Branch Privilege Injection

S. Rüegge, J. Wikner, K. Razavi

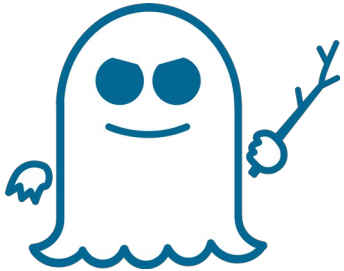
ETH zürich | COMSEC

Executive Summary

Executive Summary

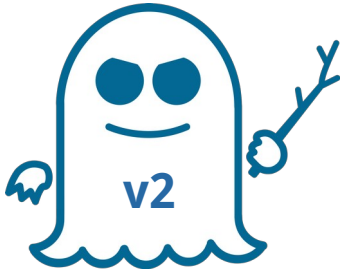
Executive Summary

Executive Summary



2018

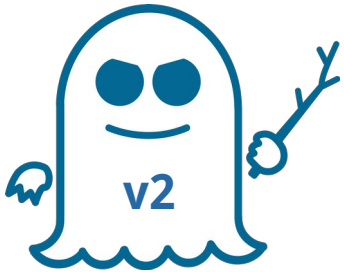
Executive Summary



2018

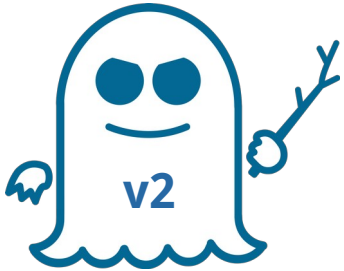
Executive Summary

call

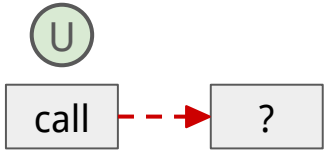


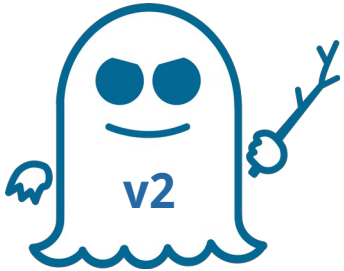
2018

Executive Summary

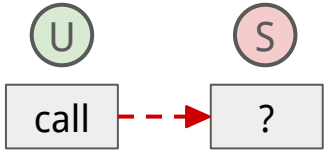


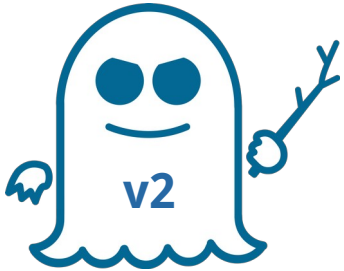
Executive Summary





Executive Summary

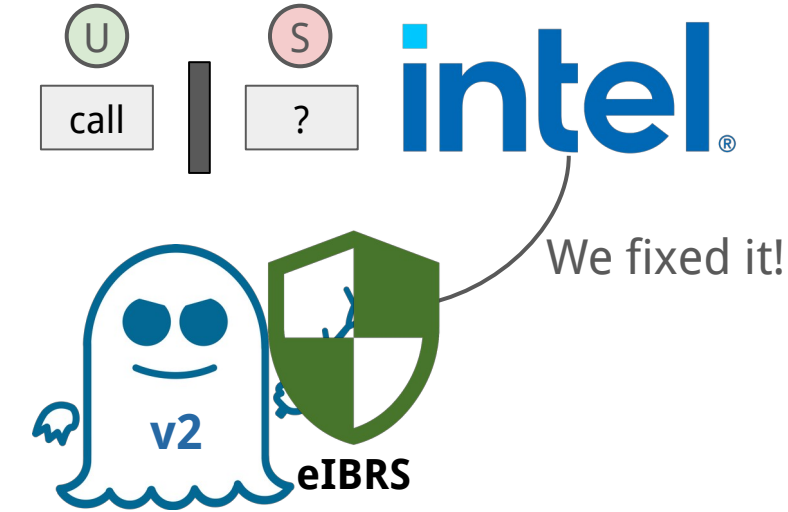




Executive Summary

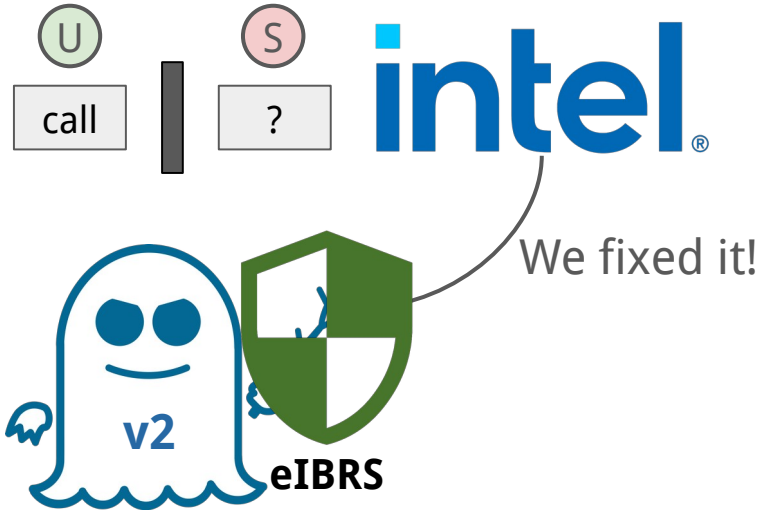
Executive Summary

Executive Summary

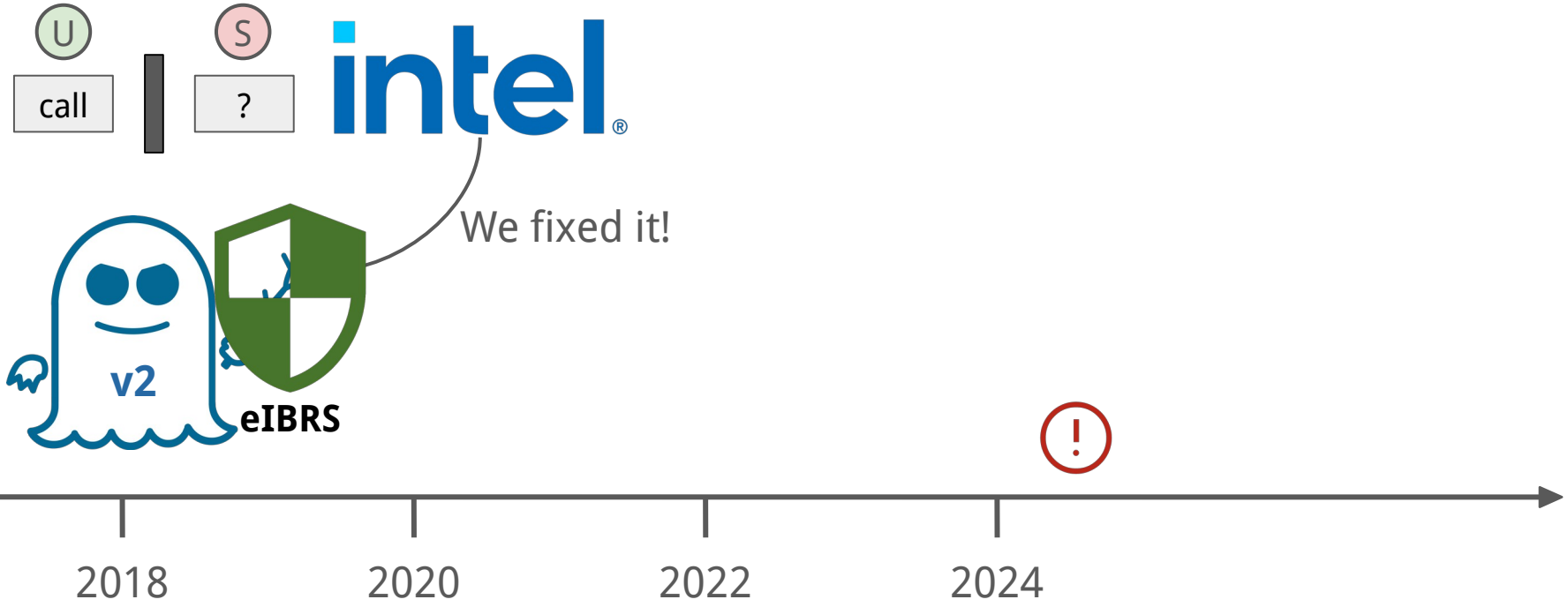


2018

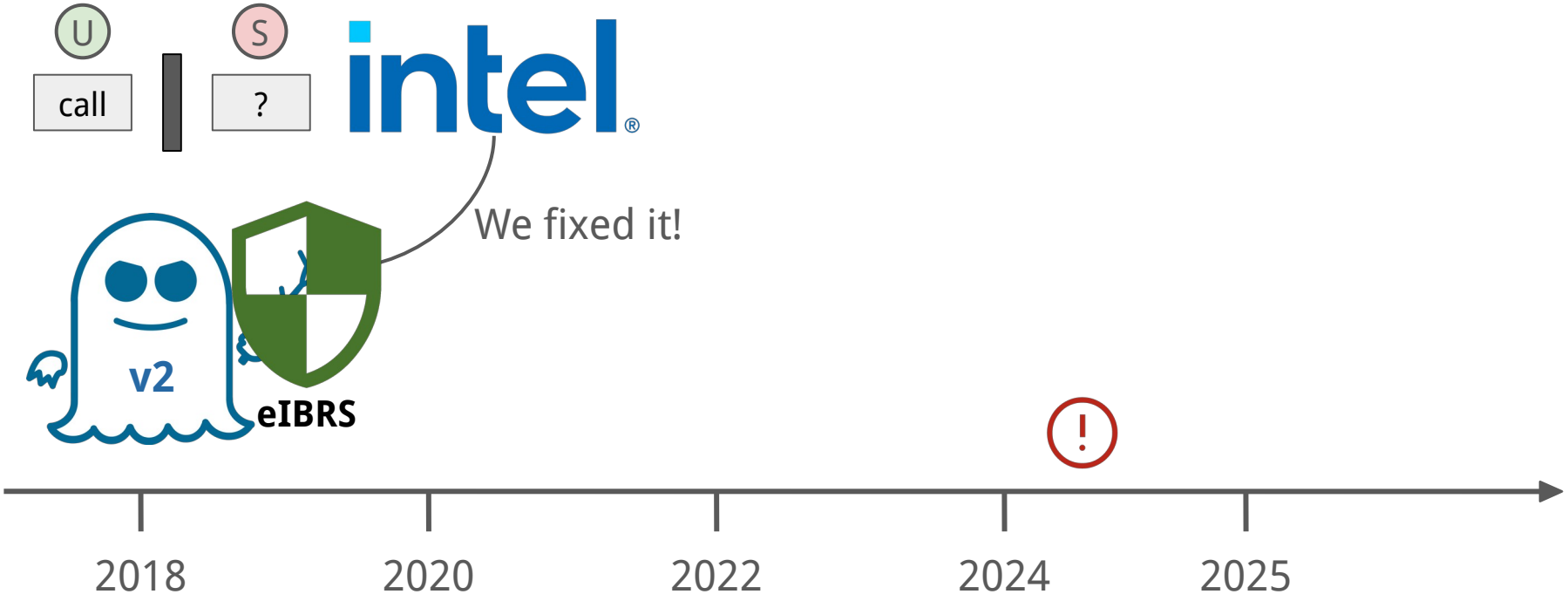
Executive Summary



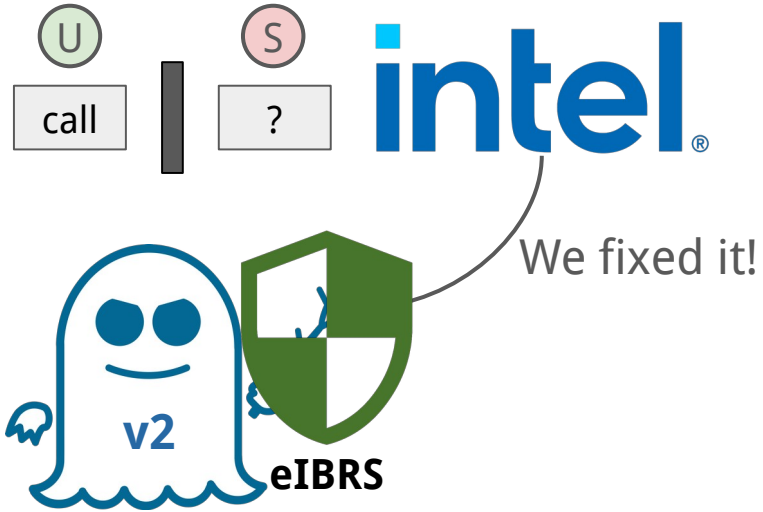
Executive Summary

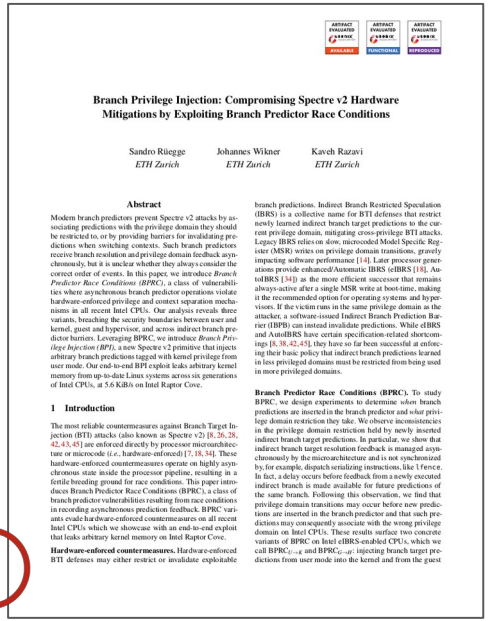


Executive Summary



Executive Summary





Branch Privilege Injection: Compromising Spectre v2 Hardware Mitigations by Exploiting Branch Predictor Race Conditions

Sandro Rüegge, Johannes Wikner, Kaveh Razavi
ETH Zurich

Abstract

Modern branch predictors prevent Spectre v2 attacks by associating predictions with the privilege domain they should be restricted to, or by providing barriers for invalidating predictions when switching contexts. Such branch predictors receive branch resolution and privilege domain feedback asynchronously, but it is unclear whether they always consider the correct order of events. In this paper, we introduce *Branch Predictor Race Conditions (BPRC)*, a class of vulnerabilities where asynchronous branch predictor operations violate hardware-enforced privilege and context separation mechanisms in all recent Intel CPUs. Our analysis reveals three variants, breaching the security boundaries between user and kernel, guest and hypervisor, and across indirect branch predictor barriers. Leveraging BPRC, we introduce *Branch Privilege Injection (BPI)*, a new Spectre v2 primitive that injects arbitrary branch predictions tagged with kernel privilege from user mode. Our end-to-end BPI exploit leaks arbitrary kernel memory from up-to-date Linux systems across six generations of Intel CPUs, at 5.6 KiB/s on Intel Raptor Cove.

1 Introduction

The most reliable countermeasures against Branch Target Injection (BTI) attacks (also known as Spectre v2) [8, 26, 28, 42, 43, 45] are enforced directly by processor microarchitecture or microcode (*i.e.*, hardware-enforced) [7, 18, 34]. These hardware-enforced countermeasures operate on highly asynchronous state inside the processor pipeline, resulting in a fertile breeding ground for race conditions. This paper introduces Branch Predictor Race Conditions (BPRC), a class of branch predictor vulnerabilities resulting from race conditions in recording asynchronous prediction feedback. BPRC variants evade hardware-enforced countermeasures on all recent Intel CPUs which we showcase with an end-to-end exploit that leaks arbitrary kernel memory on Intel Raptor Cove.

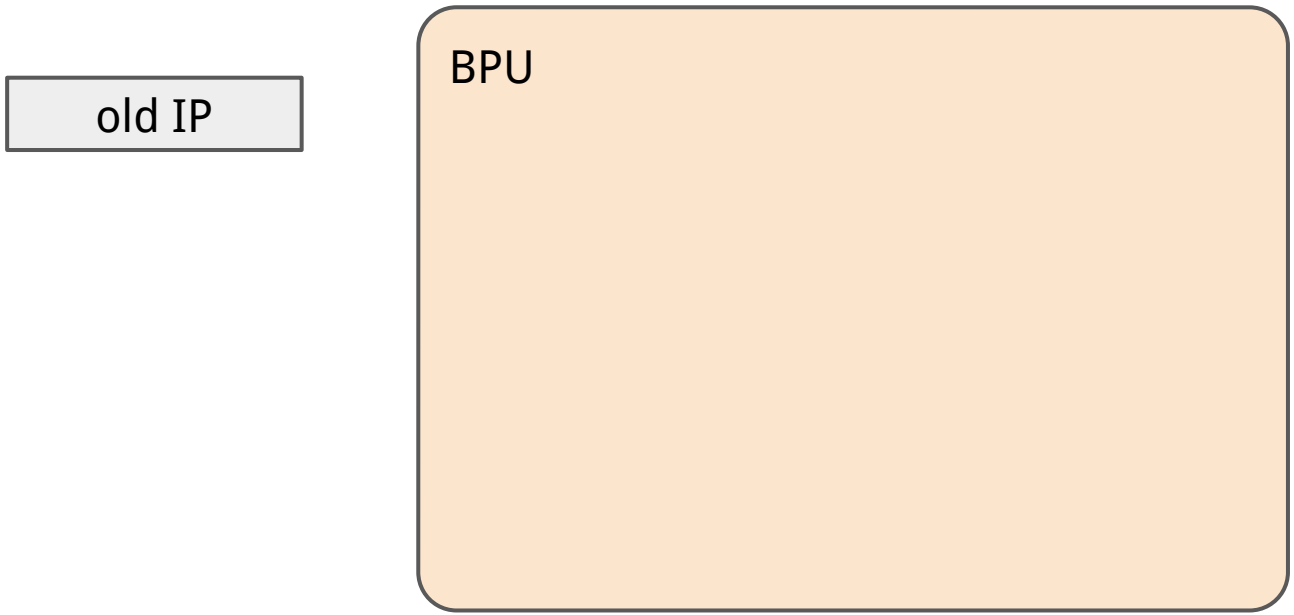
Hardware-enforced countermeasures. Hardware-enforced BTI defenses may either restrict or invalidate exploitable branch predictions. Indirect Branch Restricted Speculation (IBRS) is a collective name for BTI defenses that restrict newly learned indirect branch target predictions to the current privilege domain, mitigating cross-privilege BTI attacks. Legacy IBRS relies on slow, microcoded Model Specific Register (MSR) writes on privilege domain transitions, gravely impacting software performance [14]. Later processor generations provide enhanced/Automatic IBRS (eIBRS [18]. AutoIBRS [34]) as the more efficient successor that remains always-active after a single MSR write at boot-time, making it the recommended option for operating systems and hypervisors. If the victim runs in the same privilege domain as the attacker, a software-issued Indirect Branch Prediction Barrier (IBPB) can instead invalidate predictions. While eIBRS and AutoIBRS have certain specification-related shortcomings [8, 38, 42, 45], they have so far been successful at enforcing their basic policy that indirect branch predictions learned in less privileged domains must be restricted from being used in more privileged domains.

Branch Predictor Race Conditions (BPRC). To study BPRC, we design experiments to determine *when* branch predictions are inserted in the branch predictor and *what* privilege domain restriction they take. We observe inconsistencies in the privilege domain restriction held by newly inserted indirect branch target predictions. In particular, we show that indirect branch target resolution feedback is managed asynchronously by the microarchitecture and is not synchronized by, for example, dispatch serializing instructions, like `lfence`. In fact, a delay occurs before feedback from a newly executed indirect branch is made available for future predictions of the same branch. Following this observation, we find that privilege domain transitions may occur before new predictions are inserted in the branch predictor and that such predictions may consequently associate with the wrong privilege domain on Intel CPUs. These results surface two concrete variants of BPRC on Intel eIBRS-enabled CPUs, which we call $\text{BPRC}_{U\to K}$ and $\text{BPRC}_{U\to U}$: injecting branch target predictions from user mode into the kernel and from the guest

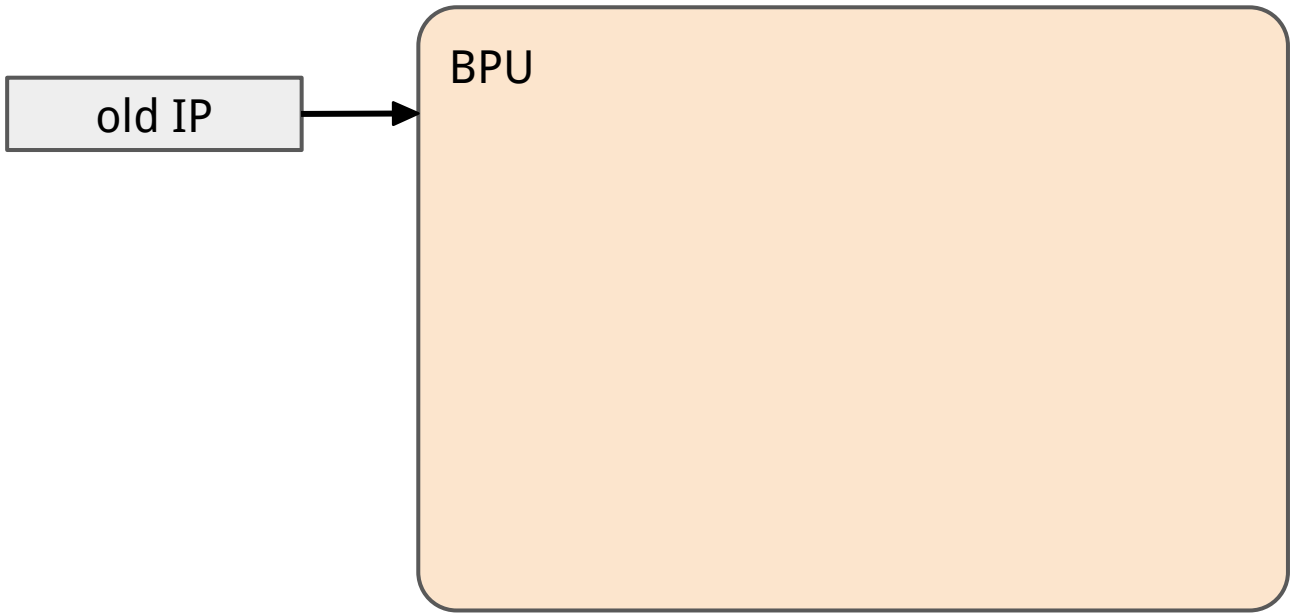
Branch Prediction Unit

Branch Prediction Unit

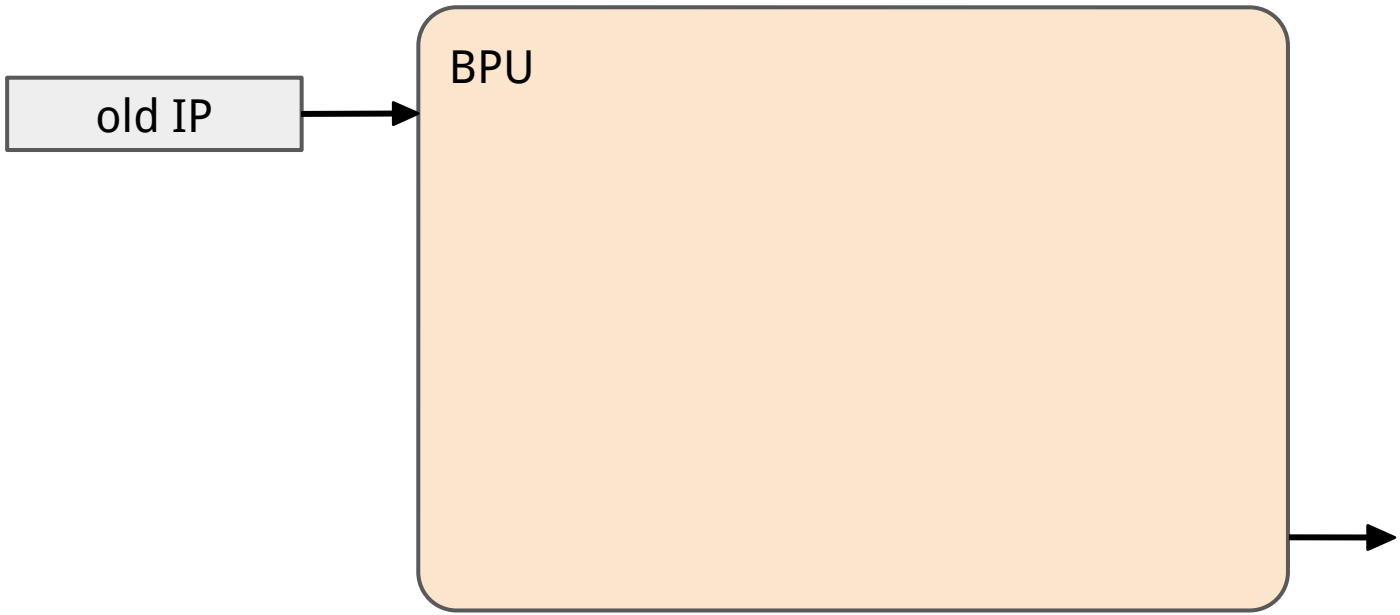
Branch Prediction Unit



Branch Prediction Unit

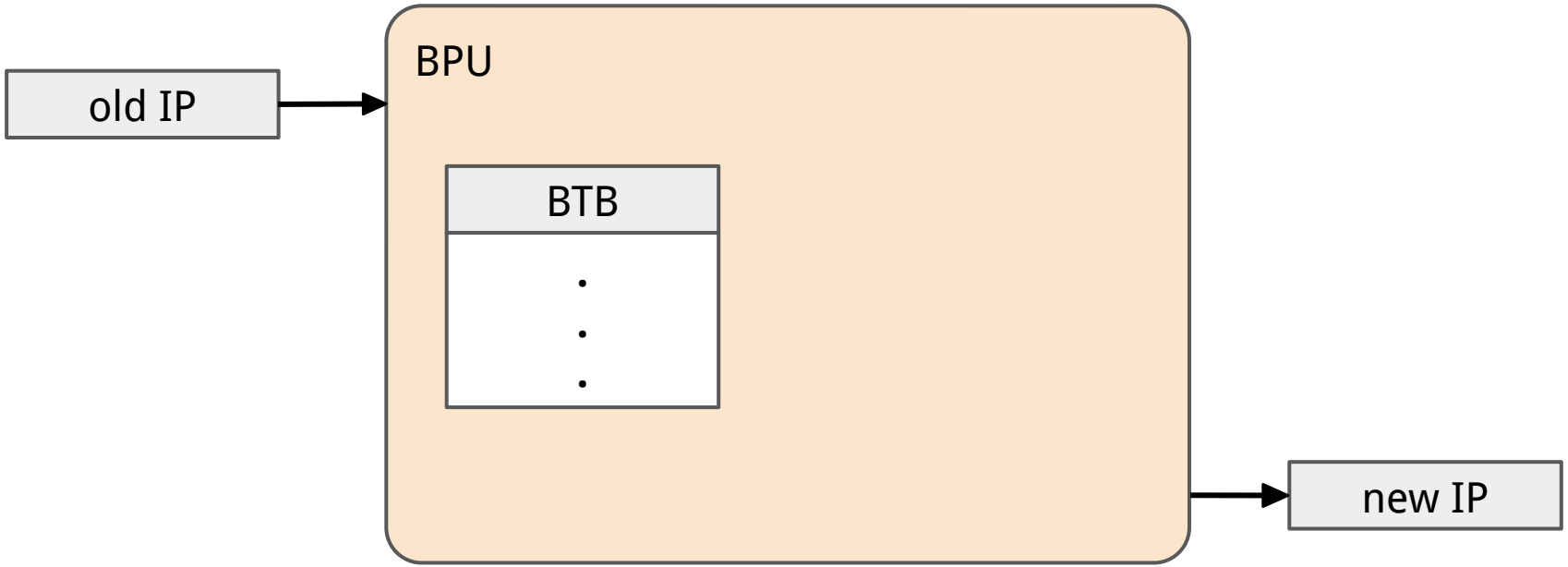


Branch Prediction Unit

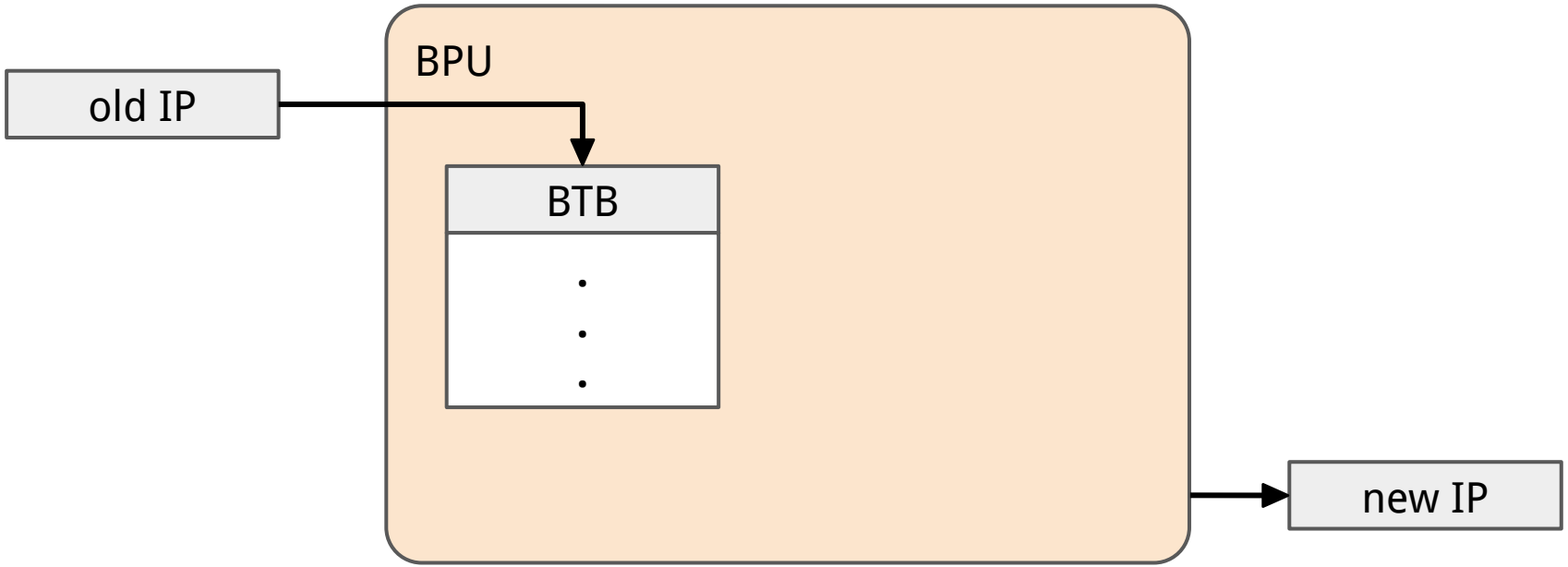


Branch Prediction Unit

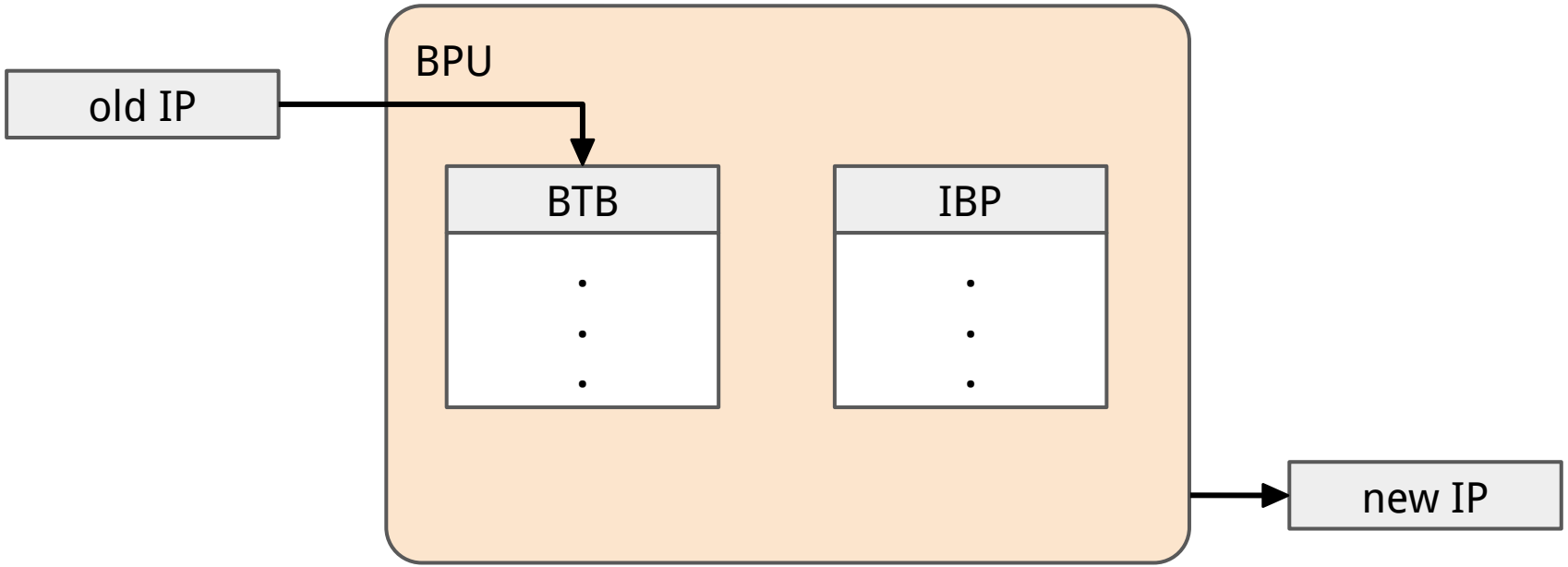
Branch Prediction Unit



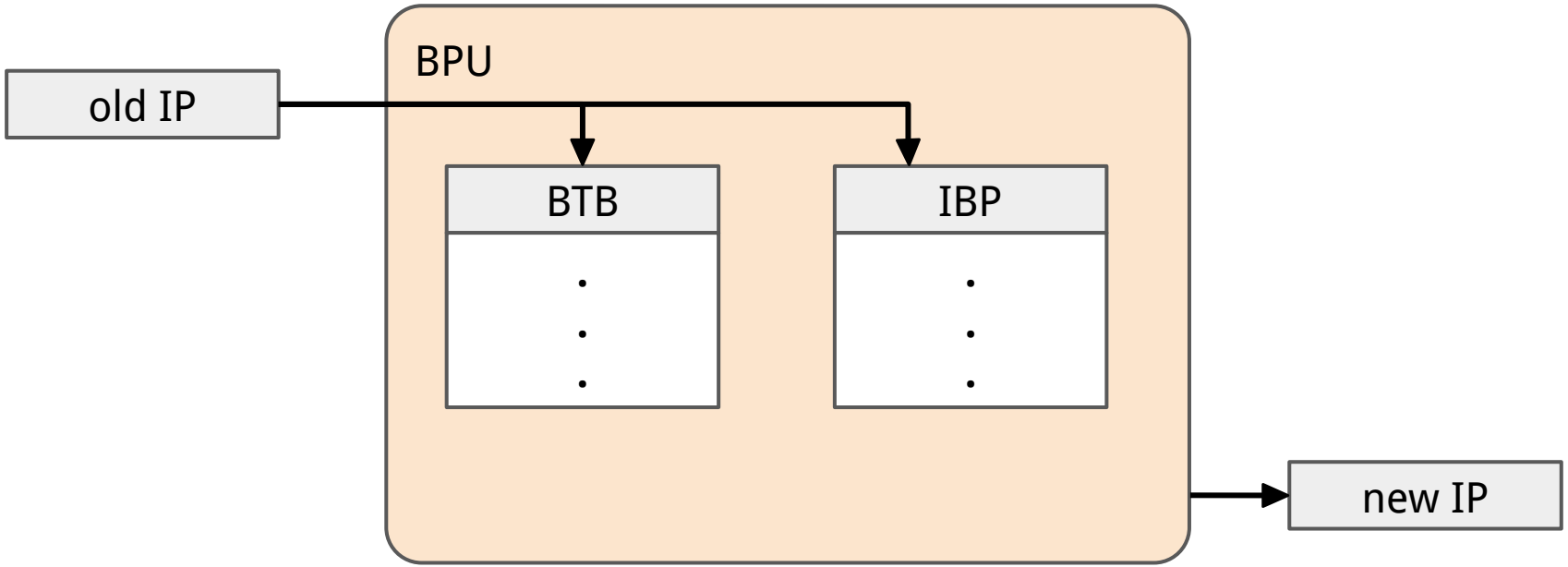
Branch Prediction Unit



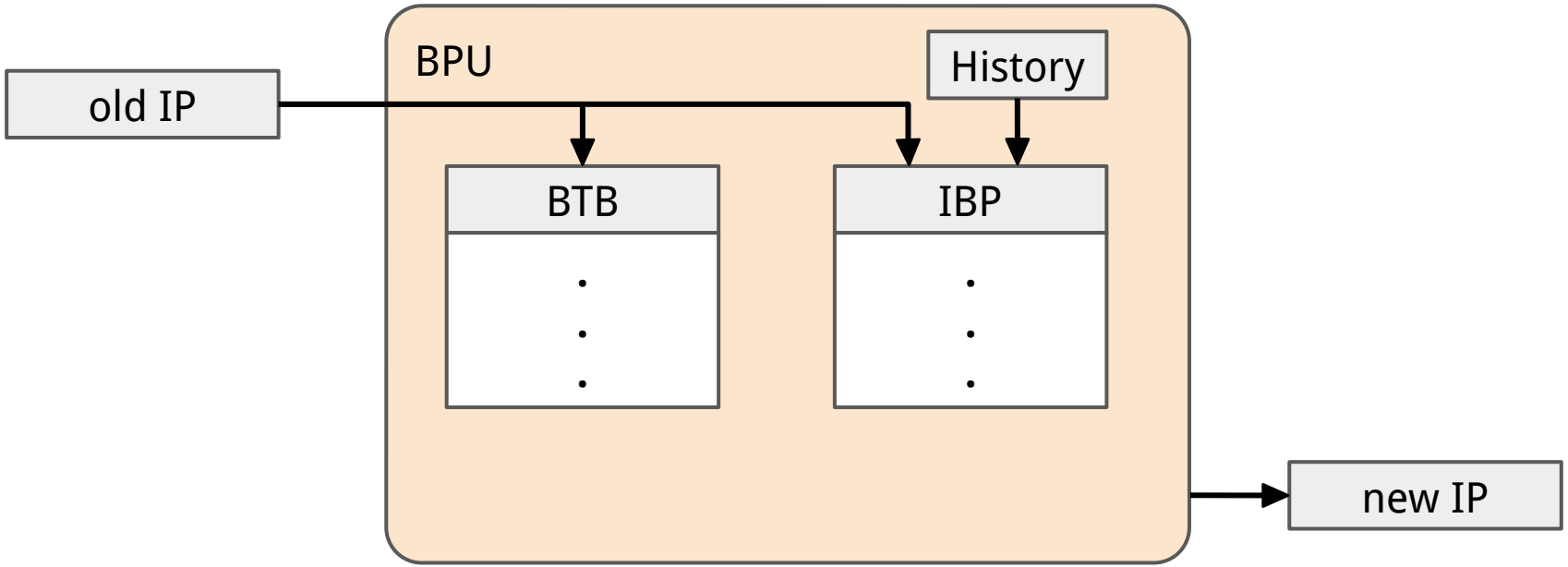
Branch Prediction Unit



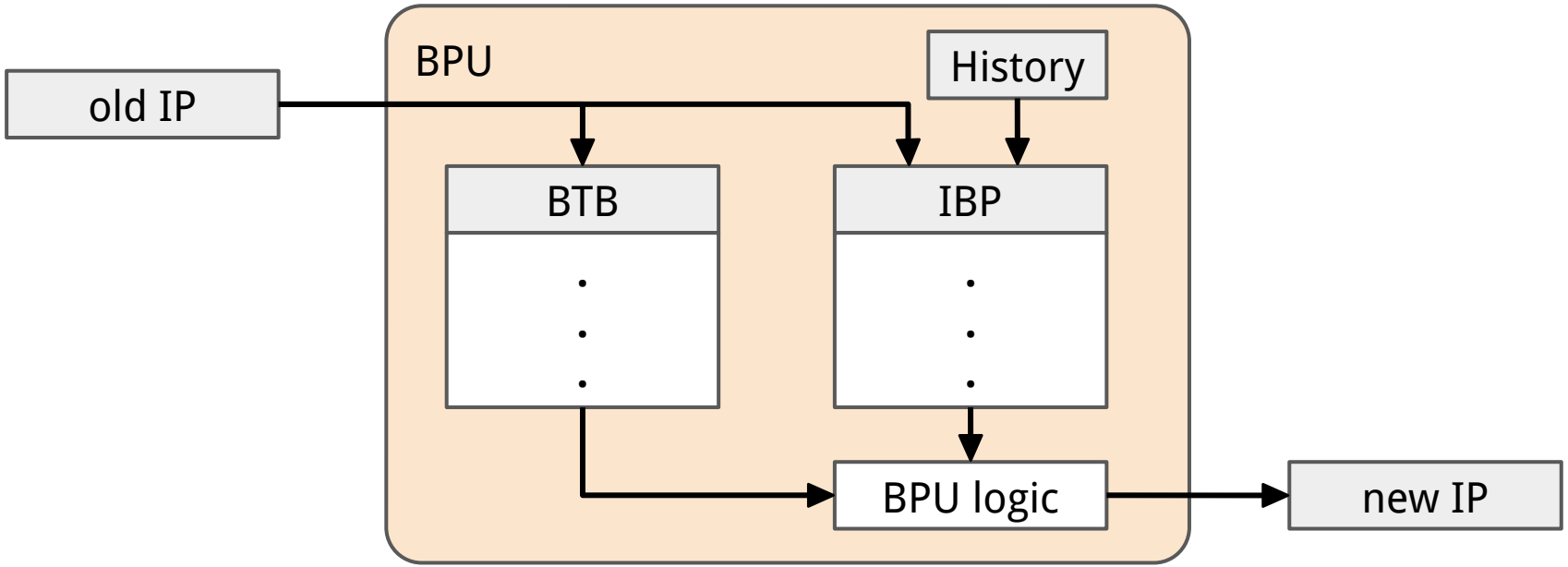
Branch Prediction Unit



Branch Prediction Unit

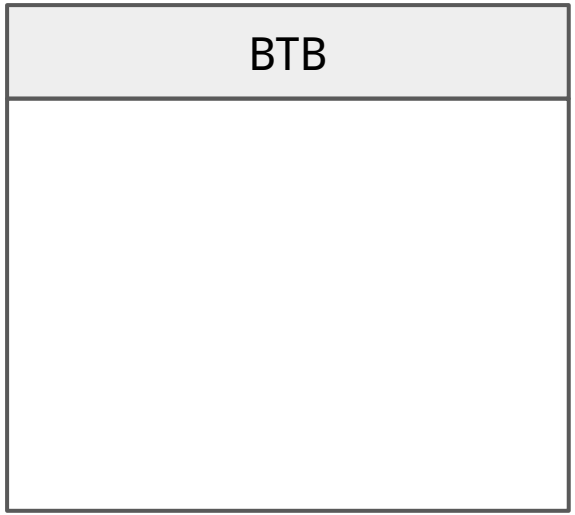


Branch Prediction Unit

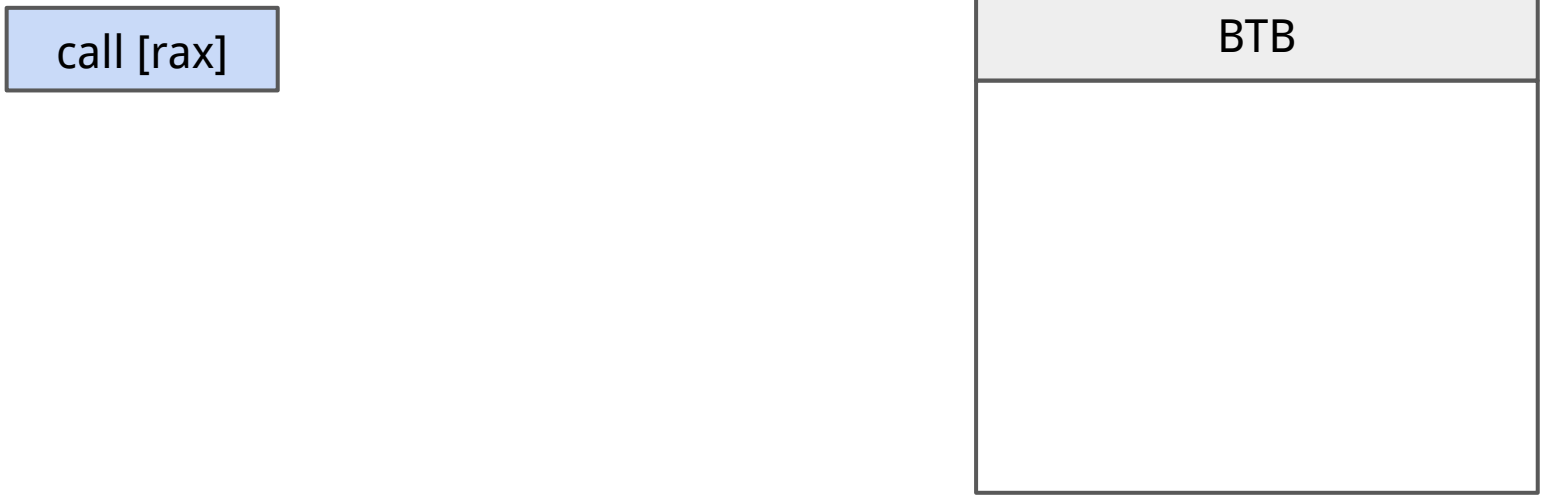


Spectre v2

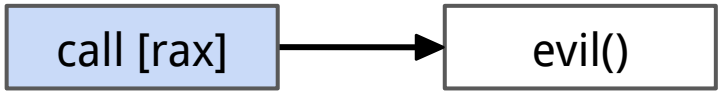
Spectre v2

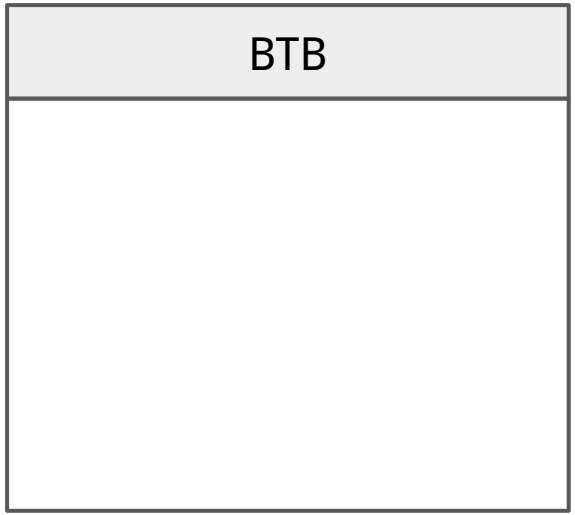


Spectre v2

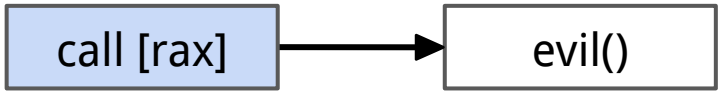


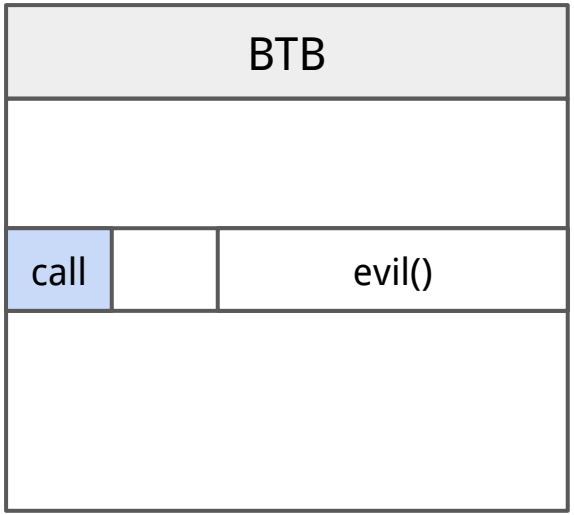
Spectre v2



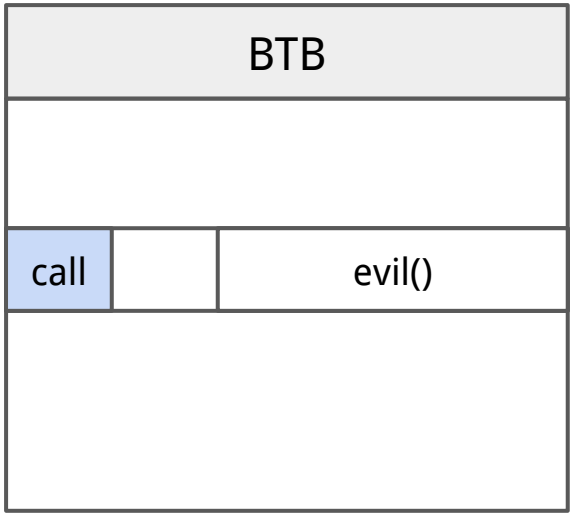


Spectre v2

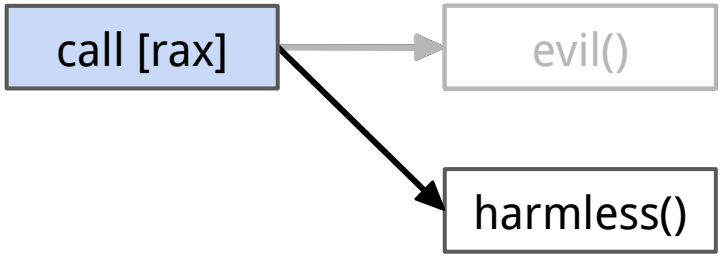


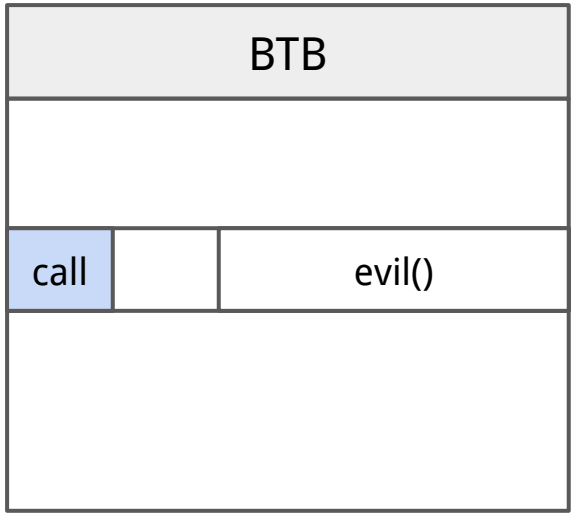


Spectre v2

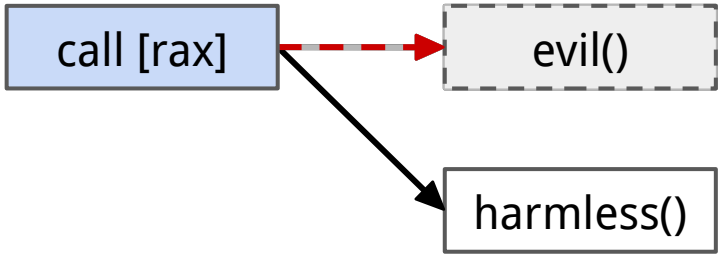


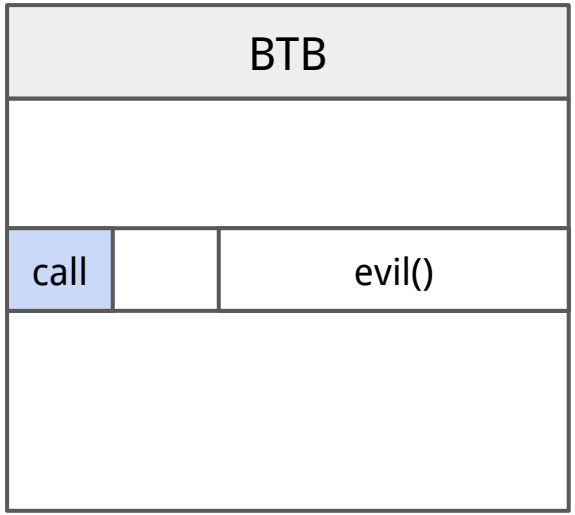
Spectre v2



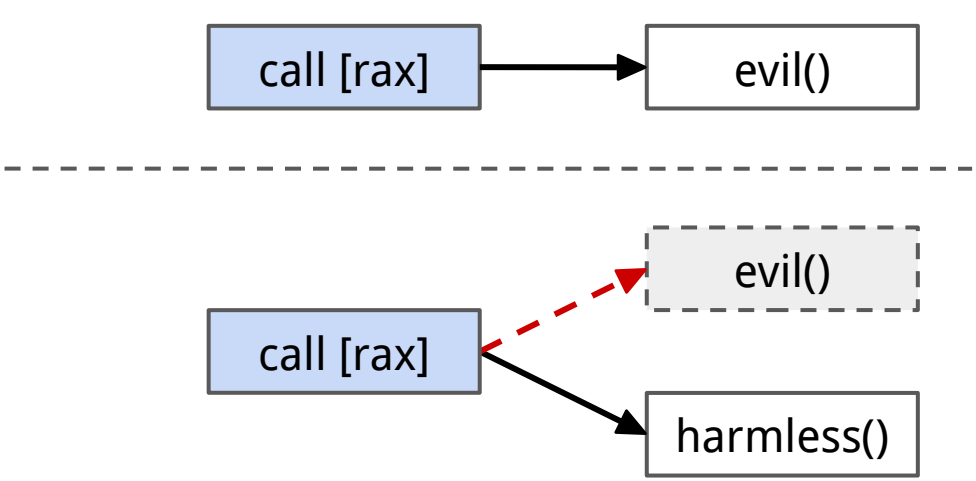


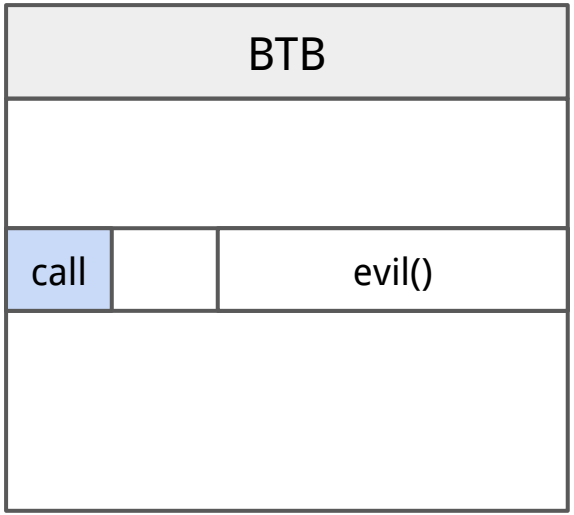
Spectre v2



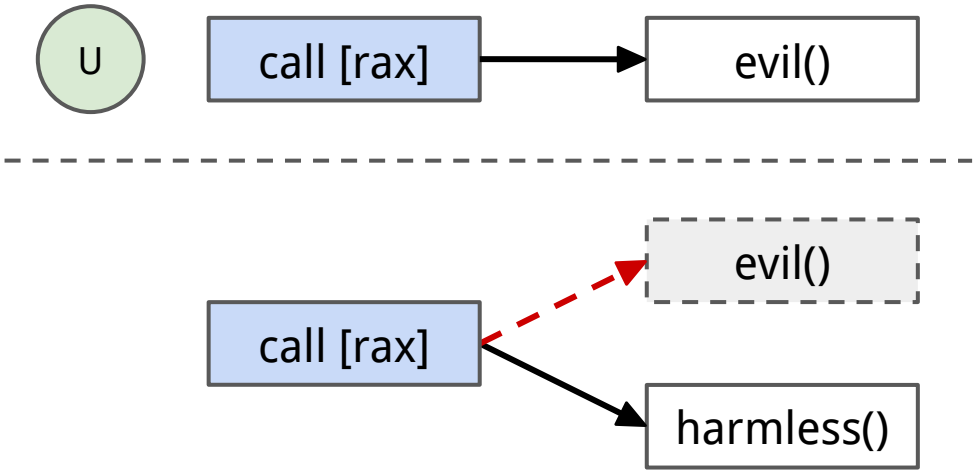


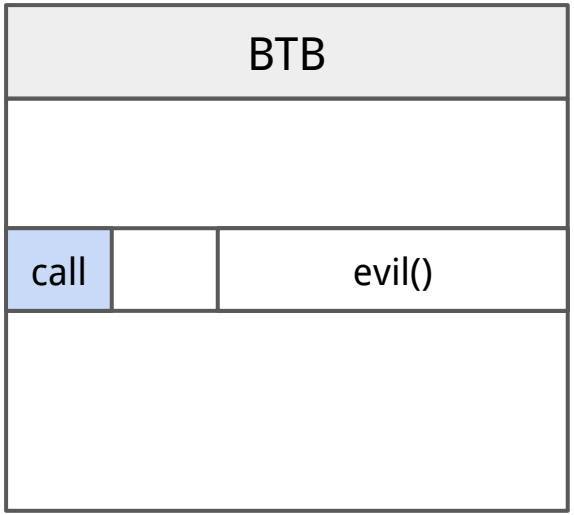
Spectre v2



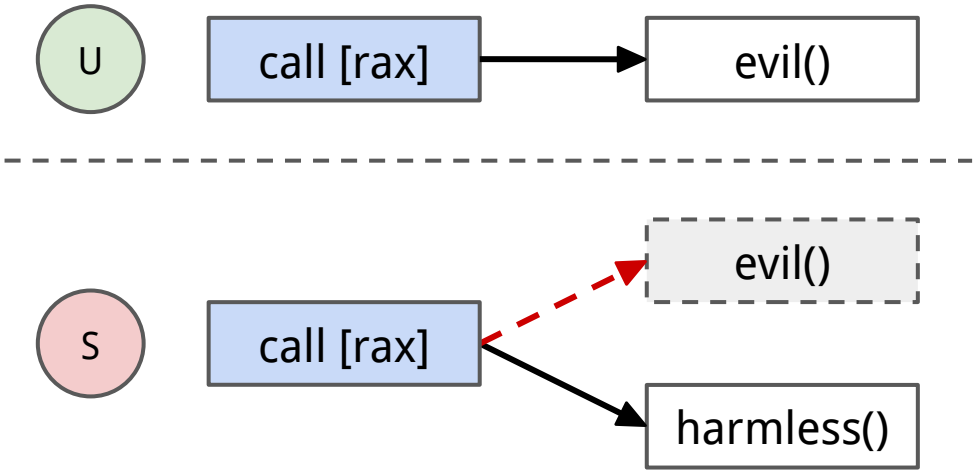


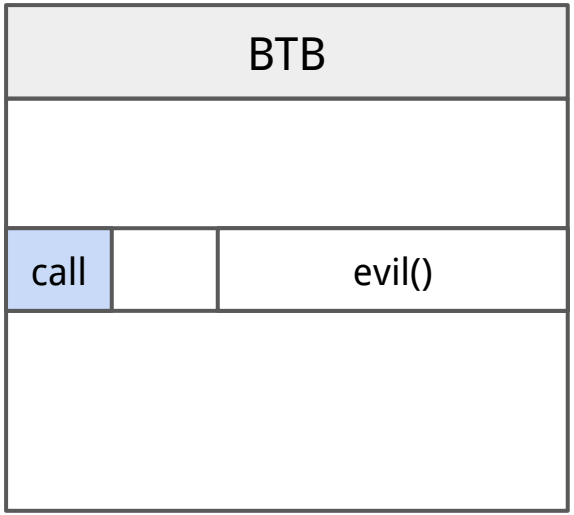
Spectre v2



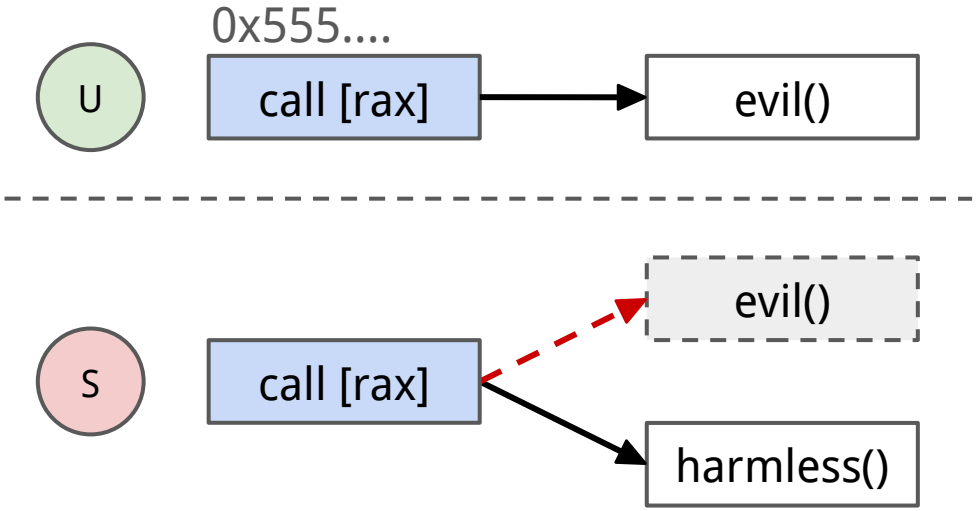


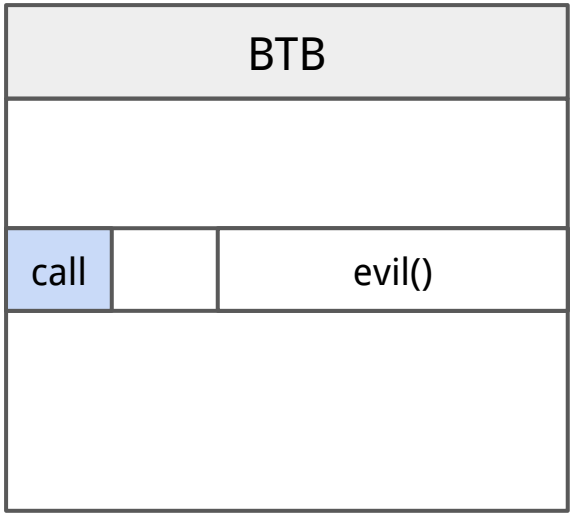
Spectre v2



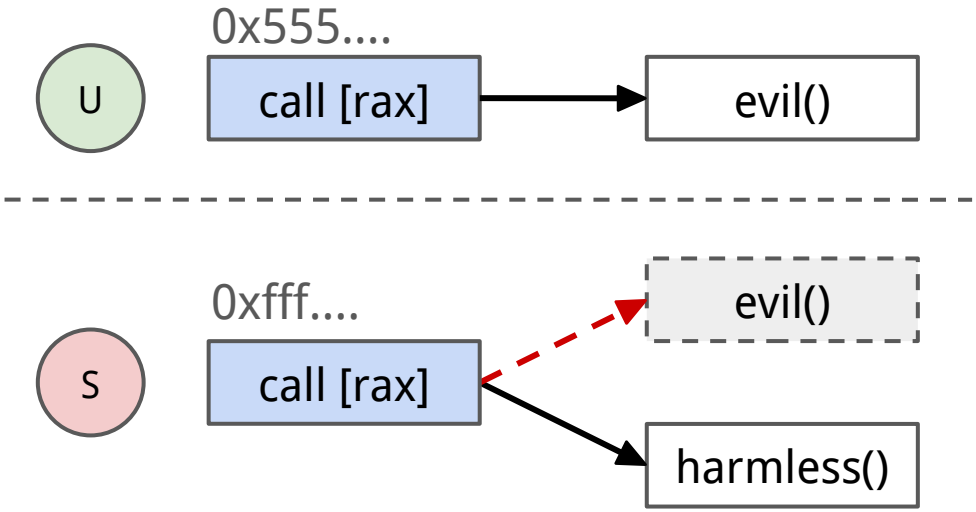


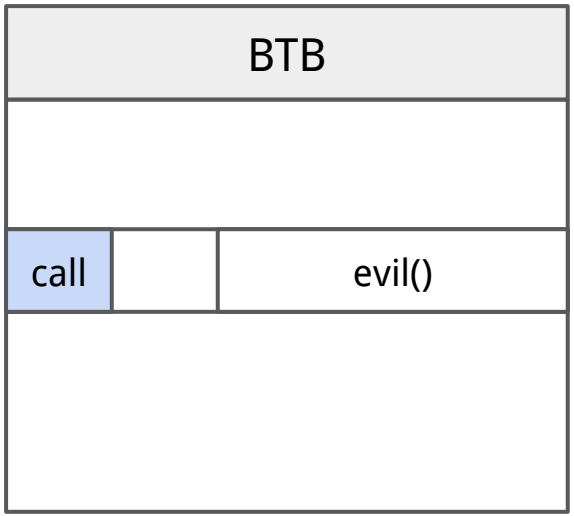
Spectre v2



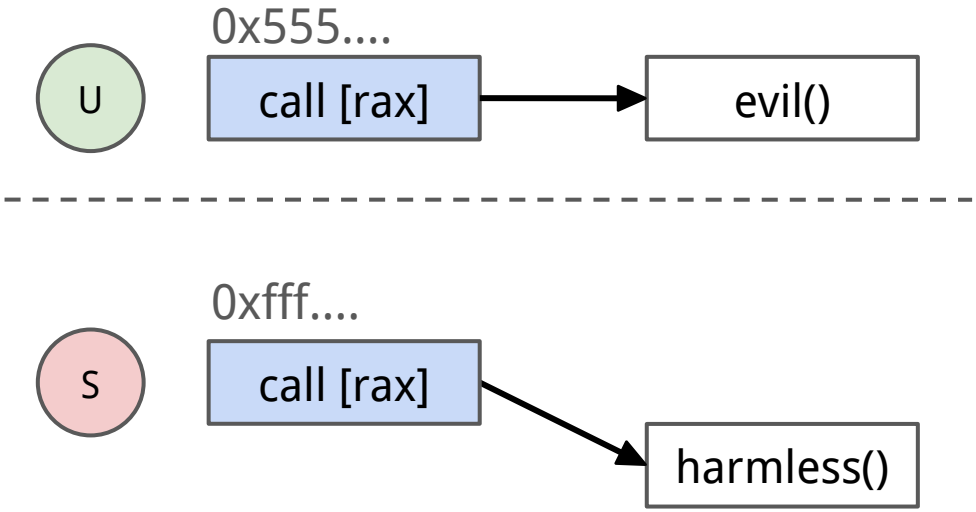


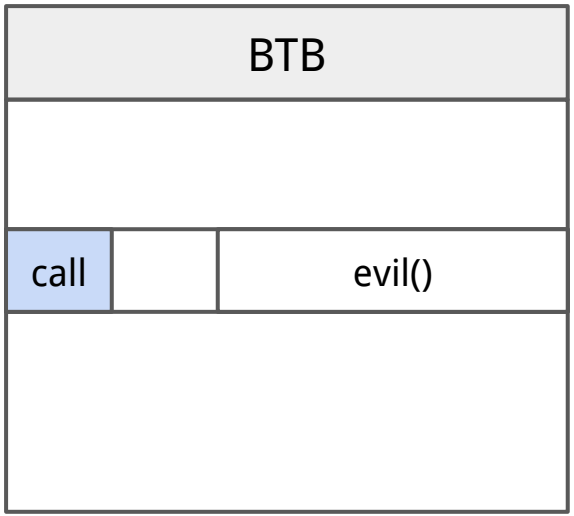
Spectre v2


0x555....
U
call [rax]
evil()
0xfff....
S
call [rax]
evil()
harmless()

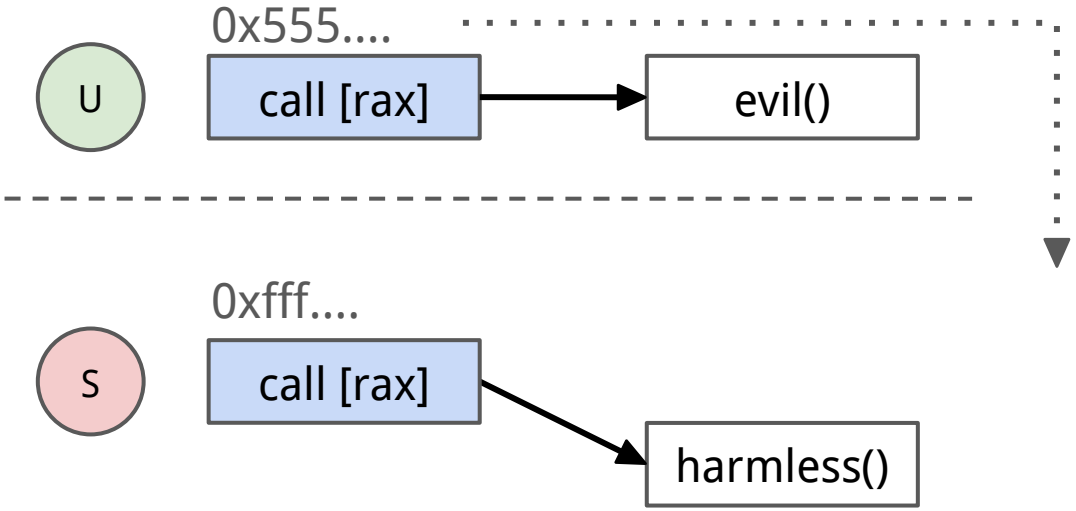

BTB
call
evil()

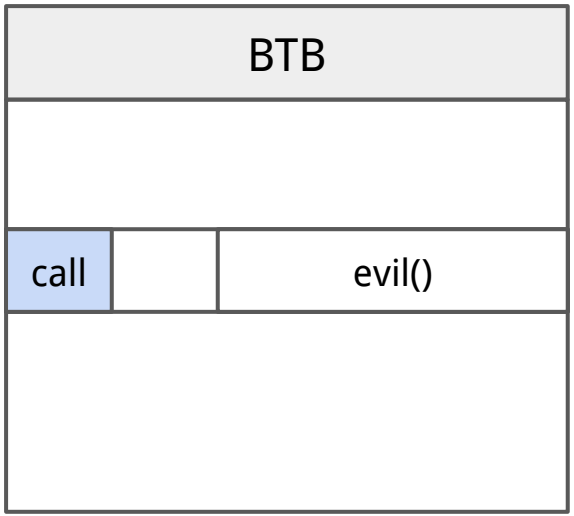
Spectre v2



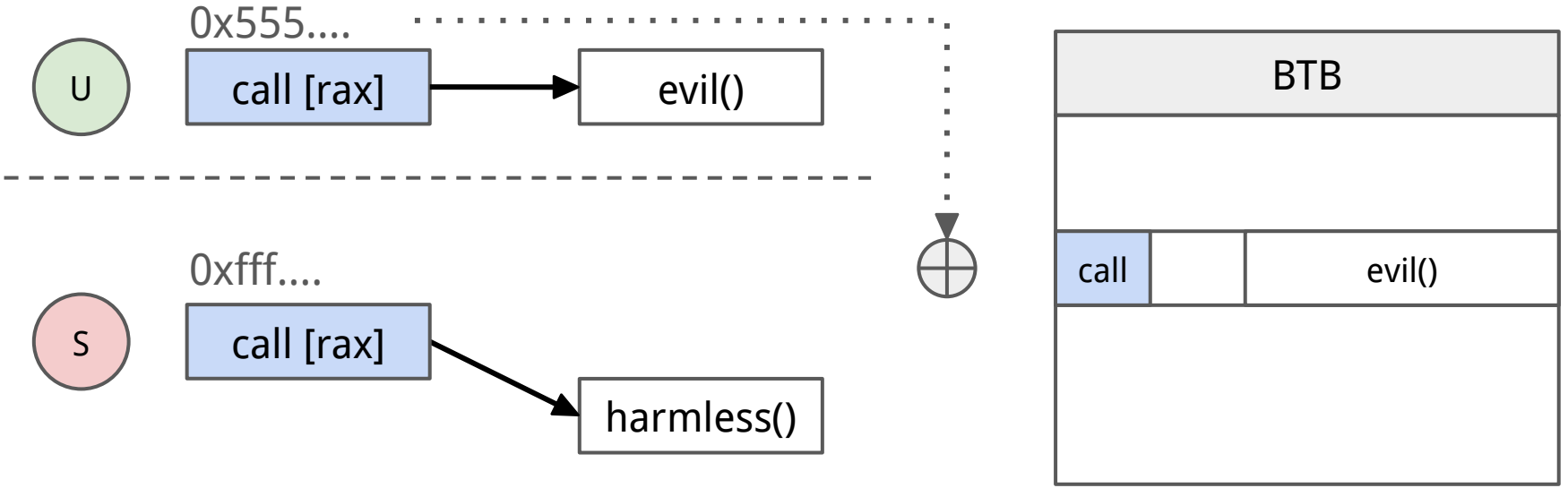


Spectre v2

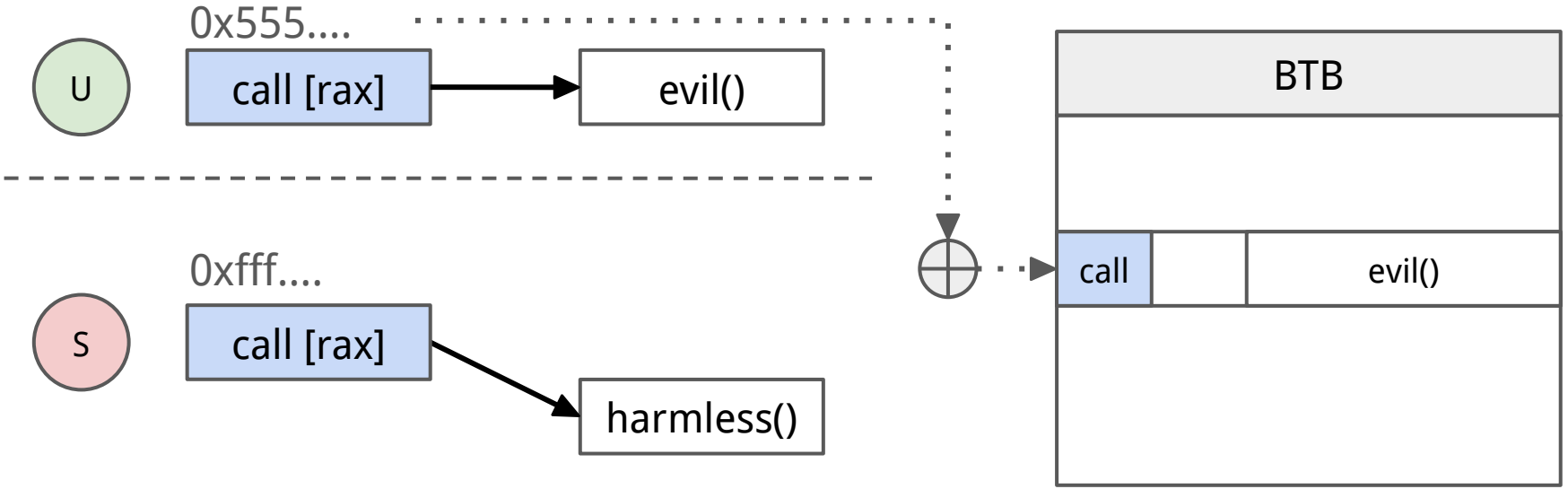




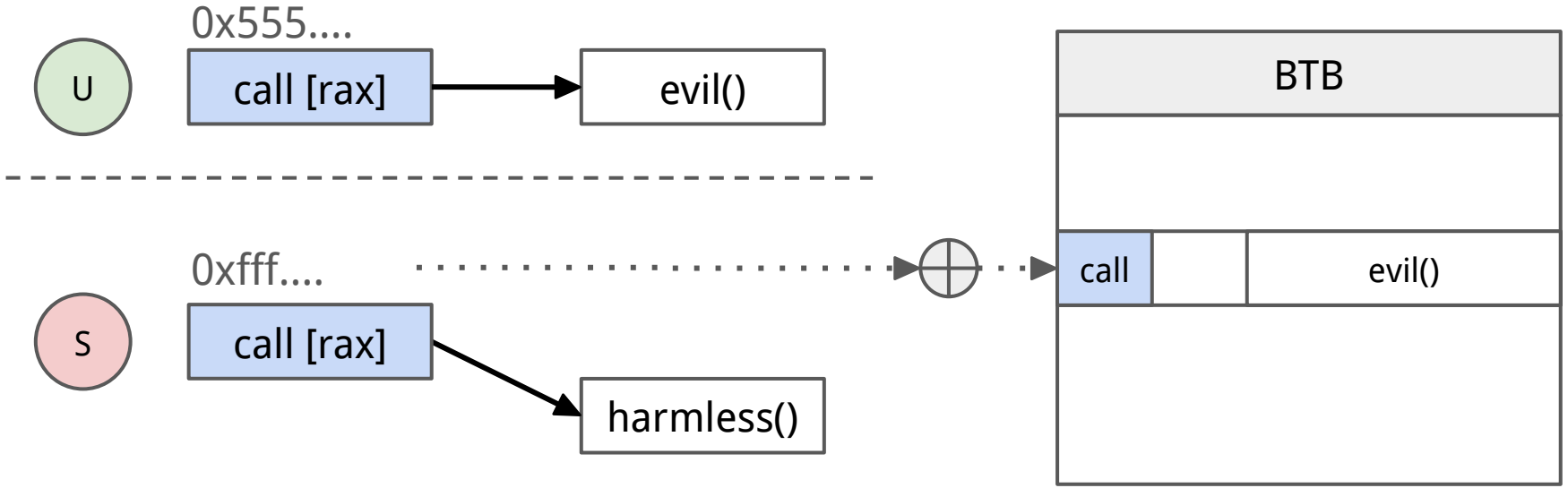
Spectre v2



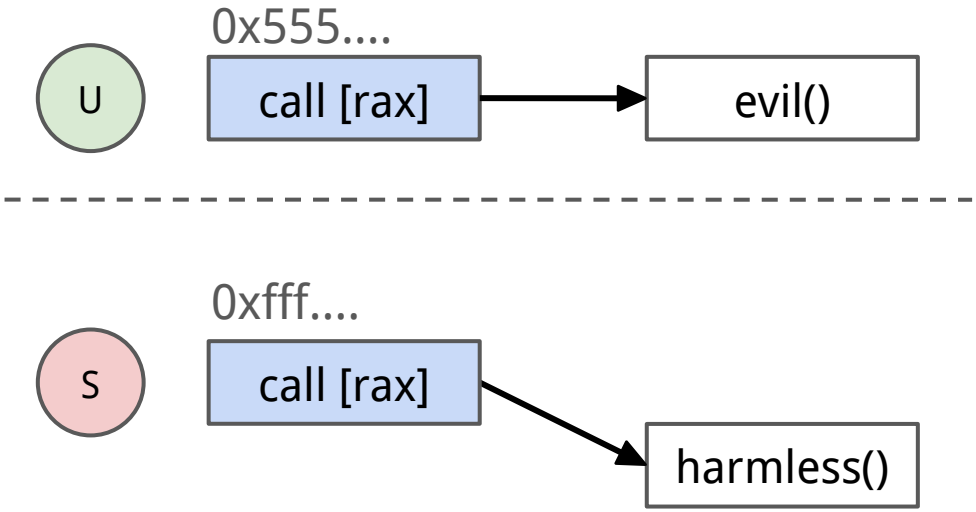
Spectre v2

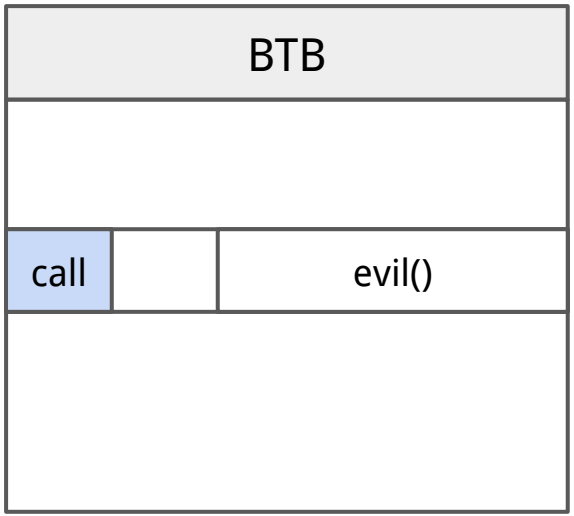


Spectre v2

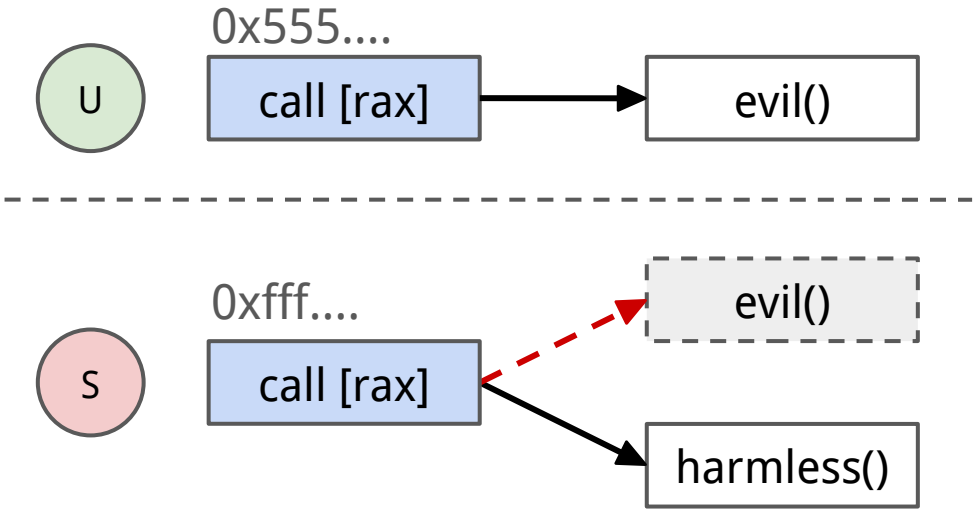


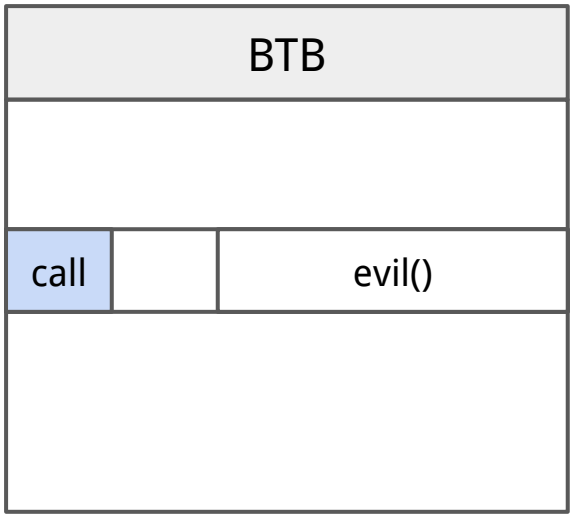
Spectre v2



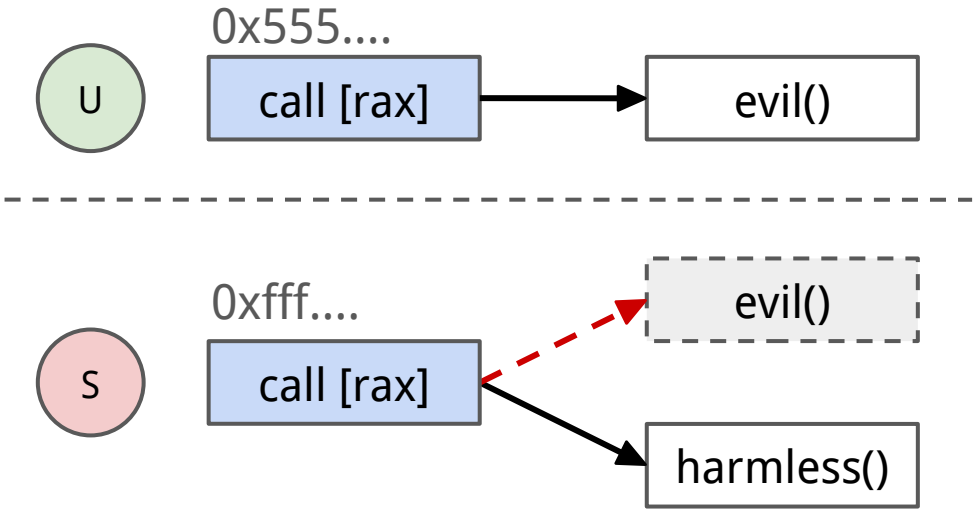


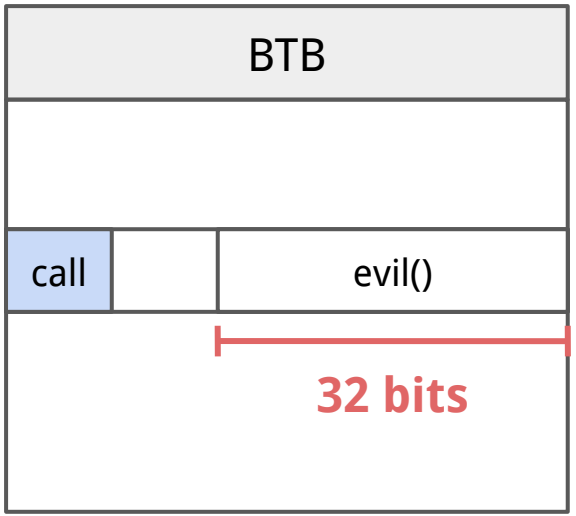
Spectre v2


0x555....
U
call [rax]
evil()
0xfff....
S
call [rax]
evil()
harmless()

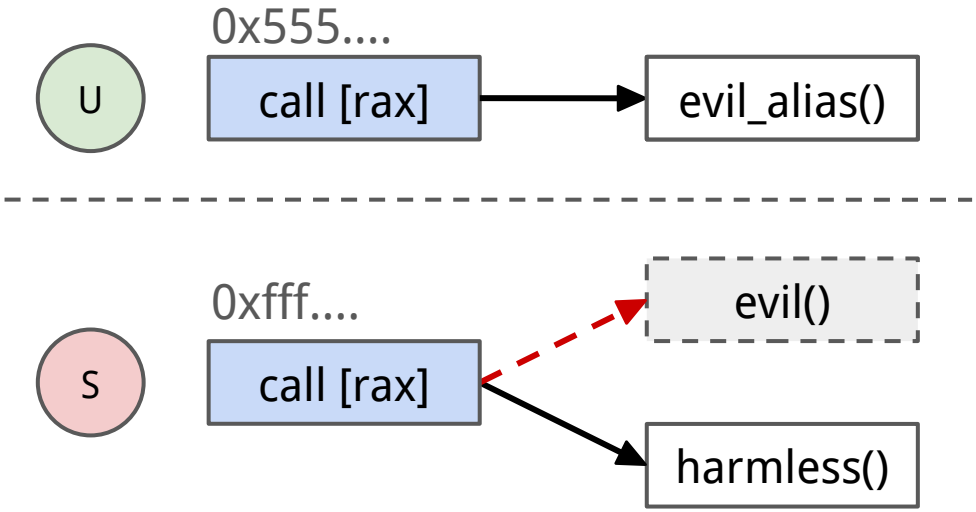

BTB
call
evil()

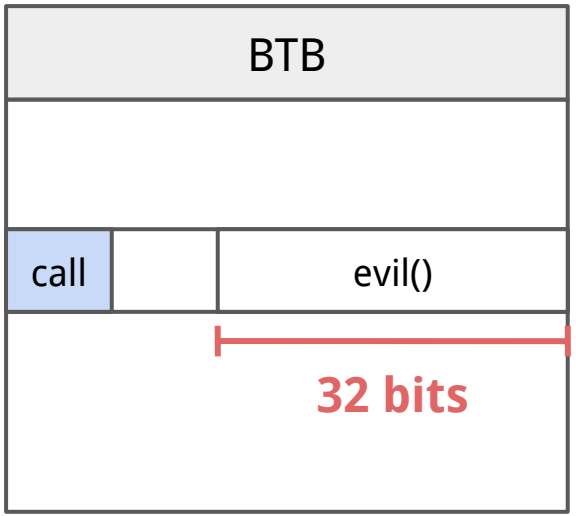
Spectre v2


0x555....
U
call [rax]
evil()
0xfff....
S
call [rax]
evil()
harmless()

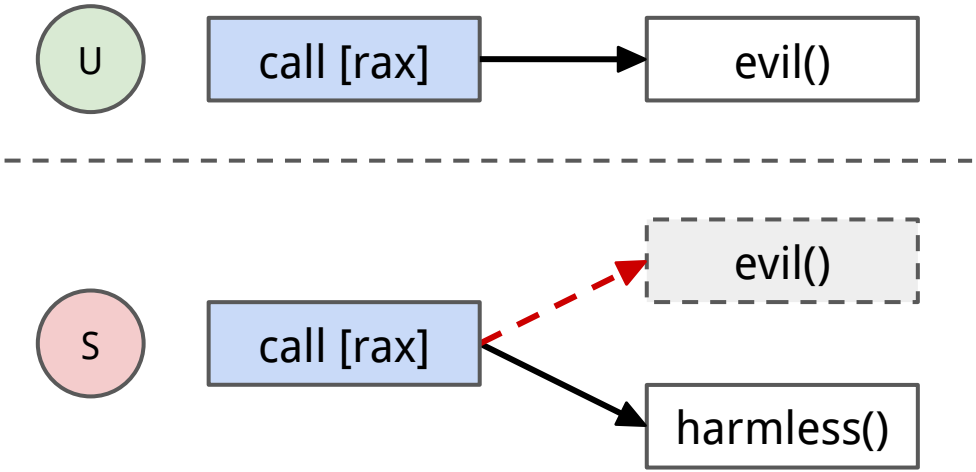

BTB
call
evil()
32 bits

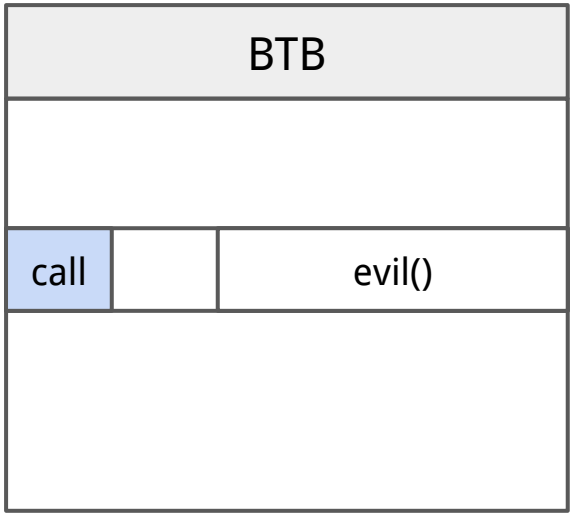
Spectre v2


0x555....
U
call [rax]
evil_alias()
0xfff....
S
call [rax]
evil()
harmless()

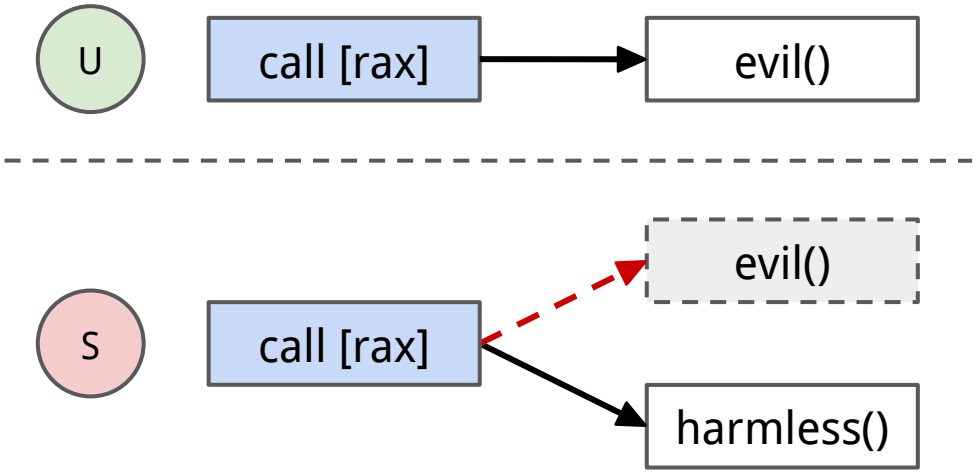

BTB
call
evil()
32 bits

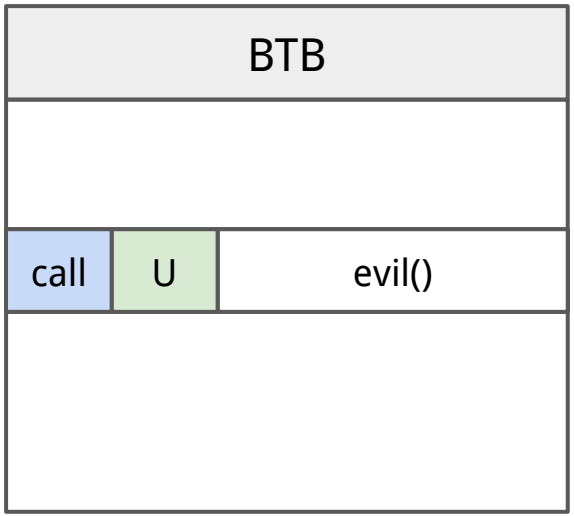
eIBRS



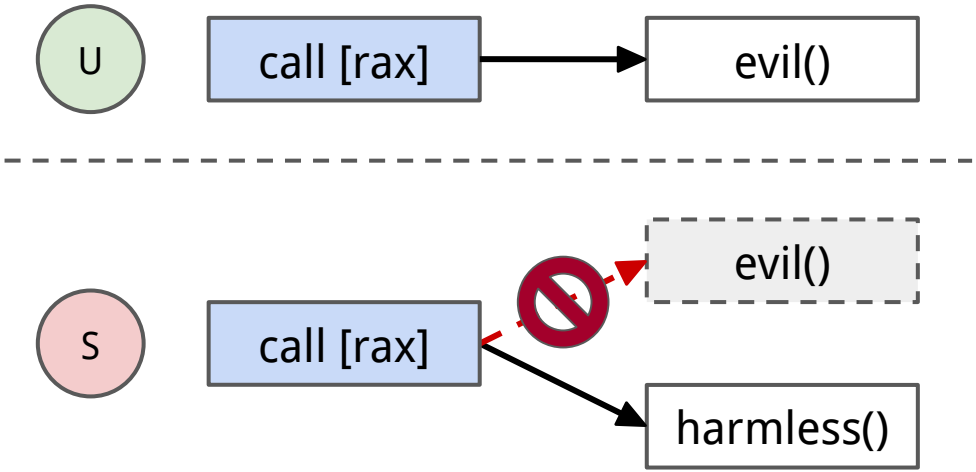


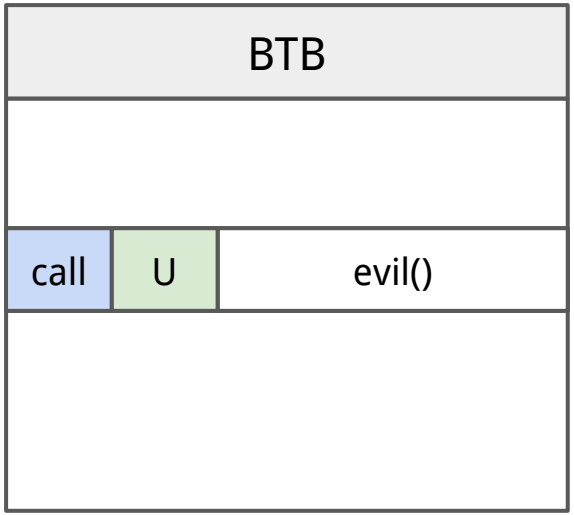
eIBRS



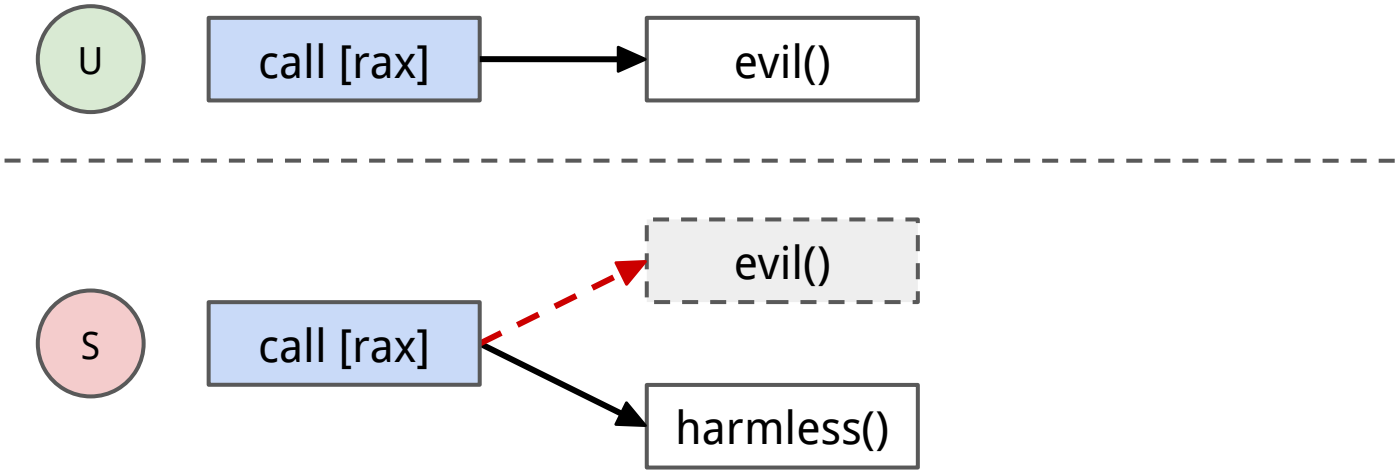


eIBRS

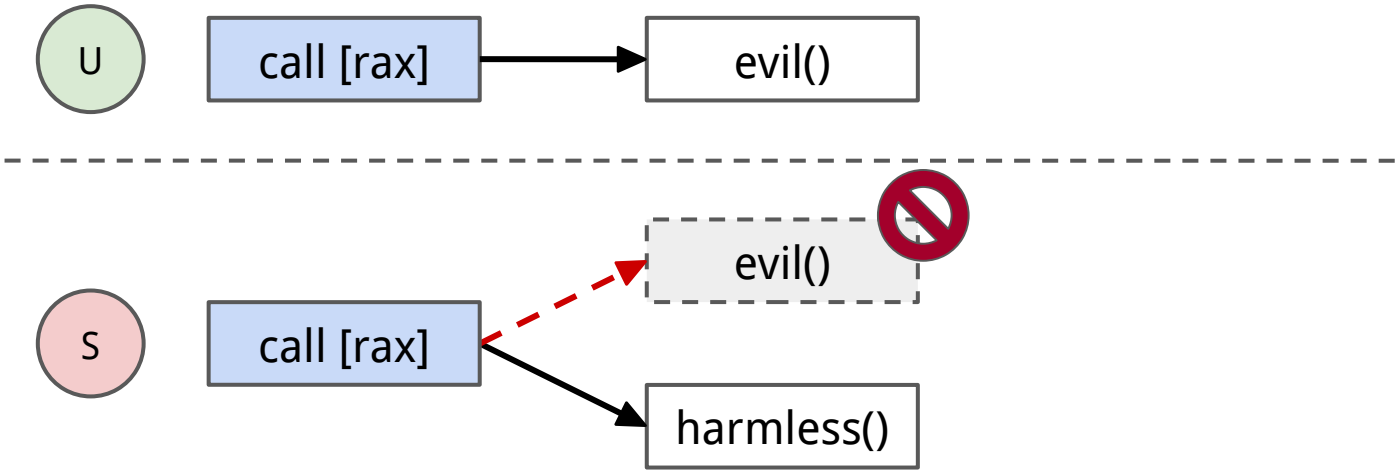




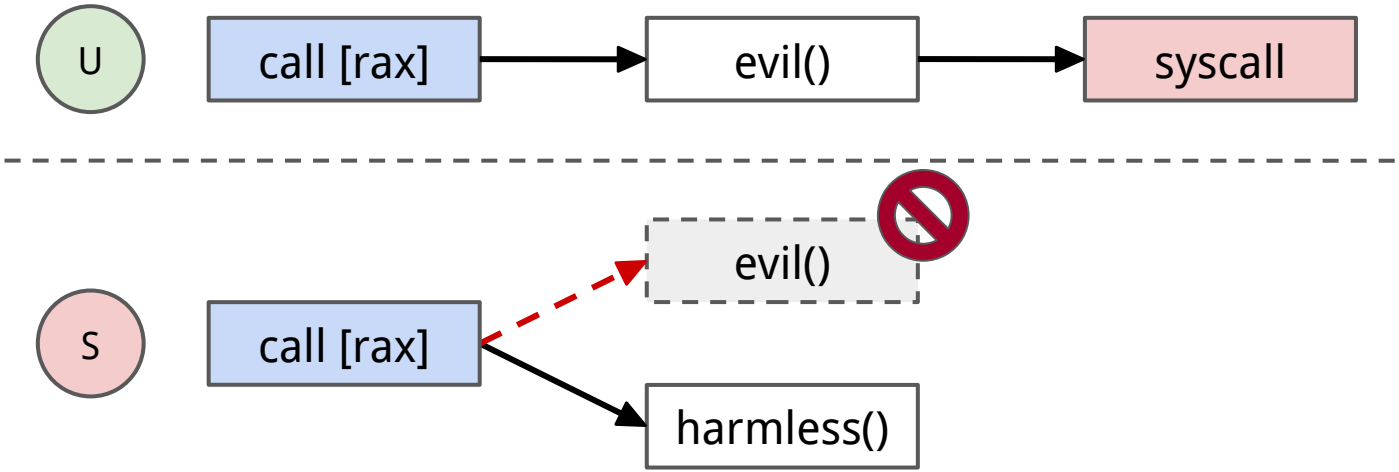
Testing eIBRS



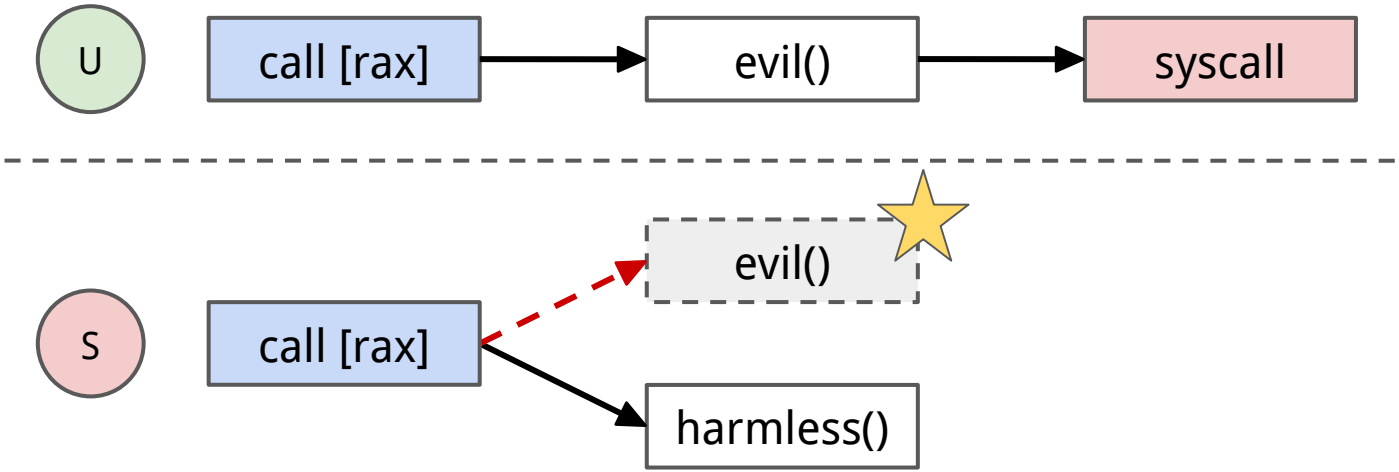
Testing eIBRS



Testing eIBRS



Testing eIBRS

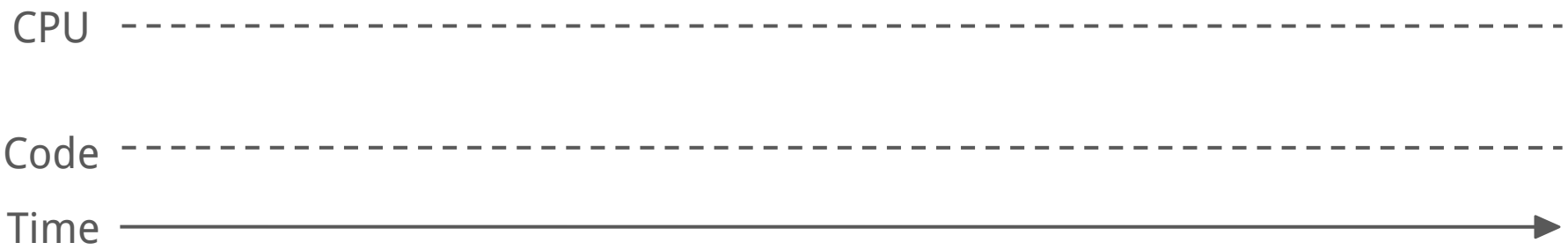


Branch Prediction Updates

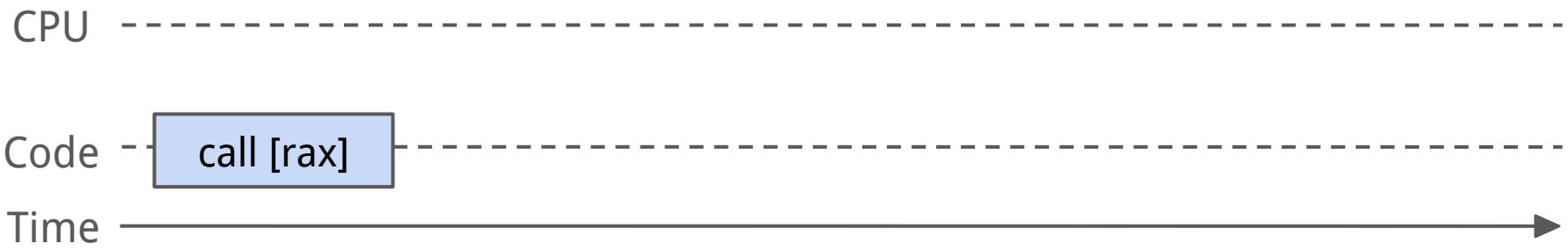
Branch Prediction Updates

Branch Prediction Updates

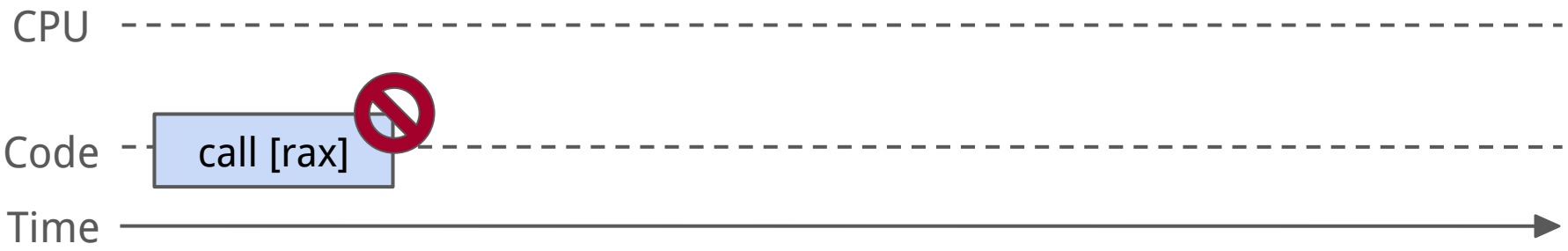
Branch Prediction Updates



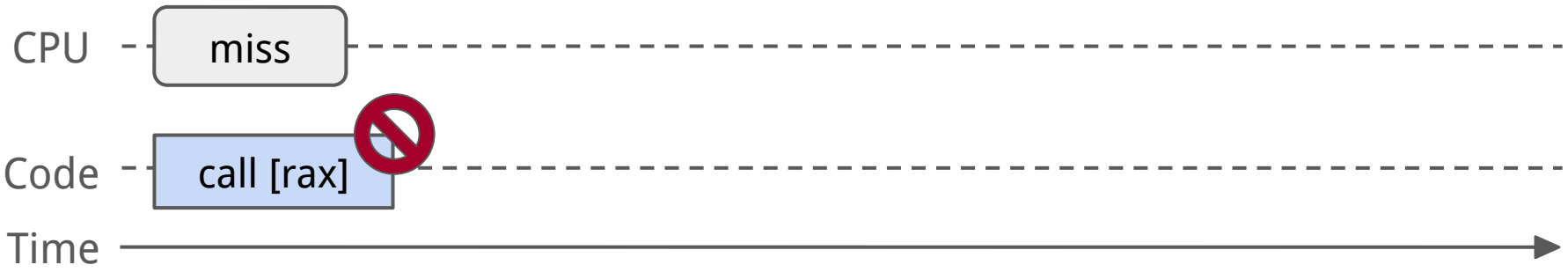
Branch Prediction Updates



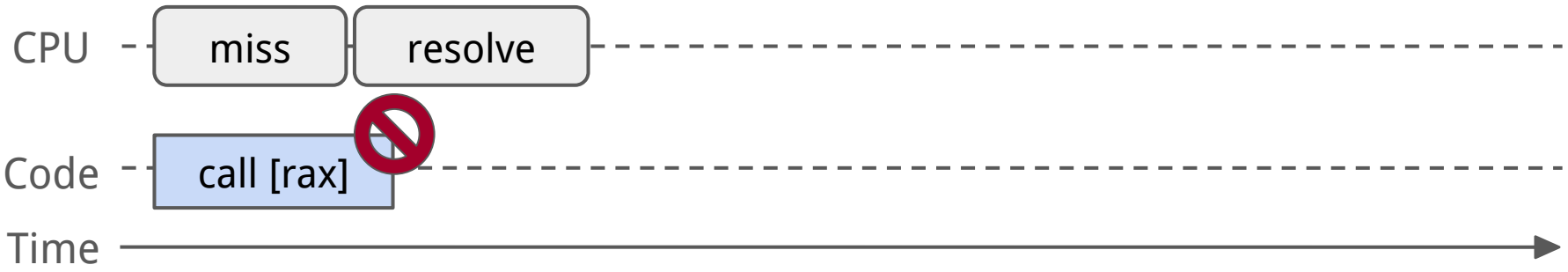
Branch Prediction Updates



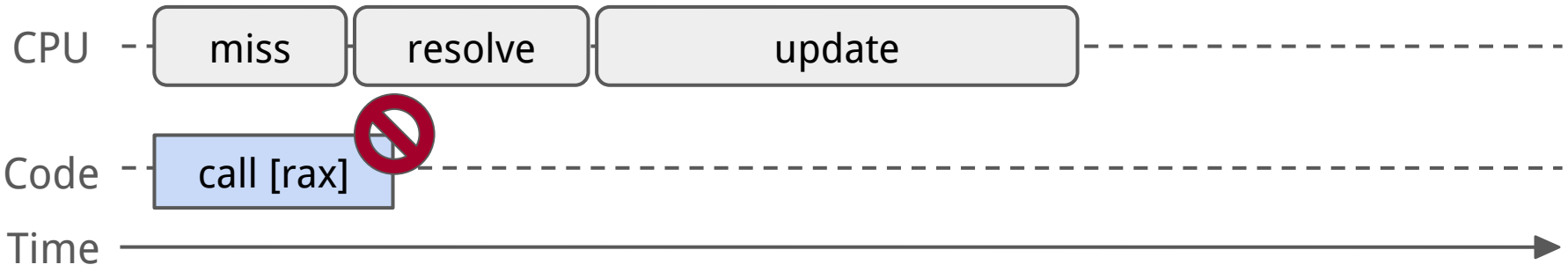
Branch Prediction Updates



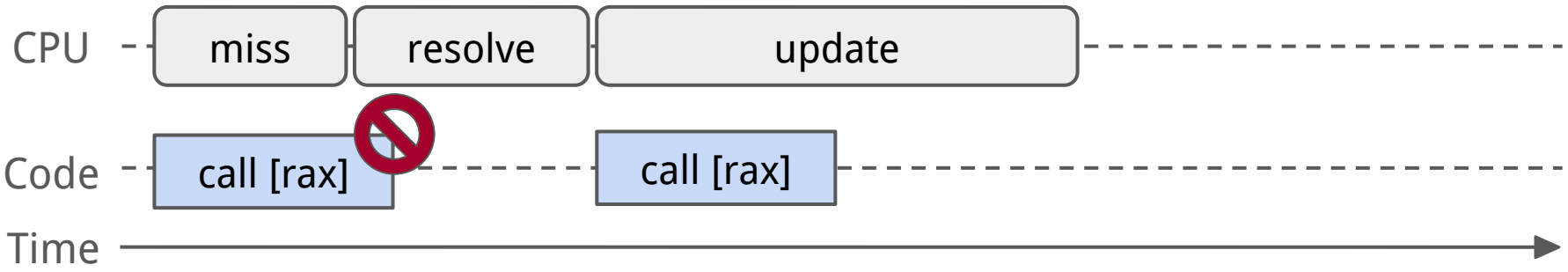
Branch Prediction Updates



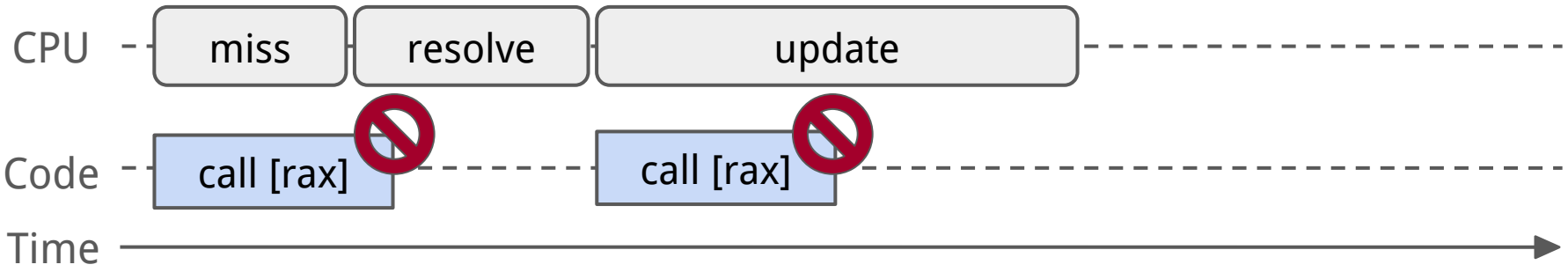
Branch Prediction Updates



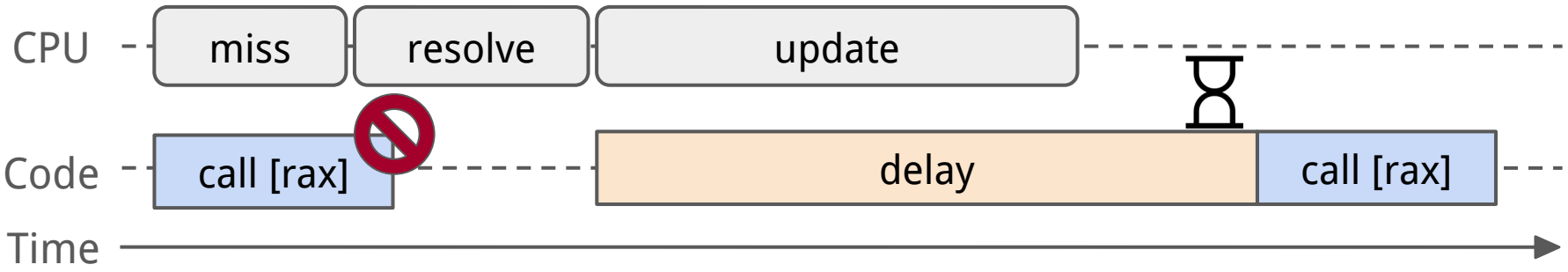
Branch Prediction Updates



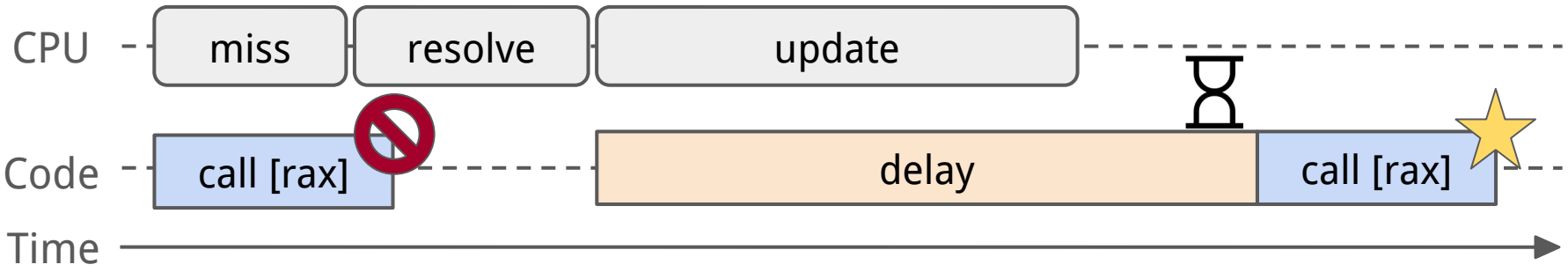
Branch Prediction Updates



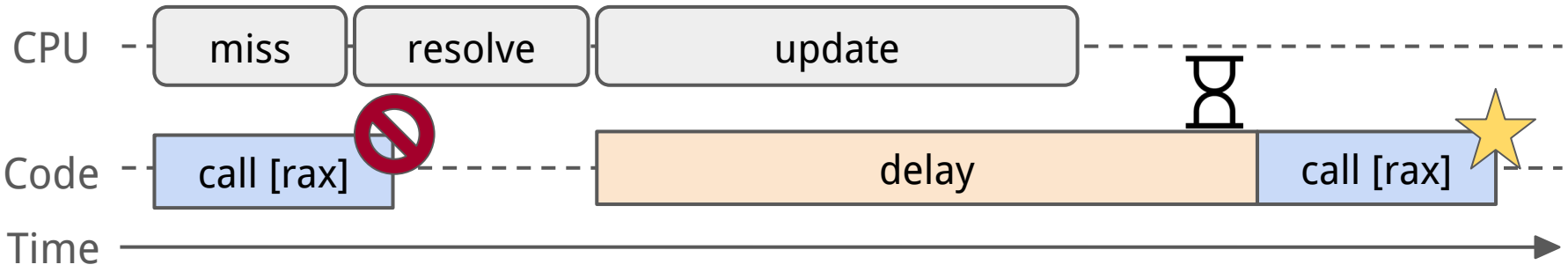
Branch Prediction Updates

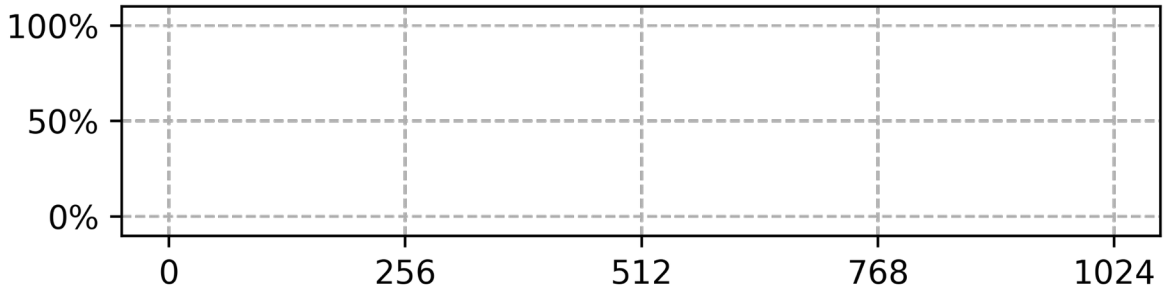


Branch Prediction Updates

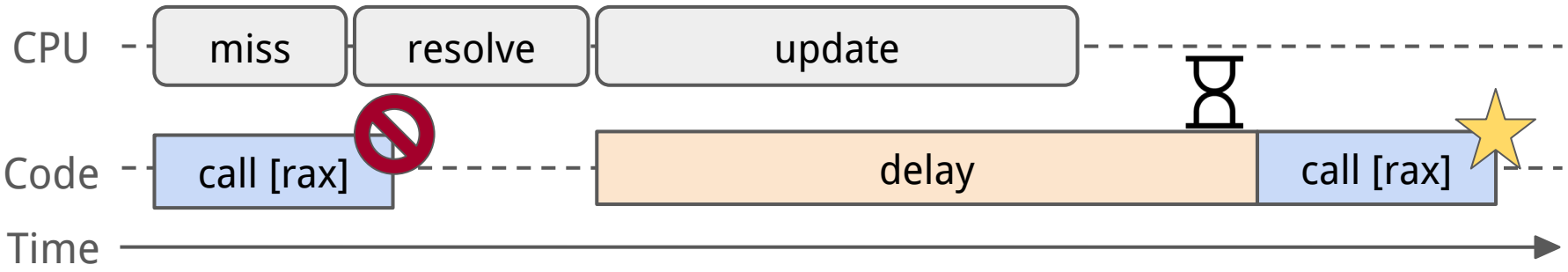


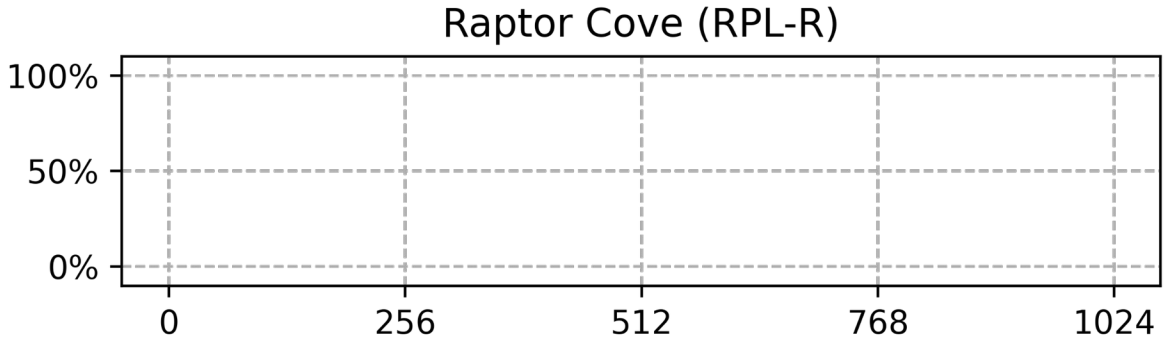
Branch Prediction Updates



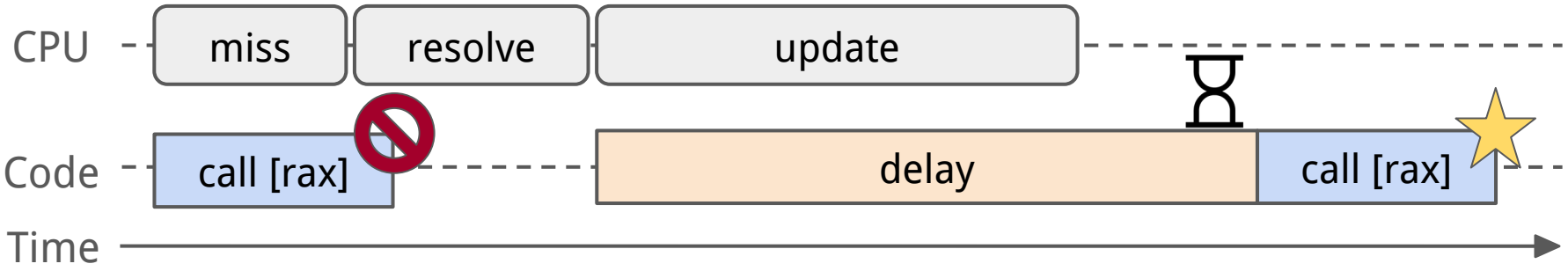


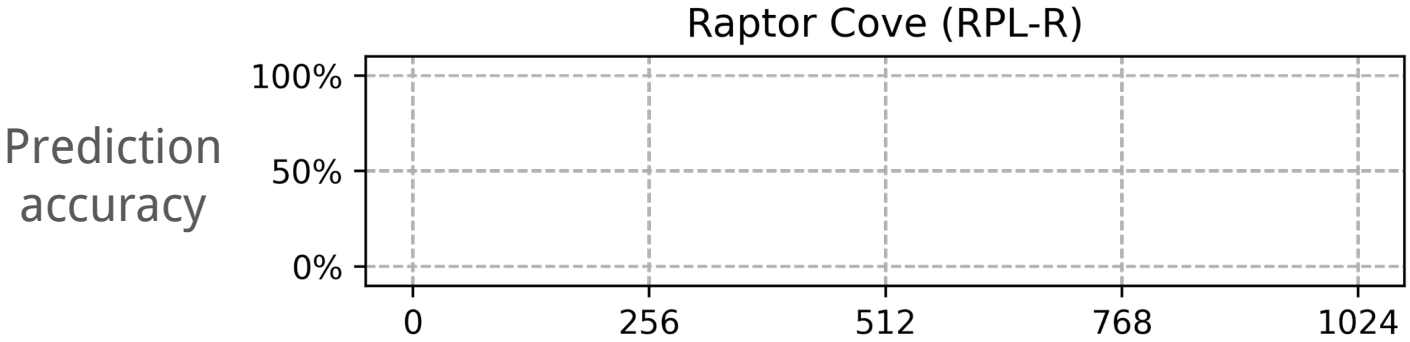
Branch Prediction Updates



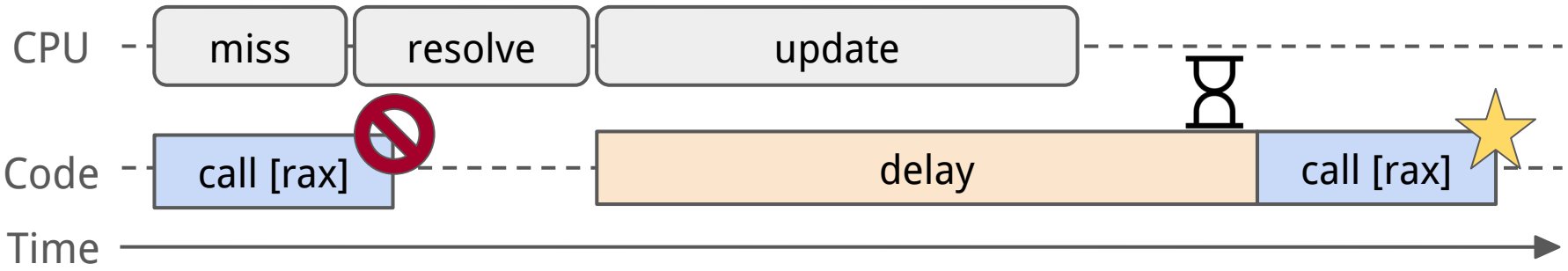


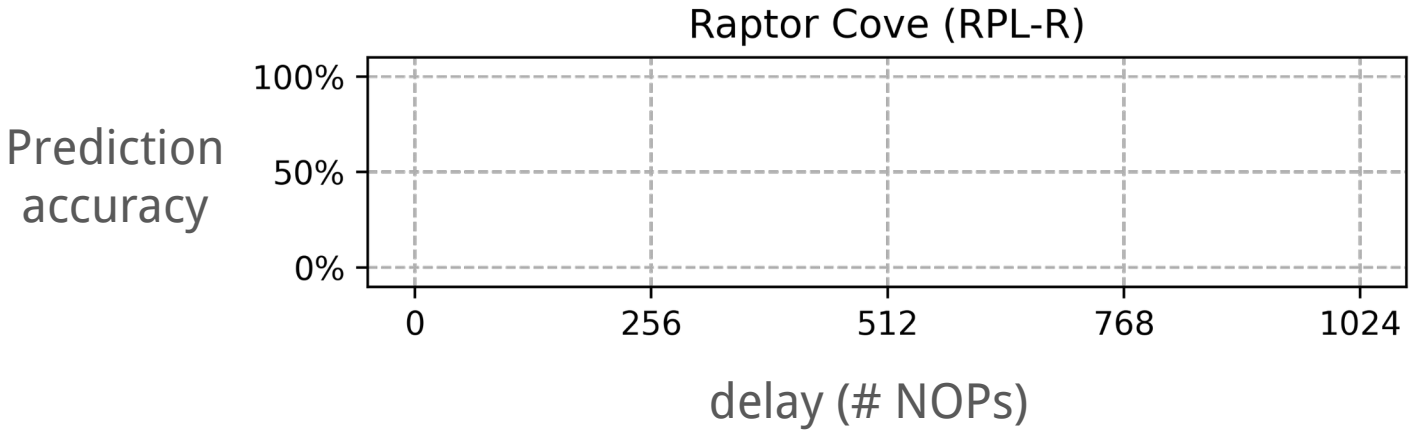
Branch Prediction Updates



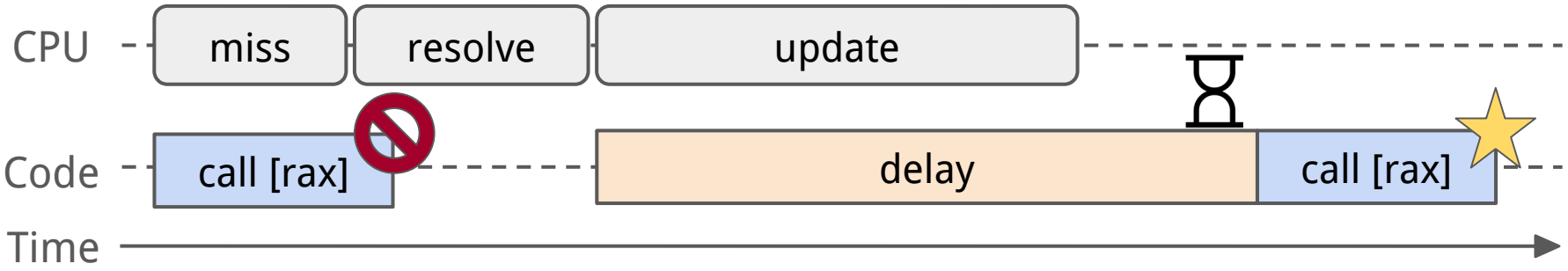


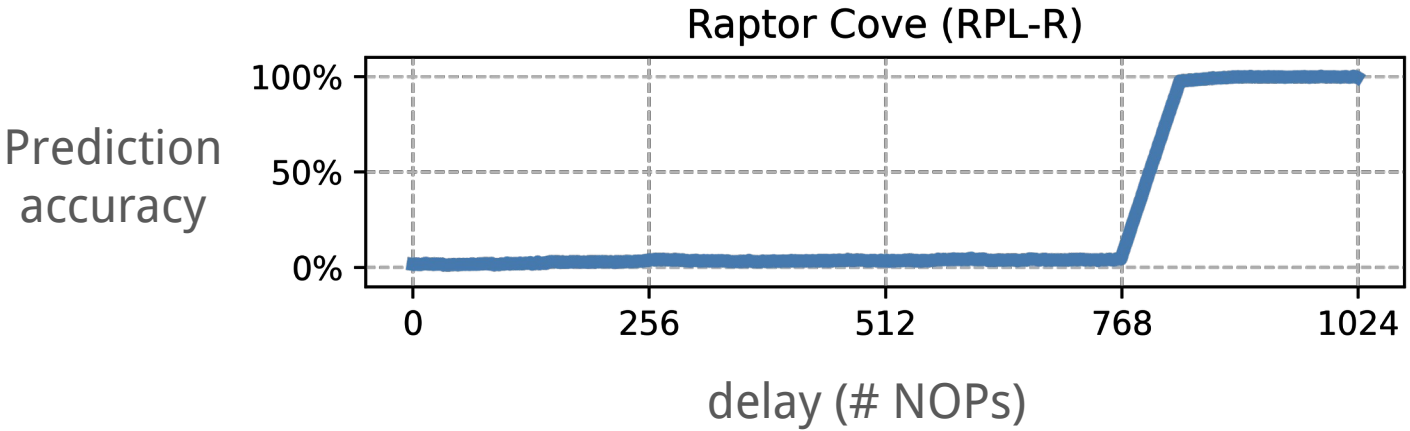
Branch Prediction Updates



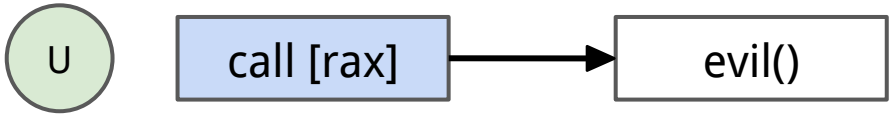


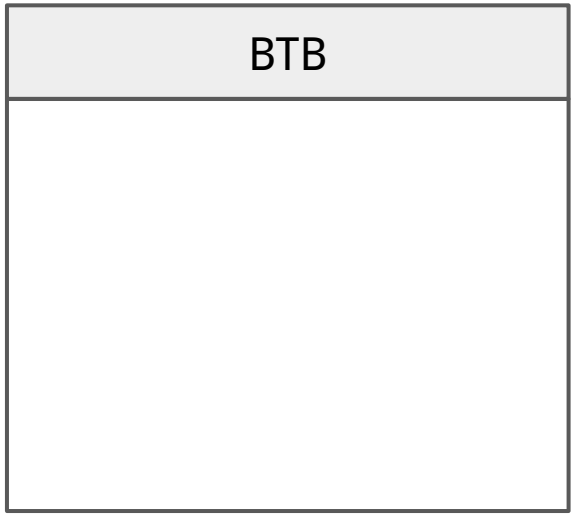
Branch Prediction Updates



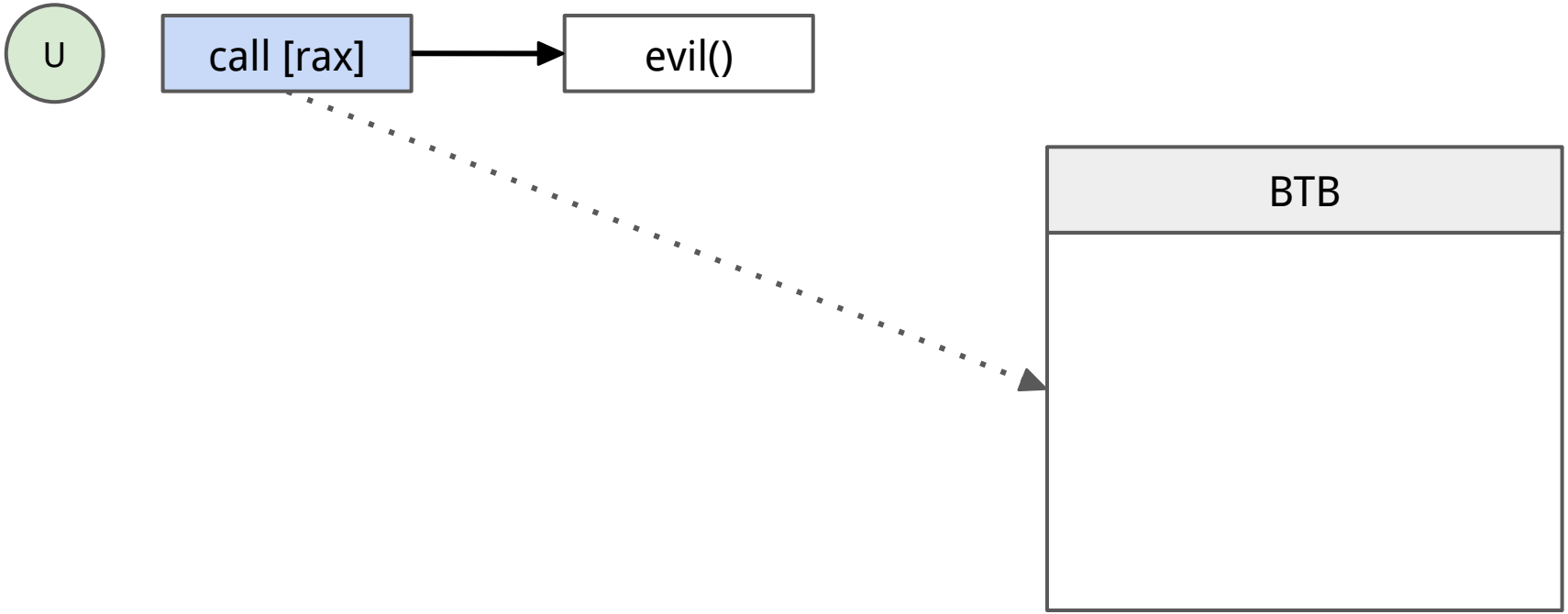


Branch Prediction Updates

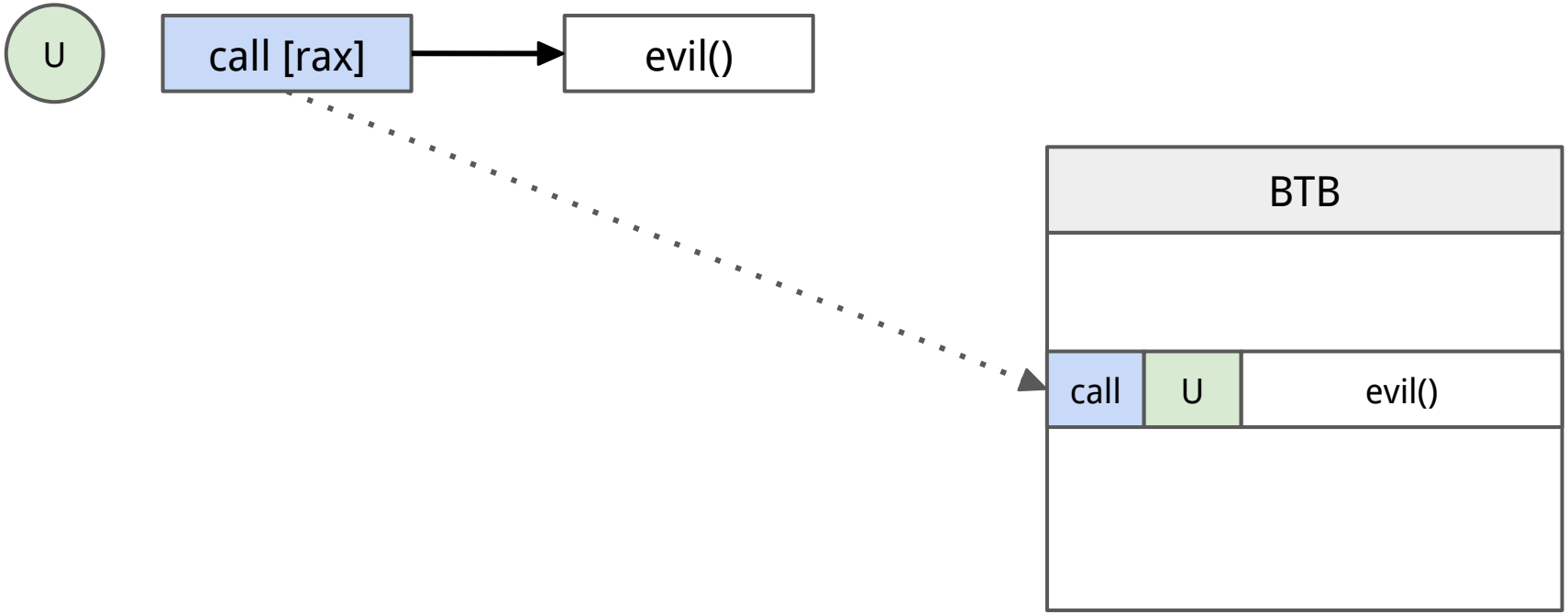




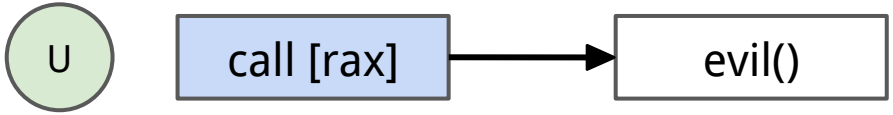
Branch Prediction Updates

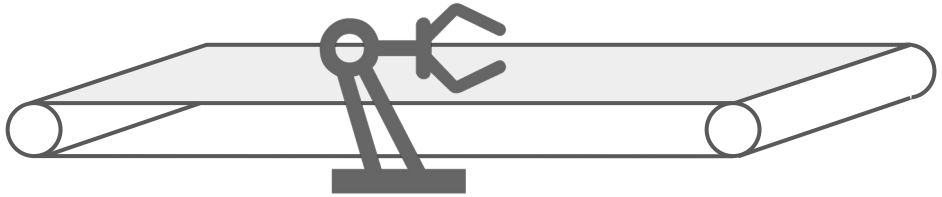


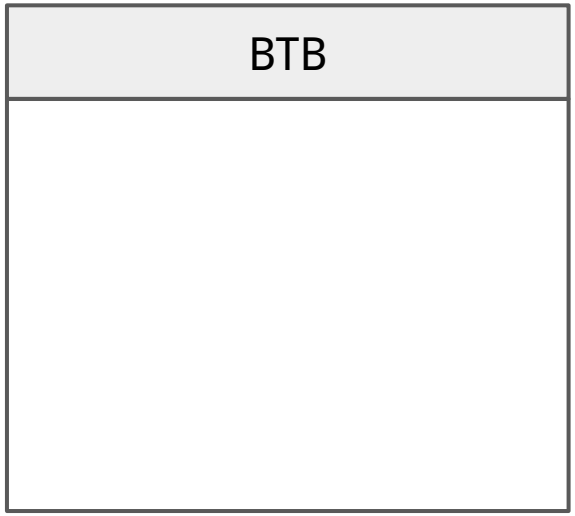
Branch Prediction Updates



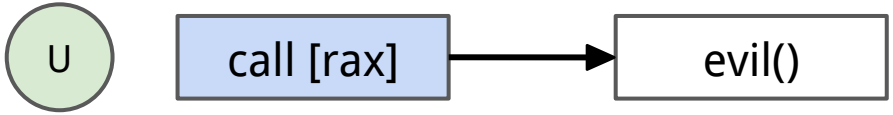
Branch Prediction Updates

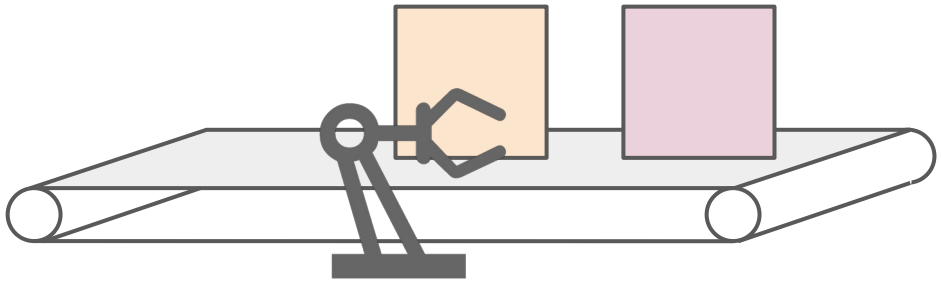


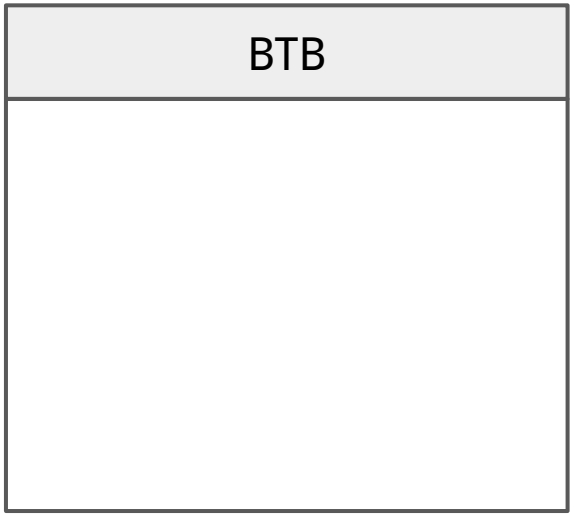




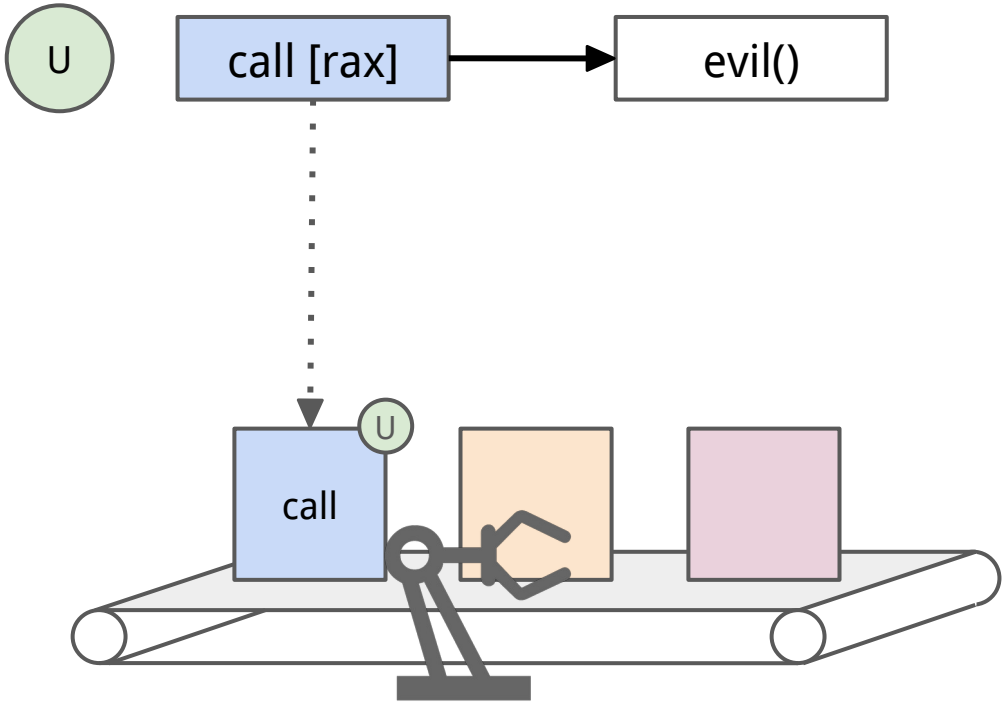
Branch Prediction Updates

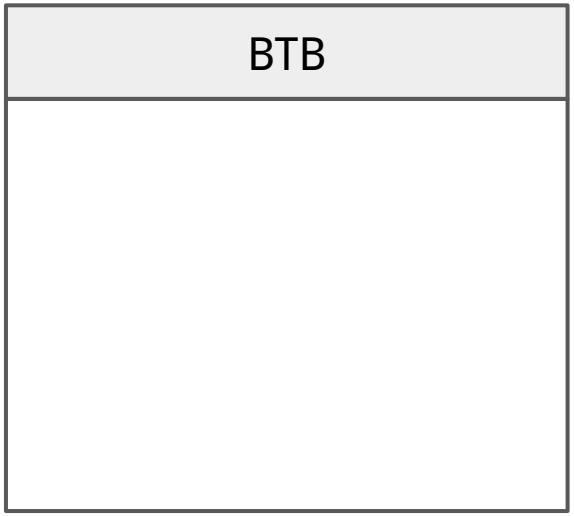




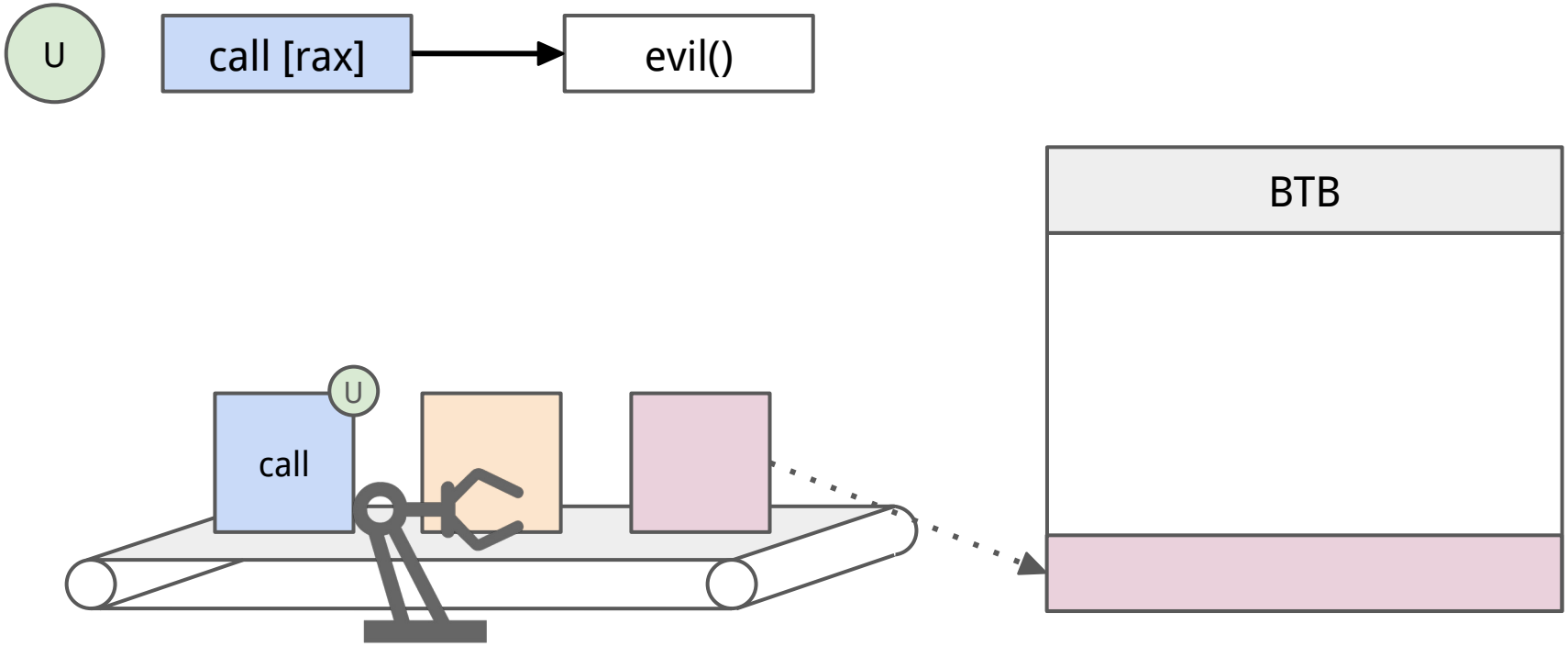


Branch Prediction Updates

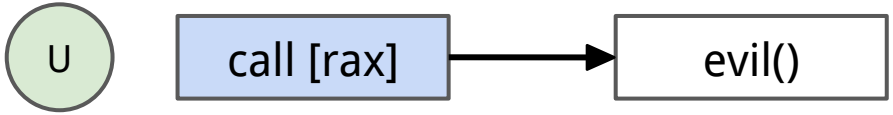


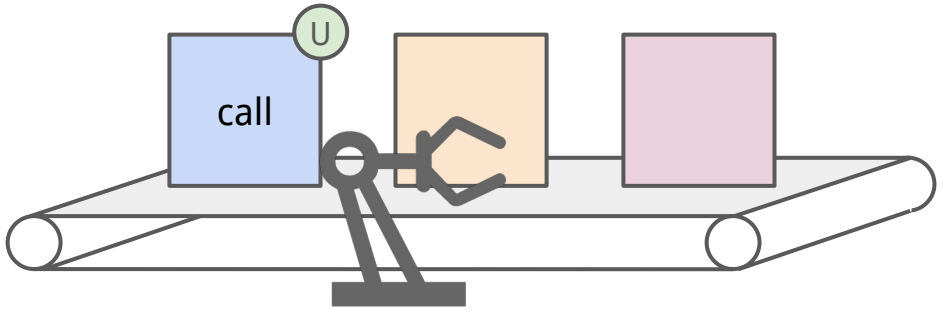


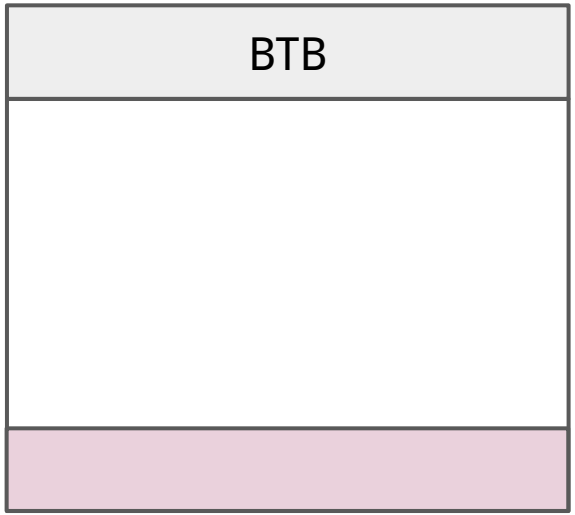
Branch Prediction Updates



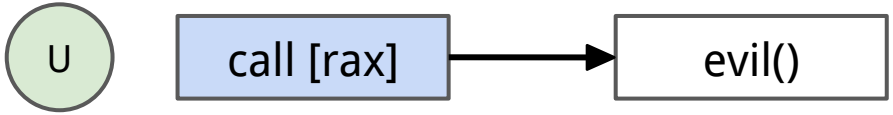
Branch Prediction Updates

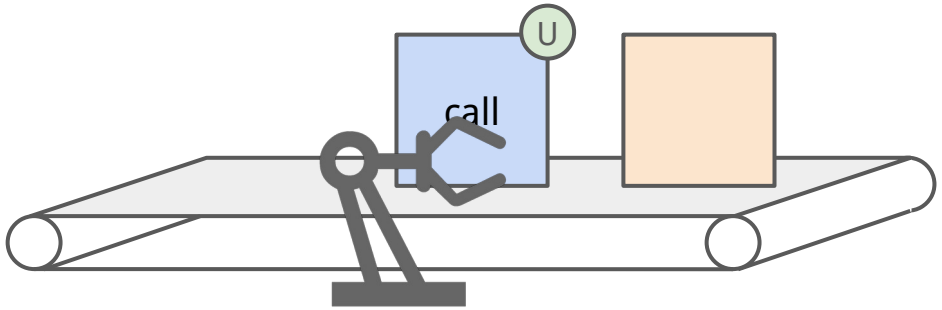


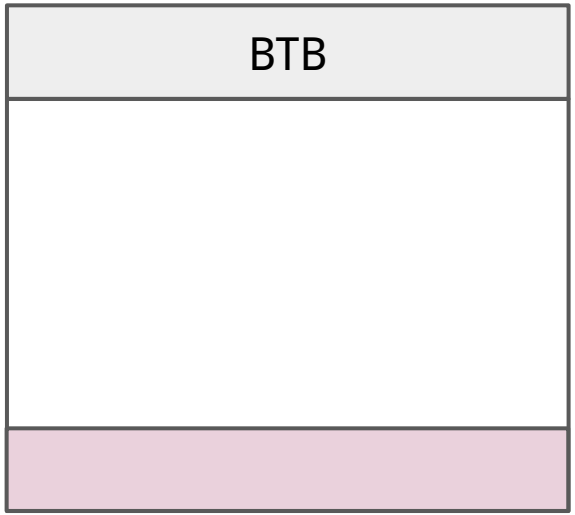




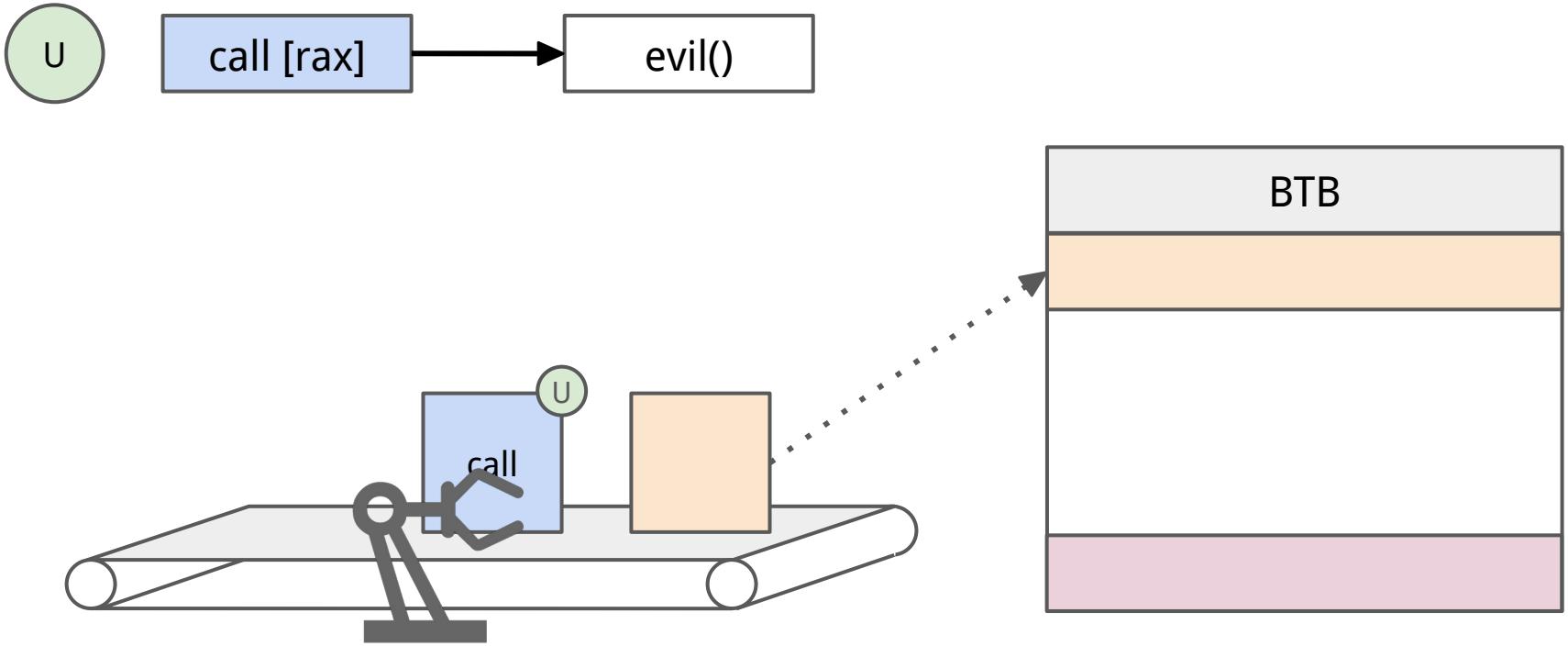
Branch Prediction Updates



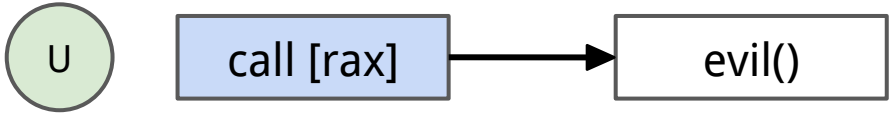


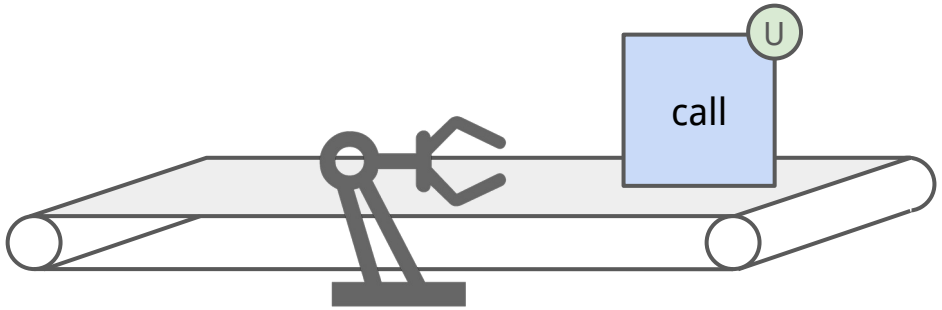


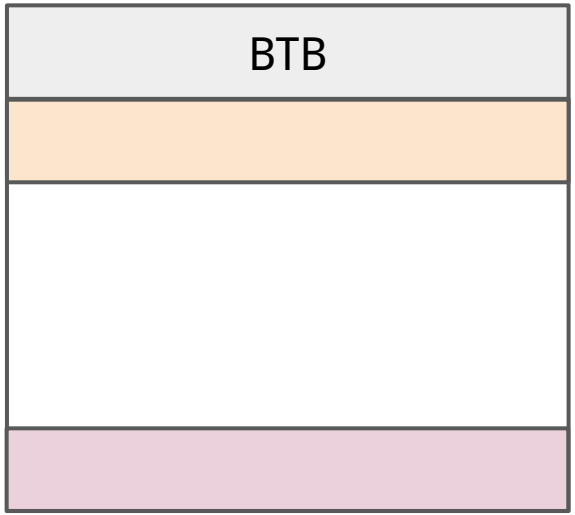
Branch Prediction Updates



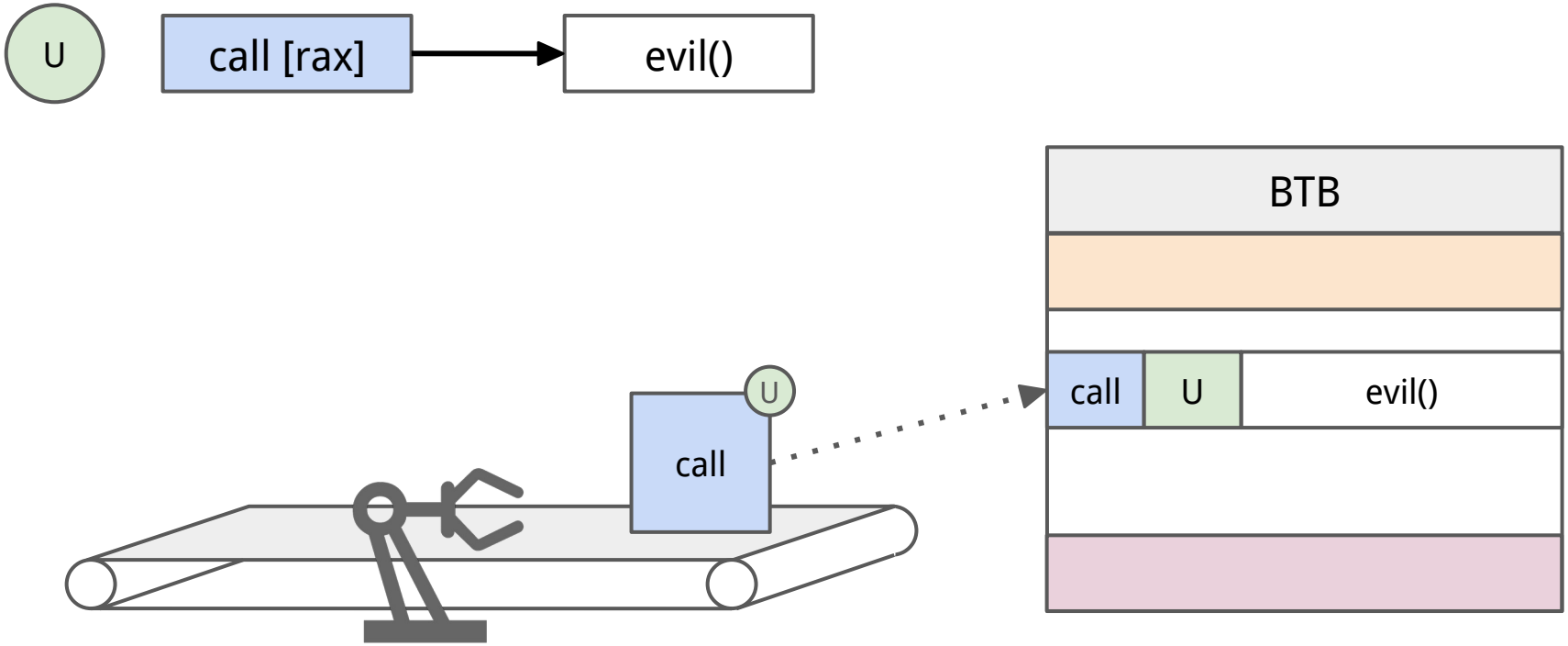
Branch Prediction Updates



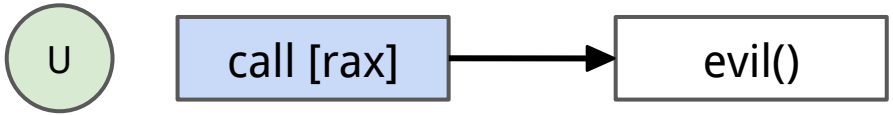




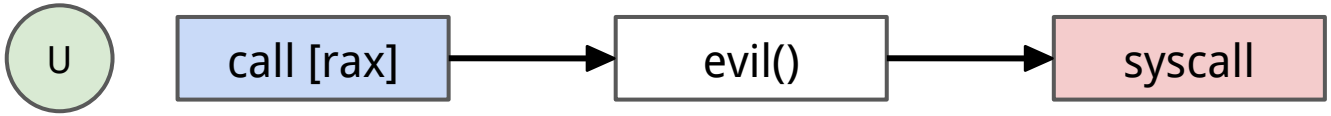
Branch Prediction Updates



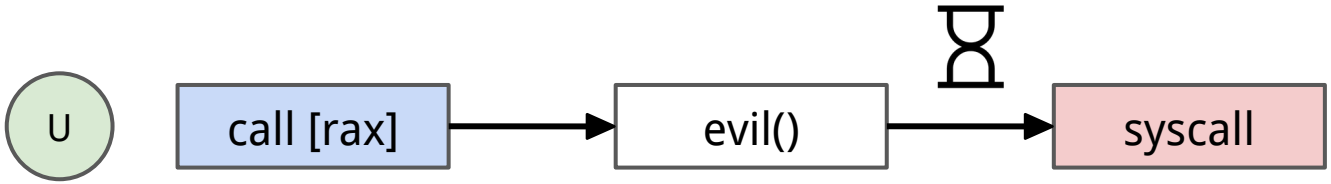
Privilege Switch



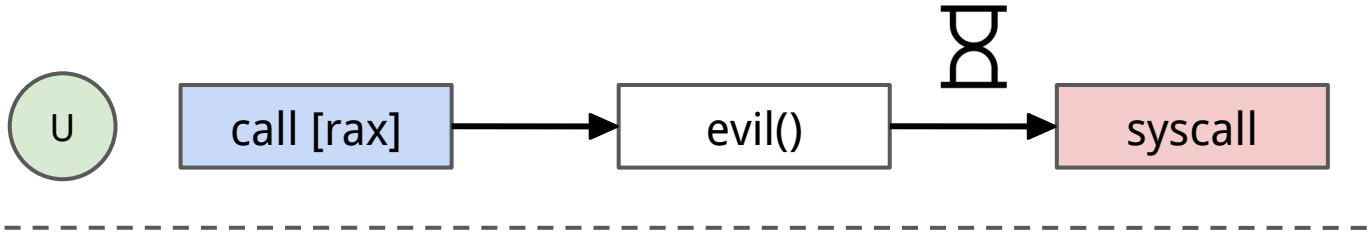
Privilege Switch



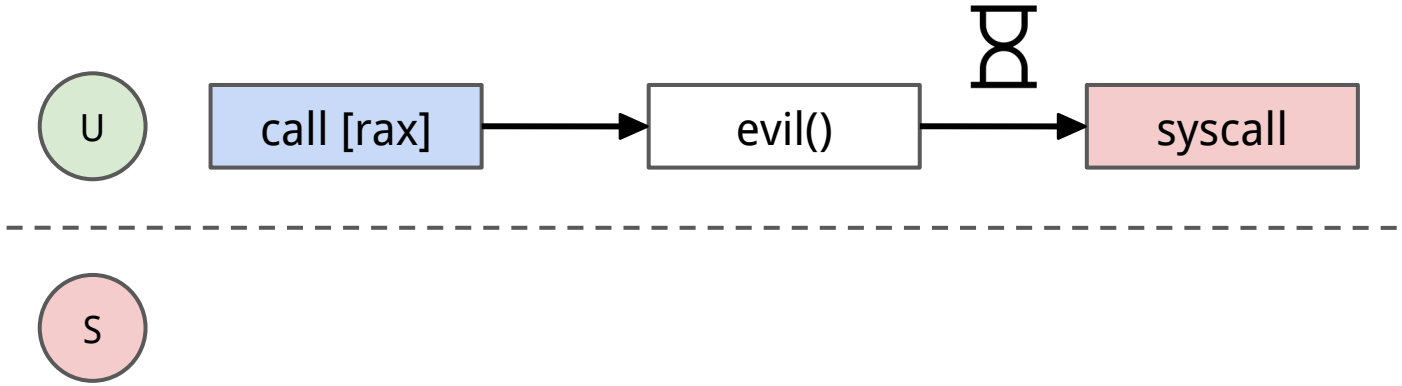
Privilege Switch



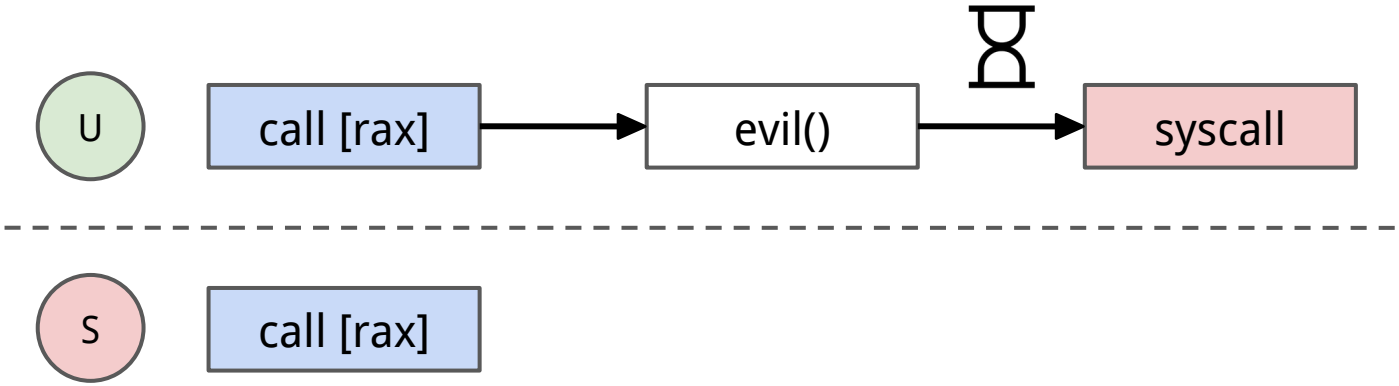
Privilege Switch



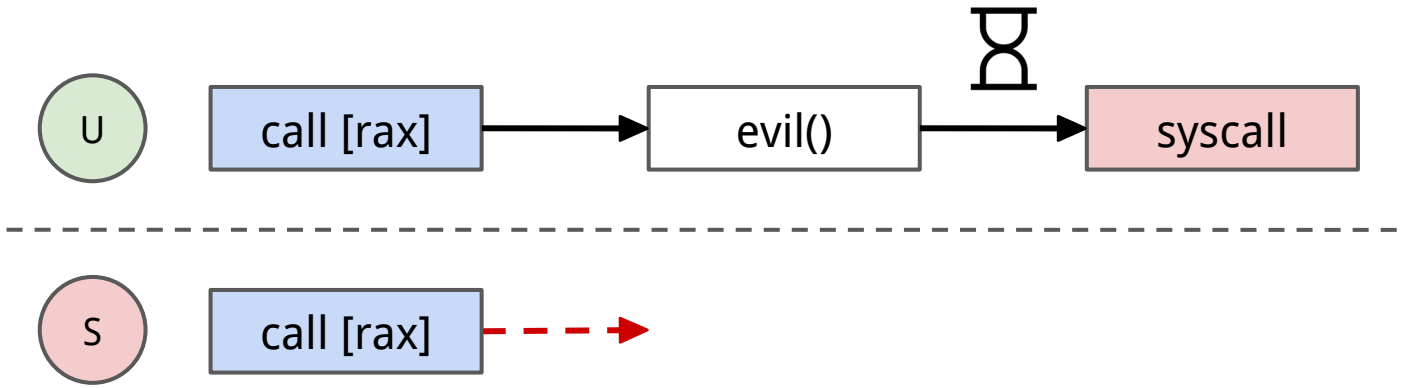
Privilege Switch



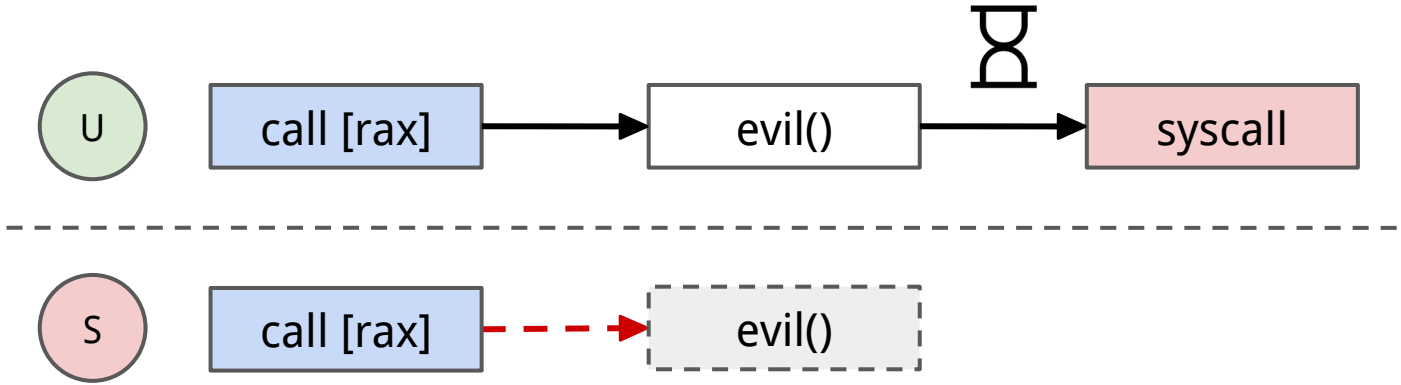
Privilege Switch



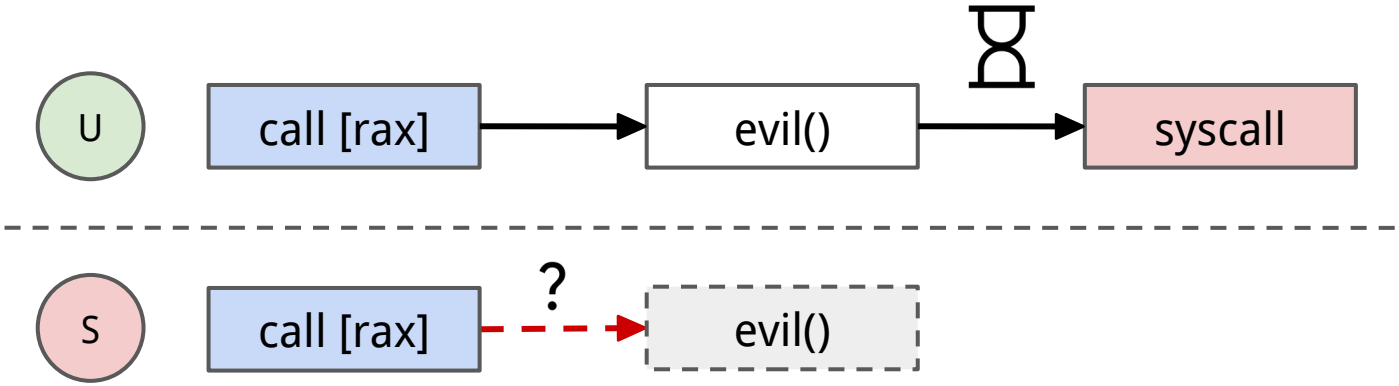
Privilege Switch



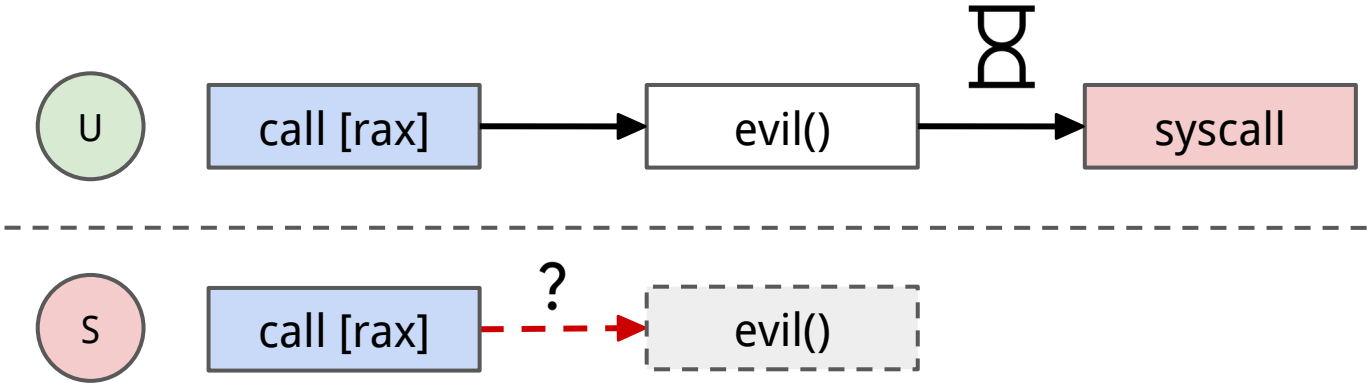
Privilege Switch

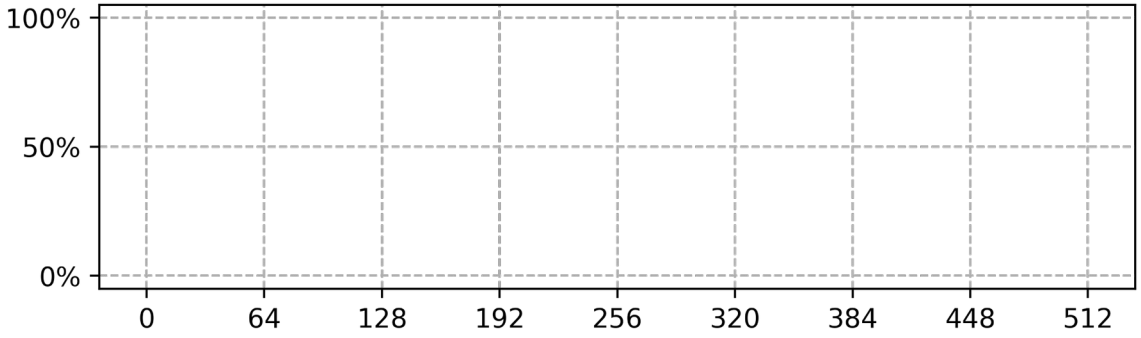


Privilege Switch

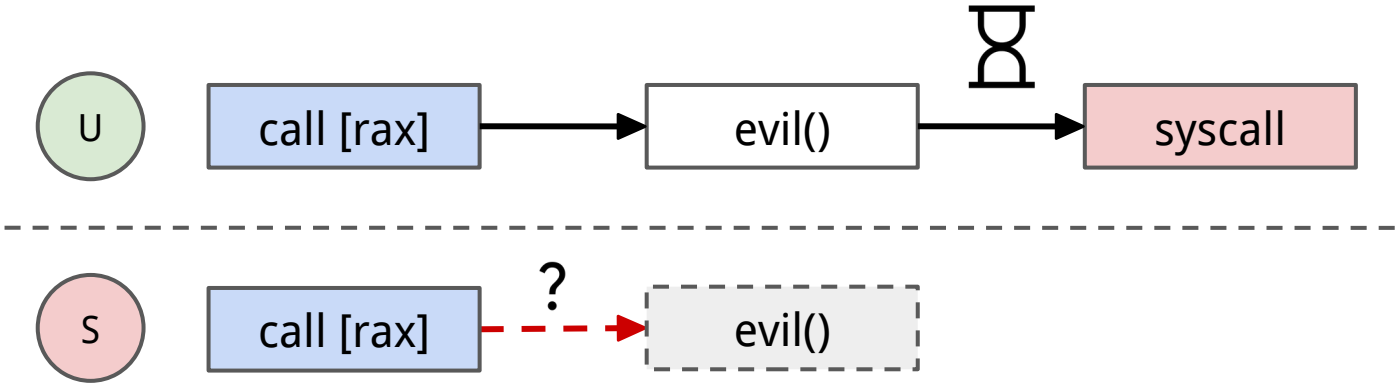


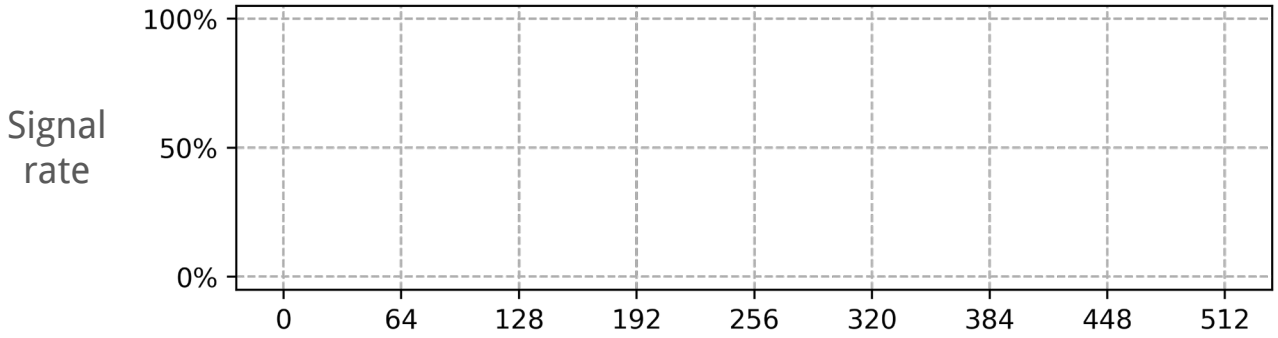
Privilege Switch



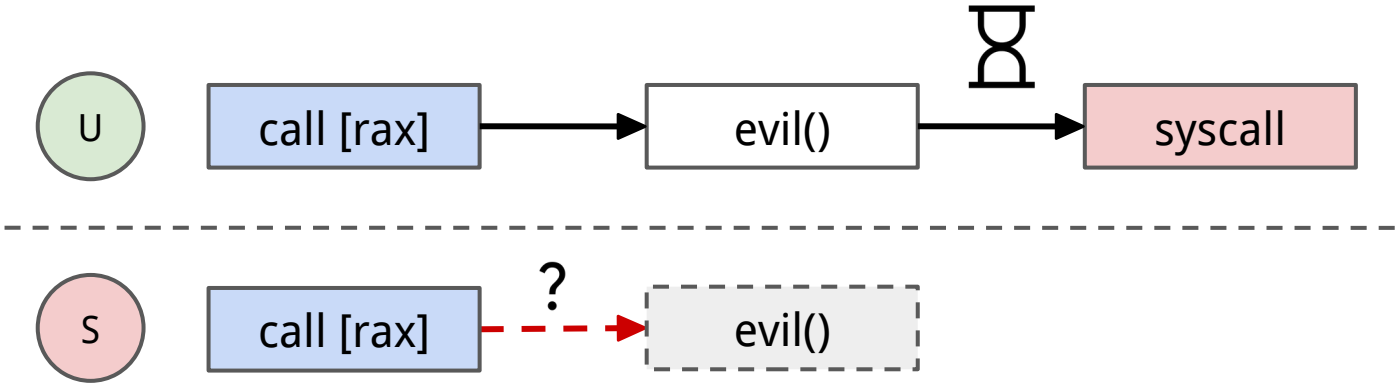


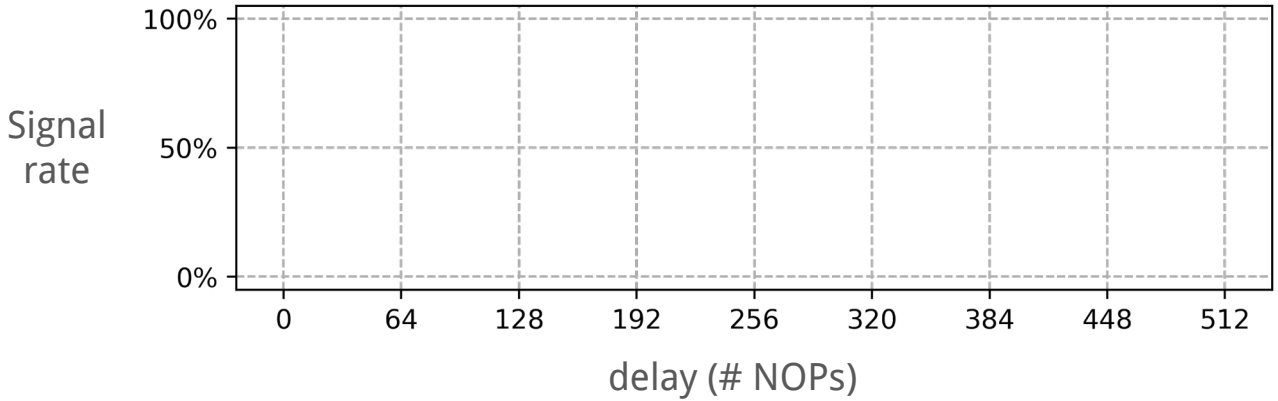
Privilege Switch



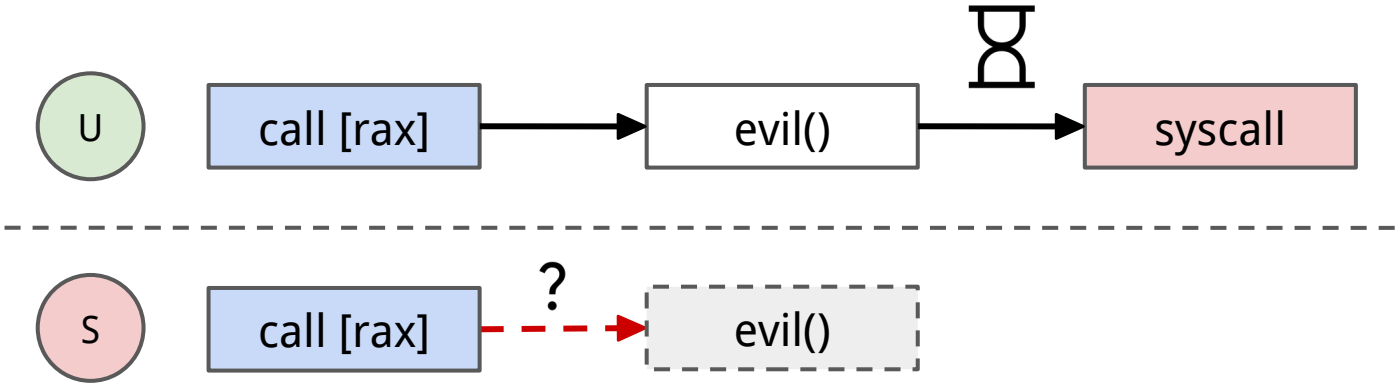


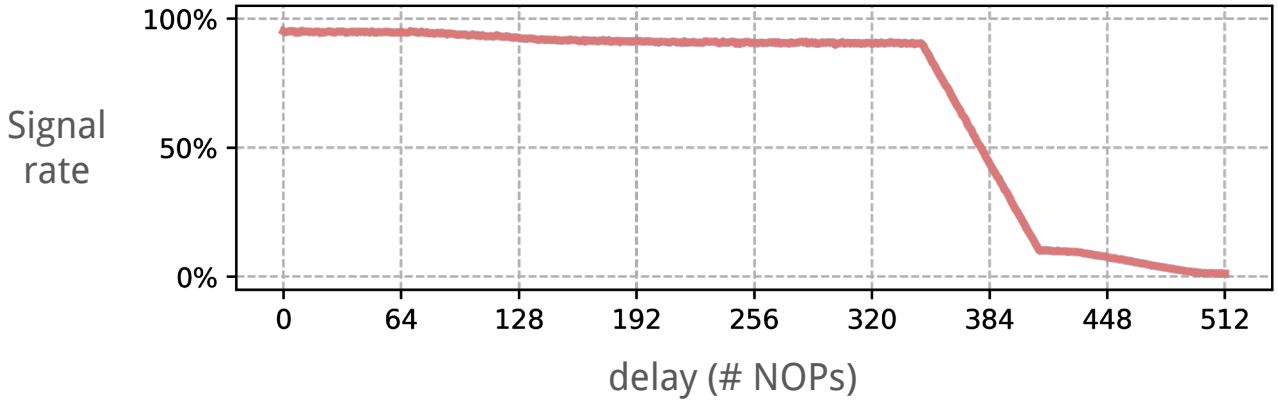
Privilege Switch



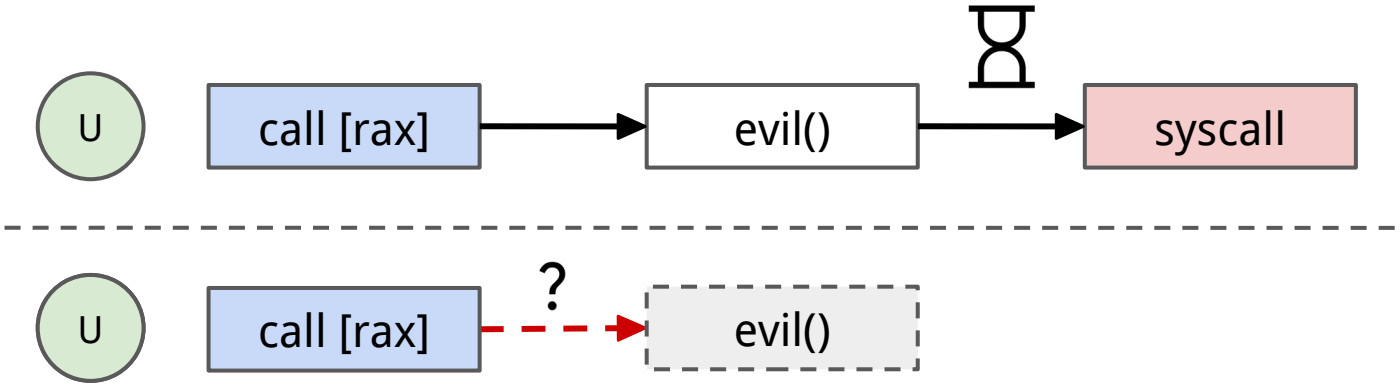


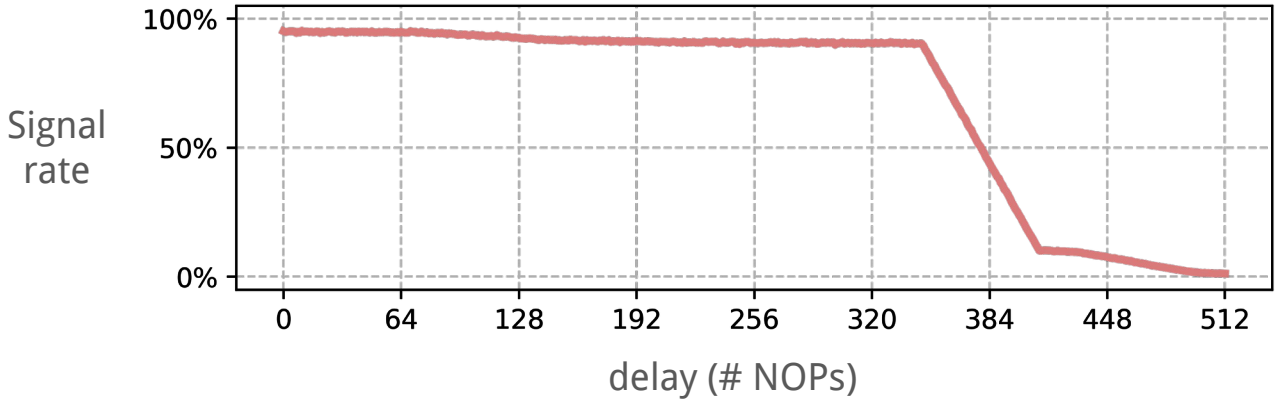
Privilege Switch



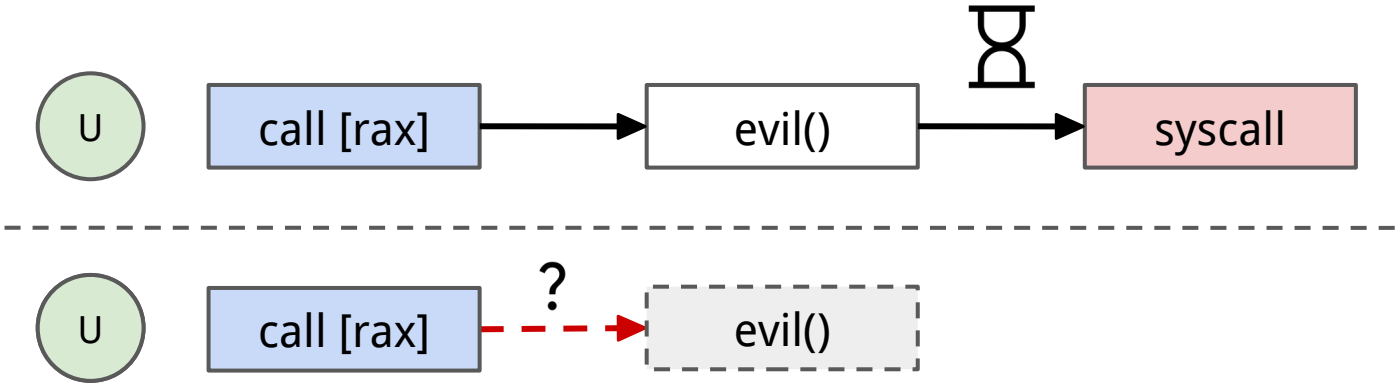


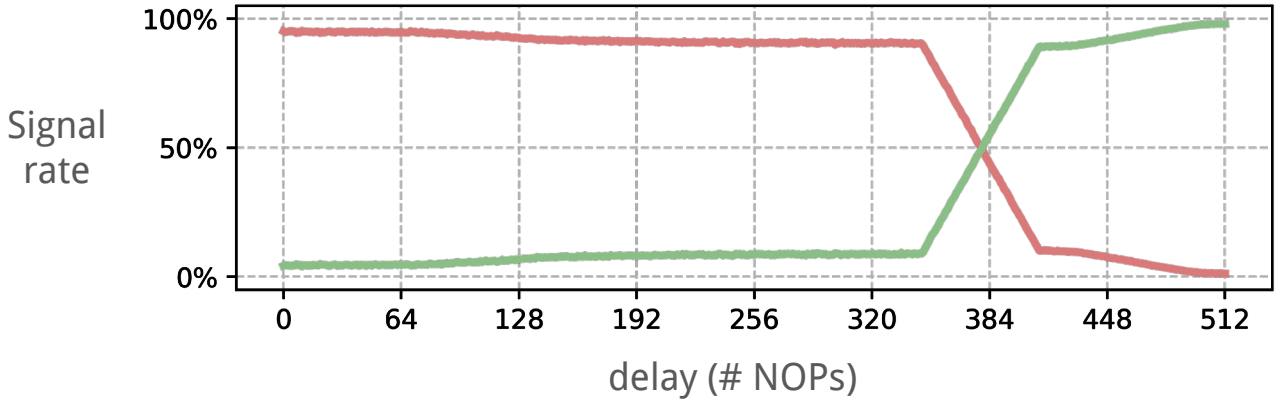
Privilege Switch



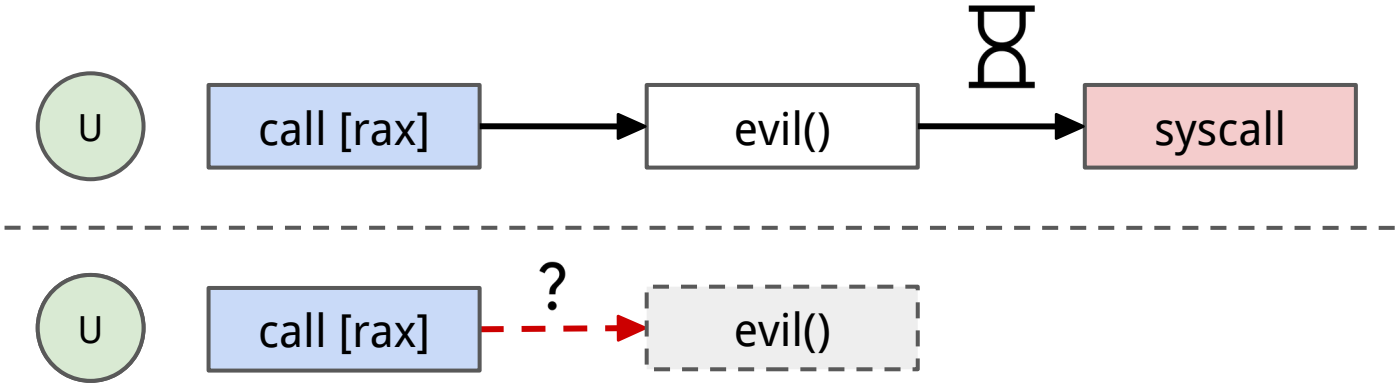


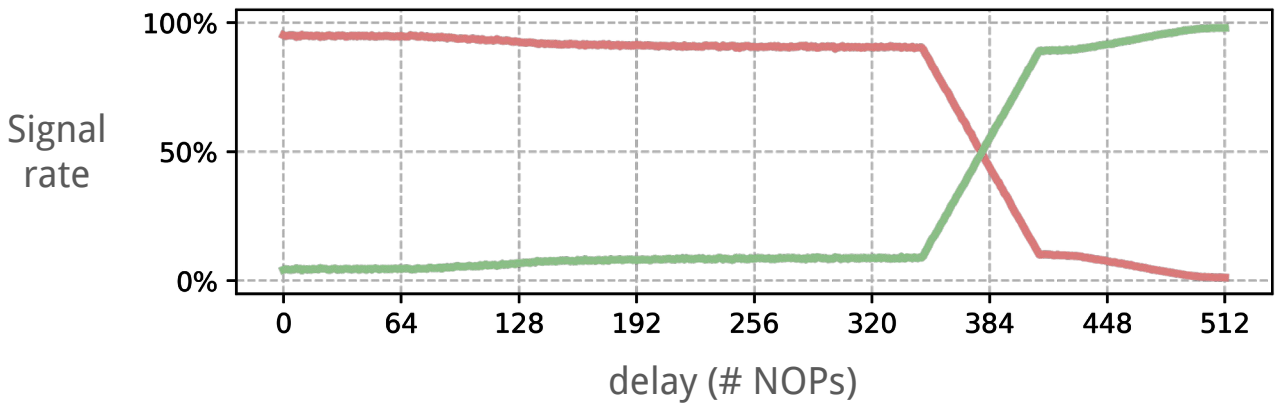
Privilege Switch

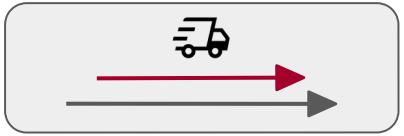




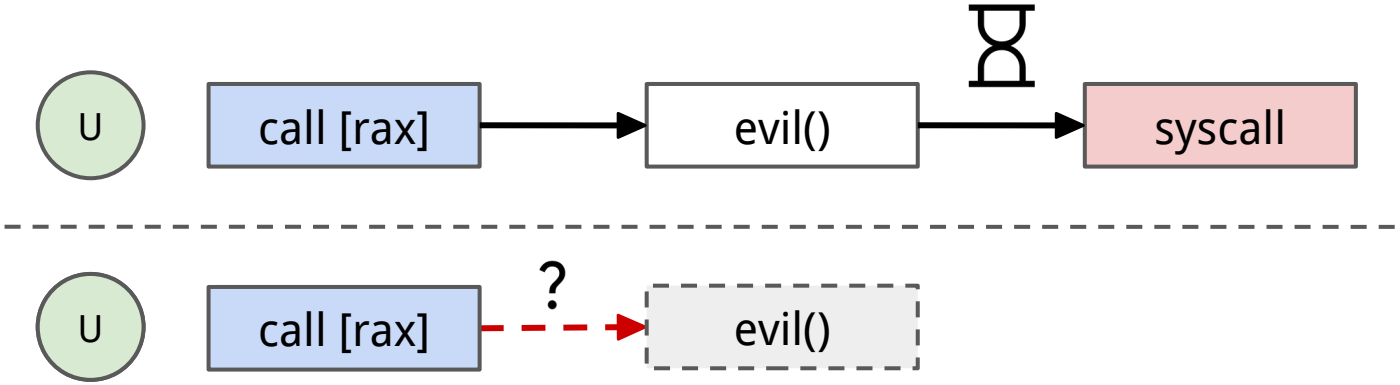
Privilege Switch

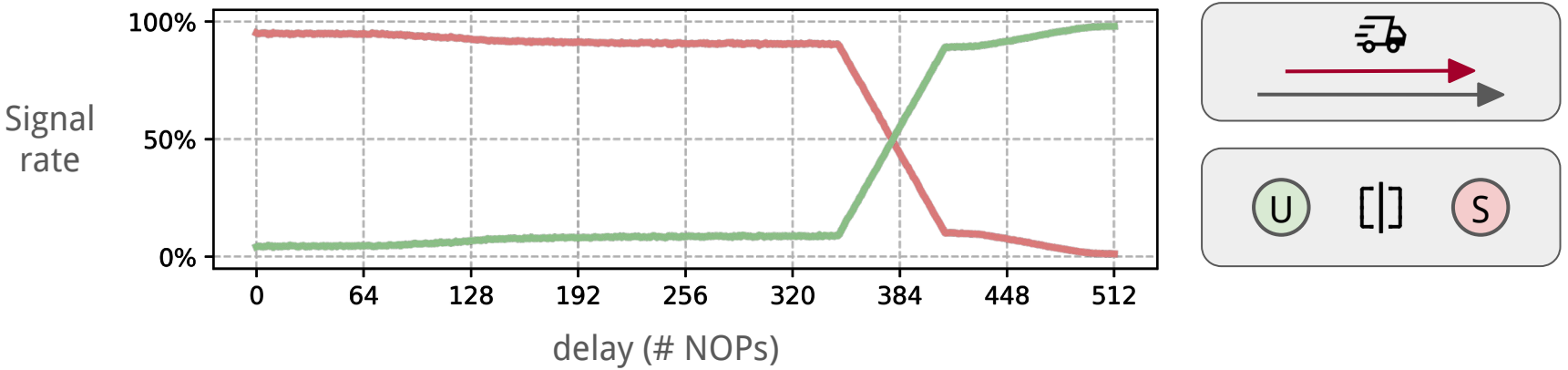




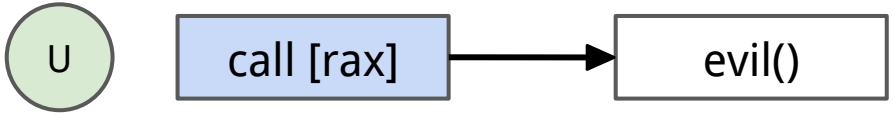


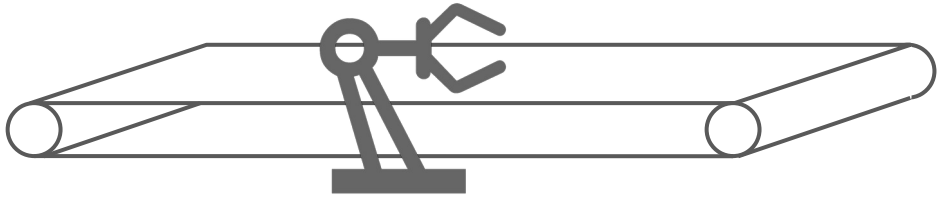
Privilege Switch

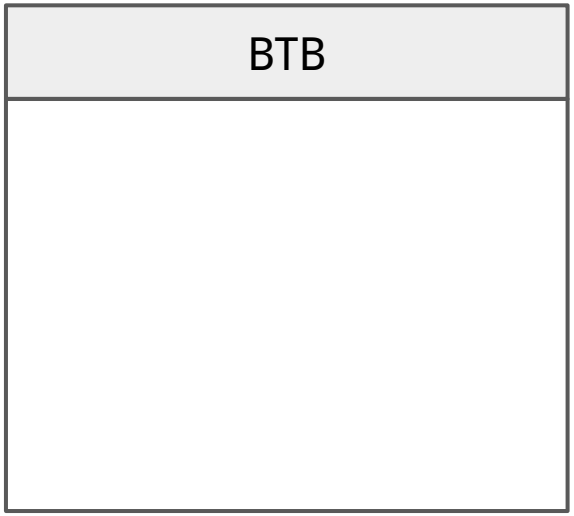




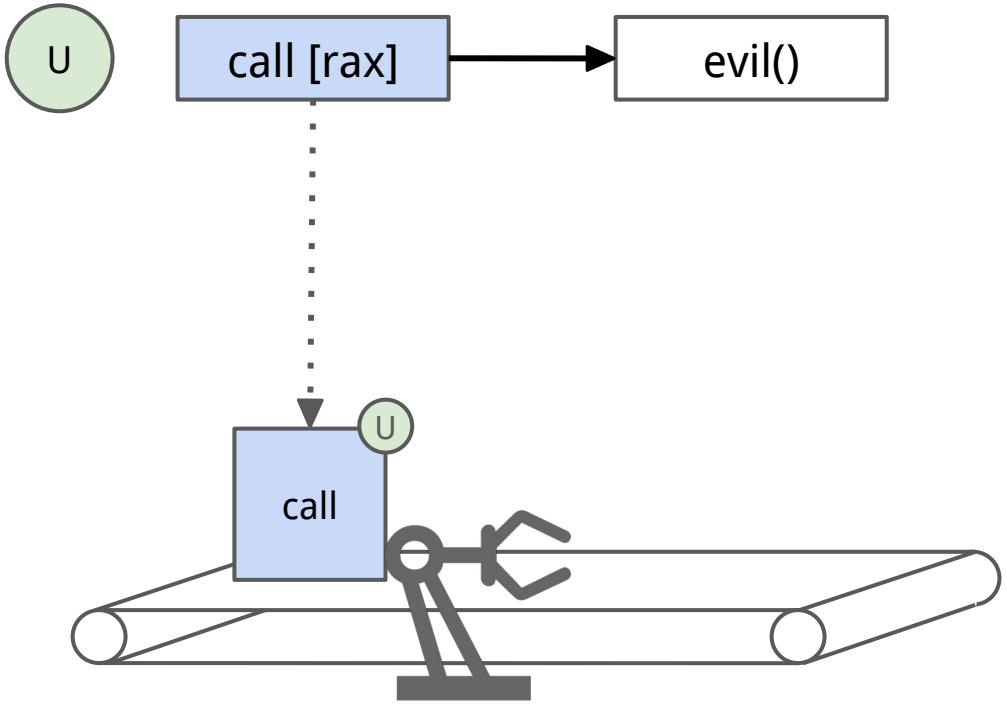
Privilege Switch

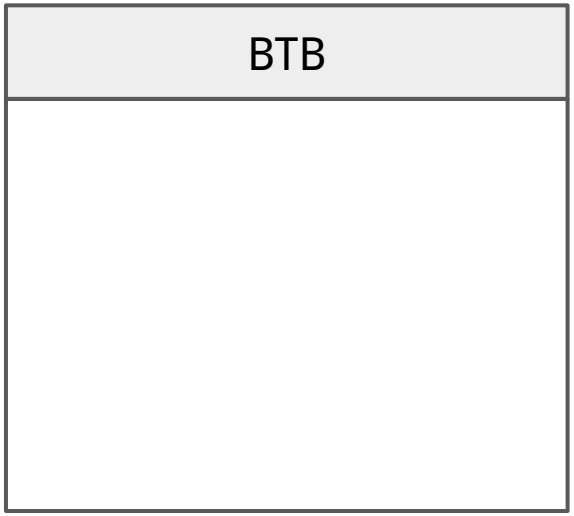




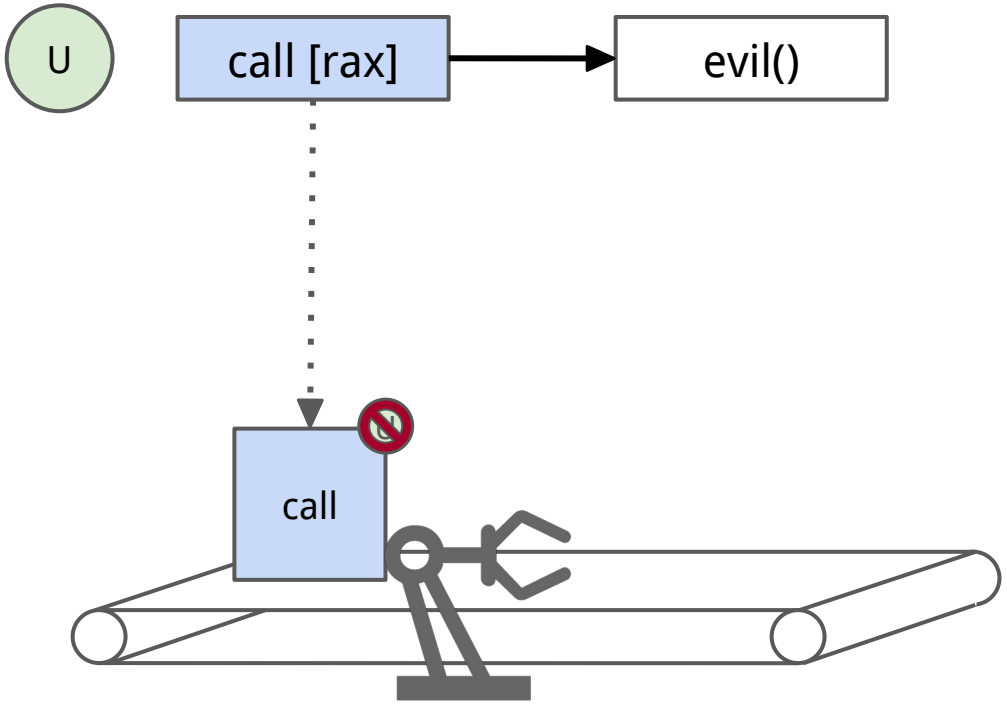


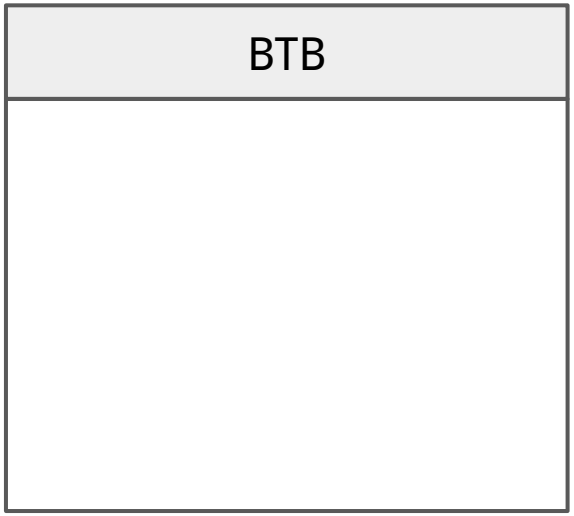
Privilege Switch



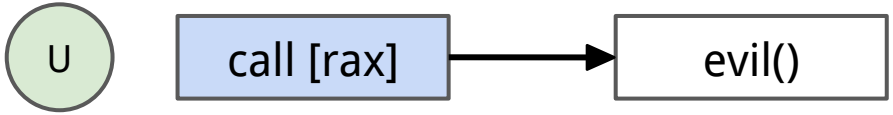


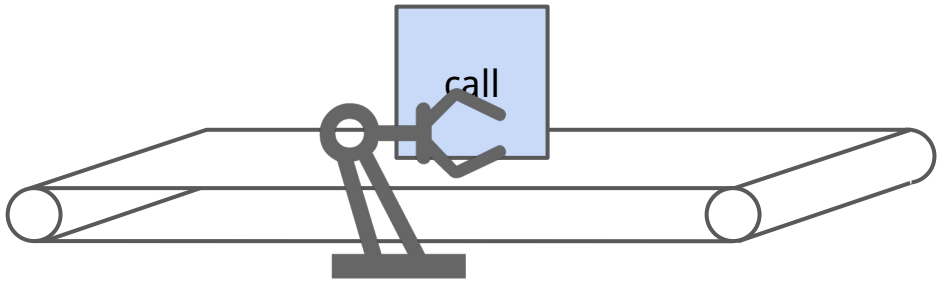
Privilege Switch

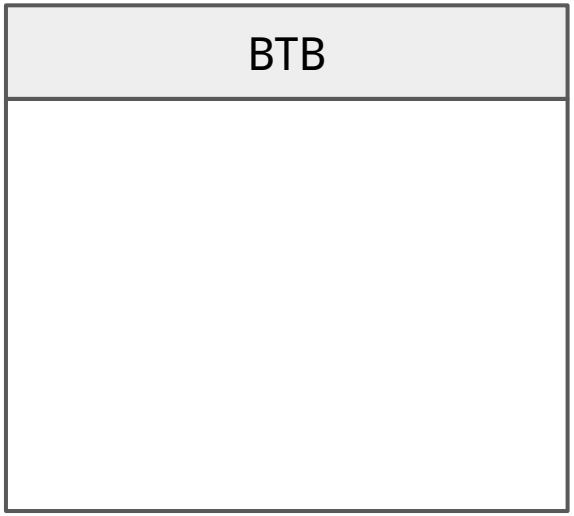




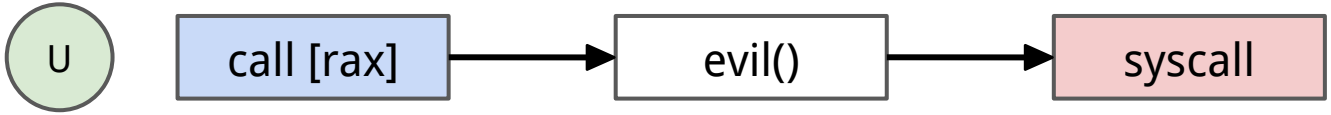
Privilege Switch

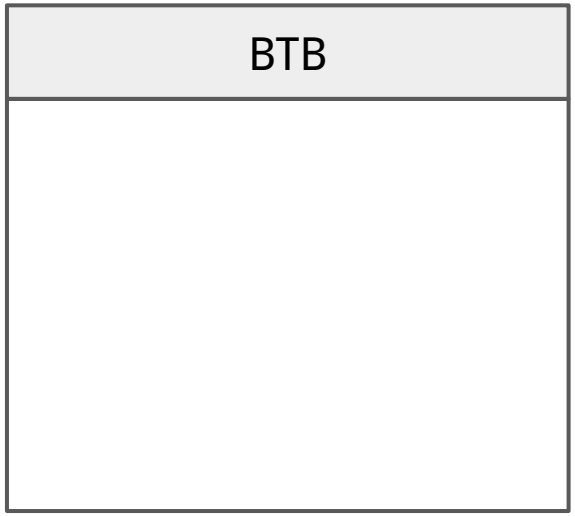


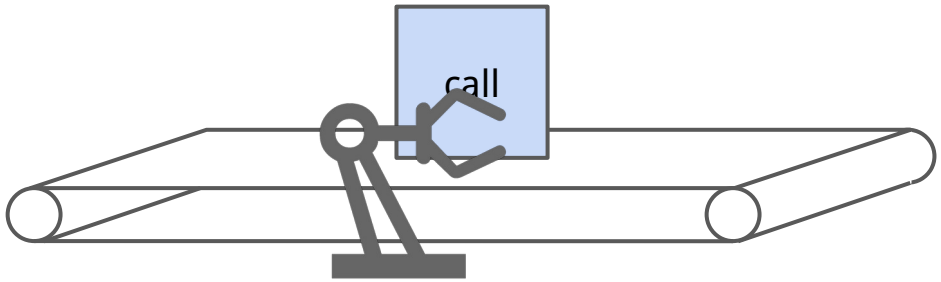




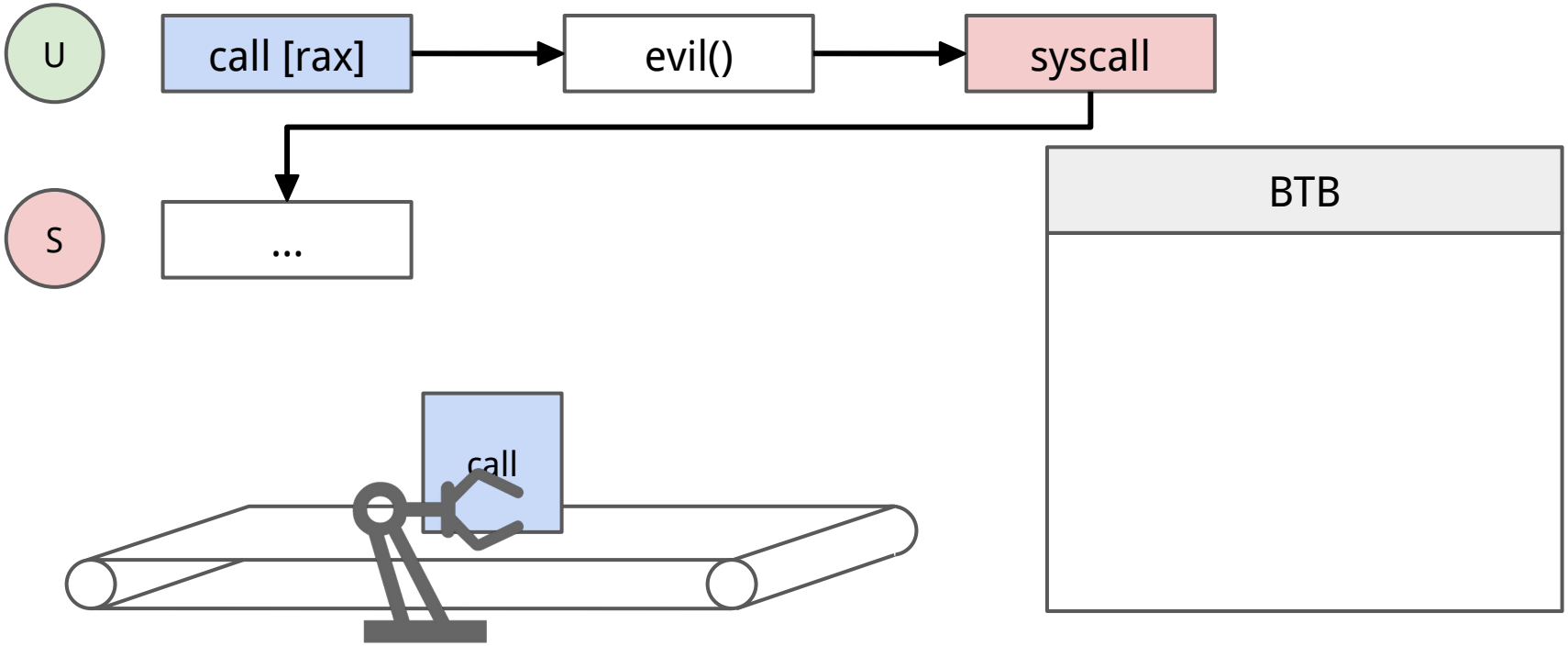
Privilege Switch



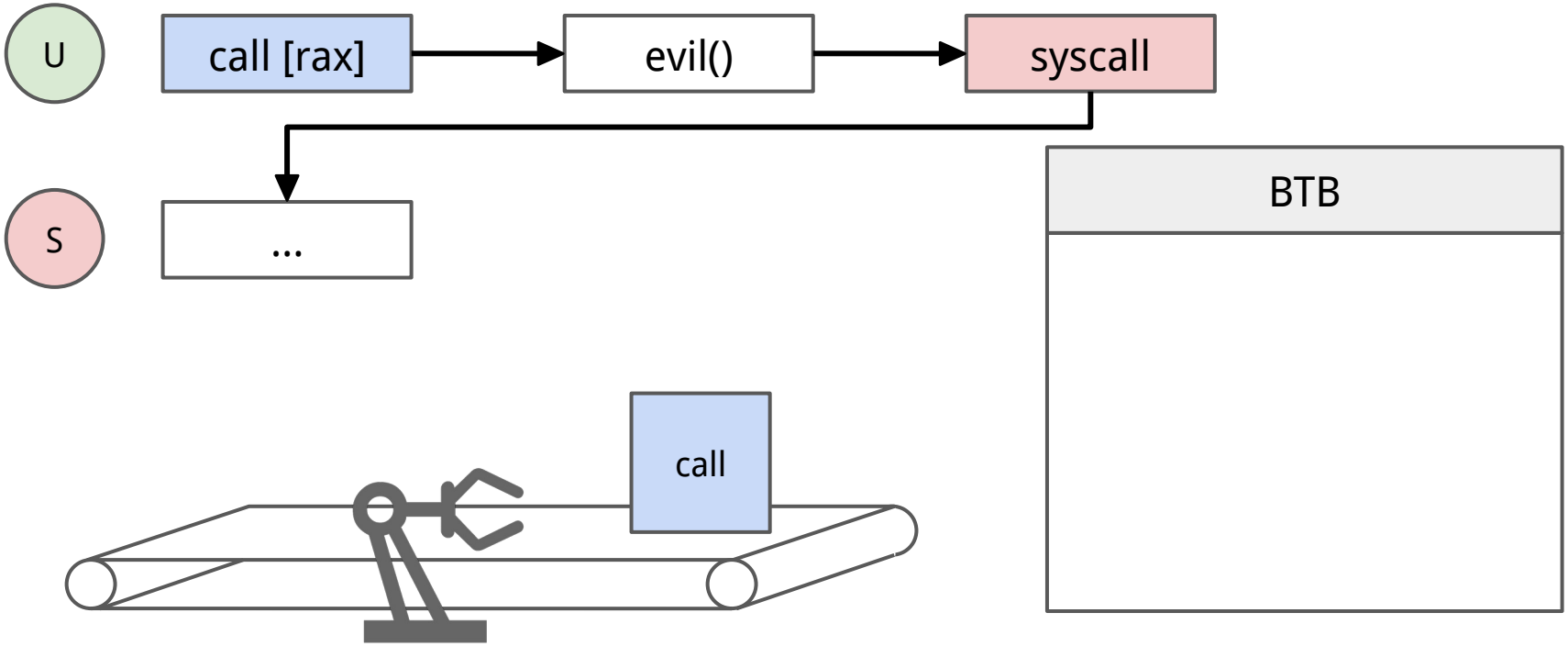




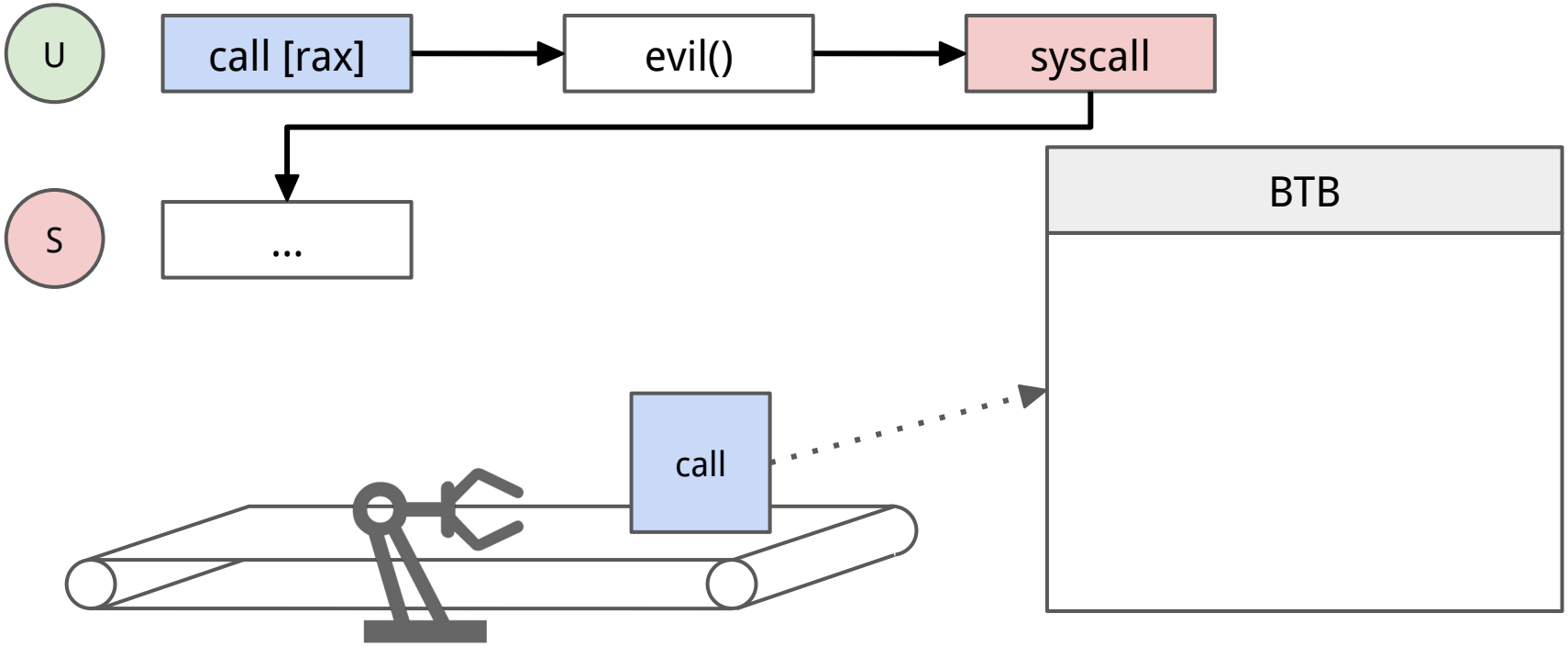
Privilege Switch



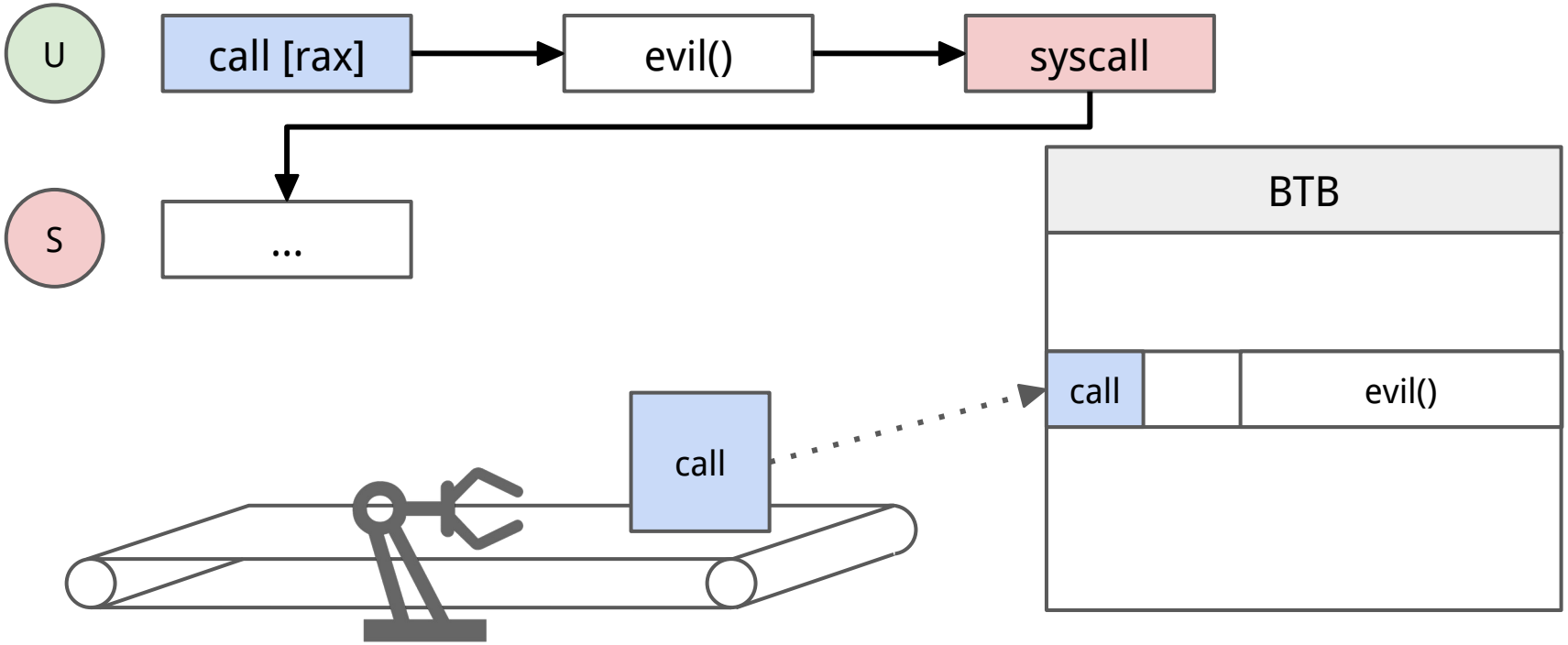
Privilege Switch



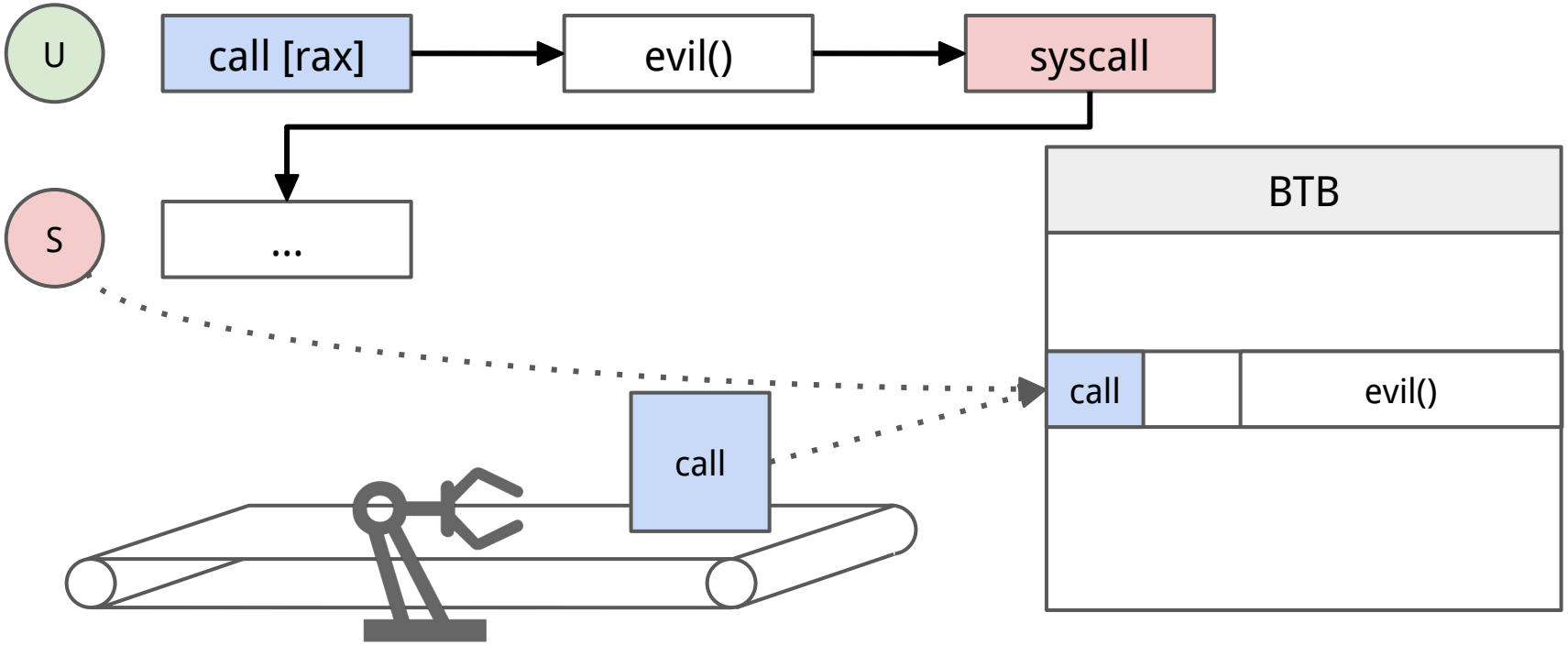
Privilege Switch



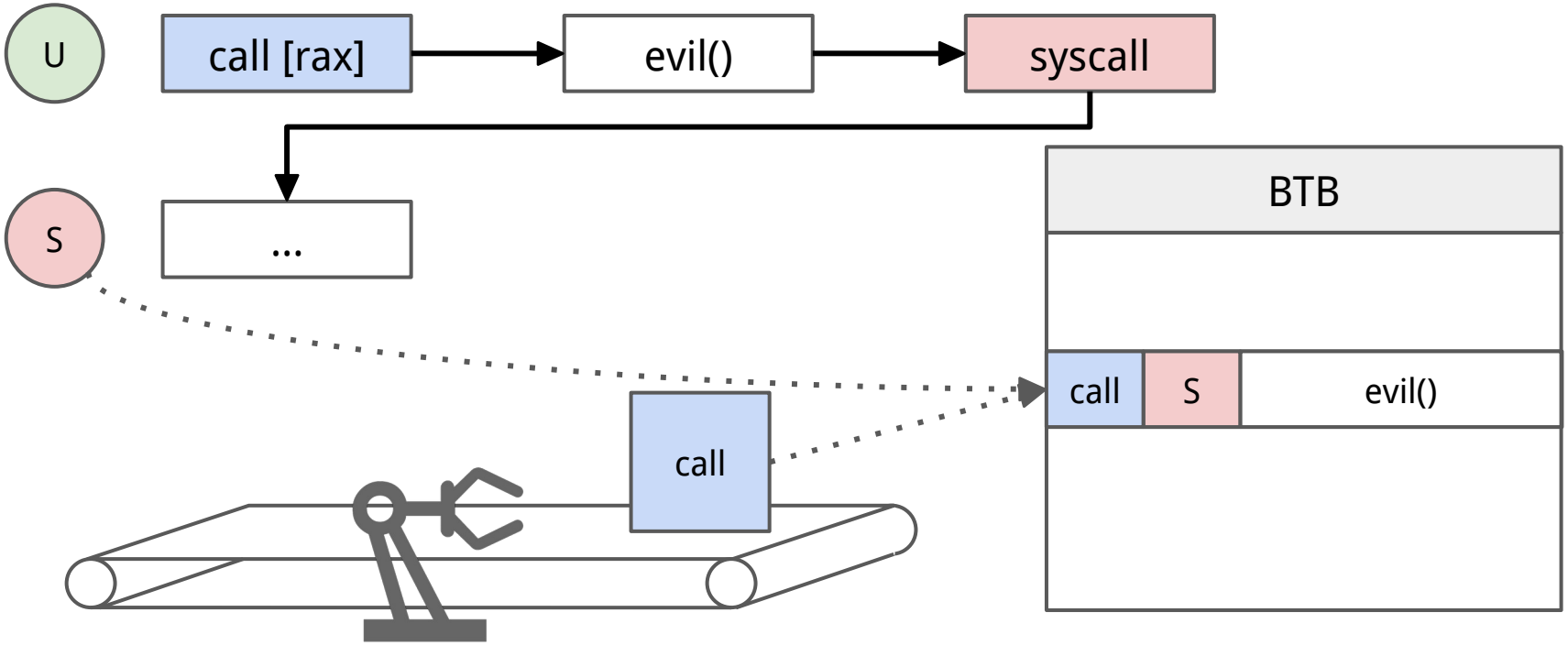
Privilege Switch



Privilege Switch

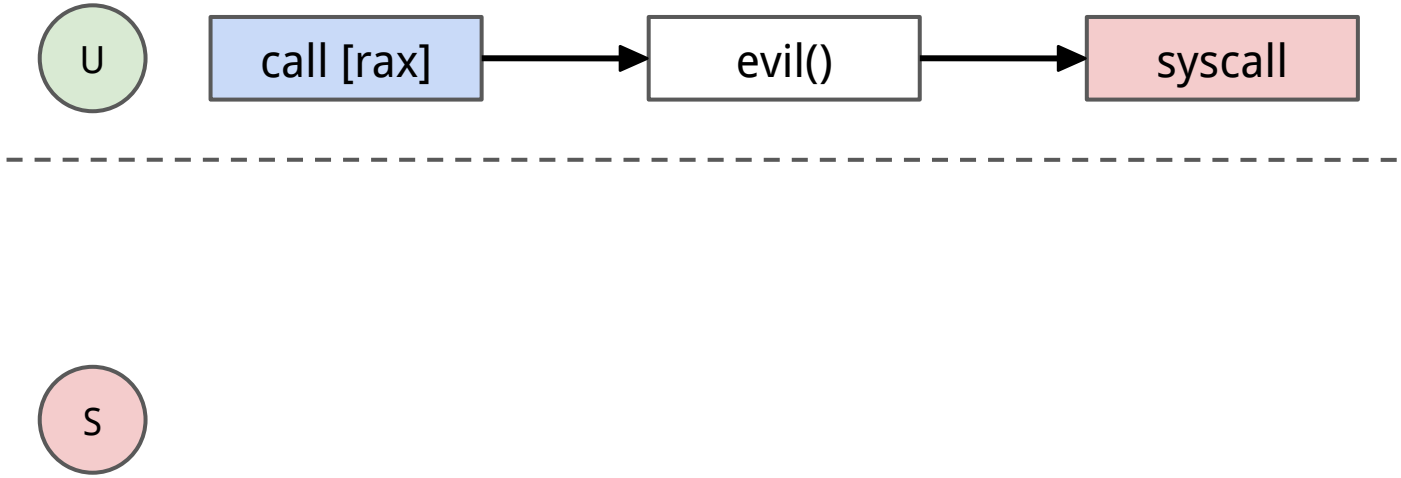


Privilege Switch

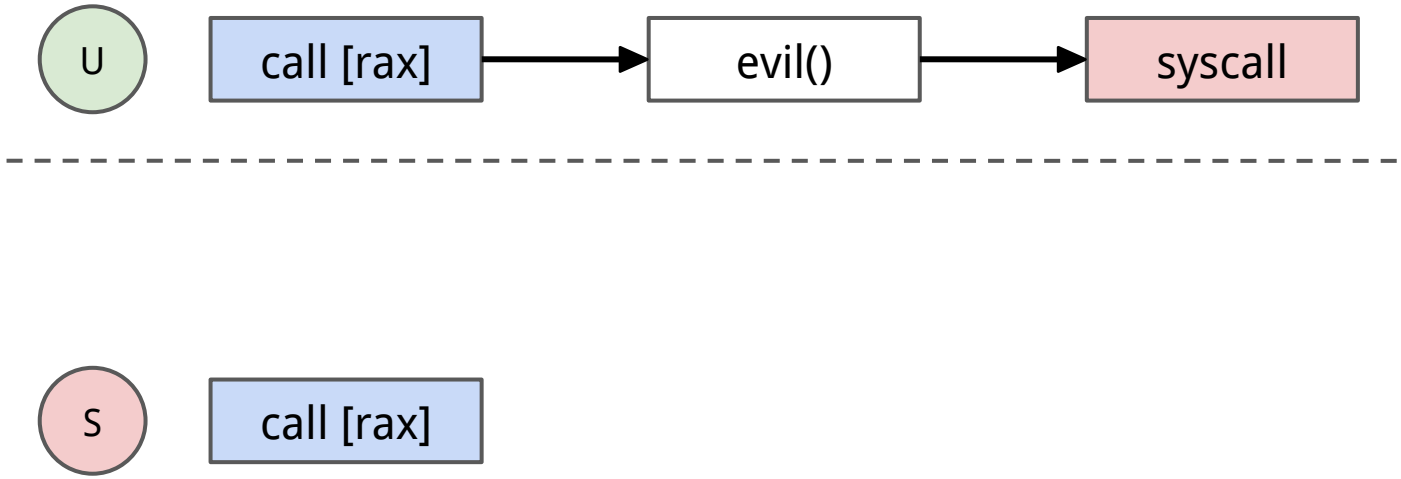


Attack

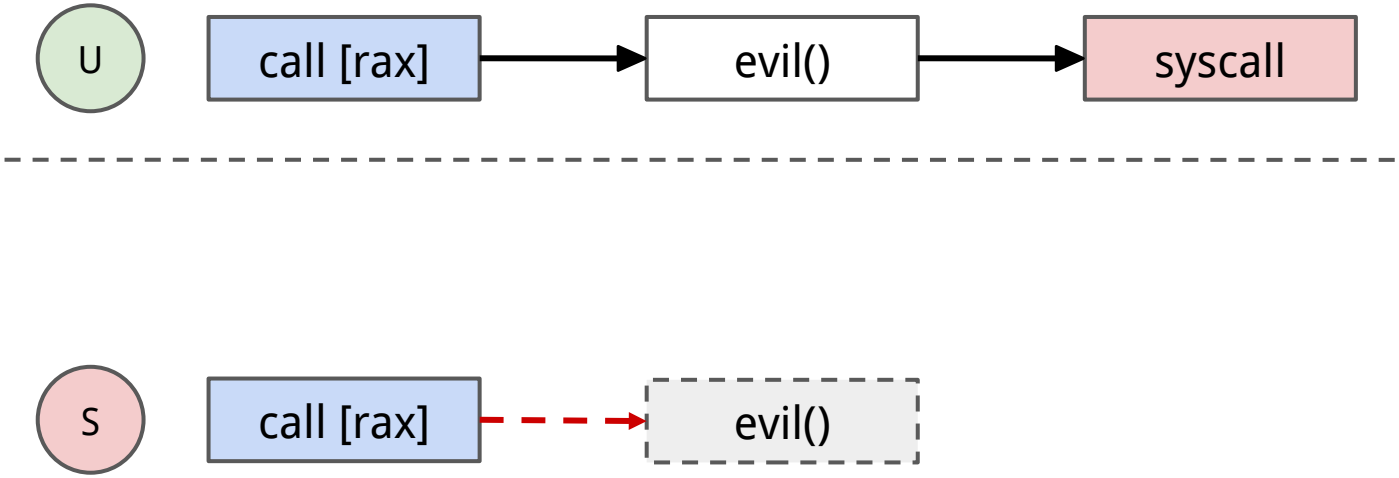
Attack



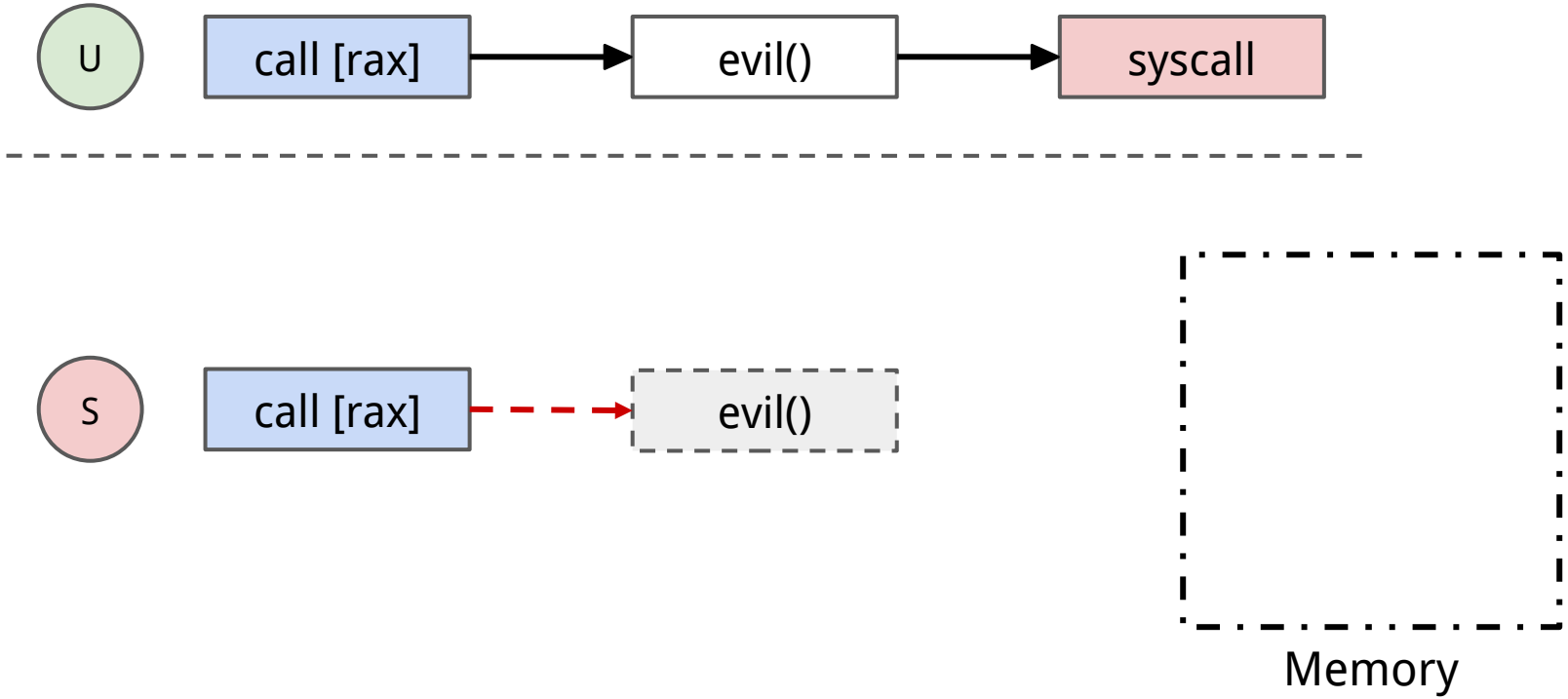
Attack



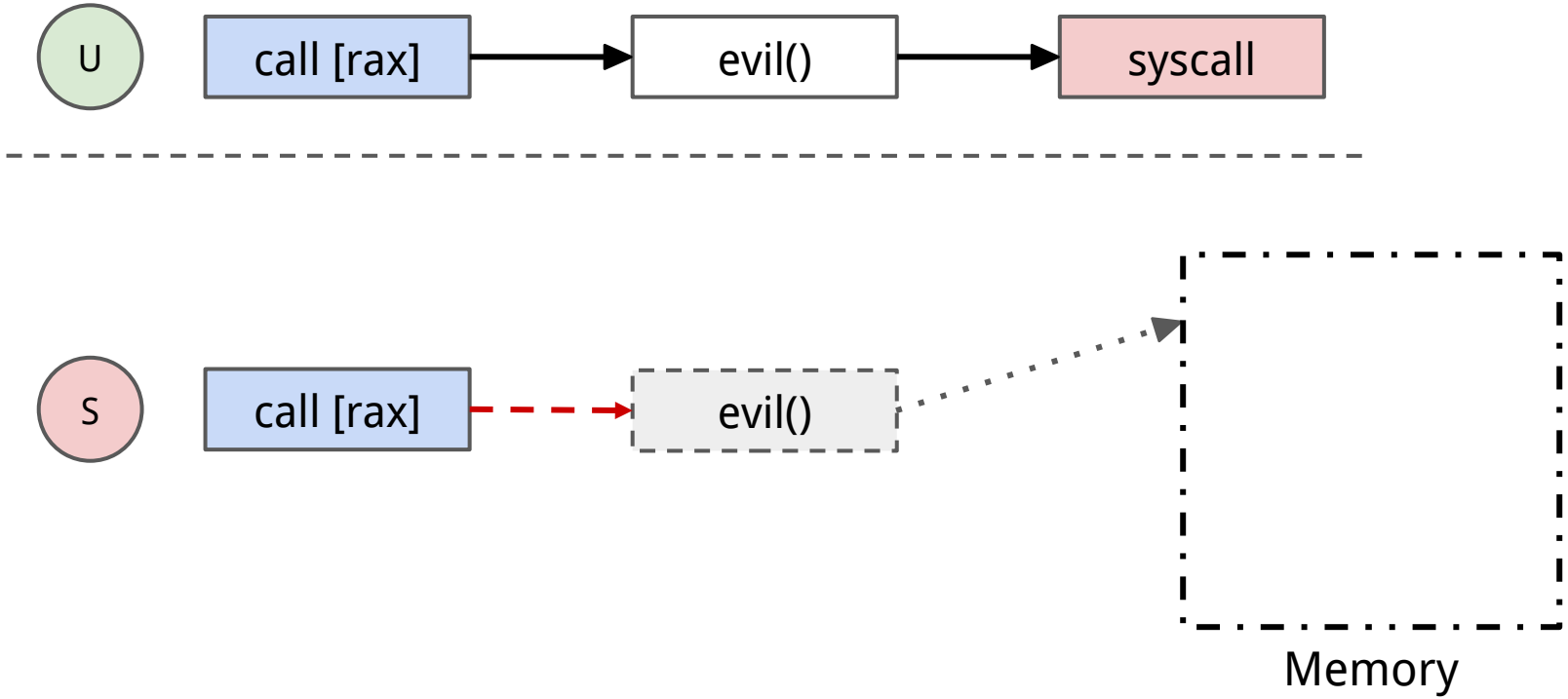
Attack



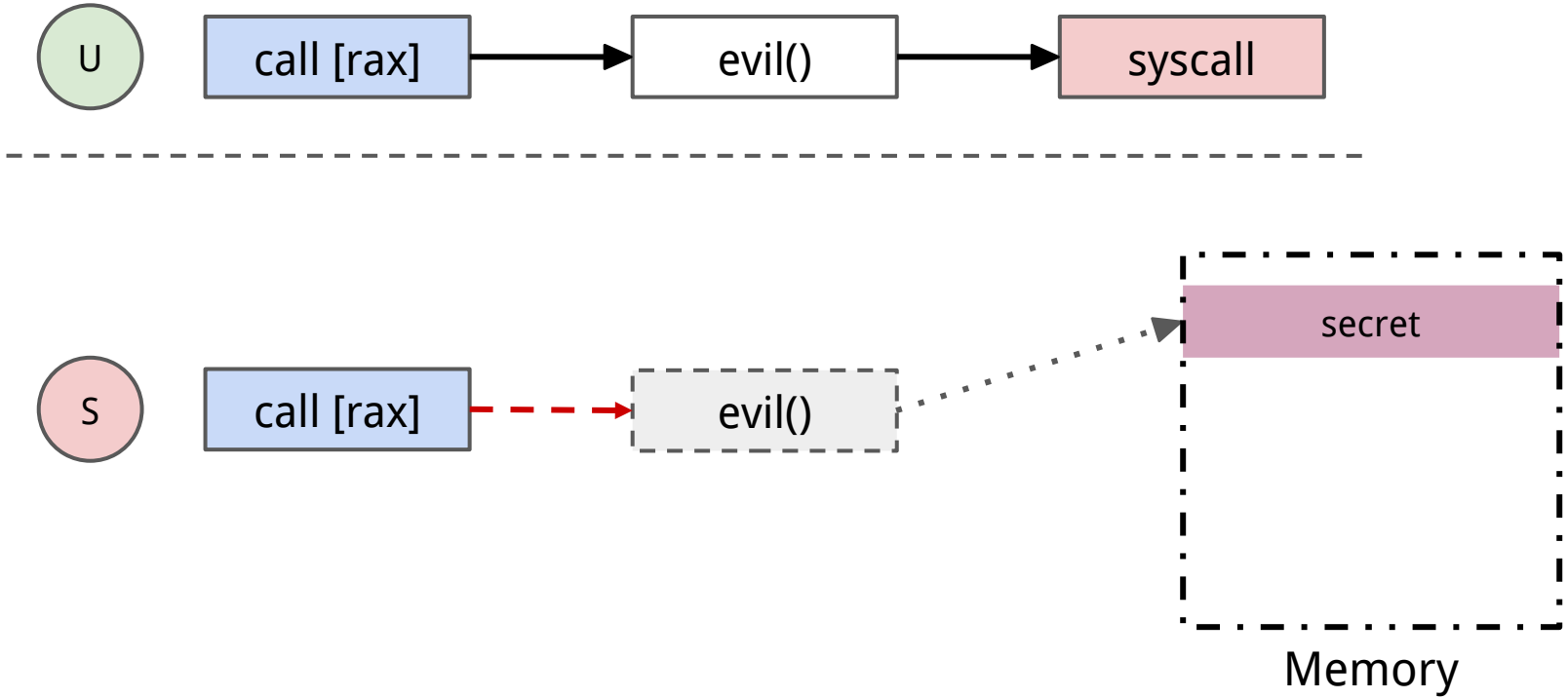
Attack



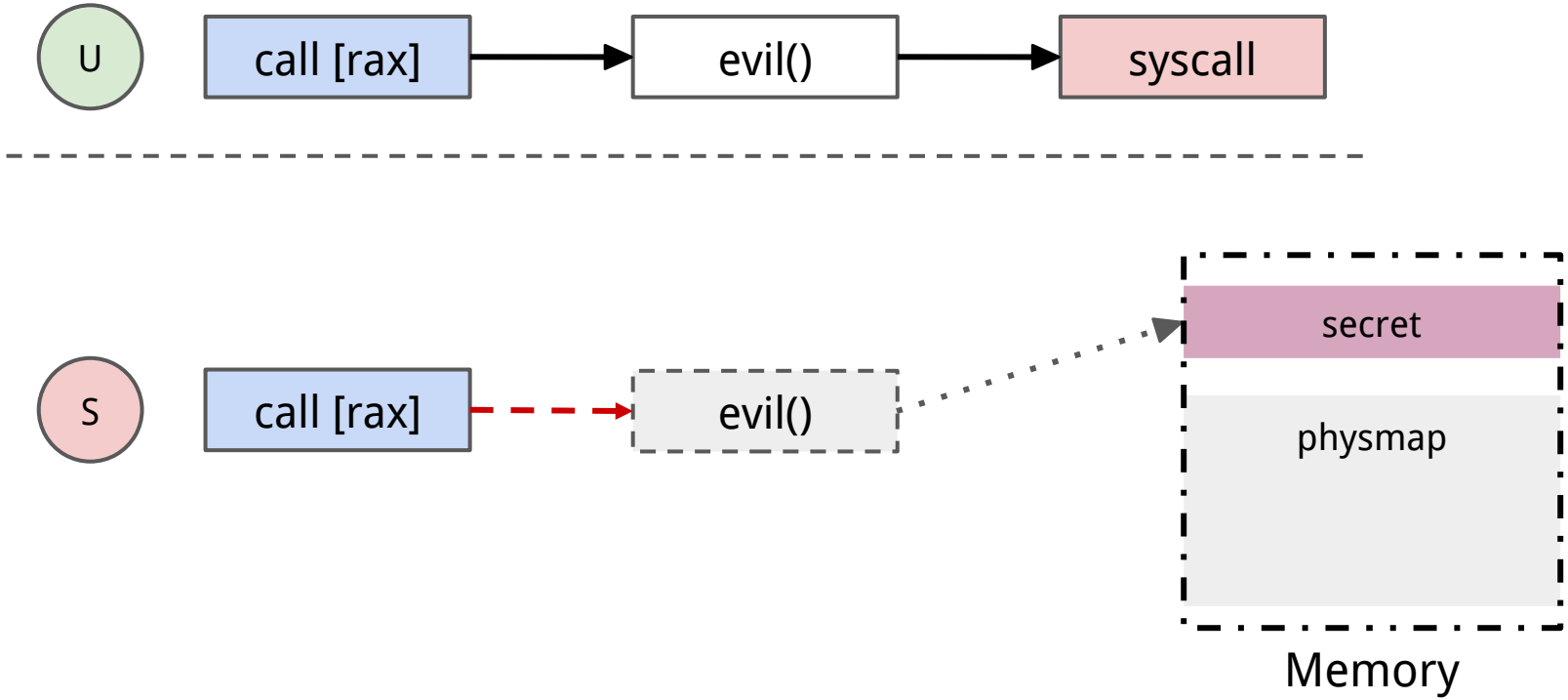
Attack



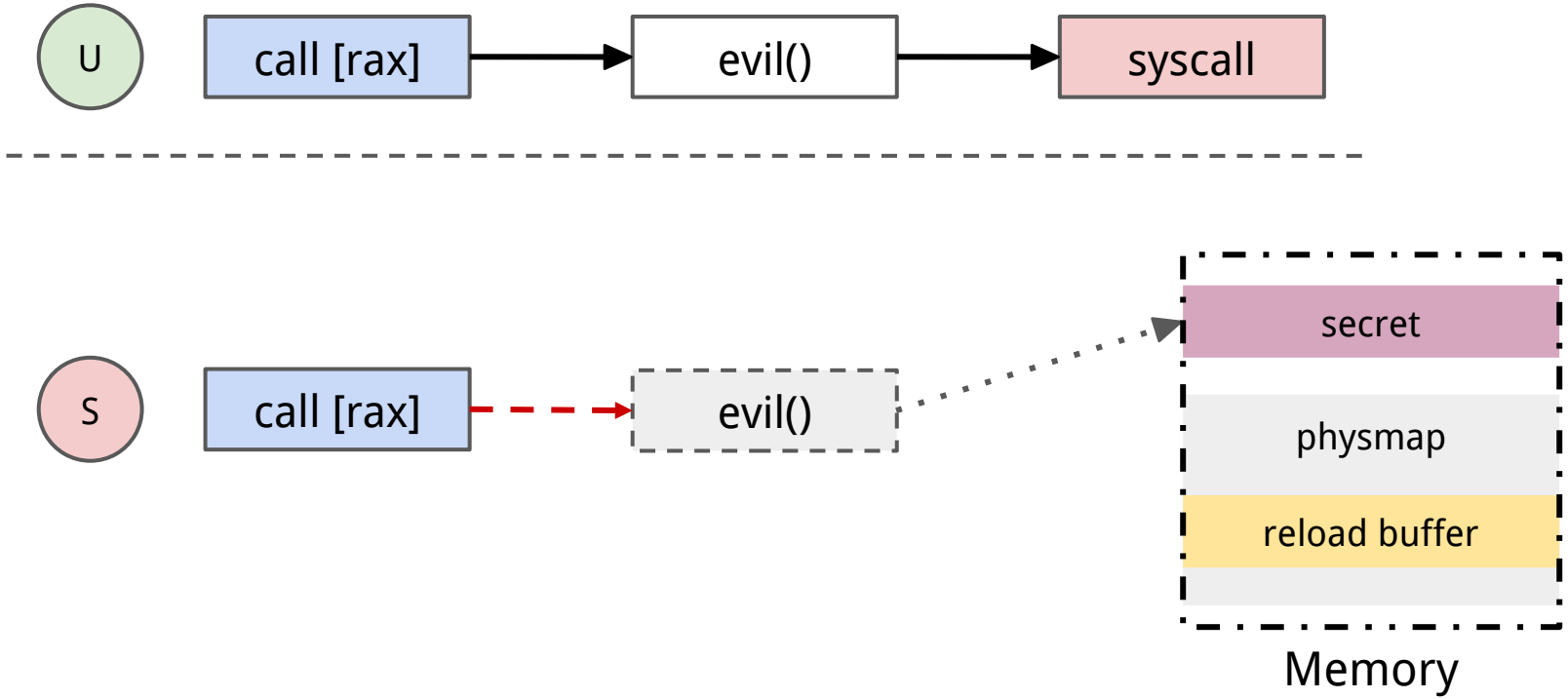
Attack



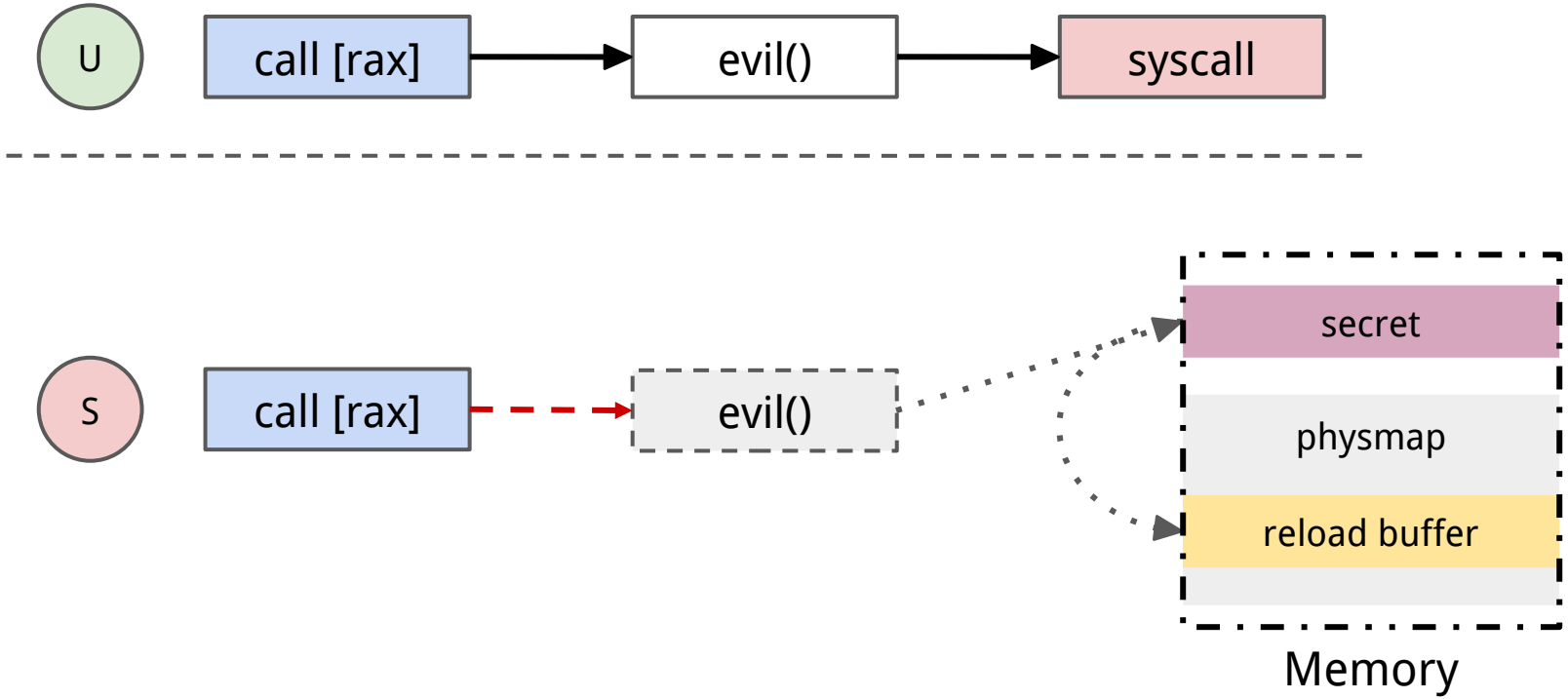
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
Memory

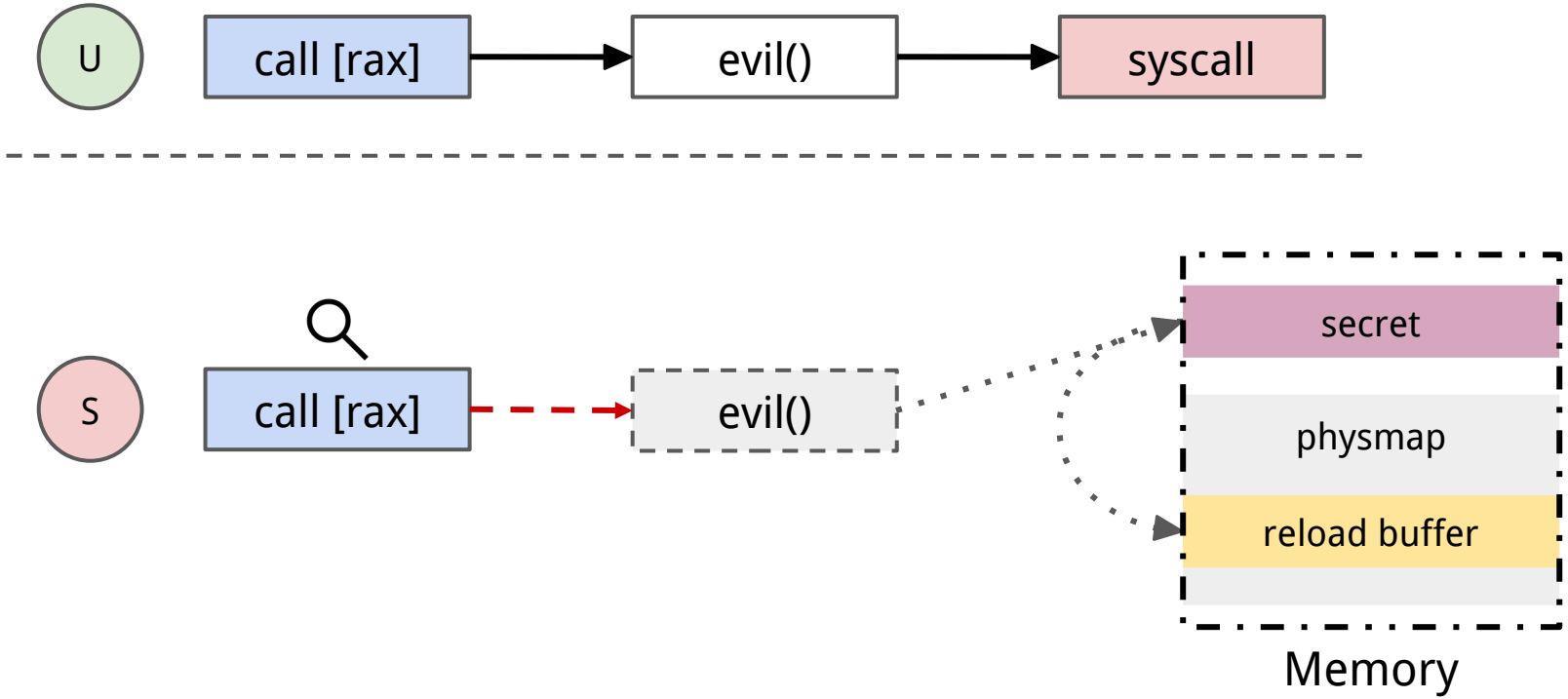
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

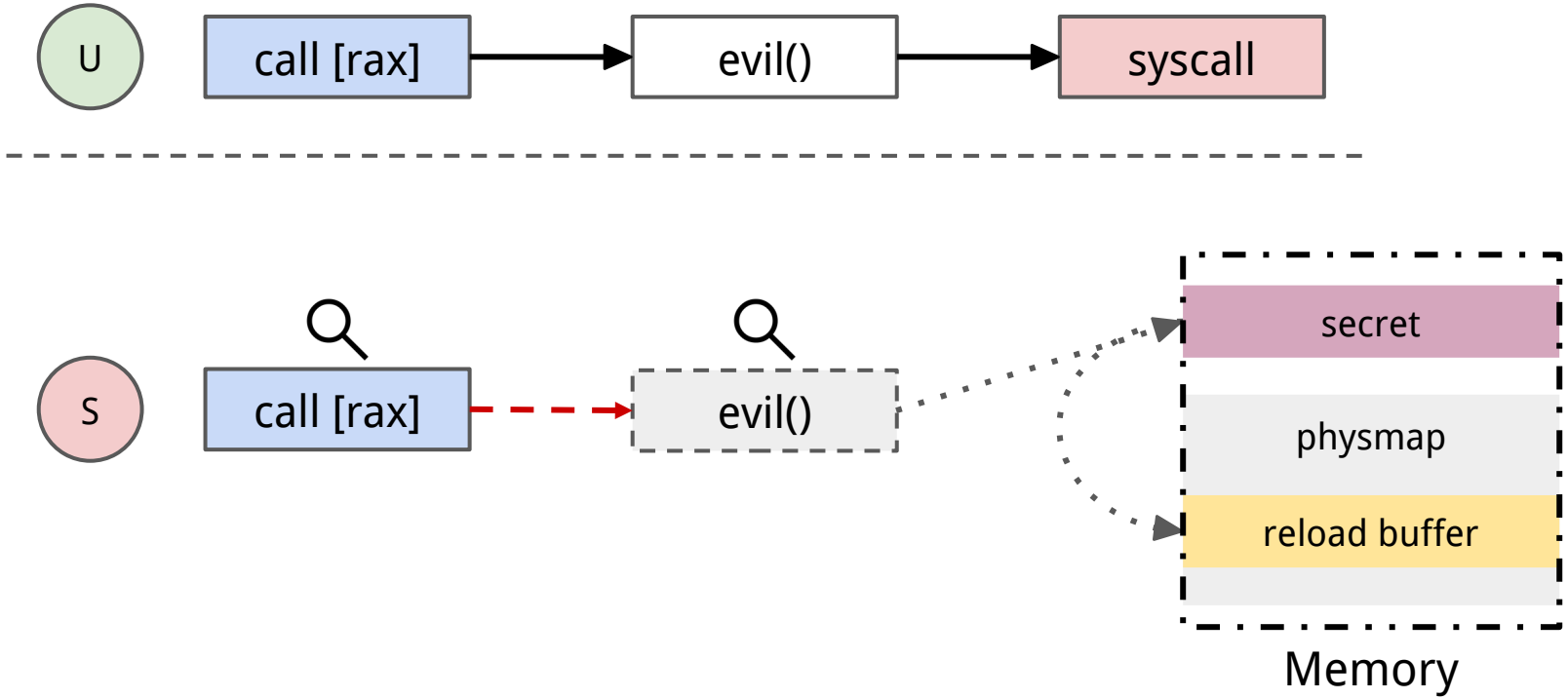
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

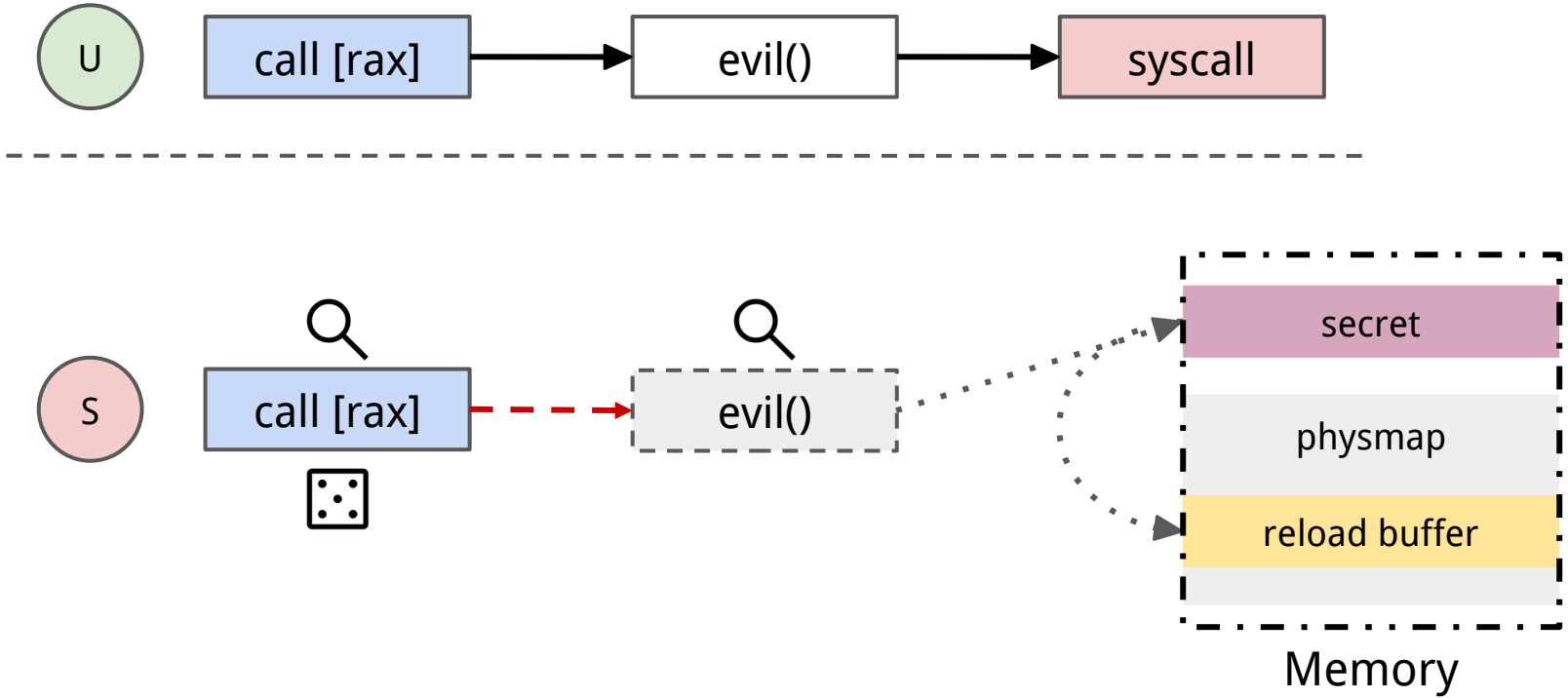
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

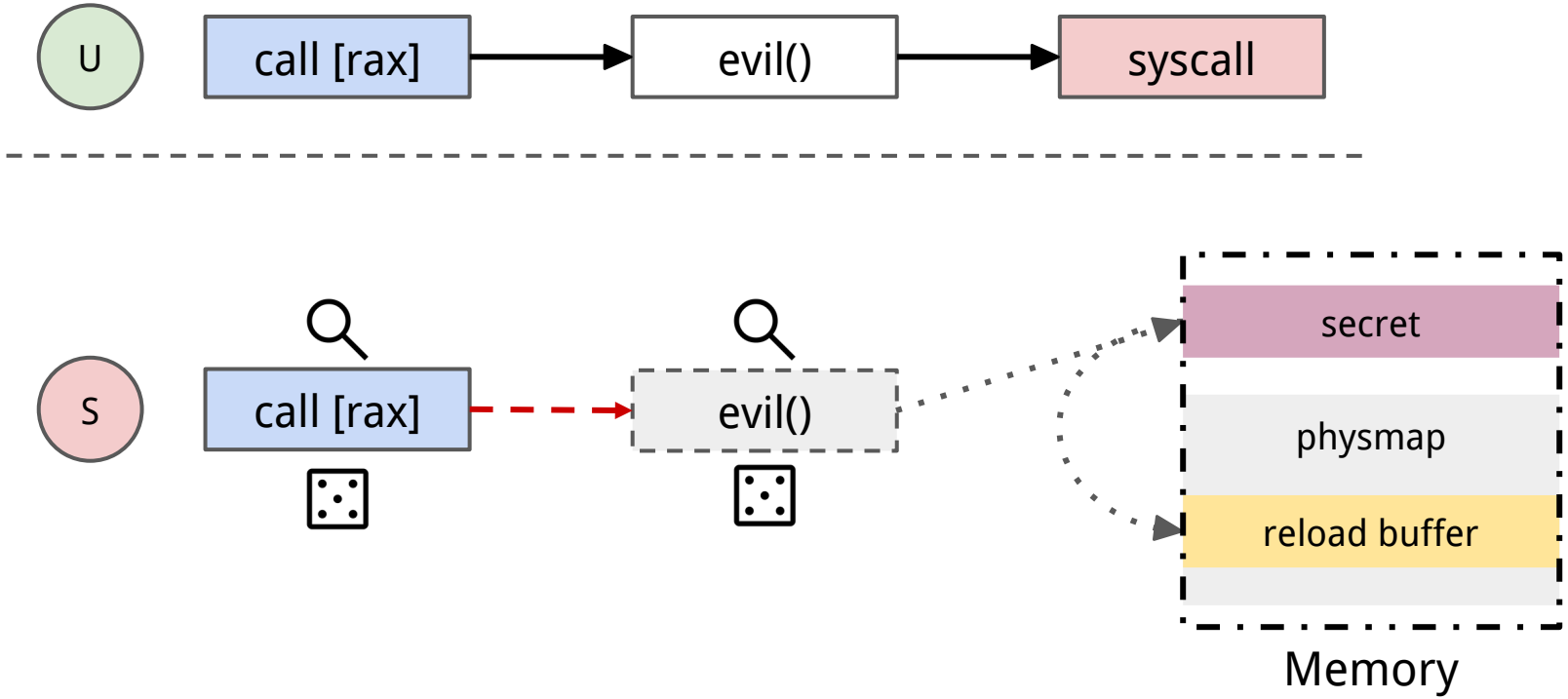
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

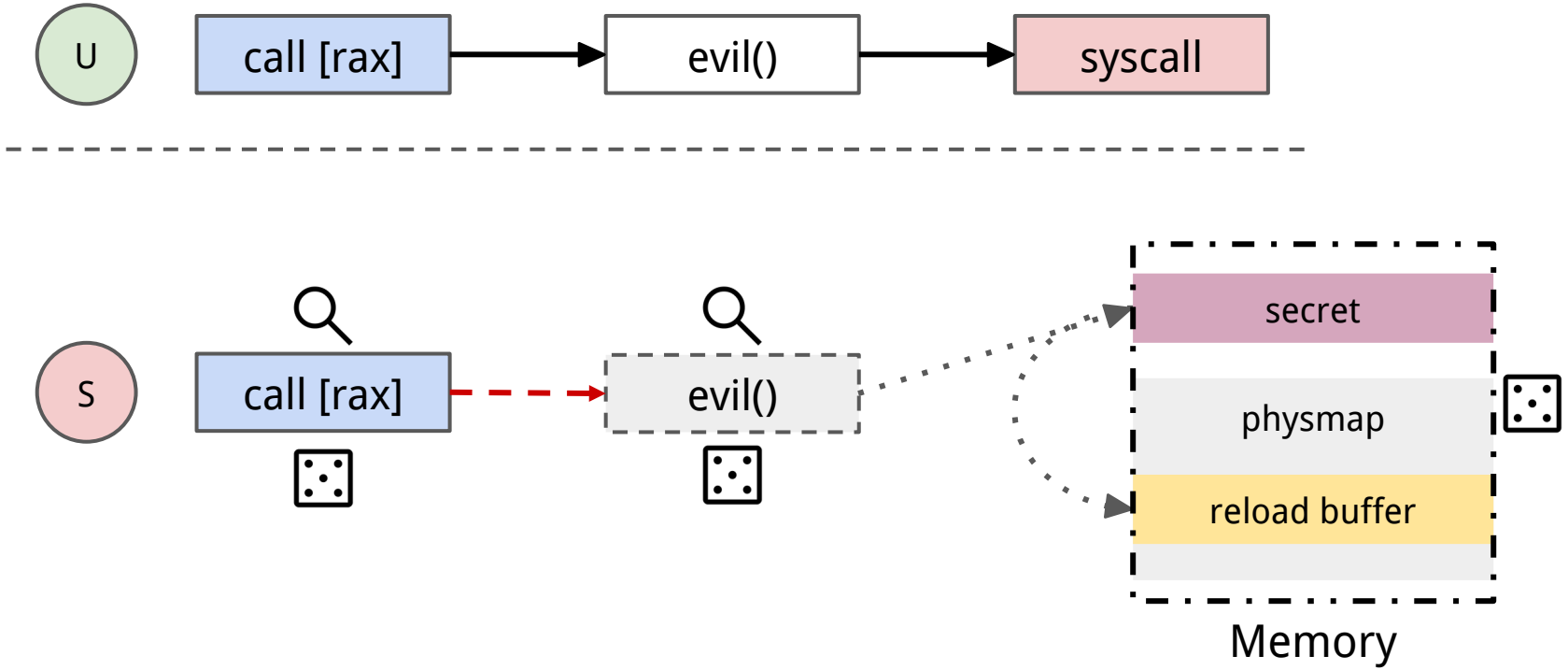
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

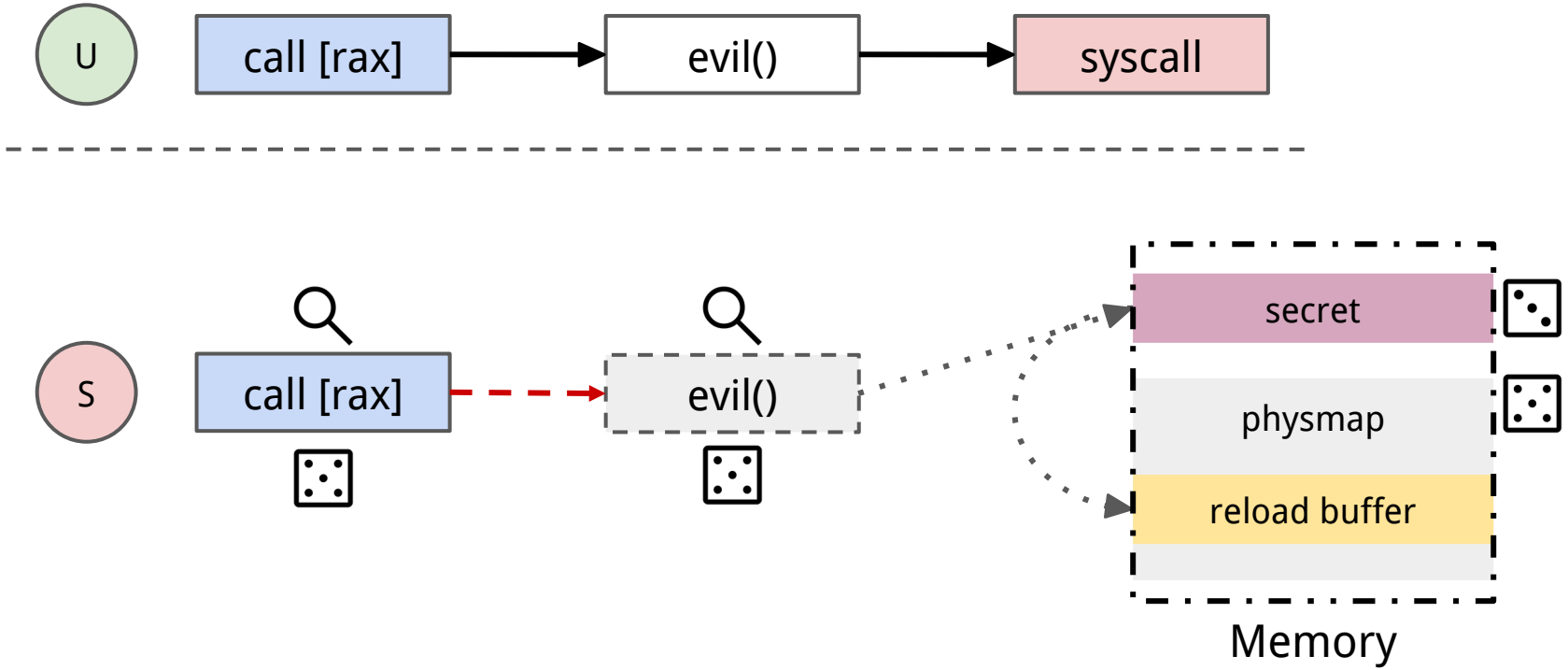
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

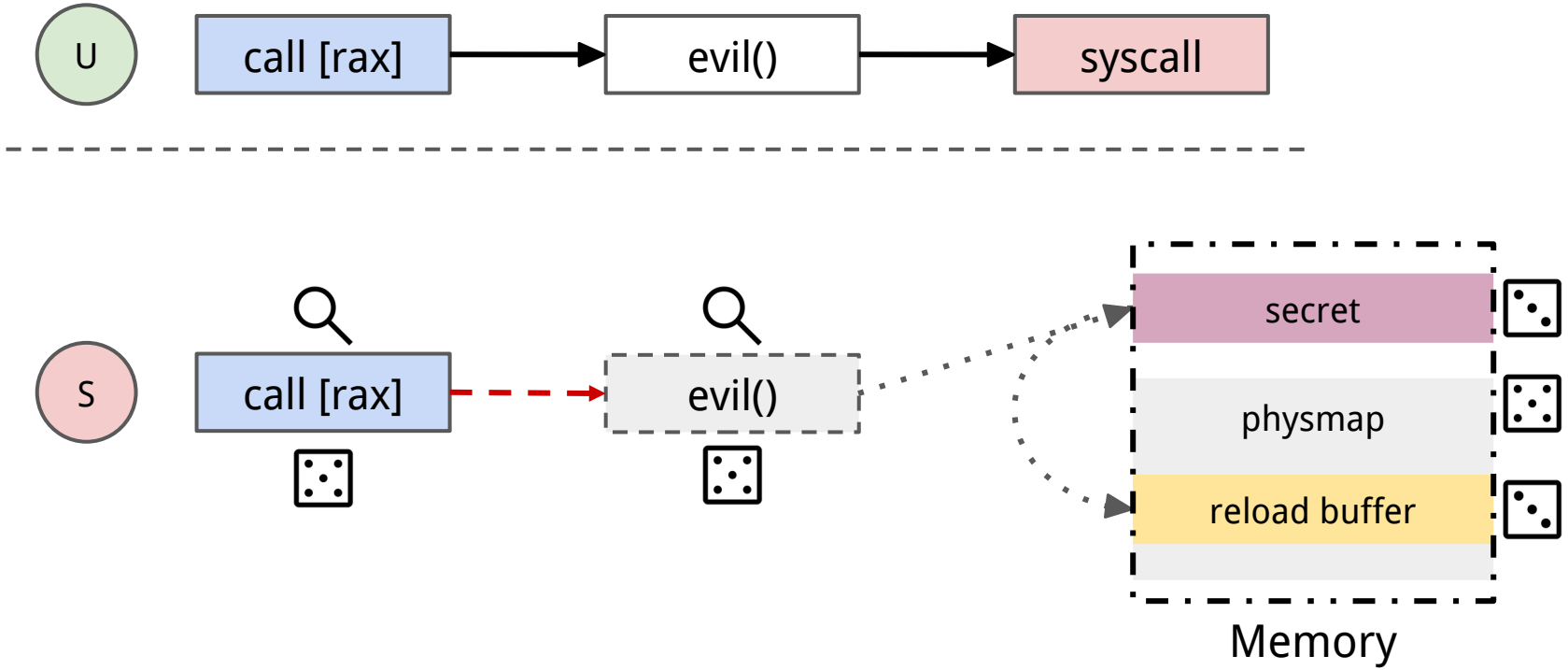
Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

Attack


U
call [rax]
evil()
syscall
S
call [rax]
evil()
secret
physmap
reload buffer
Memory

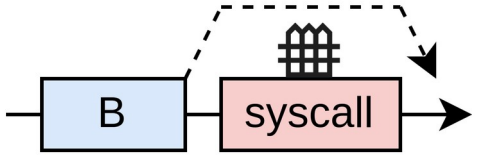
BPRC - Variants

Vendor	Microarch.	Year	Defense	Primitive
Intel	Raptor Cove (RPL-R) Gracemont (RPL-R)	2023	eIBRS	
	Golden Cove (SPR)	2023	eIBRS	
	Raptor Cove (RPL) Gracemont (RPL)	2022	eIBRS	
	Golden Cove (ADL) Gracemont (ADL)	2021	eIBRS	
	Cypress Cove (RKL)	2021	eIBRS	
	Skylake (CML)	2019	eIBRS	
	Skylake (CFL-R)	2018	eIBRS	
	Skylake (CFL)	2017	IBRS	
	Kaby Lake (KBL)	2017	IBRS	
	Sandy Bridge (SNB)	2012	IBRS	

BPRC - Variants

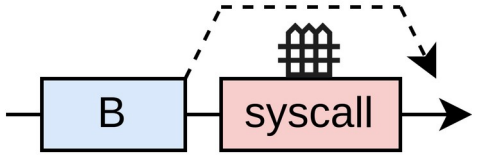
Vendor	Microarch.	Year	Defense	ABPU[a]	Primitive
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	
	Gracemont (RPL-R)			✓	
	Golden Cove (SPR)	2023	eIBRS	✓	
	Raptor Cove (RPL)	2022	eIBRS	✓	
	Gracemont (RPL)			✓	
	Golden Cove (ADL)	2021	eIBRS	✓	
	Gracemont (ADL)			✓	
	Cypress Cove (RKL)	2021	eIBRS	✓	
	Skylake (CML)	2019	eIBRS	✓	
	Skylake (CFL-R)	2018	eIBRS	✓	
	Skylake (CFL)	2017	IBRS	✓	
	Kaby Lake (KBL)	2017	IBRS	✓	
	Sandy Bridge (SNB)	2012	IBRS	✓	

BPRC - Variants



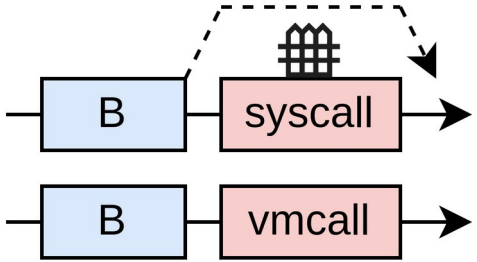
Vendor	Microarch.	Year	Defense	ABPU[a]	Primitive
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	
	Gracemont (RPL-R)			✓	
	Golden Cove (SPR)	2023	eIBRS	✓	
	Raptor Cove (RPL)	2022	eIBRS	✓	
	Gracemont (RPL)			✓	
	Golden Cove (ADL)	2021	eIBRS	✓	
	Gracemont (ADL)			✓	
	Cypress Cove (RKL)	2021	eIBRS	✓	
	Skylake (CML)	2019	eIBRS	✓	
	Skylake (CFL-R)	2018	eIBRS	✓	
	Skylake (CFL)	2017	IBRS	✓	
	Kaby Lake (KBL)	2017	IBRS	✓	
	Sandy Bridge (SNB)	2012	IBRS	✓	

BPRC - Variants



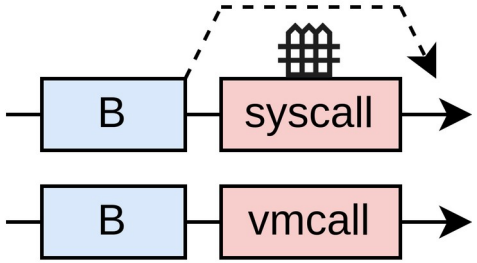
Vendor	Microarch.	Year	Defense	ABPU[a]	$BPRC_{U \to K}$	Primitive
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	✓	
	Gracemont (RPL-R)			✓	✓	
	Golden Cove (SPR)	2023	eIBRS	✓	✓	
	Raptor Cove (RPL)	2022	eIBRS	✓	✓	
	Gracemont (RPL)			✓	✓	
	Golden Cove (ADL)	2021	eIBRS	✓	✓	
	Gracemont (ADL)			✓	✓	
	Cypress Cove (RKL)	2021	eIBRS	✓	✓	
	Skylake (CML)	2019	eIBRS	✓	✓	
	Skylake (CFL-R)	2018	eIBRS	✓	✓	
	Skylake (CFL)	2017	IBRS	✓	✗	
	Kaby Lake (KBL)	2017	IBRS	✓	✗	
	Sandy Bridge (SNB)	2012	IBRS	✓	✗	

BPRC - Variants



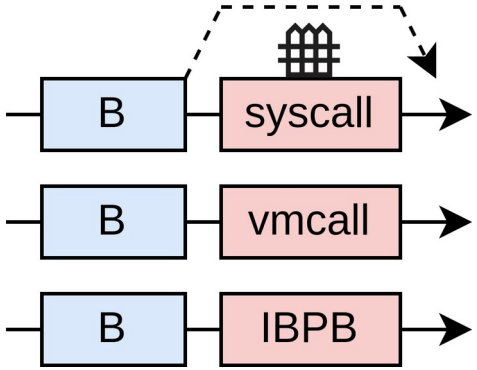
Vendor	Microarch.	Year	Defense	Primitive	
				ABPU[a]	$BPRC_{U \to K}$
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	✓
	Gracemont (RPL-R)			✓	✓
	Golden Cove (SPR)	2023	eIBRS	✓	✓
	Raptor Cove (RPL)	2022	eIBRS	✓	✓
	Gracemont (RPL)			✓	✓
	Golden Cove (ADL)	2021	eIBRS	✓	✓
	Gracemont (ADL)			✓	✓
	Cypress Cove (RKL)	2021	eIBRS	✓	✓
	Skylake (CML)	2019	eIBRS	✓	✓
	Skylake (CFL-R)	2018	eIBRS	✓	✓
	Skylake (CFL)	2017	IBRS	✓	✗
	Kaby Lake (KBL)	2017	IBRS	✓	✗
	Sandy Bridge (SNB)	2012	IBRS	✓	✗

BPRC - Variants



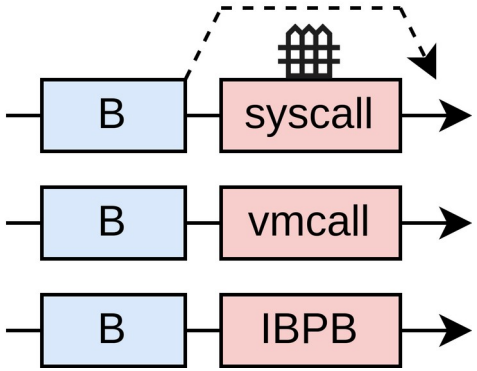
Vendor	Microarch.	Year	Defense	Primitive		
				ABPU[a]	$BPRC_{U \to K}$	$BPRC_{G \to H}$
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	✓	✓
	Gracemont (RPL-R)			✓	✓	✗
	Golden Cove (SPR)	2023	eIBRS	✓	✓	✓
	Raptor Cove (RPL)	2022	eIBRS	✓	✓	✓
	Gracemont (RPL)			✓	✓	✗
	Golden Cove (ADL)	2021	eIBRS	✓	✓	✓
	Gracemont (ADL)			✓	✓	✗
	Cypress Cove (RKL)	2021	eIBRS	✓	✓	✓
	Skylake (CML)	2019	eIBRS	✓	✓	✓
	Skylake (CFL-R)	2018	eIBRS	✓	✓	✓
	Skylake (CFL)	2017	IBRS	✓	✗	✗
	Kaby Lake (KBL)	2017	IBRS	✓	✗	✗
	Sandy Bridge (SNB)	2012	IBRS	✓	✗	✗

BPRC - Variants



Vendor	Microarch.	Year	Defense	Primitive		
				ABPU[a]	$BPRC_{U \to K}$	$BPRC_{G \to H}$
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	✓	✓
	Gracemont (RPL-R)			✓	✓	✗
	Golden Cove (SPR)	2023	eIBRS	✓	✓	✓
	Raptor Cove (RPL)	2022	eIBRS	✓	✓	✓
	Gracemont (RPL)			✓	✓	✗
	Golden Cove (ADL)	2021	eIBRS	✓	✓	✓
	Gracemont (ADL)			✓	✓	✗
	Cypress Cove (RKL)	2021	eIBRS	✓	✓	✓
	Skylake (CML)	2019	eIBRS	✓	✓	✓
	Skylake (CFL-R)	2018	eIBRS	✓	✓	✓
	Skylake (CFL)	2017	IBRS	✓	✗	✗
	Kaby Lake (KBL)	2017	IBRS	✓	✗	✗
	Sandy Bridge (SNB)	2012	IBRS	✓	✗	✗

BPRC - Variants



Vendor	Microarch.	Year	Defense	Primitive			
				ABPU[a]	$BPRC_{U \to K}$	$BPRC_{G \to H}$	$BPRC_{IBPB}$
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	✓	✓	✓
	Gracemont (RPL-R)			✓	✓	✗	✗
	Golden Cove (SPR)	2023	eIBRS	✓	✓	✓	✓
	Raptor Cove (RPL)	2022	eIBRS	✓	✓	✓	✓
	Gracemont (RPL)			✓	✓	✗	✗
	Golden Cove (ADL)	2021	eIBRS	✓	✓	✓	✓
	Gracemont (ADL)			✓	✓	✗	✗
	Cypress Cove (RKL)	2021	eIBRS	✓	✓	✓	✓
	Skylake (CML)	2019	eIBRS	✓	✓	✓	✓
	Skylake (CFL-R)	2018	eIBRS	✓	✓	✓	✓
	Skylake (CFL)	2017	IBRS	✓	✗	✗	✓
	Kaby Lake (KBL)	2017	IBRS	✓	✗	✗	✓
	Sandy Bridge (SNB)	2012	IBRS	✓	✗	✗	✗

Conclusion

Conclusion

- Asynchronous Branch Predictor Updates

Conclusion

- Asynchronous Branch Predictor Updates
- Branch Predictor Race Conditions

Conclusion

- Asynchronous Branch Predictor Updates
- Branch Predictor Race Conditions
- Proposed and evaluated mitigations

Conclusion

- Asynchronous Branch Predictor Updates
- Branch Predictor Race Conditions
- Proposed and evaluated mitigations

Conclusion

- Asynchronous Branch Predictor Updates
- Branch Predictor Race Conditions
- Proposed and evaluated mitigations

Disclosure:

Conclusion

- Asynchronous Branch Predictor Updates
- Branch Predictor Race Conditions
- Proposed and evaluated mitigations

Disclosure:
- 9-month embargo

Conclusion

- Asynchronous Branch Predictor Updates
- Branch Predictor Race Conditions
- Proposed and evaluated mitigations

Disclosure:
- 9-month embargo
- microcode patches

Conclusion

- Asynchronous Branch Predictor Updates
- Branch Predictor Race Conditions
- Proposed and evaluated mitigations

Disclosure:
- 9-month embargo
- microcode patches

Vendor	Microarch.	Year	Defense	Primitive					Exploitable
				ABPU[a]	BPRC$_{U\to K}$	BPRC$_{G\to H}$	BPRC$_{IBPB}$	Bypass Mitig.[b]	
Intel	Raptor Cove (RPL-R)	2023	eIBRS	✓	✓	✓	✓	✓	✓
	Gracemont (RPL-R)			✓	✓	✗	✗	✓[c]	
	Golden Cove (SPR)	2023	eIBRS	✓	✓	✓	✓	✓	✓
	Raptor Cove (RPL)	2022	eIBRS	✓	✓	✓	✓	✓	✓
	Gracemont (RPL)			✓	✓	✗	✗	✓[c]	
	Golden Cove (ADL)	2021	eIBRS	✓	✓	✓	✓	✓	✓
	Gracemont (ADL)			✓	✓	✗	✗	✓[c]	
	Cypress Cove (RKL)	2021	eIBRS	✓	✓	✓	✓	–[d]	✓
	Skylake (CML)	2019	eIBRS	✓	✓	✓	✓	–[d]	✓
	Skylake (CFL-R)	2018	eIBRS	✓	✓	✓	✓	–[d]	✓

[a] Asynchronous Branch Predictor Updates; [b] BPI exploitable despite `BHI_DIS_S`; [c] mitigation reduces success rate; [d] mitigation unavailable