Jasraj Singh
1/24/2018
jasrajsinghdgn@gmail.com
jsingh20@terpmail.umd.edu

HACS 479 Research Proposal

1. Project Title: Reconstructing private databases via Side Channel Cache attacks
2. Research Objectives:
    - Primary Objective: Design and launch a cache-based side channel attacks
    - Secondary Objective: Run attacks on real data and use reconstruction algorithms to reconstruct databases
    - Hypothesis: Can cache-based side channel attacks launched on SQL execution query be used to reconstruct database.
3. Overview: There are two research papers mainly being used from which Dr. Dachman's team is performing the research. The first paper shapes the theoretical idea behind the research and the main research question has been reduced so that we can use a specific attack to reconstruct database. The first paper listed the idea of how reconstruction of a database can be achieved and also told what piece of information is needed to reconstruct the database. The second paper focuses on the specific attack we are using to reconstruct databases, which is cache-based side channel attack. By using both papers, the team can hopefully reconstruct databases using side channel attack.
4. Student Involvement
    - There are mainly three four people involved in this project
        - Jasraj Singh (Me), Nithin, and Stuart: We are to implement the cache-based attacks and get them to work. Later on if we get good results, we will improve the attacks by trying better database reconstruction algorithms, or try to reduce the noise in the measurements by using basic Machine Learning techniques to reconstruct better than what humans can. Please note that Nithin and Stuart are not part of the ACES program
        - Aria: He is overseeing the work and figuring out the high-level ideas. He is also managing what me and the other team members are doing.
        - Dr. Dana Dachman-Soled: She will serve as my advisor for this experience
5. Methodology:
    - Tools: Writing C code based on prior work and public/open-source work, GDB, and basic Machine Learning techniques
    - We are doing cache attacks (flush and reload; prime and probe) to analyze the security of SQLite database. In order to do this we will be writing C code on Linux machine and also analyze the measurements by using Matlab
6. Project Schedule
    - Getting basic cache-based attack to work
    - Improve attack to work on real data
    - Mid-Semester Report
    - Collecting Data
    - Writing results for publication

Jasraj Singh
1/24/2018
jasrajsinghdgn@gmail.com
jsingh20@terpmail.umd.edu

7. Student Learning Outcomes: C code, GDB, Cache-based attacks, low level programming, statistics, basic Machine Learning.

8. References:

   - *Generic Attacks on Secure Outsourced Databases* by Georgios Kellaris, George Kollios, Kobbi Nissim, and Adam O'Neill
   - *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds* by Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage
   - *Cache Attacks Enable Bulk Key Recovery on the Cloud* by Mehmet Sinan Inci, Berk Gulmezoglu, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar
   - *Flush+Reload: a High Resolution, Low Noise, L3 Cache Side-Channel Attack* by Yuval Yarom, and Katrina Falkner
   - *Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage* by Marie-Sarah Lacharit, Brice Minaud, and Kenneth G. Paterson