主要学术贡献、成果及评价

重点引用

Detection and Analysis of Cryptographic Data inside software

Ruoxu Zhao, Dawu Gu, Ran Yu, and Juanru Li

Lab of Cryptology and Computer Security
Dept. of Computer Science, Shanghai Jiao Tong University, Shanghai, China

我们的工作发表于Information Security Conference, 2011

研究了基于输入/输出关系的算法识别概念，被国际最顶级计算机安全会议CCS的论文工作沿用。

extracted based on their size and therefore variable-length parameter functions like RC4 are hard to recognize. Zhao *et al.* also used I/O relationship to identify cryptographic functions [37]. Again, they made several assumptions on their programs, e.g. the ratio of exclusive-ors in cryptographic code or the use of certain types of functions, that are rarely satisfied in obfuscated programs.

Aligot: Cryptographic Function Identification in Obfuscated Binary Programs

Joan Calvet
Université de Lorraine, LORIA
Nancy, France
joan.calvet@loria.fr

José M. Fernandez
École Polytechnique
Montréal, Canada
jose.fernandez@polymtl.ca

Jean-Yves Marion
Université de Lorraine, LORIA
Nancy, France
jean-yves.marion@loria.fr

[35] D. Wheeler and R. Needham. TEA, a tiny encryption algorithm. In *Proc. Fast Software Encryption*, pages 363–366. Springer, 1995.

[36] V. Zakorzhevsky. A new version of Sality at large. `http://www.securelist.com/en/blog/180/A_new_version_of_Sality_at_large`.

[37] R. Zhao, D. Gu, J. Li, and R. Yu. Detection and analysis of cryptographic data inside software. *Information Security*, pages 182–196, 2011.