International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.2, No.II (2009), pp 219-228

STATISTICAL ANALYSIS OF /DEV/RANDOM A, PSEUDORANDOM NUMBER GENERATOR

RAAD A. MUHAJJAR, S. KAZIM NAQVI, NUPUR PRAKASH AND RAFAT PARVEEN

Abstract

It is hard to imagine a well-designed cryptographic application that does not use random numbers [1]. It is essential for generating secret keys and thus any secure application. Inadequate source of randomness can compromise the strongest cryptographic protocol [2]. This paper analyses the /dev/random Pseudo Random Number Generation (PRNG) using standard statistical tests [3] and "A new statistical test for bit strings" [4]. The result shows that although /dev/random PRNG passes the standard statistical test it fails the later test, which is based on "predict or pass test" [5]. The result exposes the weakness of PRNG based on /dev/random usually used in Linux systems.

Keywords: Predict and pass, statistical tests, /dev/random pseudorandom Number Generator, cryptographic.