BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN 2348-0513
Vol. 2, Issue 5, May 2014, 9-14

SOFTWARE AND HARDWARE DEFENSE METHODS AGAINST CACHE-BASED SIDE CHANNEL ATTACKS

DEEVI RADHA RANI[1] & S. VENKATESWARLU[2]

[1]Women Scientist, Department of CSE, KL University Vaddeswaram, Guntur, Andhra Pradesh, India

[2]Mentor, Professor Department of CSE, KL University Vaddeswaram, Guntur, Andhra Pradesh, India

ABSTRACT

Cryptographic algorithms implementing on a cryptographic device leak information through side channels. Cache behavior in modern processors can be used as a side channel and retrieve the key used in cryptographic implementations. Cache based side channel attacks are serious hazard against modern computers with cache memory. This paper surveys the software and hardware defense methods against cache-based side channel attacks and analyze the efficient defense method against cache based side channel attack.

KEYWORDS: Cryptographic Algorithms, Cache Based Side Channel Attack, Software Defense, Hardware Defense