文章编号：2095-2163(2023)05-0114-03 中图分类号：TP393 文献标志码：A

基于蜜罐技术的虚拟交易网络安全防御系统

王彩玲
(河南警察学院 网络安全系，郑州 450046)

摘 要：由于虚拟交易的过程易受到网络攻击，从而泄露大量用户隐私信息数据，为此本文引入蜜罐技术，设计虚拟交易网络安全防御系统。采用蜜罐技术监控攻击者行为，根据监控结果，构建攻击数据集合，划分虚拟交易过程中的安全风险等级，构建虚拟交易网络安全防御决策模型，完成系统软件设计。通过对比实验验证，新的防御系统应用可保障虚拟交易安全，使攻击者无法获取用户隐私信息，保障用户权益不受损害。

关键词：蜜罐技术；隐私信息数据；防御系统；虚拟交易；安全风险等级

Virtual transaction network security defense system based on honeypot technology

WANG Cailing
(Network Security Department, Network Security Department of Henan police college, Zhengzhou 450046, China)

【Abstract】 Because the process of virtual transaction is vulnerable to network attacks, thus revealing a large number of user privacy information data, this paper introduces honeypot technology and designs a network security defense system for virtual copy transaction. The honeypot technology is used to monitor the behavior of attackers. According to the monitoring results, the attack data set is built, the security risk level in the virtual transaction process is divided, the security defense decision-making model of the virtual transaction network is built, and the system software design is completed. Through comparative experiments, the new defense system application can ensure the security of virtual transactions, make attackers unable to obtain user privacy information, and protect user rights and interests from being damaged.

【Key words】 honeypot technology; privacy information data; defense system; virtual transaction; safety risk level

0 引 言

随着网络技术的不断发展与创新，网络犯罪活动也日益猖獗，黑客往往利用计算机技术漏洞和系统漏洞、网络病毒等多种方式来攻击网络或窃取数据信息[1]。因此，必须要对攻击行为进行准确溯源、实时追踪和智能化主动防御，以实现对各类网络威胁和犯罪活动有效防御的目的。目前网络安全防御系统仍处于初期开发阶段，在实践中也有诸多问题，在信息攻击强度不断提升的背景下，网络安全也再次受到威胁。为提高虚拟交易网络安全性，本文开展基于蜜罐技术的虚拟交易网络安全防御系统设计。具体研究路线如下：

(1)设计虚拟交易网络安全防御系统功能模块，包括网络扫描模块、决策模块、判断模块、蜜网网关模块、低交互蜜罐模块、高交互蜜罐模块；

(2)在系统功能模块设计的基础上，通过蜜罐技术监控攻击者行为，构建攻击数据集合，划分虚拟交易过程中的安全风险等级，根据等级划分结果，构建虚拟交易网络安全防御决策模型，获取防御决策方案。

1 虚拟交易网络安全防御系统功能模块设计

虚拟交易网络安全防御系统由扫描模块、决策模块、判断模块、蜜网网关模块、低交互蜜罐模块、高交互蜜罐模块等模块组成。

网络扫描模块按照判断模块的要求，定期扫描周围的网络；决策模块根据需求，从数据库中提取扫描信息，并对低级交互模块的结构进行调整；判断模块对扫描结果进行处理，并将数据保存在数据库中；蜜网网关模块的主要功能是管理高互动式的蜜罐，以确保高互动式的蜜罐不会对本局域网构成任何的

基金项目：2022 年度河南警察学院院级课题(HNJY202238)；2023 年度河南省高校人文社会科学研究项目(2023-ZDJH-001)。

作者简介：王彩玲(1977-)，女，硕士，副教授，主要研究方向：电子数据取证、网络安全监管。

收稿日期：2022-11-24

威胁。

系统利用两种蜜罐作为诱饵，允许攻击者进入。在攻击端存取低交互式的虚拟蜜罐主机时，若该蜜罐主机能回应该请求，在记录网路资料的同时，将资料直接传回；当目标主机上的端口和服务没有被打开时，低级互动的蜜罐会利用转发技术向高互动的蜜罐发送访问请求。高互动蜜罐提供了一个真正的虚拟交易网络服务，能够对网络的要求做出反应，并且对攻击行为的细节进行详细的记录。

基于防御系统各项功能，设计虚拟交易网络安全防御系统模块框架结构，如图 1 所示。

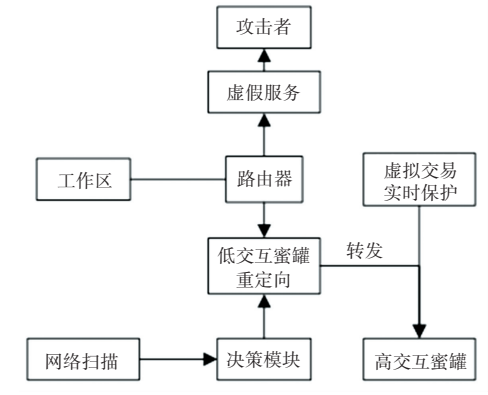

图 1　虚拟交易网络安全防御系统模块框架结构

Fig. 1　Structure of the virtual transaction network security defense system module framework

按照不同的应用场景设计若干个模块，每一个模块可独立使用。

2　系统软件设计

2.1　基于蜜罐技术的攻击者行为监控

蜜罐技术作为一种自动化和分布式文件传输机制，能够使用户在不影响业务正常运行的情况下，快速恢复已发布内容并将交易发送给用户。蜜罐的安全性主要体现在对未知内容的检测上[2]。在用户已发布内容被利用、窃取之前，系统会通过蜜罐对未知内容进行检测处理，如文件中是否有未加密传输到用户手机、服务器上的信息，因此蜜罐能够在业务系统遭受到攻击时快速地检测并采取措施，防止风险蔓延，从而为业务系统恢复提供可靠地保障机制。基于蜜罐技术实现对攻击者虚假服务的提供，并与攻击者交互，防止攻击者对虚拟交易主体产生影响。为实现这一目的，基于低交互蜜罐模块和蜜网网关模块，对攻击者行为监控。

低交互式蜜罐模型基于持久的信息，对目标主机虚拟化处理，并通过与攻击者仿真。如果攻击者的存取要求蜜罐语义响应，蜜罐就会和攻击者互动；若存取要求蜜罐自身无法响应，则蜜罐应采取适当的措施，以避免直接回传回应码。在蜜罐和攻击者互动的过程中，能够对攻击者行为进行监控，实时地记录用户的日志信息，以便管理人员进行分析，通过分析所获取到的数据，系统可以推测出攻击者的行为意图，系统通过对攻击者行为监控，实现对攻击者与防御者的动态信息获取。攻击者与防御者的动态如式(1)、式(2)：

$$Dx(q_x^i)=\xi\frac{q_x^i(h)}{dt} \tag{1}$$

$$Ax(q_x^j)=\xi\frac{q_x^j(h)}{dt} \tag{2}$$

其中，$Dx(q_x^i)$ 表示攻击者的动态方程；$Ax(q_x^j)$ 表示防御者的动态方程；q_x^j 表示某一防御策略 j 的选择概率；q_x^i 表示某一防御策略 i 的选取概率。

2.2　虚拟交易安全风险等级划分

根据虚拟交易对信息的保密性、可用性、完整性和不可否认性以及对网络资源的安全性需求，以基于蜜罐技术的攻击者行为监控结果为基础，构建攻击数据集合，划分虚拟交易过程中的安全风险等级。虚拟交易过程中的各类攻击数据集合，如式(3)：

$$T=\{t_1,t_2,t_3,t_4,t_5,\cdots\} \tag{3}$$

其中，t_1 表示未授权访问数据；t_2 表示病毒数据；t_3 表示木马攻击数据；t_4 表示欺骗攻击数据；t_5 表示操作攻击数据。

在确定攻击数据集后，对各个攻击环境下虚拟交易过程中产生的安全风险进行分类，分为低级、中级和高级。根据攻击类型和攻击次数确定具体等级，并为后续安全防御决策提供方向。

2.3　安全防御决策模型构建

根据上述划分的虚拟交易安全风险等级，构建虚拟交易网络安全防御决策模型。本文防御系统的决策模块是用于对整个系统的操作速度进行控制的，其主要功能包括以下几个方面：

首先，根据网络的动态特性，判断网络的扫描周期，确保网络环境在未来一段时间内不会发生太大的变化；

其次，将处理的结果保存到数据库中，以便在后续设置蜜罐时使用。

根据功能要求，建立安全防御决策模型，式(4)：

$$P = \sum_{i=1}^{N_D} P_{C,i} \quad (4)$$

其中，$P_{C,i}$ 表示受到攻击后虚拟交易网络第 i 种节点的负荷损失，N_D 表示系统的总节点数量。

3 对比实验

为了验证系统在实际应用中的安全防御性能，将该系统作为实验组，将基于大数据的防御系统和基于安全态势感知的防御系统作为对照 A 组和对照 B 组，将这 3 种防御系统应用到相同的运行环境中，对比其安全防御效果，实现对 3 种系统性能的比较。选择将 5 名系统用户人为虚拟交易网络中的攻击者，分别采取不同的攻击手段，获取虚拟交易过程中产生的重要信息数据，5 名攻击者基本信息记录见表 1。

表 1 5 名攻击者基本信息记录

Tab. 1 5 Basic information records of the attackers

攻击者用户名	攻击手段
用户 A	SQL 注入
用户 B	零日攻击
用户 C	DDoS 攻击
用户 D	中间人攻击
用户 E	暴力破解

表 1 中 5 名攻击者对应 5 种不同的攻击手段，其攻击强度从大到小依次为：用户 E>用户 D>用户 C>用户 B>用户 A。已知在实验过程中虚拟交易产生的隐私数据量为 1 000 Mbits，分别记录 3 种防御系统应用，5 名攻击者非法获取隐私信息的数据量，记录结果见表 2。

表 2 三种系统防御结果记录

Tab. 2 Results of the three systems

攻击类型	$W_{实}$（Mbits）	$W_{对A}$（Mbits）	$W_{对B}$（Mbits）
用户 A	0	125.25	201.32
用户 B	0	253.36	352.36
用户 C	0	325.32	458.31
用户 D	0	425.21	596.32
用户 E	0	553.25	683.42

表 2 中 $W_{实}$ 表示实验组防御系统运行中攻击者非法获取虚拟交易隐私信息数据量；$W_{对A}$ 表示对照 A 组防御系统运行中攻击者非法获取虚拟交易隐私信息数据量；$W_{对B}$ 表示对照 B 组防御系统运行中攻击者非法获取虚拟交易隐私信息数据量。从表 2 可以看出，5 名攻击者均无法获取到虚拟交易产生的隐私信息数据，而对照 A 组和对照 B 组均出现了虚拟交易隐私信息数据泄露的情况，并且随着攻击强度的增加，泄露的信息量也逐渐增加。

4 结束语

为提高虚拟交易网络的安全，本文在引入蜜罐技术的基础上，提出了一种新的防御系统，并实现了对这一系统应用可行性的验证。新的防御系统能够为用户在虚拟交易网络中开展各项交易业务提供更有利保障条件。

参考文献

[1] 李凤鸣. 基于大数据及人工智能技术的计算机网络安全防御系统[J]. 电子技术与软件工程，2022，11(17)：1-4.

[2] 宋午阳，张尼. 基于大数据及人工智能技术的网络安全防御系统设计策略[J]. 网络安全技术与应用，2022，22(7)：56-57.

(上接第 113 页)

[44] XIANGJUN L，DONG H，XIAOKANG L. Battery energy storage station (BESS)-based smoothing control of photovoltaic (PV) and wind power generation fluctuations[J]. IEEE Transactions on Sustainable Energy，2013，4(2)：464-473.

[45] 王磊，杜晓强，宋永端. 用于风电场的飞轮储能矩阵系统协调控制[J]. 电网技术，2013，37(12)：3406-3412.

[46] 靳雯皓，刘继春. 平滑风电功率波动的混合储能系统容量优化配置[J]. 分布式能源，2017，2(2)：32-38.

[47] 李亚楠，王倩，宋文峰，等. 基于变分模态分解和 Hilbert 变换的平滑风电出力混合储能容量优化配置[J]. 电测与仪表，2019，56(1)：82-88，95.

[48] 张野，郭力，贾宏杰，等. 基于平滑控制的混合储能系统能量管理方法[J]. 电力系统自动化，2012，36(16)：36-41.

[49] 刘仲民，齐国愿，高敬更，等. 混合储能系统平抑风光发电功率波动策略[J]. 电力电子技术，2021，55(11)：64-67.

[50] 贾鹏飞，李卫国，高兴军，等. 平抑风电功率波动的电池储能系统模糊控制方法[J]. 现代电力，2014，31(3)：7-11.

[51] 郭敏. 基于风功率预测平抑风电并网波动功率的研究[D]. 太原：山西大学，2018.

[52] 卢芸，徐骏. 基于小波包分解的风电混合储能容量配置方法[J]. 电力系统保护与控制，2016，44(11)：149-154.

[53] 赵雅文. 融合风功率趋势预测信息的波动平滑控制研究[D]. 济南：山东大学，2020.

[54] 王利猛，刘久成，田春光，等. 基于统计学方法的微网混合储能容量优化配置[J]. 电网技术，2018，42(1)：187-194.

[55] 马速良，马会萌，蒋小平，等. 基于 Bloch 球面的量子遗传算法的混合储能系统容量配置[J]. 中国电机工程学报，2015，35(3)：592-599.

[56] 杨珺，张建成，周阳，等. 针对独立风光发电中混合储能容量优化配置研究[J]. 电力系统保护与控制，2013，41(4)：38-44.

[57] 王苏蓬，张新慧，吴文浩，等. 用于风电平抑的混合储能选型和容量优化配置方法[J]. 智慧电力，2021，49(9)：16-23.