Cache-Based Side-Channel Attack on AES

R.V. College of Engineering, Bangalore

Sonali Tandon | Srushti S B | Vartika Agrawal

Objectives

- Set up a private cloud environment using OpenStack.
- Demonstrate a cache-based side-channel attack on AES algorithm which uses lookup tables.
- Techniques to mitigate the attack.

Assumptions

- Known-plaintext attack.
- The attacker knows where the lookup tables of the victim VM reside in memory.
- From the reduced group of affected cache sets, the attacker knows exact 16 cache sets affected by AES after permutation.

Experimental Result and Analysis

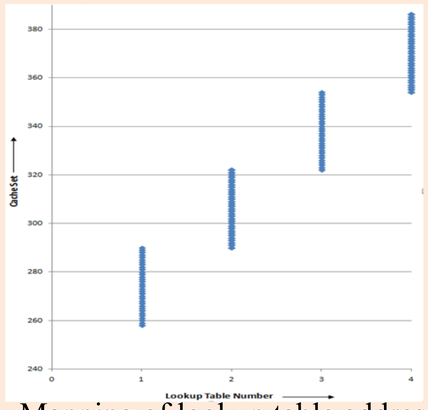

Fig 1. Mapping of lookup table addresses

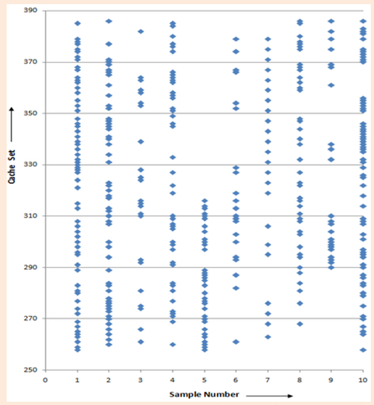

Fig 2. Constant/negative drop in clock cycles

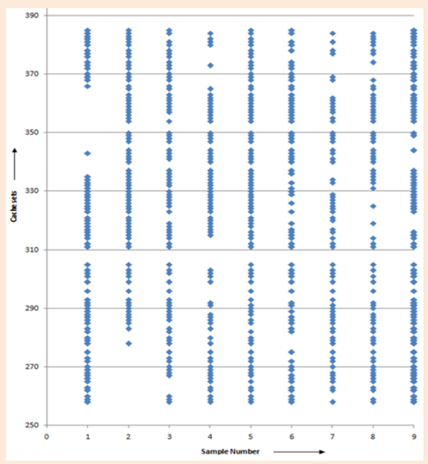

Fig 3. Small Positive Change in clock cycles

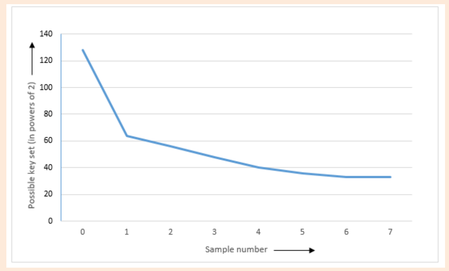

Fig 4. Reduction in possible key set

Setting up Private Cloud

- Open source software, OpenStack.
- The side channel attack is shown among the virtual machines created in this private cloud.
- Compute and Controller nodes.

AES : Cache pattern analysis and Key Extraction

- AES is a symmetric key algorithm.
- Round function vs lookup tables for speed.
- The four lookup tables: t0, t1, t2 and t3 are used in the first round of AES where 16 values of the lookup table corresponding to the 16 indices are accessed.
- From each lookup table maximum of 4 memory accesses are possible in the first round.
- These 16 memory accesses affect a max of 16 cache sets.

Cache Access Pattern Analysis

Attacker creates side channel for communication and waits in a loop for sudden increase in the clock cycle values.

- analyze effect on cache
- mapping of addresses of lookup table indices
- constant or negative drop in clock cycles
- small positive change in clock cycles

Mitigation

- Clearing of the cache before running AES avoids side channel creation.
- Random access of lookup tables which disrupts the cache access pattern.
- Clear cache by doing mathematical operations which do not involve any memory accesses.

Conclusion

- Architecture of the cloud is vulnerable to cache driven side-channel attack.
- During the attack, the possible key sets are reduced from 2^{128} to 2^{33} effectively before brute force to fully recover 128 bit AES key.
- Cache flushing and randomized access to lookup tables avoid the creation of cache based channel.