Review of

"Hey, you, get off of my cloud:
Exploring information leakage in third-party compute clouds"

HT. Ristenpart, E. Tromer, H. Shacham, and S. Savage

IN PROCEEDINGS OF THE 16TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PP. 199-212.

Denny Stohr

University of Auckland

August 21, 2012

Summary

- The paper presents the practicability of cross-VM attacks on the example of Amazon EC2.
- The authors examined the following subtasks:
    - Methods mapping the infrastructure of cloud computing providers and achieving placement on the same physical server allowing cross-VM attacks
    - Possible side channel attacks and usage measurements using this placement

Appreciation

Positive aspects:

- ► The paper shows that public cloud computing enables attackers to exploit the confidentiality of customers by being assigned on the same physical hardware using side channel attacks.
- ► According to the example scenario, getting assigned to the same physical hardware could be achieved at low cost and with easy methods.

Appreciation

Negative aspects:

- Attacks aiming on the actual leakage of data (such as cryptographic keys) haven't been demonstrated.
- The successful usage of other attacks suggested to be used in cross-VM settings could not be proved on Amazon EC2.
  - Keystroke measurement was only tested in a local simulated cloud computing environment.

Question

As a result of their research, the authors claim that the *best* solution to tackle these risks is to give users more direct placement control when they launch instances.
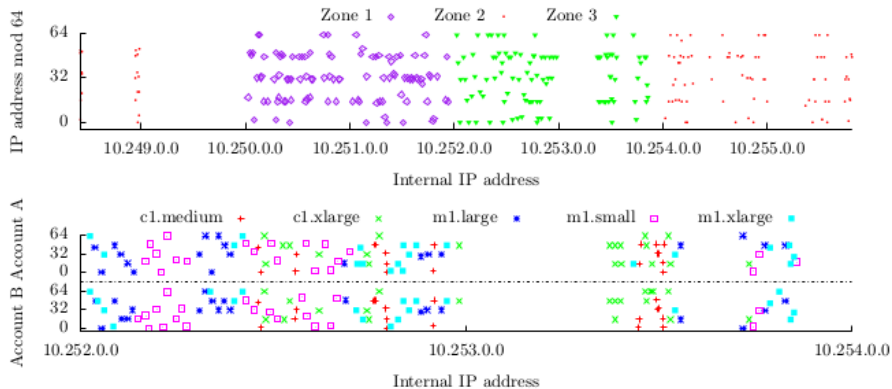
- ▸ Does this really solve the problem?

Appendix

Figure: Map of Amazon EC2 Cloud Computing Servers