Abstract

White box cryptographic algorithms aim to denying the key readout even if the source code embedding the key is disclosed. Full-privileged attack software shares a host with cryptographic software, having complete access to the implementation of algorithms, dynamic execution (with instantiated cryptographic keys) can be observed and internal algorithm details are completely visible and alterable. Chow proposed a new technique to secure cryptographic algorithms and key against white-box attacks, called white-box cryptography. Another technique such as obfuscation is mainly designed to facilitate securing of e-commerce and e-banking applications, which often embed cryptographic keys and critical information. In general, it can be used to protect all distributed client software where an owner loses control or where the user wants to protect against automated attacks. As we know main challenges in modern cryptography does how to encrypt or decrypt content without directly revealing any portion of the key and or the data and how to perform strong encryption mechanisms know that hackers can observe and or alter the code during execution. Considering these problems we have suggested a novel approach in e-banking system (credit card processing) using white box cryptography to encrypt the key and obfuscation which gives a strong encryption. Combination of these two concepts gives a new level in modern cryptography as well as optimizes its performance and additionally we will make end points (Client and server) secure.
Implementation of White-Box Cryptography in Credit Card Processing Combined with Code Obfuscation

References

- S. Chow, P. Eisen, H. Johnson, P. C. van Oorschot, 16 August 2002, "White-Box Cryptography and an AES Implementation", (SAC'02), Ottawa, Canada.
- Olivier Billet, Henri Gilbert, "Cryptanalysis of a White Box AES Implementation", Charaf Ech-Chatti France T’el’e.com R&D, France, 2009.

Index Terms

Computer Science

Security

Keywords

White-Box cryptography  Credit card  Code obfuscation  White-box attacks