Abstract

Security threats such as viruses, worms, trojans and spyware affects the security and authentication of software codes, forcing software developers to build security schemes for better software protection. These software threats exploit the authenticated data of the software and confidentiality, integrity and accessibility is greatly affected by these software threats. A number of code security techniques like tamper resistant packaging, code obfuscation, register encoding etc have been developed which mainly concentrates on providing solutions for a particular type of threats and are vulnerable to code tampering and code injection by complicated attackers. Hence, code encryption technique has become an active area of research. This paper proposes a novel software protection code encryption scheme based on the index table. This approach uses a novel and efficient encryption technique called quasigroup encryption for encryption the indexed table. It provides least resemblance of the original data when encrypted. But, quasi group encryption is not efficient in diffusing the statistics of the plain text. This drawback can be overcome by using transforms. Hence, this approach uses chained Hadamard transforms and Number Theoretic Transforms to introduce diffusion along with the quasigroup transformation. The proposed approach is compared with the other encryption approaches and is observed to provide better results.
Refer

- Collberg, C., C. Thomborson, and D. Low, "Breaking abstractions and unstructuring data structures", Proceedings from International Conference on Computer Languages, pp. 28-38,
- Tieming Chen; Shilong Ma, "A Secure Email Encryption Proxy Based on Identity-Based Cryptography", International Conference on MultiMedia and Information Technology, 2008. MMIT &aposos:08.
An Enhanced Code Encryption Approach with HNT Transformations for Software Security

USENIX Security Symposium.
- Vaigmana Spoorhally Ella, Sequence Randomization Using Quasigroups and Number Theoretic Transforms; Third Conference on Theoretical and Applied Computer Science (TACS 2012).

Index Terms

Computer Science  
Security
Keywords
Software Piracy  Cryptography  Encryption  Quasigroup  Indexed Table  Number
Theoretic Transforms and Hadamard Transforms