Aion Attacks:
Exposing Software Timer Problem in Trusted Execution Environment

Wei Huang [1], Shengjie Xu [1], Yueqiang Cheng [2], David Lie [1]

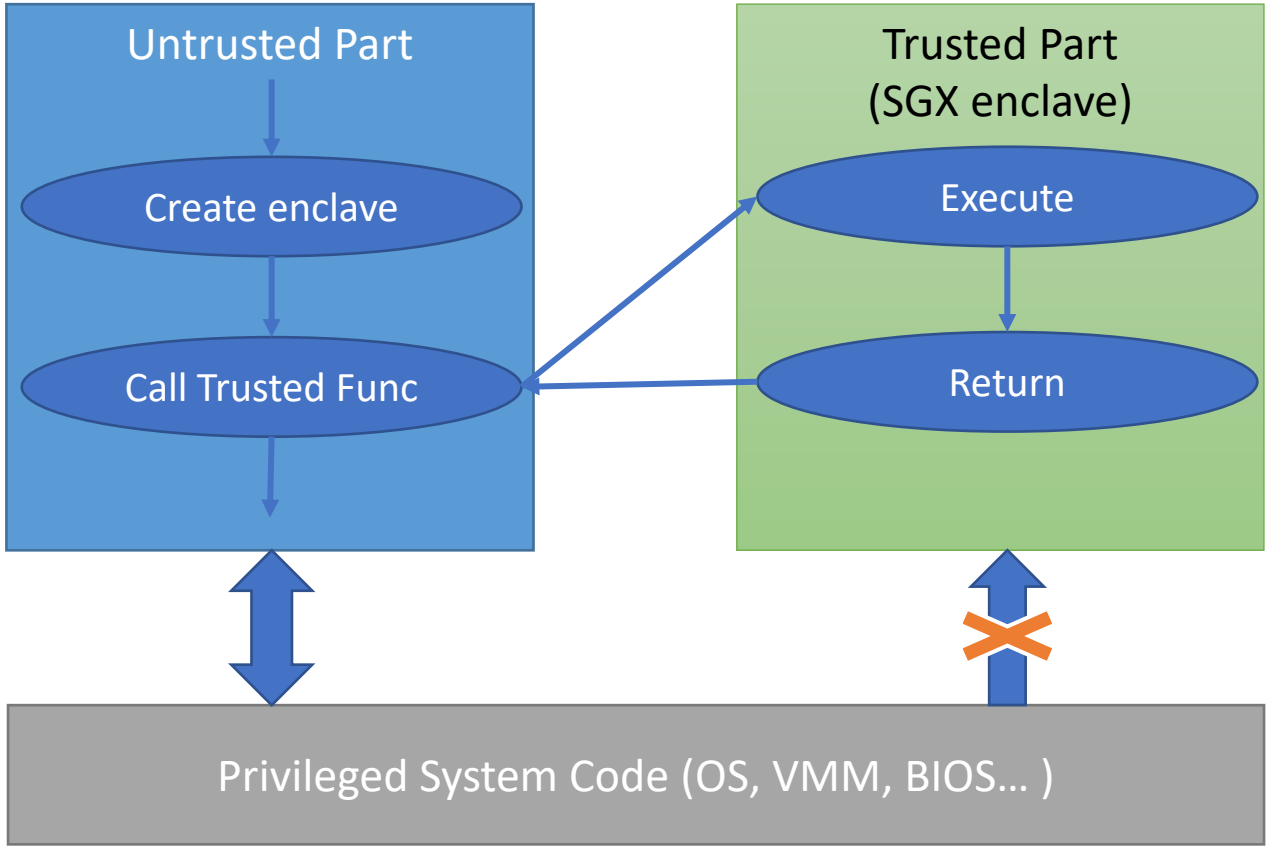
[1] University of Toronto

[2] NIO

Outline

- Introduction and Background
- SGX Defence and Issues
- Software Timer Model
- Attack Design
- Evaluation
- Conclusion

Background of Intel SGX



Background of Intel SGX

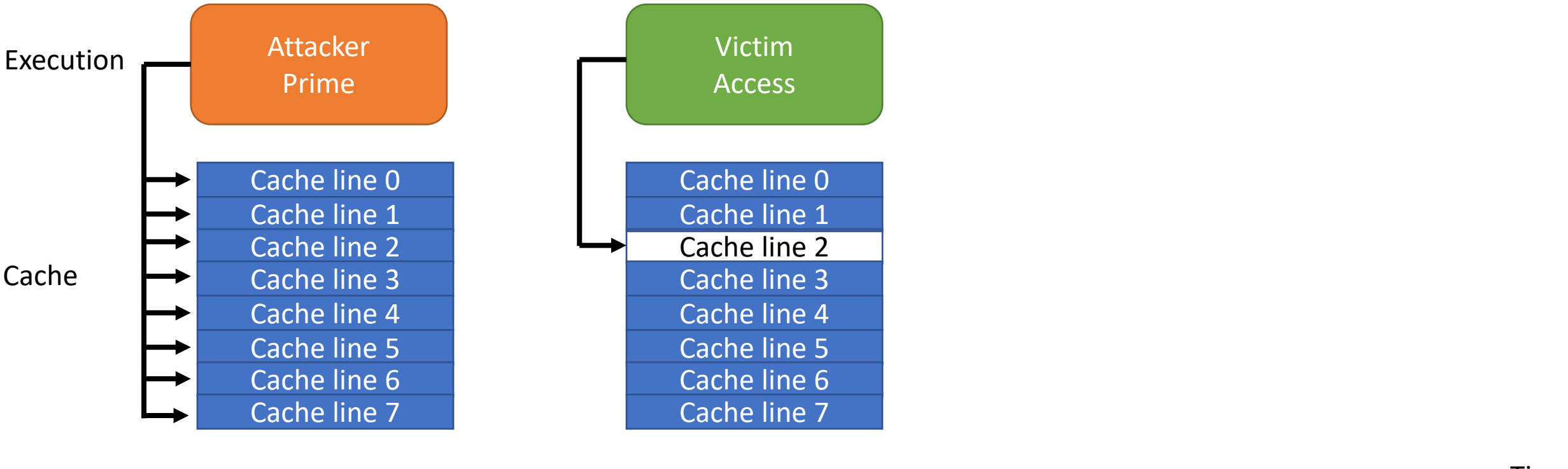
- Side-channel vulnerabilities
- Cache-channel attack

Background of Intel SGX

- Side-channel vulnerabilities
- Cache-channel attack

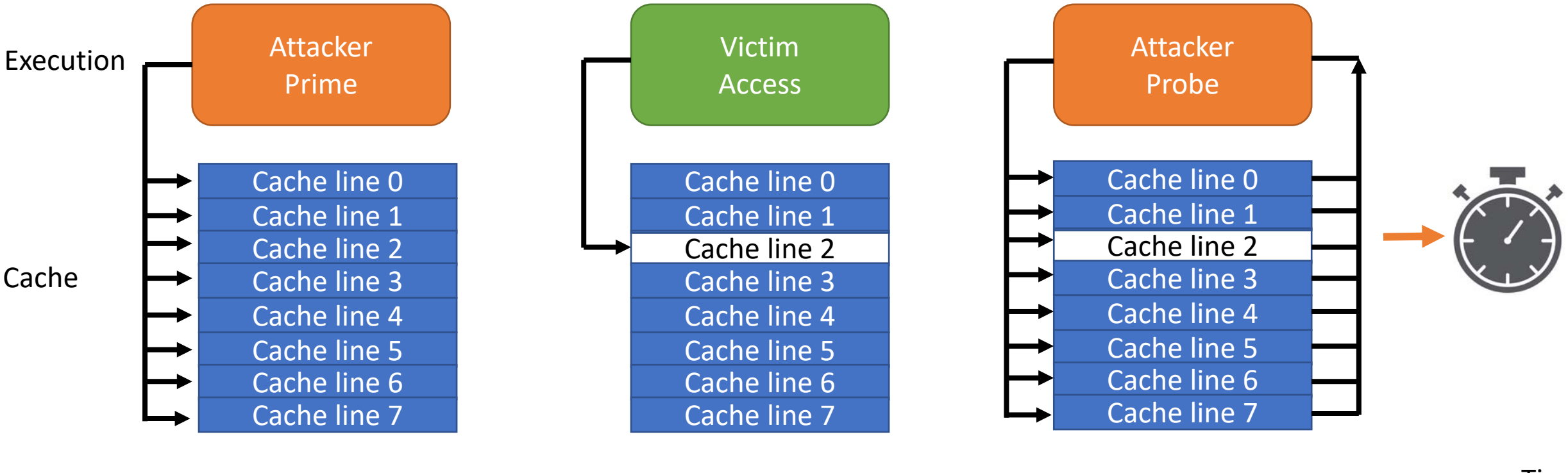
Background of Intel SGX

- Side-channel vulnerabilities
- Cache-channel attack



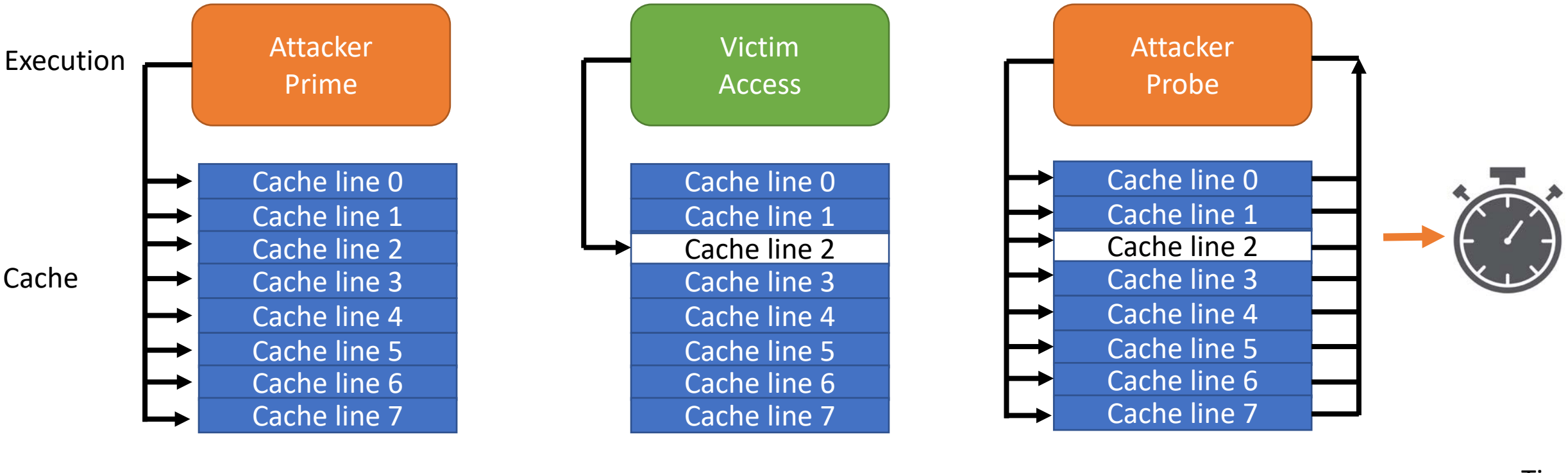
Background of Intel SGX

- Side-channel vulnerabilities
- Cache-channel attack



Background of Intel SGX

- Side-channel vulnerabilities
- Cache-channel attack
  - Attacking thread shares cache with victim
  - Proper timing of Prime and Probe
  - Timing all cache lines



SGX Defender Review

- Defending SGX side-channel attacks
  - Software developers' job [Intel SDM]

SGX Defender Review

- Defending SGX side-channel attacks
  - Software developers' job [Intel SDM]

- Defenders need high-resolution timers

SGX Defender Review

- Defending SGX side-channel attacks
  - Software developers' job [Intel SDM]

- Defenders need high-resolution timers:
  - To count the time interval of certain events [Déjà Vu'17]
    - Period of time before another enclave interrupt
    - Compare against baseline during calibration

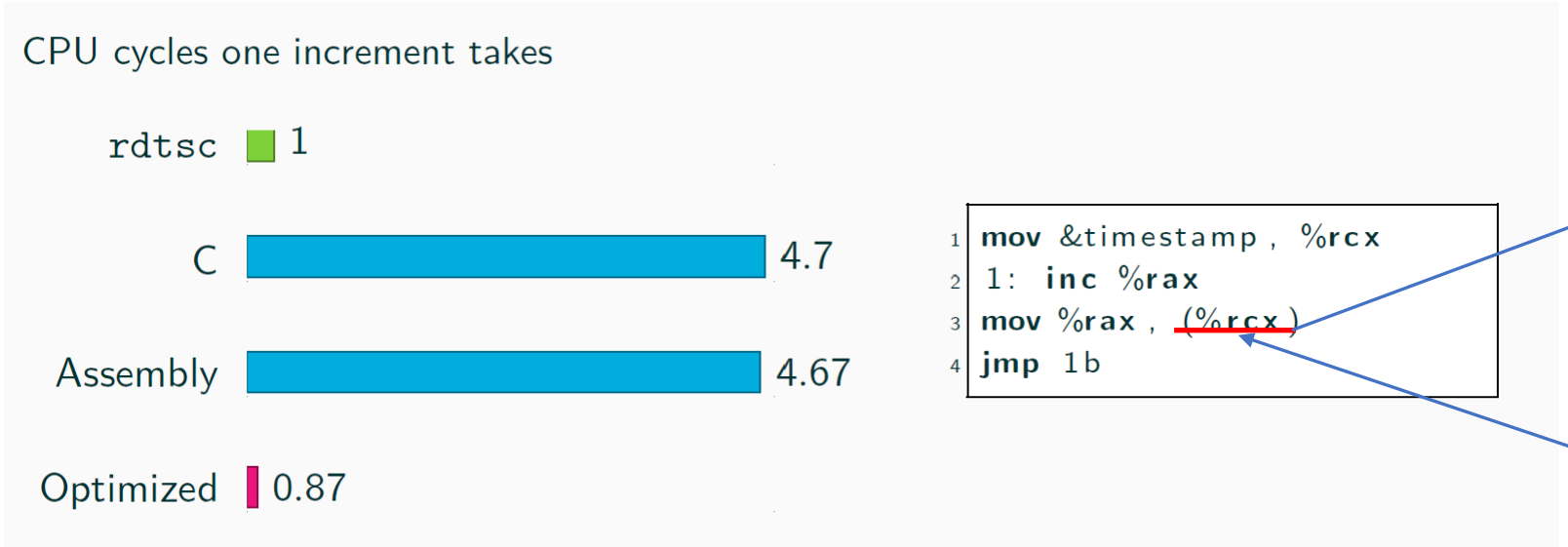
SGX Defender Review

- Defending SGX side-channel attacks
  - Software developers' job [Intel SDM]

- Defenders need high-resolution timers:
  - To count the frequency of abnormal behaviors [Déjà Vu'17]
    - Number of interrupts to victim enclave
    - Compare against baseline during calibration
  - To determine if two threads are co-located [Varys'19]
    - On the same physical core, share L2 cache
    - Compare access time of same variable, L2 normally ~ 10 cycles

SGX defence review

- No hardware timer available in SGX
- Importance of an accurate software timer
  - Set a baseline of how much time an event takes
  - Decide how often suspicious behaviors happen
- Challenge: granularity of timer

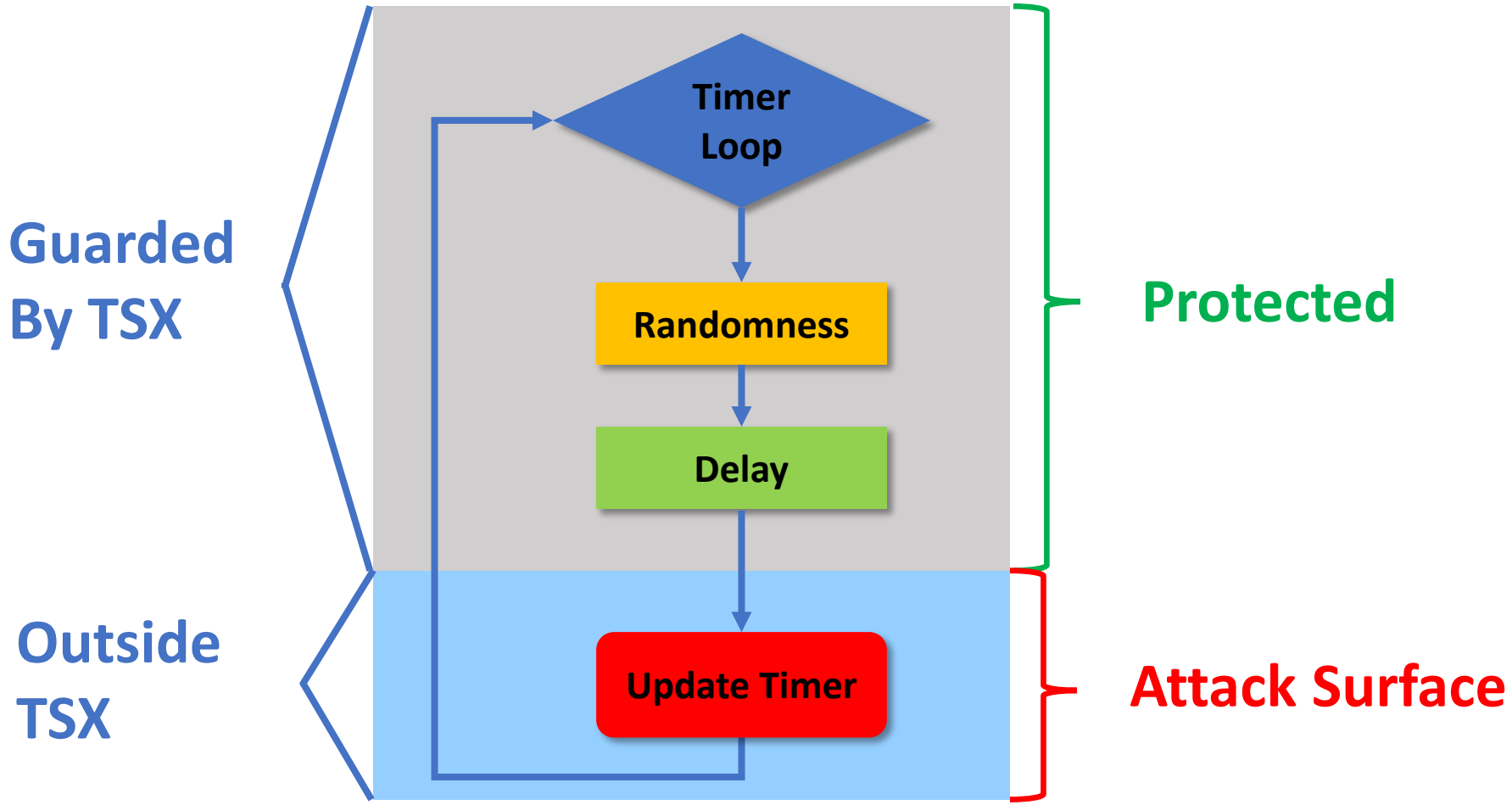



```
1 while(1) {
2   timestamp++;
3 }
```

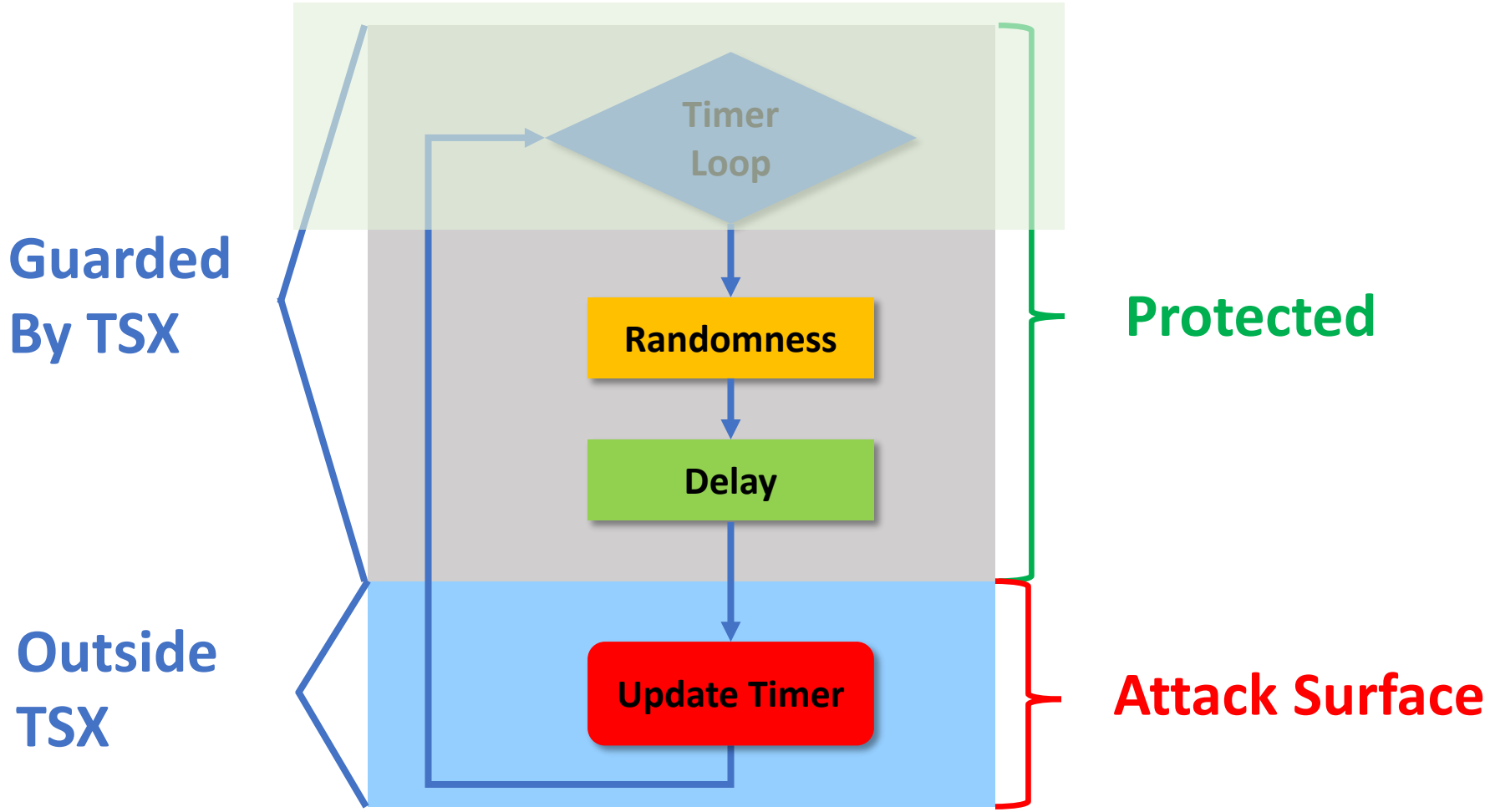
```
1 mov &timestamp, %rcx
2 1: inc %rax
3 mov %rax, (%rcx)
4 jmp 1b
```

DRAM/Cache Access

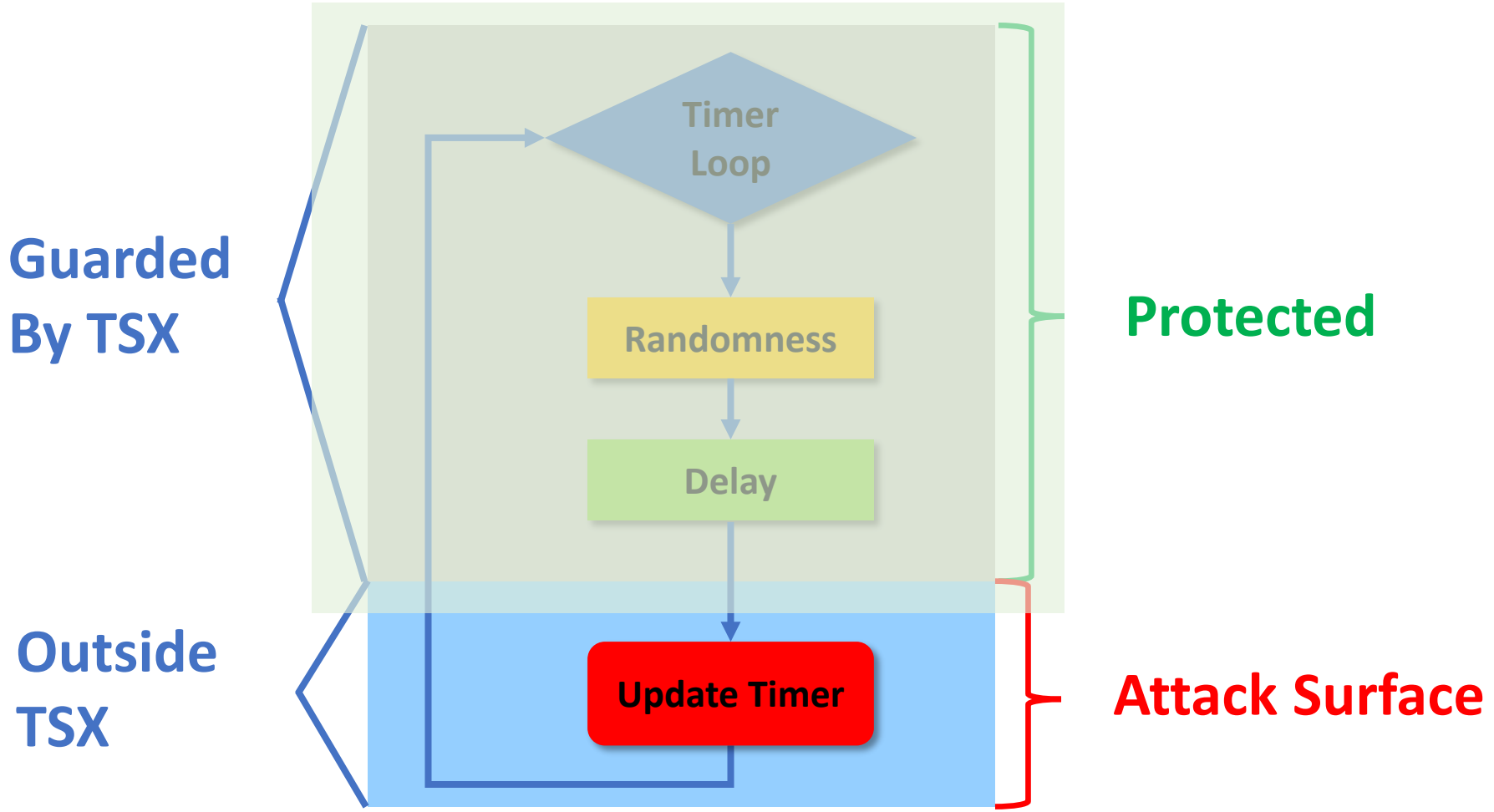
Software Timer Modeling



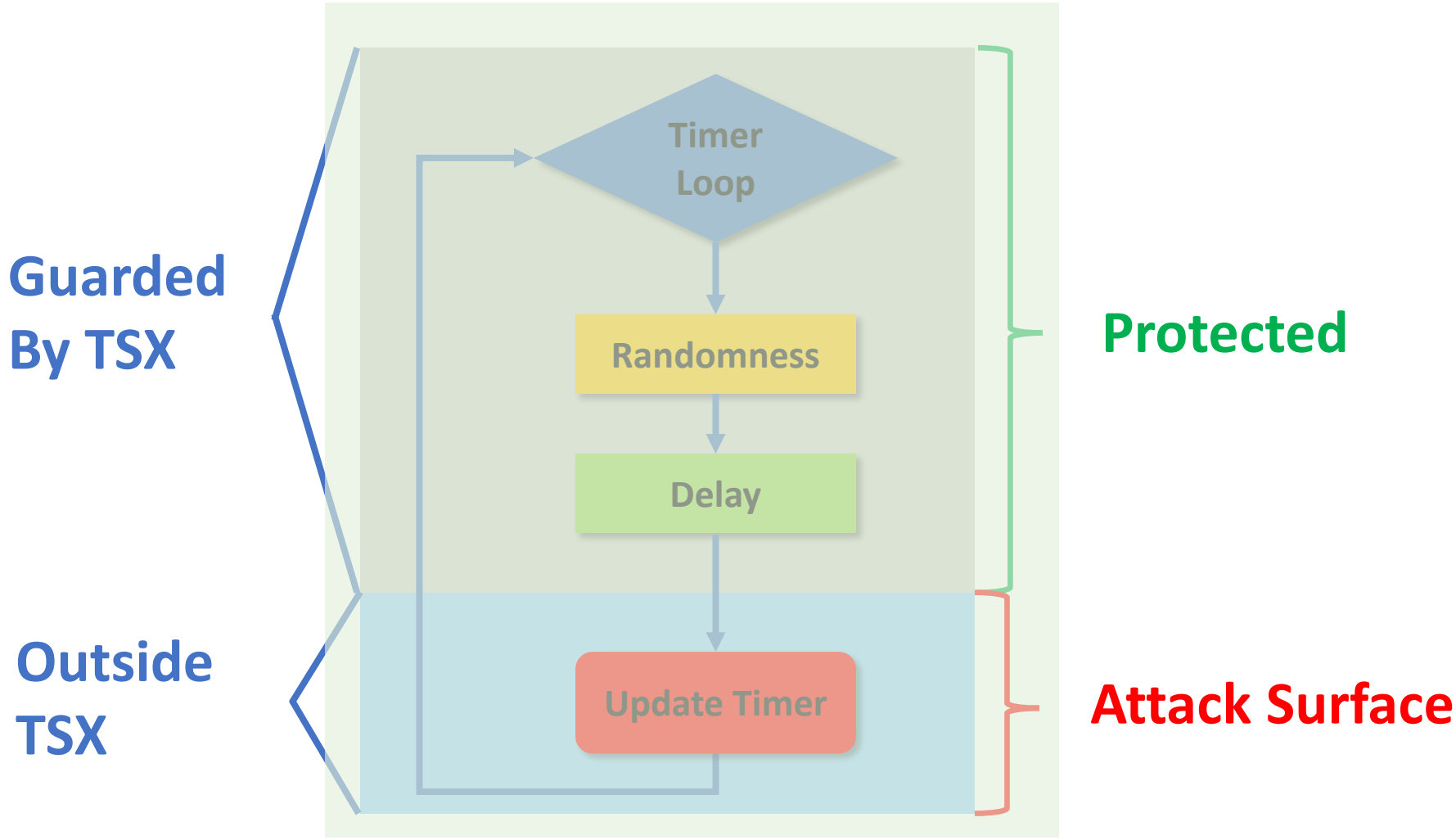
Software Timer Modeling



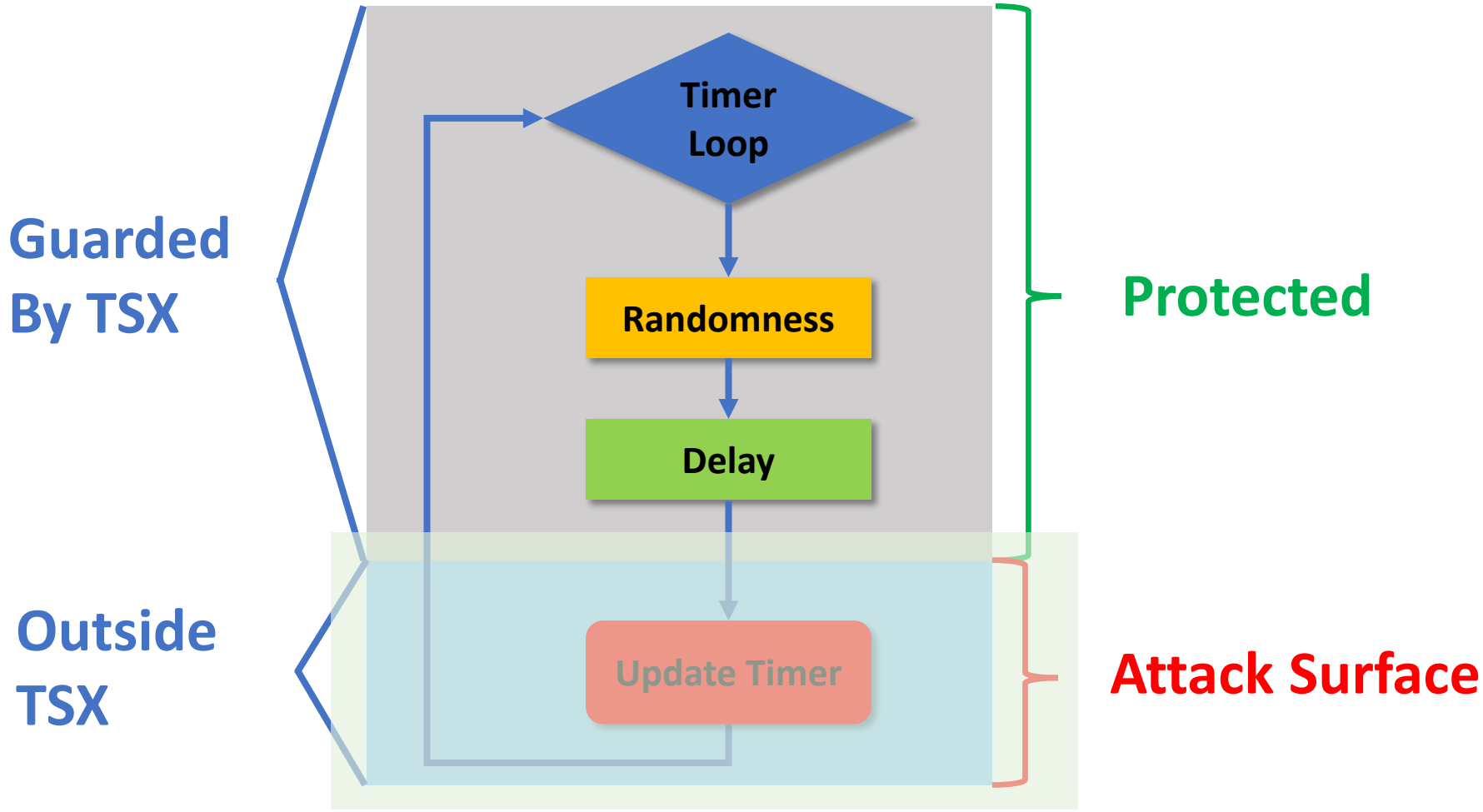
Software Timer Modeling



Software Timer Modeling



Software Timer Modeling

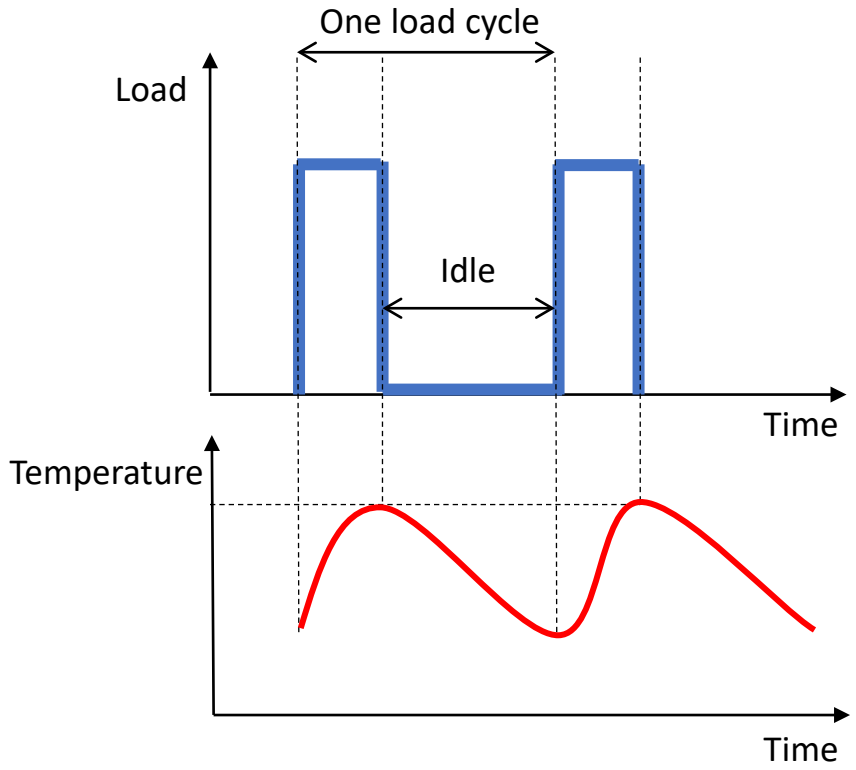


Aion Attacks: Thermal Attack Background

- Intel Processors:
  - TCC
    - Software-adjustable Thermal activation offset
    - Slow down target cores when triggered

Aion Attacks: Thermal Attack Background

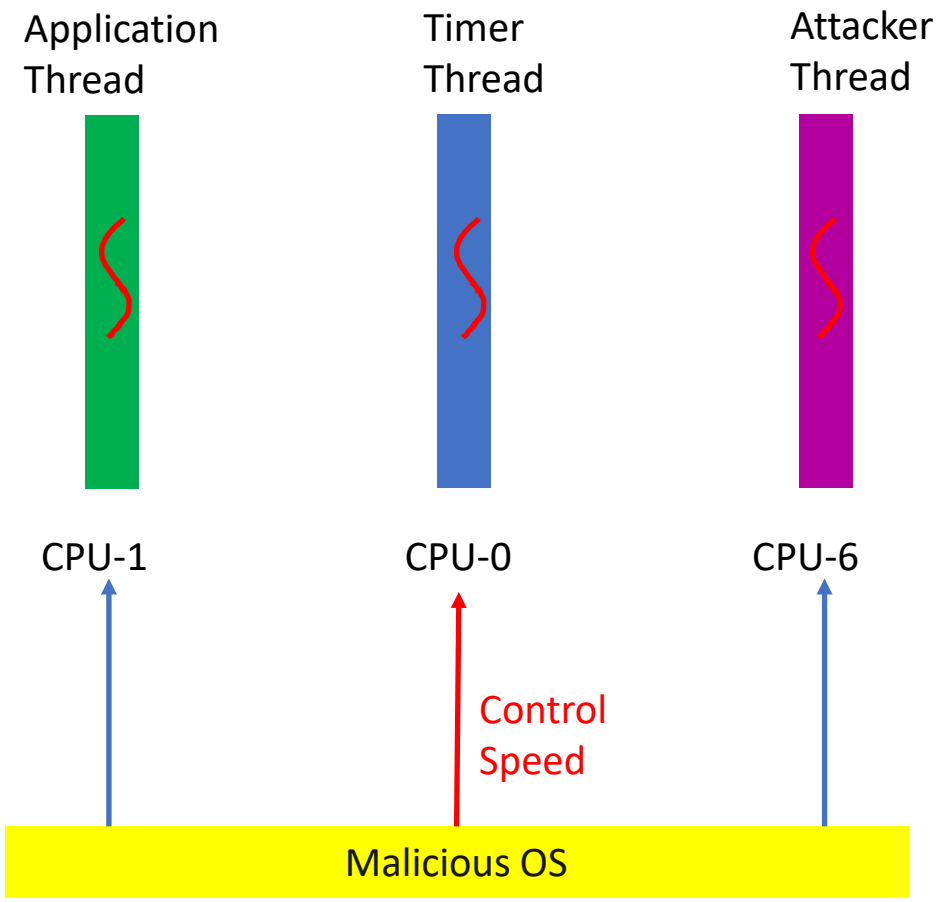
- Intel Processors:
  - TCC
    - Software-adjustable Thermal activation offset
    - Slow down target cores when triggered
  - HDC
    - MSRs to control hardware duty cycling
    - Per-core control, works with hyper-threading
    - Slow down target threads by more than 20x



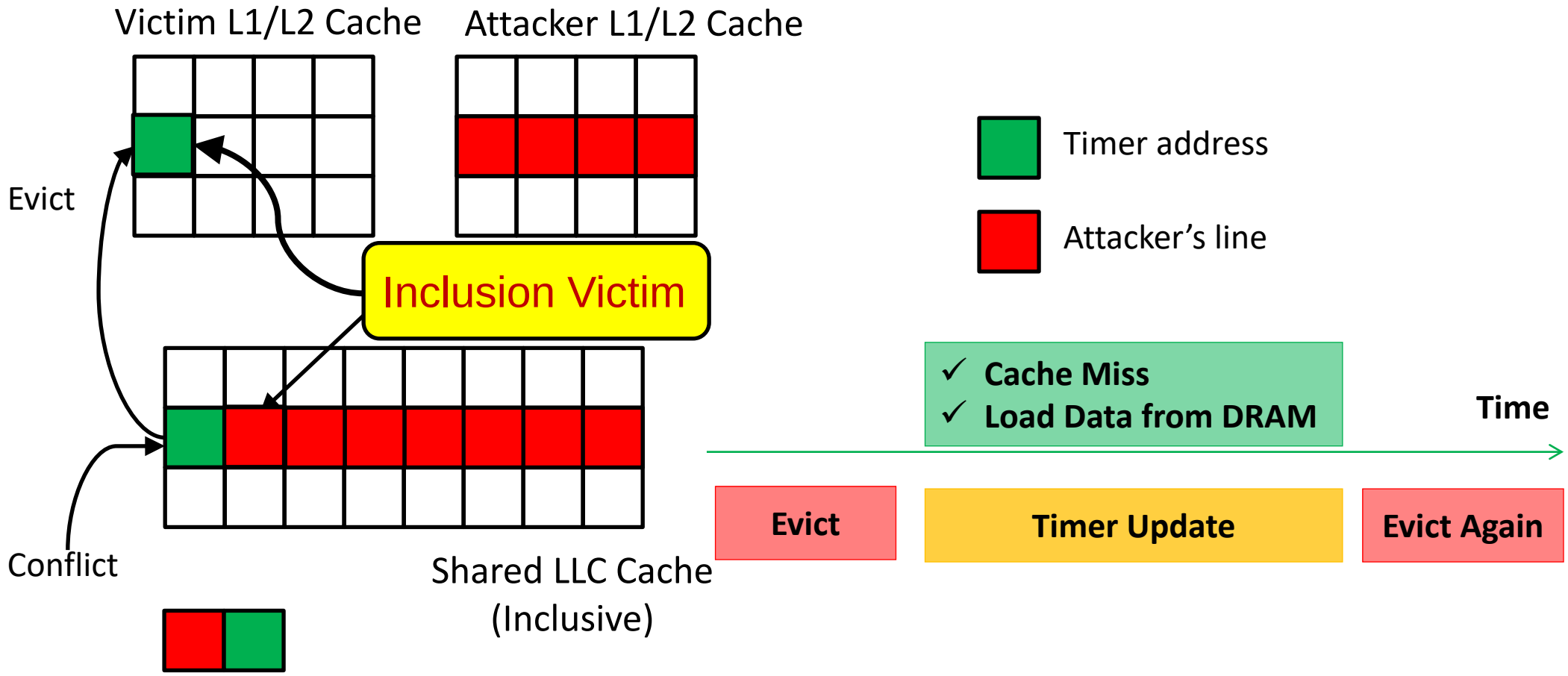
Aion Attacks: Thermal Attack Background

- Intel Processors:
  - TCC
    - Software-adjustable Thermal activation offset
    - Slow down target cores when triggered
  - HDC
    - MSRs to control hardware duty cycling
    - Per-core control, works with hyper-threading
    - Slow down target threads by more than 20x
- Other processors
  - Similar mechanisms
    - AMD: Hardware Thermal Control, P-state MSRs

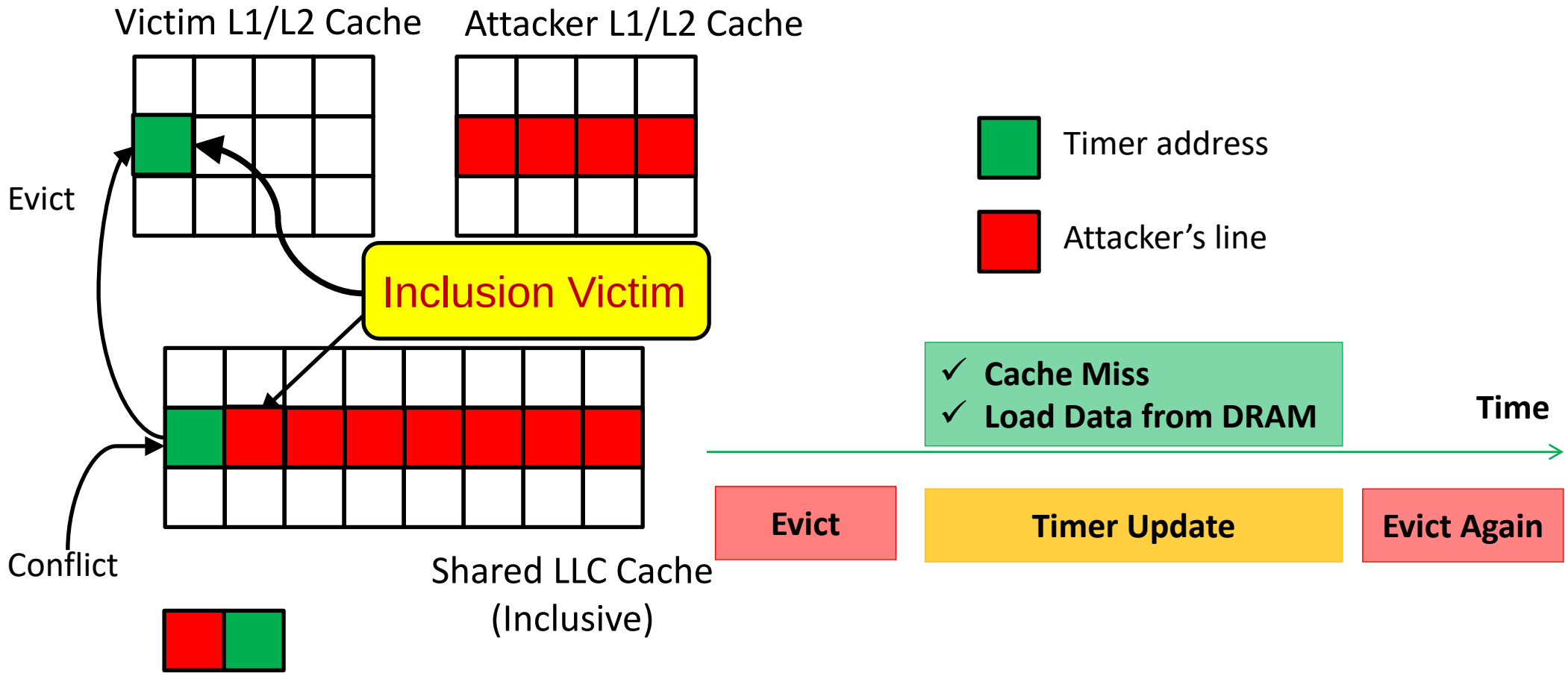
Aion Attacks: Thermal Attack



Aion Attacks: Eviction Attack



Aion Attacks: Eviction Attack



Evaluation Results

- Software timer to measure the same piece of code
- Attackers try to slow down the software timer

	Xeon E3-1230v6		i7-6700K	
	RNG-1	**RNG-2**	**RNG-1**	**RNG-2**
Baseline time (s)	256.3	337.4	225.9	302.5
Eviction Attack	1.6x	1.9x	1.5x	2.0x
Multi-thread Eviction Attack	2.7x	6.2x	2.5x	7.3x
Multi-thread Eviction + Thermal Attack	111x	187x	120x	202x

Evaluation Results

- Software timer to measure the same piece of code
- Attackers try to slow down the software timer

	Xeon E3-1230v6		i7-6700K	
	RNG-1	**RNG-2**	**RNG-1**	**RNG-2**
Baseline time (s)	256.3	337.4	225.9	302.5
Eviction Attack	1.6x	1.9x	1.5x	2.0x
Multi-thread Eviction Attack	2.7x	6.2x	2.5x	7.3x
Multi-thread Eviction + Thermal Attack	111x	187x	120x	202x

Evaluation Results

- Software timer to measure the same piece of code
- Attackers try to slow down the software timer

	Xeon E3-1230v6		i7-6700K	
	RNG-1	**RNG-2**	**RNG-1**	**RNG-2**
Baseline time (s)	256.3	337.4	225.9	302.5
Eviction Attack	1.6x	1.9x	1.5x	2.0x
Multi-thread Eviction Attack	2.7x	6.2x	2.5x	7.3x
Multi-thread Eviction + Thermal Attack	111x	187x	120x	202x

Evaluation Results

- Software timer to measure the same piece of code
- Attackers try to slow down the software timer

	Xeon E3-1230v6		i7-6700K	
	RNG-1	**RNG-2**	**RNG-1**	**RNG-2**
Baseline time (s)	256.3	337.4	225.9	302.5
Eviction Attack	1.6x	1.9x	1.5x	2.0x
Multi-thread Eviction Attack	2.7x	6.2x	2.5x	7.3x
Multi-thread Eviction + Thermal Attack	111x	187x	120x	202x

Evaluation Results

- End-to-end test
- Aion attack to help other side-channel attacks evade detection

Benchmark	Baseline Defence			Defence Under Aion Attack		
	Threshold	Acc %	False-Positive %	Threshold	Acc % (E3)	Acc % (i7)
Numeric sort	4	100	97	4	95	94
	40	100	40	40	17	15
	80	**95**	**3**	**80**	**2**	**2**
	160	87	2	160	1	0
	320	40	0	320	0	0
	640	9	0	-	-	-
	1280	3	0	-	-	-
Fourier	4	100	98	4	95	92
	40	100	46	40	19	18
	80	**96**	**4**	**80**	**2**	**1**
	160	74	2	160	0	0
	320	30	0	320	0	0
	640	10	0	-	-	-
	1280	2	0	-	-	-

Evaluation Results

- End-to-end test
- Aion attack to help other side-channel attacks evade detection

Benchmark	Baseline Defence			Defence Under Aion Attack		
	Threshold	Acc %	False-Positive %	Threshold	Acc % (E3)	Acc % (i7)
Numeric sort	4	100	97	4	95	94
	40	100	40	40	17	15
	80	**95**	**3**	**80**	**2**	**2**
	160	87	2	160	1	0
	320	40	0	320	0	0
	640	9	0	-	-	-
	1280	3	0	-	-	-
Fourier	4	100	98	4	95	92
	40	100	46	40	19	18
	80	**96**	**4**	**80**	**2**	**1**
	160	74	2	160	0	0
	320	30	0	320	0	0
	640	10	0	-	-	-
	1280	2	0	-	-	-

Evaluation Results

- End-to-end test
- Aion attack to help other side-channel attacks evade detection

Benchmark	Baseline Defence			Defence Under Aion Attack		
	Threshold	Acc %	False-Positive %	Threshold	Acc % (E3)	Acc % (i7)
Numeric sort	4	100	97	4	95	94
	40	100	40	40	17	15
	80	**95**	**3**	**80**	**2**	**2**
	160	87	2	160	1	0
	320	40	0	320	0	0
	640	9	0	-	-	-
	1280	3	0	-	-	-
Fourier	4	100	98	4	95	92
	40	100	46	40	19	18
	80	**96**	**4**	**80**	**2**	**1**
	160	74	2	160	0	0
	320	30	0	320	0	0
	640	10	0	-	-	-
	1280	2	0	-	-	-

Evaluation Results

- End-to-end test
- Aion attack to help other side-channel attacks evade detection

Benchmark	Baseline Defence			Defence Under Aion Attack		
	Threshold	Acc %	False-Positive %	Threshold	Acc % (E3)	Acc % (i7)
Numeric sort	4	100	97	4	95	94
	40	100	40	40	17	15
	80	**95**	**3**	**80**	**2**	**2**
	160	87	2	160	1	0
	320	40	0	320	0	0
	640	9	0	-	-	-
	1280	3	0	-	-	-
Fourier	4	100	98	4	95	92
	40	100	46	40	19	18
	80	**96**	**4**	**80**	**2**	**1**
	160	74	2	160	0	0
	320	30	0	320	0	0
	640	10	0	-	-	-
	1280	2	0	-	-	-

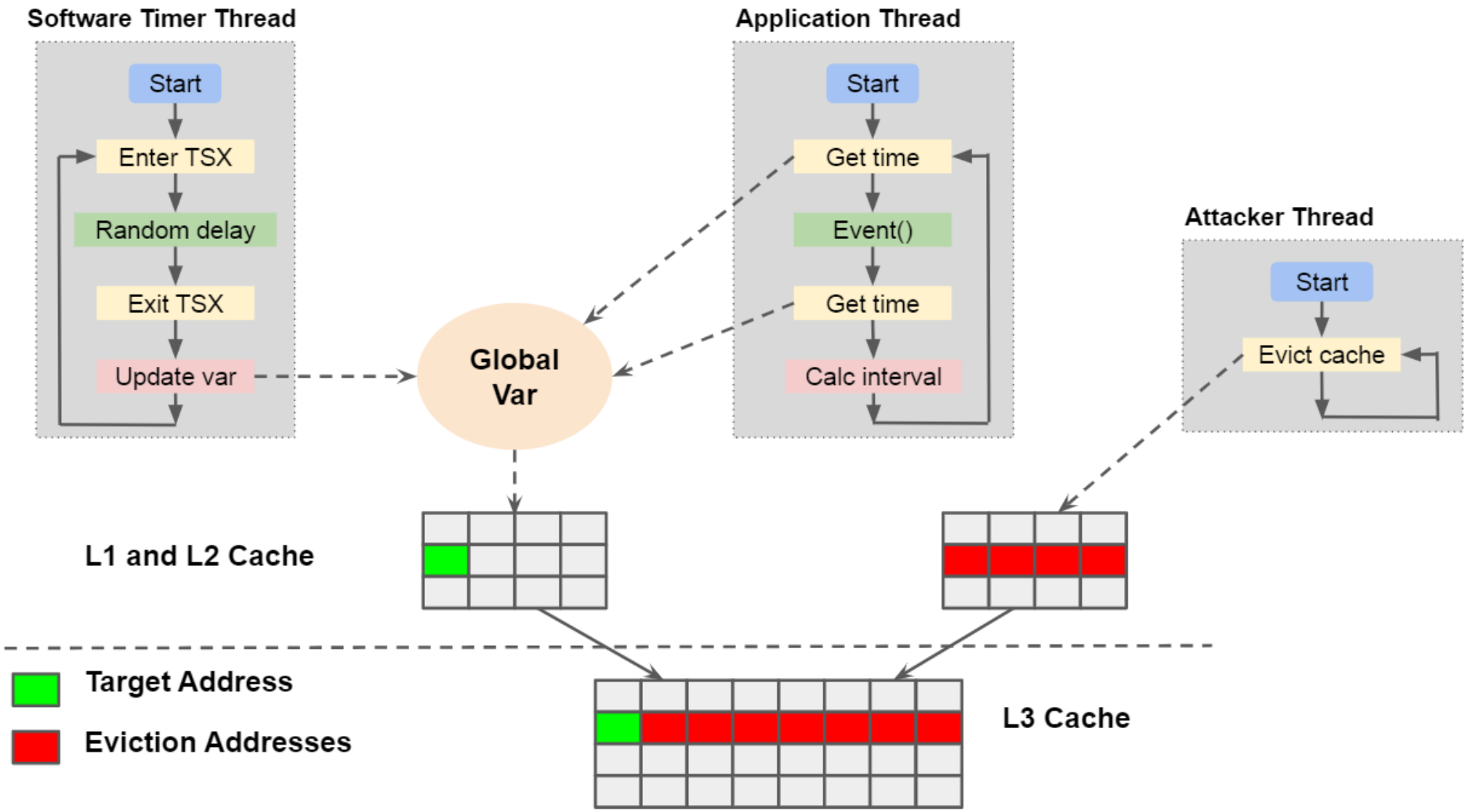
Conclusion and Discussions

- Software timer will always be unreliable
- Better seek hardware assistance
- What about SGX 2.0?

Q&A

- Thanks!

Back-up Slide 1: Eviction algorithm



Back-up Slide 2: Cache slices