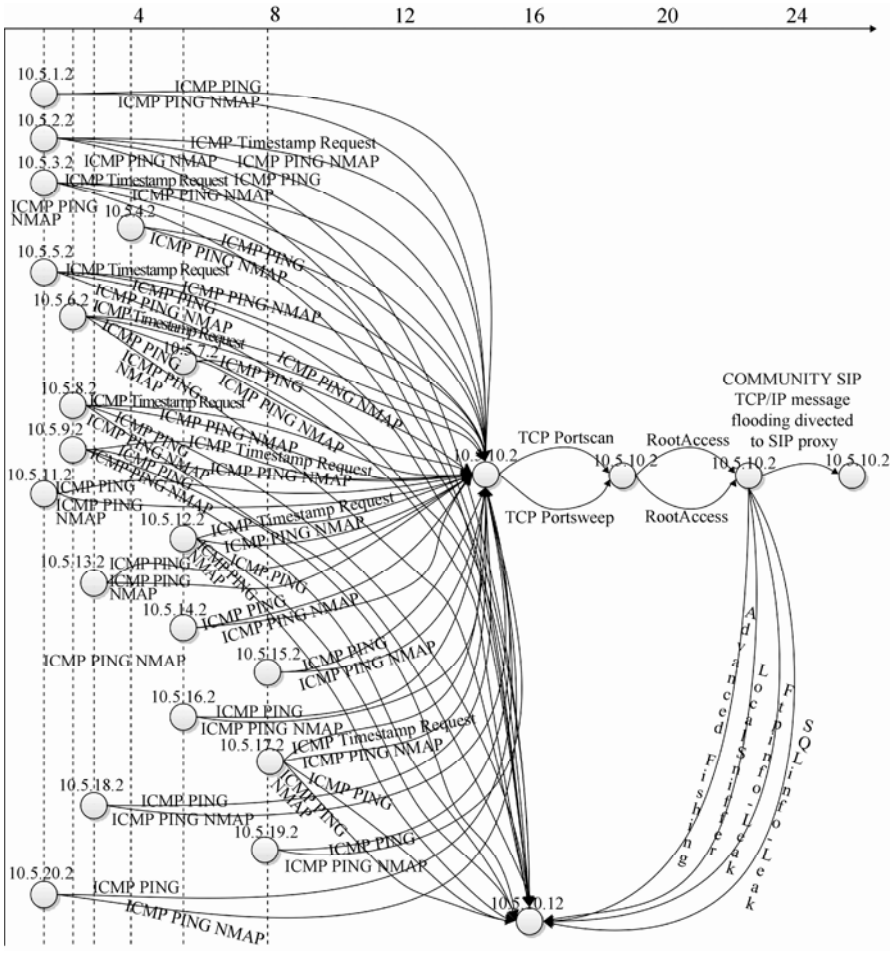

图 4 攻击动态因果行为链
Fig. 4 Dynamic Causal Attack Behavior Paths

https://dc-china-simulation.researchcommons.org/journal/vol30/iss10/25
DOI: 10.16182/j.issn1004731x.joss.201810025

第 30 卷第 10 期 系统仿真学报 Vol. 30 No. 10
2018 年 10 月 Journal of System Simulation Oct., 2018

由于攻击意图明显，将图 4 中关联得到的动态因果行为链提炼，抛开时间因素，则共有以下 11 条不同攻击路径：

$P1:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSCAN] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow ADVANCEDPHISHING \rightarrow 10.5.10.12$

$P2:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSCAN] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow LOACLSNIFFER \rightarrow 10.5.10.12$

$P3:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSCAN] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow TCPinfo\_LEAK \rightarrow 10.5.10.12$

$P4:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSCAN] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow SQLinfo\_LEAK \rightarrow 10.5.10.12$

$P5:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSCAN] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow MESSAGEFLOODING \rightarrow 10.5.10.12$

$P6:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSWEEP] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow ADVANCEDPHISHING \rightarrow 10.5.10.12$

$P7:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSWEEP] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow LOACLSNIFFER \rightarrow 10.5.10.12$

$P8:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSWEEP] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow TCPinfo\_LEAK \rightarrow 10.5.10.12$

$P9:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSWEEP] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow SQLinfo\_LEAK \rightarrow 10.5.10.12$

$P10:10.5.X.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.2 \rightarrow [PORTSWEEP] \rightarrow 10.5.10.2 \rightarrow [ROOTACCESS] \rightarrow 10.5.10.2 \rightarrow MESSAGEFLOODING \rightarrow 10.5.10.12$

$P11:10.5.Y.2 \rightarrow [ICMPPING] \rightarrow 10.5.10.12$

其中主要出现的攻击行为包括：{ICMP PING, PORTSCAN, PORTSWEEP, ADVANCEDPHISHINIG, LOCALSNIFFER, TCPinfo_LEAK, SQLinfo_LEAK, MESSAGEFLOODING} 8 种，利用公式(5)计算这 8 种行为的单个行为收益(此处仅求解生存周期内的收益值)，如表 2 所示。

从图 2 中可以看出，在 1~8 时之间攻击者主要采取了 ICMP PING 的行为，且大约可分为 6 个不同批次分别进行，其余的攻击行为均不再分批执行，本文所提的动态量化评估方法与攻击行为的执行时间相关，因此 ICMP PING 执行时间不同的行为链其量化结果也不相同。将评估时刻设为 24 时，具体量化结果见表 3。

表 2 单个攻击行为收益

Tab. 2 Payoffs of Single Attack Behavior

行为	ICMP PING	PORTSCAN	PORTSWEEP	ADVANCED PHISHINIG	LOCAL SNIFFER	TCPinfo_ LEAK	SQLinfo_ LEAK	MESSAGEFLOODING
收益	0.014	0.086	0.098	0.896	0.420	0.535	0.432	0.650

表 3 动态量化评估结果
Tab. 3 Dynamic Quantitative Assessment

		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
	1.3	4.721	2.300	2.427	2.316	3.684	4.762	2.311	2.407	2.313	3.029	0.089
	1.9	4.674	2.187	2.309	2.203	3.523	4.691	2.193	2.298	2.205	3.389	0.064
执行	2.4	4.532	2.079	2.194	2.074	3.481	4.558	2.082	2.187	2.079	2.837	
时刻	3.9	4.211	1.739	1.786	1.742	3.183	4.218	1.746	1.713	1.748	2.538	
	5.5	3.957	1.410	1.407	1.418	2.789	3.988	1.421	1.400	1.423	2.193	0.028
	8	3.376	0.986	1.075	1.004	2.353	3.565	0.987	1.001	0.995	1.642	0.017

对表 3 中的数据进行分析。首先需要注意在(t=2.4，P11)和(t=3.9，P11)两处无数据，这是由于 P11 代表了由攻击主机向 SIP 代理服务器发起 ICMP PING 操作的攻击行为，而在 t=2.4 和 t=3.9 这两个时刻发起的攻击行为均是针对目标主机而非 SIP 代理服务器，因此在这两个时刻无 P11 的收益值；此外，P11 行为链无论在任何时刻发起攻击，其攻击收益都显著较低，这是由于由攻击主机无法直接向代理服务器发起访问，也无法基于此获取任何有效信息，无法对攻击产生作用，因此这一行为的收益几乎为零。其次对表中 P1 到 P10 的数据进行横向分析，即对相同时刻发起攻击的不同行为链之间的收益差距进行对比，可以看出，在任意时刻的 10 条攻击行为链中，P1 和 P6 的收益明显较高，其次是 P5 和 P10，P11 的收益最低，其余的几条行为链之间的收益相差较小。这是由于 P1 和 P6 两条行为链中含有 ADVANCEDPHISHING 行为，这是一种先进的钓鱼攻击，其对攻击者的能力要求较高，同时其行为收益也较高；同理，P5 和 P10 行为链中的 MESSAGEFLOODING 攻击使得整条行为链的收益值高于其余的行为链收益。然后对表中 P1 到 P10 的数据进行纵向分析，即对同一行为链由于不同的攻击行为执行时间所导致的收益差距进行对比，对每一条攻击行为链而言，其整体收益值随着攻击发起时间的推迟而减小，这是由于行为链的整体收益是整条行为链所有攻击行为收益的叠加，攻击行为发生得越早，对后续攻击所提供的有效信息或帮助则越大，因此其整体收益值也就越大。结合实际攻击对该数据的合理性进行分析，攻击者在目标系统中潜伏的时间越长，攻击的目标越明确，采取的攻击行为越先进，则攻击效果越明显，攻击收益也越高，例如 ADVANCEDPHISHING 攻击行为与 PORTSCAN 行为相比，前者钓鱼攻击的攻击针对性强、技术先进，一旦攻击成功则可获得十分有利的信息，对后续攻击提供极大的帮助；而后者端口扫描针则目标广泛，收集大量数据，而其中的有效信息含量低，对攻击的推进效果不如前者明显，因此前者的攻击收益必然大于后者，在上述评估数据中可直观地反映出这一结论。因此，本文所提攻击行为动态量化方法可以较为合理地对实际攻击进行评估。

4 结论

为准确分析 APT 攻击行为的影响与关联性，有效量化评估 APT 攻击行为收益，本文提出一种面向 APT 攻击的攻击行为动态评估方法。首先对攻击行为在空间上进行初步关联，识别存在因果关系的攻击行为链；然后再根据 APT 攻击的持续性特征，在时间上对攻击行为链进行修正与补充，最大限度识别包含攻击信息的动态因果行为链；最后借鉴 CVSS 体系提出具体的攻击行为评估方法，对单个攻击行为及完整行为链的收益进行量化表示。通过实验及分析，可以看出利用本文所提方法对攻击行为进行关联与量化，其结果能够真实反映攻击情况，具有很好的参考价值。接下来的研究将主要包括：(1)算法优化，降低算法的时间复杂度；(2)基于该算法的 APT 攻击预测研究；(3)面向 APT 攻击的最优防御策略选择研究。

https://dc-china-simulation.researchcommons.org/journal/vol30/iss10/25
DOI: 10.16182/j.issn1004731x.joss.201810025

第 30 卷第 10 期 系统仿真学报 Vol. 30 No. 10
2018 年 10 月 Journal of System Simulation Oct., 2018

参考文献:

[1] Defense USA Department of Trusted Computer System Evaluation Criteria [S]. DoD-5200, 28-STD, DoD, 1985.

[2] Board Common Criteria Editing. Common Criteria of Information Technology Security Evaluation [S]. 1998.

[3] M Schiffman. Common Vulnerability Scoring System Version 2.0 [EB/OL]. [2013-7-8]. http://www.first.org/cvss/cvss-guide.html.

[4] Mell P, Scarfone K, Romanosky S. The common vulnerability scoring system (CVSS) and its applicability to federal agency systems, NIST Interagency Report 7435 [R/OL]. (2007) [2014-01-17]. http:csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf.

[5] GB 17859-1999. 计算机信息系统安全保护等级划分准则 [S]. 中国标准出版社, 1999.
GB 17859-1999. Classification criteria for computer information system security protection [S]. Standards Press of China, 1999.

[6] GB/T18336-2001. 信息技术安全技术信息技术信息安全评估准则 [S]. 中华人民共和国国家标准, 2001.
GB/T18336-2001. Information technology safety technology information technology information security evaluation criteria [S]. National Standard of the People's Republic of China, 2001

[7] GB/T 20984-2007. 信息安全技术信息系统的风险评估规范 [S]. 中华人民共和国国家标准, 2005.
GB/T 20984-2007. Risk assessment specification for information security technology information system [S]. National Standard of the People's Republic of China, 2005

[8] Poolsappasit N, Dewri R, Ray I. Dynamic security risk management using Bayesian attack graph [J]. IEEE Trans on Dependable and Secure Computing, 2012, 9(1): 61-74.

[9] 方研, 殷肖川, 李景志. 基于贝叶斯攻击图的网络安全量化评估研究 [J]. 计算机研究应用, 2013, 30(9): 2763-2766.
FANG Yan, YIN Xiao-chuan, LI Jing-zhi. Research of quantitative network security assessment based on Bayesian-attack graphs [J]. Application Research of Computers, 2013, 30(9): 2763-2766.

[10] Helmer C, Wong J, Slagell M, et al. Software Fault Tree and Colored Petri net based Specification, Design and Implementation of Agent-based Intrusion Detection System [J]. Requirements Engineering, 2000, 7(4): 207-220.

[11] 张勇, 谭笑彬, 崔孝林, 等. 基于 Markov 博弈模型的网络安全态势感知方法 [J]. 软件学报, 2011, 22(3): 495-508.
Zhang Yong, Tan Xiao-bin, Cui Xiao-lin. Network Security Situation Awareness Approach Based on Markov Game Model [J]. Journal of Software, 2011, 22(3): 495-508.

[12] Yee Weilaw, Tansu Alpcan, Marimuthu Palaniswami. Security Games for Risk Minization in Automatic Generation Control [J]. IEEE Transactions on Power Systems, 2015, 30(1): 223-232.

[13] 张少俊, 李建华, 宋珊珊. 贝叶斯推理在攻击图节点置信度计算中的应用 [J]. 软件学报, 2010, 21(9): 2376-2386.
Zhang Shao-jun, Li Jian-hua, Song Shan-shan. Using Bayesian Inference for Computing Attack Graph Node Beliefs [J]. Journal of Software, 2010, 21(9): 2376-2386.

[14] Joint Task Force Transformation Initiative. Managing Information Security Risk: Organization, Mission, and Information System View [EB/OL]. [2011-03-01] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[15] Fatemeh Kavousi, Behzad Akbari. Automatic learning of attack behavior patterns using Bayesian networks [C]// 6'th International Symposium on Telecommunications (IST'2012). USA: IEEE, 2012: 999-1004.

[16] 陈剑锋, 王强, 伍淼. 网络 APT 攻击及防范策略 [J]. 信息安全与通信保密, 2012(7): 24-27.
Chen Jian-feng, Wang Qiang, Wu Miao. Network-based APT attack and defense strategies [J]. Information Security and Communications Privacy, 2012(7): 24-27.

[17] 林龙成, 陈波, 郭向民. 传统网络安全防御面临的新威胁：APT 攻击 [J]. 信息安全, 2013, 4(3): 20-25.
Lin Long-cheng, Chen Bo, Guo Xiang-min. The new threat to traditional network security defense: APT attack [J]. Information Security, 2013, 4(3): 20-25.

[18] 杜跃进, 翟立东, 李跃, 等. 一种应对 APT 攻击的安全架构: 异常发现 [J]. 计算机研究与发展, 2014, 51(7): 1633-1645.
Du Yue-jin, Zhai Li-dong, Li Yue. Security architecture to deal with APT attacks: abnormal discovery [J]. Journal of Computer Research and Development, 2014, 51(7): 1633-1645.

[19] J Moss. Capture the flag traffic dump [EB/OL]. [2017-09-04] http://www.defcon.org/html/links/dc-cft.html.