基于 GCC 插件的堆栈保护技术研究

王亚刚，曹耀彬，王 萌
（西安邮电大学 计算机学院，陕西 西安 710121）

摘 要： 缓冲区溢出攻击是计算机中最主要的漏洞之一，在所有的缓冲区溢出中主要攻击的区域是程序的堆栈，为了改进 GCC 编译器对于基于字节猜测的堆栈溢出防护的不足，在 GCC 提供的最新插件基础上，提出了一种堆栈保护增强插件，并将其作为 GCC 编译器后端的一个编译优化过程.实验结果表明，新增的编译优化遍，在一定程度上增加了攻击者对 canary 暴力破解的难度，有效地缓解了 GCC 编译器堆栈防护的不足.

关键词： GCC 编译器；GCC 插件；堆栈溢出；软件安全

Research on Stack Protection Technology Based on GCC Plugin

WANG Ya-gang, CAO Yao-bin,WANG Meng

(School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract： Buffer overflow attack is one of the main vulnerabilities in the computer. In all areas, the most likely to attack is the program stack. In order to enforce the GCC stack overflow protection, which is not enough to defense the byte guess attack. On the basis of the latest plug-in provided by GCC, a stack protection enhancement plug-in is proposed and used as a compilation optimization process for the back end of the GCC compiler. The final experimental results show that the new compiler optimization pass, to some extent, increasing the difficulty of the attacker to guessing the canary, which using byte for byte brute force attack. And the plugin can effectively alleviate the shortage of the GCC stack smashing protection.

Key words： GCC compiler; GCC plugin; stack overflow; software security

作者简介：
王亚刚 男，（1972-），博士，副教授.研究方向为嵌入式系统、编译器与并行计算.
曹耀彬(通讯作者）男，（1990-），硕士研究生.研究方向为 GCC 编译器与软件安全.E-mail：caoyaobin1990@qq.com.
王 萌 女，（1994-），硕士研究生.研究方向为计算机系统结构、图像处理.