Automatic Software Patching against Microarchitectual Attacks

PennState

Background:

- Microarchitectural attacks leverage secret-dependent footprints in the CPU's microarchitectural state to steal confidential information
- High impact microarchitectural attacks such as Spectre and Meltdown attacks.

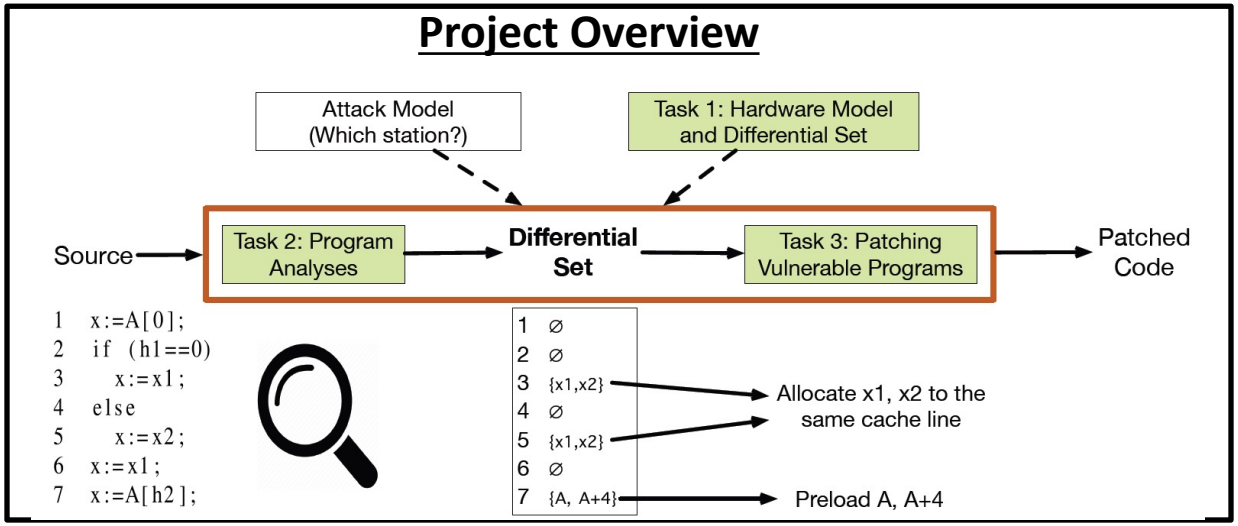
Challenge:

- Secure hardware designs can hardly be adopted in a close future
- Software-based solutions are not comprehensive and few of them automatically fix vulnerabilities

Solution:

- Differential set: a novel interface that defines security against microarchitectural attacks and guides automatic patching
- Station model: an abstraction that allows efficient and comprehensive control of microarchitectural attacks in memory systems

Project Overview



Scientific Impact:

- Automatic software patching system against microarchitectural attacks without modifying the OS or hardware
- The success of the project will lead to a more secure and trustworthy cyberspace

Broader Impact and Broader Participation:

- Integrated research and educational activities
- Involvement of students from under-represented groups

NSF Award # 1956032

Pis: Danfeng Zhang, Gang Tan, Dinghao Wu, Mahmut Kandemir

Institute: Penn State University