通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

潘 璠,洪 征,周振吉,吴礼发.语义层次的协议格式提取方法[J].通信学报,2013,(10):162~173

语义层次的协议格式提取方法

Protocol format extraction at semantic level

投稿时间： 2012-05-08

DOI：10.3969/j.issn.1000-436x.2013.10.019

中文关键词：协议逆向工程 协议格式提取 动态污点分析 中间语言

英文关键词:protocol reverse engineering protocol format extraction dynamic taint analysis intermediate language

基金项目:国家自然科学基金资助项目(61070173)；江苏省自然科学基金资助项目(BK2011115)；军用网络技术实验室创新开放基金资助项目

作者	单位
潘 璠，洪 征，周振吉，吴礼发	解放军理工大学 指挥信息系统学院，江苏 南京 210007

中文摘要:

现有协议格式提取方法在语法层次对程序执行轨迹进行分析，字段识别结果可能存在冗余和冲突。为了提高字段识别准确率，提出了一种语义层次的协议格式提取方法。方法首先将执行轨迹中的二进制指令转换为语义等价的中间语言形式，并通过细粒度的动态污点分析跟踪字段语义解析过程，在此基础上，依据字段的语义不可分割性，利用语义层次的字段识别策略实现了协议格式提取。测试结果表明，该方法具有较高的识别精度和较低的分析复杂度。

英文摘要:

Present methods for protocol format extraction analyze the execution traces of programs at syntax level, which leads to redundancy and conflict in the results of field identification. In order to improve the accuracy of field identification, a semantic level method was proposed for protocol format extraction. The method firstly translated the binary instructions into equivalent intermediate language, and then tracked the parsing process of field semantics through fine-grained dynamic taint analysis. Further, it extracted protocol format using semantic level policies of field identification, based on the semantic indivisibility of fields. Experimental results show that the proposed method can achieve high identification accuracy with low complexity.

查看全文 查看/发表评论 下载PDF阅读器

关闭