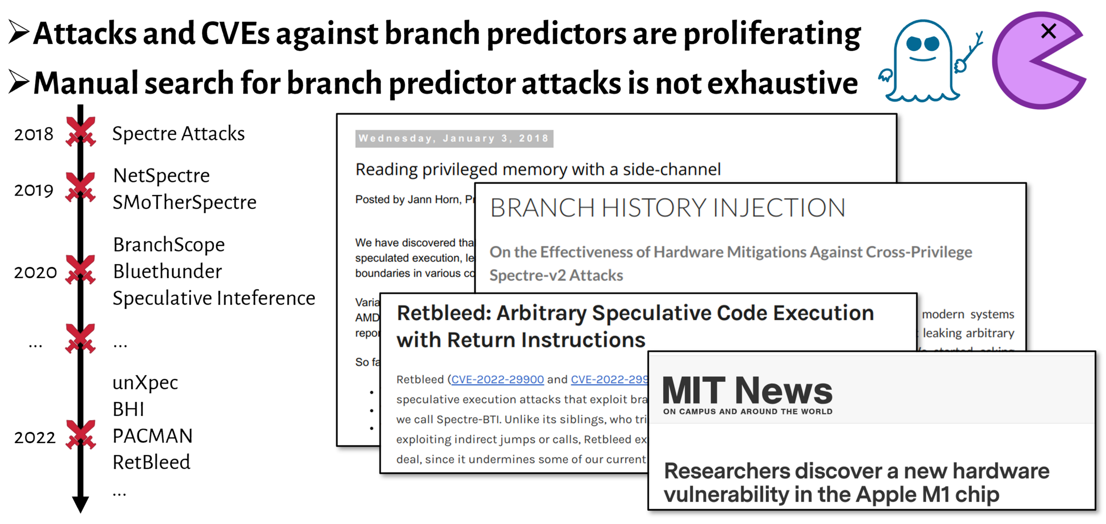
Modeling, Derivation, and Automated Analysis of Branch Predictor Security Vulnerabilities

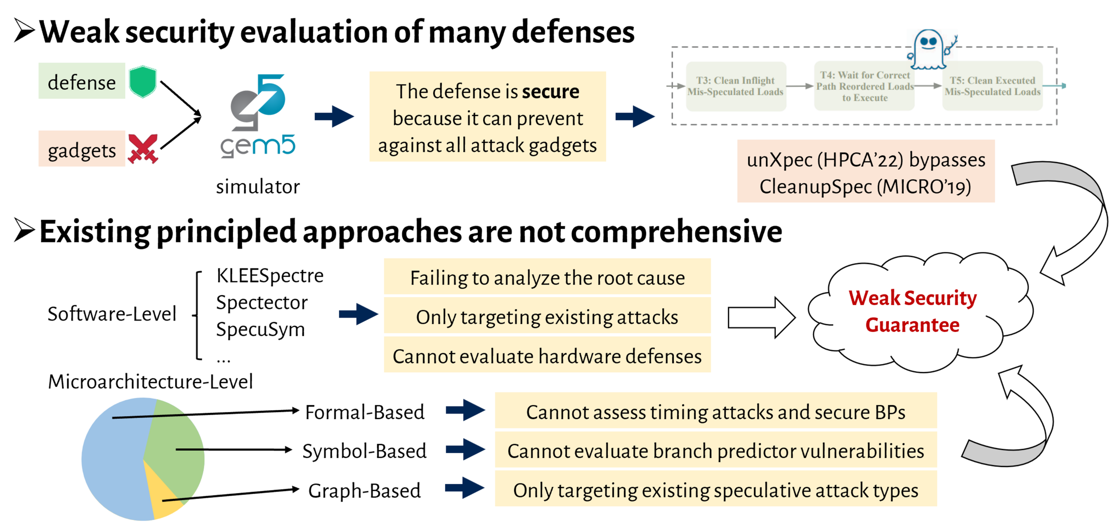
Quancheng Wang, Ming Tang, Ke Xu, Han Wang
Wuhan University

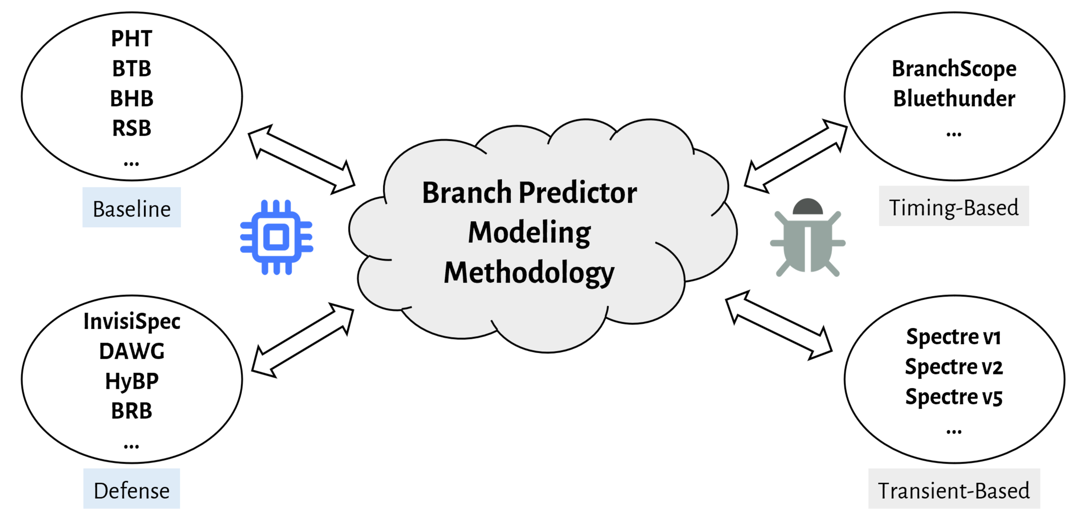
Introduction

With the intensification of microarchitectural side-channel attacks targeting branch predictors, the security boundary of computer systems and users' security-critical data are under serious threat. Since the root cause of these attacks is the neglect of security issues in the microarchitecture design of branch predictors, an analysis framework that can exhaustively and automatically explore these concerns in the design phase is imminent. In this paper, we propose a comprehensive and automated evaluation framework for inspecting the security guarantees of branch predictors at the microarchitecture design stage. Our technique involves a three-step modeling approach that abstractly characterizes 19 branch predictor states and 53 operations that could affect these states. Subsequently, we develop a symbolic execution-based framework to investigate all three-step combinations and derive 156 valid attack patterns against branch predictors, including 89 novel attacks never considered in the previous work. Finally, we apply our framework to 8 secure branch predictor designs and four typical hardware-based countermeasures against speculative execution attacks to evaluate their security capabilities. The result demonstrates that these security branch predictors provide efficient security guarantees and outperform those hardware-based alleviations against speculative execution attacks, indicating that the security branch predictors are promising in mitigating branch predictor security vulnerabilities.

Motivation and Goal







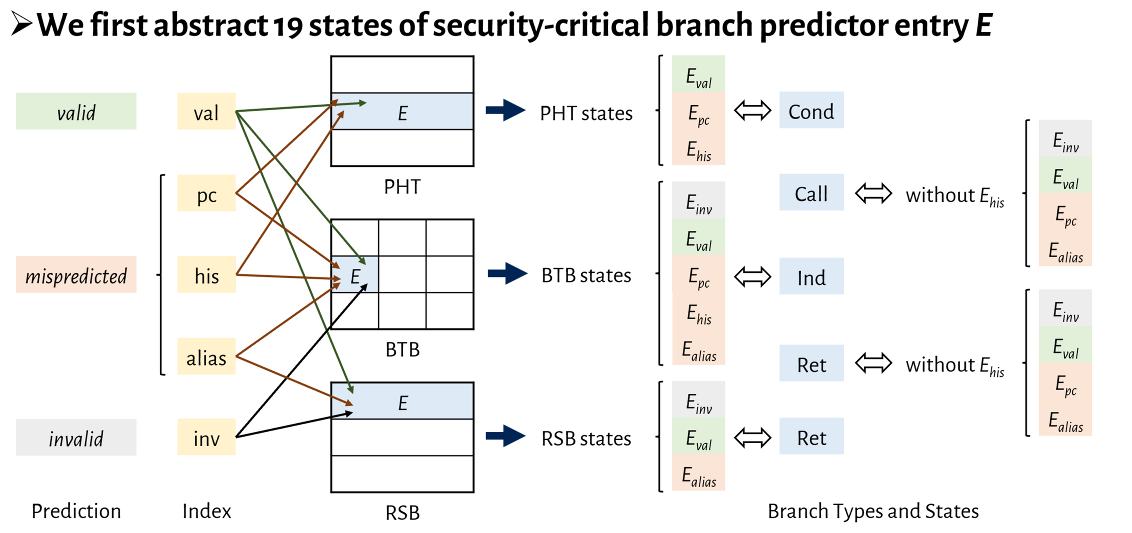
Goal: A novel branch predictor modeling method that can **1) exhaustively analyze security vulnerabilities** and **2) comprehensively evaluate secure defenses**.

Challenge: This modeling methodology should **1) cover key branch predictor components with sound extensibility to secure design; 2) be capable of analyzing both the timing-based attacks and the transient-based attacks.**

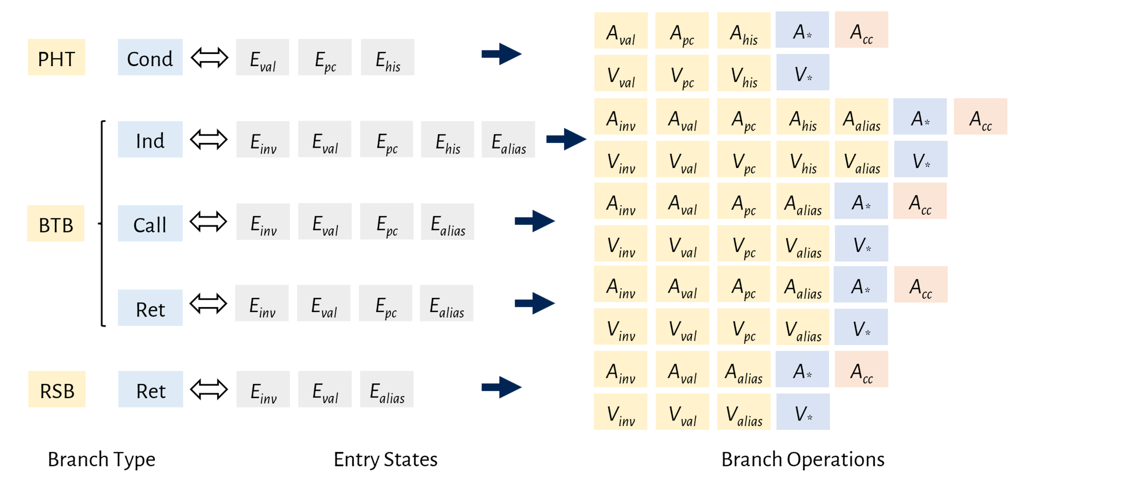
Methodology and Result

1 **Modeling** 19 branch predictor states and 53 operations of the attacker and victim that could affect these states

➢ **We first abstract 19 states of security-critical branch predictor entry E**

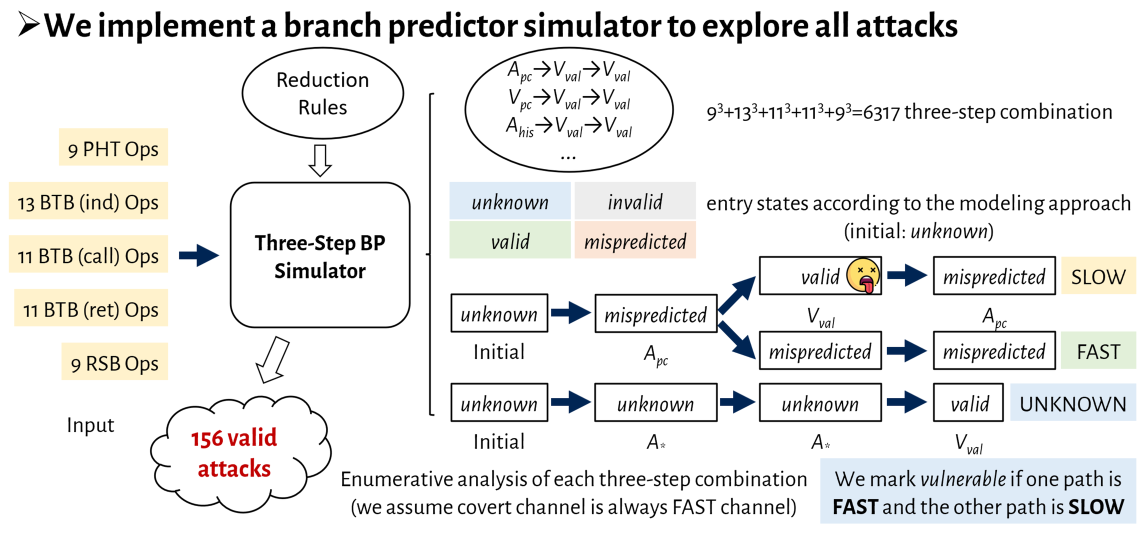


➢ **We then model 53 possible operations in the three-step attack model**



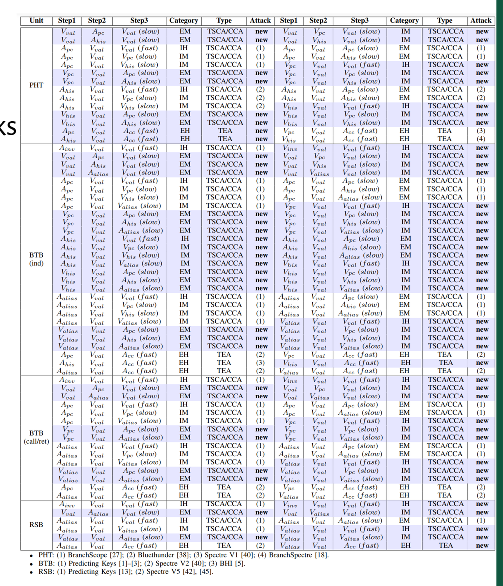
2 **Derivation** of 156 valid three-step attack patterns against branch predictors, with 89 novel attacks never discovered

➢ **We implement a branch predictor simulator to explore all attacks**



➢ **We finally derive 156 valid attack patterns**
➢ 28 PHT attacks, 116 BTB attacks and 12 RSB attacks
➢ 67 known attacks and 89 novel attacks

Branch Predictor	Known Attacks	Novel Attacks	Total Attacks
PHT	12	16	28
BTB (ind)	20	36	56
BTB (call)	15	15	30
BTB (ret)	15	15	30
RSB	5	7	12
Total	67	89	156



3 **Analysis** of 8 existing secure branch predictor designs and 4 typical hardware defenses against speculative attacks

➢ **Secure branch predictor evaluation for all 156 three-step attacks**
➢ PSC and HyBP are the most effective secure branch predictors for mitigating PHT and BTB security vulnerabilities under ideal circumstances
➢ The best-performing HyBP can shield about 79% of the attack patterns
➢ The worst-performing MI6 and BRB can only cover about 16% of the attack patterns

Secure BP	PHT	BTB (ind)	BTB (call)	BTB (ret)	RSB	Total
Lock-Based BTB	28/28	19/56	11/30	11/30	5/12	74/156
MI6	10/28	56/56	30/30	30/30	5/12	131/156
BRB	10/28	56/56	30/30	30/30	5/12	131/156
Two-Level Encryption	18/28	12/56	2/30	2/30	5/12	39/156
Noisy-XOR-BP	18/28	12/56	2/30	2/30	5/12	39/156
PSC (ideal)	0/28	56/56	30/30	30/30	5/12	121/156
LS-BP	18/28	12/56	2/30	2/30	5/12	39/156
HyBP	18/28	10/56	0/30	0/30	5/12	33/156

➢ **Secure branch predictor evaluation for known/new attacks**
➢ HyBP provides the best protection against known and newly derived attacks
➢ Two-Level Encryption, Noisy-XOR-BP, and LS-BP have better protection coverage
➢ Lock-Based BTB has significant omissions for newly derived attacks
➢ MI6 and BRB do not adequately protect against known and newly derived attacks

Secure BP	PHT (known)	BTB (known)	RSB (known)	PHT (new)	BTB (new)	RSB (new)
Lock-Based BTB	12/12	6/50	0/5	16/16	35/66	5/7
MI6	2/12	50/50	0/5	8/16	66/66	5/7
BRB	2/12	50/50	0/5	8/16	66/66	5/7
Two-Level Encryption	5/12	7/50	0/5	9/16	35/66	5/7
Noisy-XOR-BP	5/12	7/50	0/5	9/16	35/66	5/7
PSC (ideal)	0/12	50/50	0/5	0/16	66/66	5/7
LS-BP	5/12	7/50	0/5	9/16	35/66	5/7
HyBP	5/12	4/50	0/5	13/16	6/66	5/7

Conclusion

- ➢ We propose a three-step modeling approach for evaluating the security properties of branch predictors at the design stage.
- ➢ We develop a comprehensive and automated framework to derive 156 effective attack patterns, with 89 novel attacks never discovered.
- ➢ We conduct security analysis of 8 existing secure branch predictor designs and 4 typical hardware defenses against speculative attacks.
- ➢ Results shows that secure branch predictors are promising solutions in preserving the confidentiality and integrity of computer systems.

Artifact and Open-Source

Rust Linux

Archival: https://doi.org/10.5281/zenodo.10297402
Latest: https://github.com/iamywang/bp-security-framework

Contact

Web: http://csccl.whu.edu.cn
E-Mail: wangquancheng@whu.edu.cn
GitHub: https://github.com/iamywang