THESIS ABSTRACT

IMAGE ENCRYPTION AND COMPRESSION

Thesis Submitted To
JAMIA MILLIA ISLAMIA
IN FULFILLMENT OF THE REQUIREMENTS OF THE
DEGREE OF

DOCTOR OF PHILOSOPHY
In
Computer Science

By
NAHLA ABBAS FLAYH

DEPARTMENT OF COMPUTER SCIENCE
JAMIA MILLIA ISLAMIA
(A CENTRAL UNIVERSITY)
NEW DELHI -110 025
JULY 2009

Image Encryption and Compression

Scholar:	Supervisor	Co-Supervisor
Nahla Abbas Flayh	Dr. Rafat Parveen	Prof. S.I.Ahson
ICCR Scholarship,	*Asst. professor,*	*Pro-VC Patna University*
Department of	*Department of*	
Computer Science,	*Computer Science,*	
Jamia Millia Islamia	*Jamia Millia Islamia*	

ABSTRACT

In this thesis popular and secure methods of setting up hotspot networks, including Universal Authentication Mechanism (UAM), Port based Authentication (IEEE 802.1x), and (Universal) Subscriber Identity Module ((U) SIM) based authentication have been studied.

The UAM is a web browser based access control method recommended by Wireless Internet Service Provider Roaming (WISPr) forum. The method addresses the problem of roaming users in different Wireless Fidelity (Wi-Fi) hotspots. The method uses the authentication and encryption protocol of Secure Sockets Layer/ Transport Layer Security (SSL/TLS). As the UAM security is based on SSL encryption which in turn is based on Pseudo-Random Number Generators (PRNGs), the PRNG of Linux and Windows is studied in detail. The Linux pseudo-random number generator (LPRNG) is the most popular open source pseudo-random number generator. The LPRNG is part of the kernel of all Linux distributions and is based on generating randomness from entropy of operating system events. The output of this generator is used for almost every security protocol, including TLS/SSL key generation, choosing TCP sequence numbers, and files system and email encryption. The study carried out on LRNG shows that 100% of the sequences generated from /dev/random generator passes the National Institute of Standards and Technology (NIST) test suite and the standard statistical test. However, 30% of these sequences fail to pass tests based on the next-bit theory. It is thus concluded that the random bit strings generated by /dev/random random generator are weak. If a hacker is able to predict few-bits he can potentially recover the key, which can compromise the entire security.

The PRNG used by the Windows operating systems, which is denoted as the WRNG is the most commonly used PRNG. The pseudo-randomness of the output of this generator is crucial for the security of almost any application running on Windows such as the Internet Explorer, and to any application written by independent developers. In this thesis, the WPRNG is examined and the experiments on WPRNG show that the random sequences generated by WPRNG are even weaker than those generated by /dev/random. Fifty five percent of the random sequences generated using WPRG failed to pass the NIST test suite and standards statistical tests. Seventy two percent of the sequences fail in tests based on the next-bit theory such as "A new universal test for bit strings". Therefore, it is concluded that the generator used in windows operating systems is not able to produce quality random sequences, which are essential for the hotspot security.

To overcome the inherent problems of PRNGs, which hamper the hotpot security, the Universal Fuzzy Statistical Test for Pseudo Random Number Generators (UFST-PRNG) Framework and UFST-Test have been proposed. The UFST-PRNG test is based on standard statistical tests, the next-bit test theory, and fuzzy logic. The test has a very useful property that if a random string passes UFST-PRNG, the string will also pass other standard statistical test and tests based on next-bit theory. Thus, the UFST-PRNG may be used as a single test to check the quality of randomness of bit strings.

The UFST-PRNG framework is a model, which uses UFST-PRNG to test the "goodness" of random bits generated by the PRNGs. As the UFST-PRNG framework is able to solve the root problems related to weak random numbers it will definitely help in boosting the security in hotspots environment. It can be equally effective in improving the security of any application which depends on random sequences from operating system.