On the Power of Simple Branch Prediction Attacks

Onur Acıičmez

Çetin Koç

Jean-Pierre Seifert

Presented by Shay Gueron
Branch Prediction Attacks

• Recent software side channel attack (2006)
• Exploit a performance optimization feature in CPUs

• BPA uses
  – Information leak via penalty for a mispredicted branch

• BPA does
  – Unprivileged process (spy) can attack processes (crypto) running in parallel on same processor.
  – Works despite of sophisticated partitioning/protection methods such as memory protection, sandboxing, virtualization, etc.
Simple Branch Prediction Attacks

• BPA
  – Uses many execution-time measurements to statistically amplify some small but key-dependent timing differences

In contrast- Simple BPA (SBPA)
  – A carefully written spy-process running simultaneously with an RSA-process, is able to collect almost all of the secret key bits during single RSA signing execution
  – SBPA attacks on RSA/ECC cannot be mitigated by randomization or blinding techniques!
Implications of SBPA

• The bad news
• In the presence of SBPA attacks
  – The very recent countermeasures to protect the open SSL 0.9.8 RSA implementation against cache based side-channel attacks are useless.
  – Blinding and randomization techniques to protect RSA against side-channel attacks are also useless.
  – Other implications as well
• The good news
  – The paper(s) with the new results, by Acıičmez, Koç, and Seifert, will be published soon, and will be subsequently followed by a paper of Onur Acıičmez, Shay Gueron, Cetin Koç, and Jean-Pierre Seifert on proper mitigations for openSSL.