Proposing 3SEMCS- Three Step Encryption Method for Cyber Security in Modern Cryptography

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 139
Number 6

Year of Publication: 2016

Authors:
Manraj Singh, Amit Kumar, Shubham Chuchra, Navreet Kaur, Sajan Dhawan

Abstract

Cyber security is a critical issue now a days in various different domains in different disciplines. This paper presents a review analysis of cyber hacking attacks along with its experimental results and proposes a new methodology 3SEMCS named as three step encryption method for cyber security. By utilizing this new designed methodology, security at highest level will be easily provided especially on the time of request submission in the search engine as like google during client server communication. During its working a group of separate encryption algorithms are used. The benefit to utilize this three step encryption is to provide more tighten security by applying three separate encryption algorithms in each phase having different operations. And the additional benefit to utilize this methodology is to run over new designed private browser named as “RR” that is termed as Rim Rocks correspondingly this also help to check the authenticated sites or phishing sites by utilizing the strategy of passing URL address from phishing tank. This may help to block the phisher sites and user will relocate on previous page. The purpose to design this personnel browser is to enhance the level of security by
Proposing 3SEMCS- Three Step Encryption Method for Cyber Security in Modern Cryptography

sign_in on the time of client server communication that correspondingly reduce the normal attacks on browser based attacks as like Man-In-The-Middle-Attack (MITMA). This new designed private browser may help to provide online security by applying 3-step automatic encryption on path during request movement of google page from the one to the next or ultimately/towards web server by following auto-generated encrypted hash address approach. At end, this rim rocks browser provides tighten security with anti-phishing facility during client server communication.

References

9. Aaron Burstein, Conducting Cyber Security Research Legally and Ethically, School of Law, University of California.
12. Eduard Hovey and David Kepler, A Taxonomy and a knowledge portal for cyber security, US.
13. Fabio Elia, Henry Z.Lo,Joseph P Chen,Ronald S.cheung, Challenge Based Learning in Cyber Security Education ,University of Massachusetts,USA.
18. Cybconf2015.am.gdynia.p1/CYBERSEC.


24. Dr. George and A. Wright, Cyber Security: Designing and Maintaining Resilience, Georgia Technical Research Institute of Cyber Technology and information, Security Laboratory.


33. Salvatore Stolfo, Ramawamy Devarajan and Brian Bowen, Measuring the human factor of cyber security, Columbia University.


40. Tommie Singleton, October-2013. The top 5 Cyber Crime, American Institute of CPA’S.

42. Pekka Vepsalainen and Angeliki Tsocholl, 2014. “Strategic Research Agenda for Cyber Trust, DIGLE.


47. Kruegel Christopher & Kirda Engin, Protecting users against phishing attacks with Antiphish, White paper, Technical University of Vienna.


50. Cranston Christopher, Anti-Phishing as a web based user service, University of Strachlyde, UK.


55. Wolman Alec, Saroin Stefan and Ronda Troy, iTrust Page: A User assisted anti-phishing tool, UK.


59. Wang HAINING AND Yue Chauan, Anti-Phishing is offence & defense. The college of William and Marry.


management and technology.
67. Lee Ju Isug and Ku-Heng Ching, Building a frame based anti-phishing model based on phishing ontology.

Index Terms
Computer Science
Networks

Keywords
hash address, encryption algorithm, Private browser, Search Engine, Index Pointer, Uniform Resource Locator Address, and Internet, cyber-security, law Ethics.