Title	A Clock Skew Replication Attack Detection Approach Utilizing the Resolution of System Time
Author	Komang Oka Saputra, Wei-Chung Teng, and Yi-Hao Chu
Abstract	The clock skew, or the physical ticking rate difference between two digital clocks, has been revealed to have potential on serving as the device fingerprint for identification/authentication purpose. However, it remains as an open issue to detect clock skew replication behavior, which is realized by sending altered timestamps. In this study, it is confirmed that an attacker may fake any target skew with the error being no more than 1ppm in local network environments. Besides, it is also observed that the value of fake timestamps are affected by the time resolution of the attacker's system clock. When the resolution is 1 ms or lower, a relatively large jump between consecutive offsets happens regularly, and the scale of each jump is theoretically the very time resolution of the attacker's system clock. This characteristic is thus adopted to develop a filtering method such that the receiver is able to detect fake timestamps. When the periodical jumps are detected, the filter module abandons these jumps to recover the original clock skew. Experimental results on 15.6 ms and 1 ms time resolutions show that the developed method is effective to detect skew replication attacks, and the errors of the recovered clock skews are no more than 1ppm from the real skews of the attackers.
Keywords	Clock skew, replication attack, time resolution
Pages	211—214
DOI	10.1109/WI-IAT.2015.10
Online link	http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7397459