

自回归滑动平均和相关向量机的信息系统安全态势估计

李欣蔚¹, 陈辉², 张亚红³

(¹ 桂林医学院, 广西 桂林 541004; ² 桂林电子科技大学 计算机与信息安全学院,

广西 桂林 541004; ³ 桂林航天工业学院 计算机科学与工程系, 广西 桂林 541004)

摘要: 为了改善信息系统的安全态势估计效果, 提出了自回归滑动平均和相关向量机的信息系统安全态势估计模型(ARIMA-RVM). 该模型收集大量信息系统安全的历史数据, 然后采用自回归滑动平均和相关向量机描述信息系统安全态势变化特点, 建立信息系统安全态势估计模型, 最后与其他信息系统安全态势估计模型进行了对比测试, 结果表明, ARIMA-RVM 可以发现信息系统安全态势的变化趋势, 获得比其他模型更好的信息系统安全态势估计结果, 估计结果可以帮助信息系统安全管理者制定防范措施.

关键词: 信息系统; 数据挖掘; 安全态势; 估计模型

Information System Security Situation Assessment

Based on Data Mining

LI Xin-wei¹, CHEN Hui², ZHANG Ya-hong³

(¹ Guilin Medical University, Guilin 541004, China; ² School of Computer Science and Information

Security, Guilin University of Electronic Technology, Guilin 541004, China; ³ Department of

Information Engineering, Guilin University of Aerospace Technology, Guilin 541004, China)

Abstract: In order to estimate the effect of improving security situation information system, put forward the estimation model of information system based on data mining security situation. The method of collecting a lot of information system security of the historical data, and then using data mining combined kernel function to dig out the characteristics of information system security situation from the historical data, the establishment of information system security situation assessment model, finally model were compared, and the other information system security situation assessment results show that the model can be found to change the trend of information system security situation, get information system security situation better contrast model estimation results, the estimation results can improve the security of the information system and formulate corresponding preventive measures.

Key words: information system; data mining; security situation; estimation model

作者简介:

李欣蔚 男, (1973-), 硕士, 高级工程师. 研究方向为计算机网络. E-mail:lixingw908@163.com

陈辉 男, (1974-), 博士, 副研究员. 研究方向为模式识别与智能控制、智能检测与非线性控制.

张亚红 女, (1977-), 硕士, 副教授. 研究方向为图像处理与识别、信息安全.