RUMP SESSION CRYPTO 2006

A Preview on Branch Misprediction Attacks:

Using Pentium Performance Counters to reduce the Complexity of Timing Attacks

Alexander A. Veith
a.a.veith@in-sed.com
InSED RESEARCH
Institute of Social and Economical Development

Andrei V. Belenko
abelenko@elcomsoft.com
ElcomSoft Co. Ltd.

This Presentation is available at http://dissar.in-sed.com/downloads

Introduction

- At CHES 2005, in Edinburgh (Scotland), after the conference, a very passionate discussion was held in a pub (around pints of beer) on **modern processor architecture and its weaknesses** between
  - J.P.SEIFERT (Intel)
  - D. SAMYDE (Rfi)
  - A.A.VEITH (InSED RESEARCH)

- SEIFERT focused his topic on cache attacks but asked for new ideas.
- SAMYDE suggested **branch prediction** on modern architectures

- ONE YEAR LATER: No known publication on this idea and no information from either side, so we try to put the idea into practice!

What is Branch Prediction ?

- Definition from Wikipedia:
  - In computer architecture, a **branch predictor** is the part of a processor that determines whether a conditional branch in the instruction flow of a program is likely to be taken or not. This is called **branch prediction**. Branch predictors are crucial in today's modern, superscalar processors for achieving high performance. They allow processors to fetch and execute instructions without waiting for a branch to be resolved.

- **Main Question: What can we exploit if the prediction goes wrong?**

Performance vs. Security

- B.P. is used to fill the command-pipeline in order to obtain high performance (basically)
- **Problem:** If prediction is false, the pipeline-content must be flushed
  - Performance Impact: It takes time to empty the pipeline and refill it with the correct branch. This means suspending the pipeline for some instructions for some or more clock cycles. A Stall delays all instructions after the instruction that was stalled
- Performance Counters may help monitor the performance too
  - Ex. P4: 160-180 stall cycles (!)
  - These counters are also available since the Pentium 60 / Pentium 90

A simple Timing Attack

- Two Processes running on a server
  - Process A: SSL (Banking)
  - Process B: Spy (Monitoring Performance Counters)
- Process B sends plaintext to Process A and monitors the performance of the "Square 'n Multiply" on asymmetric crypto.
- Knowing the Prediction Rules, just apply a practical implementation of the timing attack

$$Power(x,n) = \begin{cases} x, & \texttt{IF n=1} \\ Power(x^2, n/2), & \texttt{IF n is even} \\ x \cdot Power(x^2, (n-1)/2), & \texttt{IF n>2 is odd} \end{cases}$$

Results (for now…)

- This **Side-Channel Attack** is very dangerous for asymmetric crypto (conditional branches)
- It seems possible to defeat some **cache attack** countermeasures using this Branch Prediction Attack
- Simple Software, easy to implement, works in real life on modern chips