附件1：

项 目 征 集 表

|  |  |  |  |
| --- | --- | --- | --- |
| 教师姓名 | 肖辉 | 职称 | 教授 |
| 课题来源 | 国家自然科学基金 | 课题名称 | 基于可靠性的最优防御策略研究 |
| 课题编号 | 71971176 | 课题研究方向 | 风险管理 |
| 课题简介 | 近年来频繁发生的金融交易所被黑客非法入侵事件，表明金融交易系统的安全性受到了巨大的威胁。而金融交易系统一旦被非法入侵，不仅仅会丢失大量的机密交易数据，还会引起巨大的经济损失。基于这一现实问题，本项目将探索如何提高金融交易系统的安全性，以防御黑客的非法入侵。 | | | |
| 拟设立国创项目题目 | 金融交易系统防御建模与优化 | | | |
| 学生要求 | （对申报项目学生的科研素养及专业要求等）   1. 具有基本的数学建模和编程基础。 2. 熟悉博弈论相关知识。 3. 统计、数学、信息学院专业优先，1-2人为佳。 | | | |
| 任务要求 | （拟设项目研究内容、实施过程及成效要求；1000字以内）  现代通信技术极大地缩短了人与人之间的时空距离，它也使得金融交易不再受时空的限制，可以连续24小时无间断地在全球范围内进行。信息传播和处理的快速化与智能化一方面使得金融交易量迅速增长，另一方面也使得金融交易系统所处的外部环境变得更加复杂和不确定。而一旦金融交易系统的安全性受到威胁，不仅会导致机密的交易信息和敏感信息被窃取，还会带来巨大的经济损失。例如，2010年，纳斯达克证券交易所的中央服务器遭受黑客的非法入侵，导致敏感信息泄露，美国国家安全局认为黑客的非法入侵不仅仅能够破坏交易，甚至可以破坏整个纳斯达克证券交易所。2018年，韩国最大的虚拟货币交易所Bithumb被黑客非法入侵，高达350亿韩元的虚拟货币遭黑客窃取；同一年，韩国中小型交易平台Coinrail也遭到黑客非法入侵，损失了约400亿韩元。以上事件表明，如果不能保证金融交易系统的安全，则极有可能会引起巨大的经济损失，因此，探索如何提高金融交易系统的安全性，防御系统遭受黑客的非法入侵至关重要。  现有的金融交易系统主要通过设置工业防火墙和布置蜜罐来防御黑客的非法入侵。工业防火墙增加了黑客非法入侵系统的难度，而一旦黑客成功入侵，系统中布置的蜜罐也可以进一步诱导和捕获黑客，从而保护金融交易系统中真实服务器的安全性。目前，黑客开发了一种被称为“蜜罐猎人”的反蜜罐措施，虽然可以帮助黑客以一定的概率识别出系统中布置的一些蜜罐，但尚且存在“误报”和“漏报”的情况。具体来说，当黑客打探到系统中布置的真实服务器时，它将以一定的概率识将其识别为真实服务器，一定的概率将其识别为蜜罐，一定的概率无法识别；同样地，当黑客打探到系统中布置的蜜罐时，它将以一定的概率将其识别为蜜罐，一定的概率将其识别为真实服务器，一定的概率无法识别。本项目将针对系统遭受黑客的非法入侵且存在“误报”和“漏报”的这一现实情形进行深入研究，探索防御者如何进行系统防御以提高系统的安全性。  本课题拟以金融交易系统为研究对象，深入研究存在“误报”和“漏报”这种复杂情形下的系统防御问题。拟构建存在“误报”和“漏报”的不完全信息攻防博弈模型，探索该情形下的防御措施，运用概率论，博弈模型等分析防御者的最优防御策略，为提高金融交易系统的安全性提供有效的支撑与保障，为防御者的决策提供科学依据。研究成果拟发表外B或外A论文一篇。 | | | |