SG^{XL}: Enhancing Security and Performance of SGX

Sujay Yadalam, Vinod Ganapathy, Arkaprava Basu

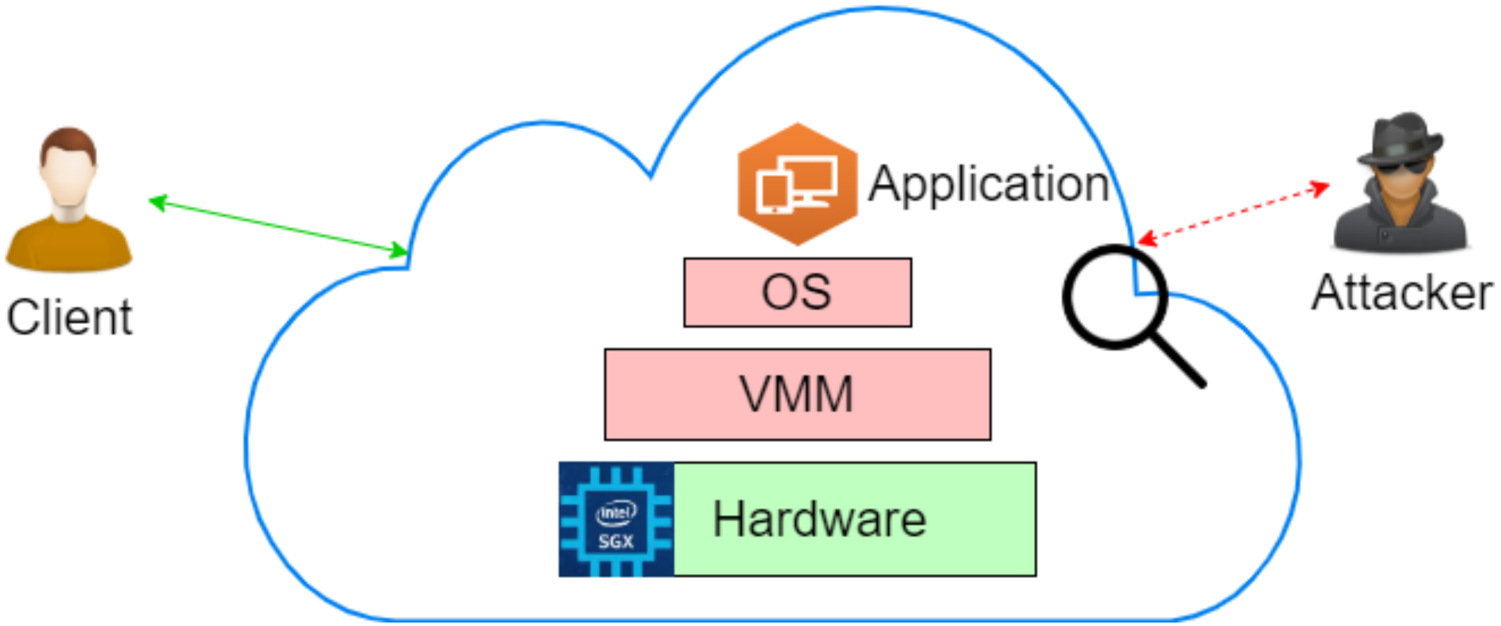
Indian Institute of Science (IISc)

Agenda

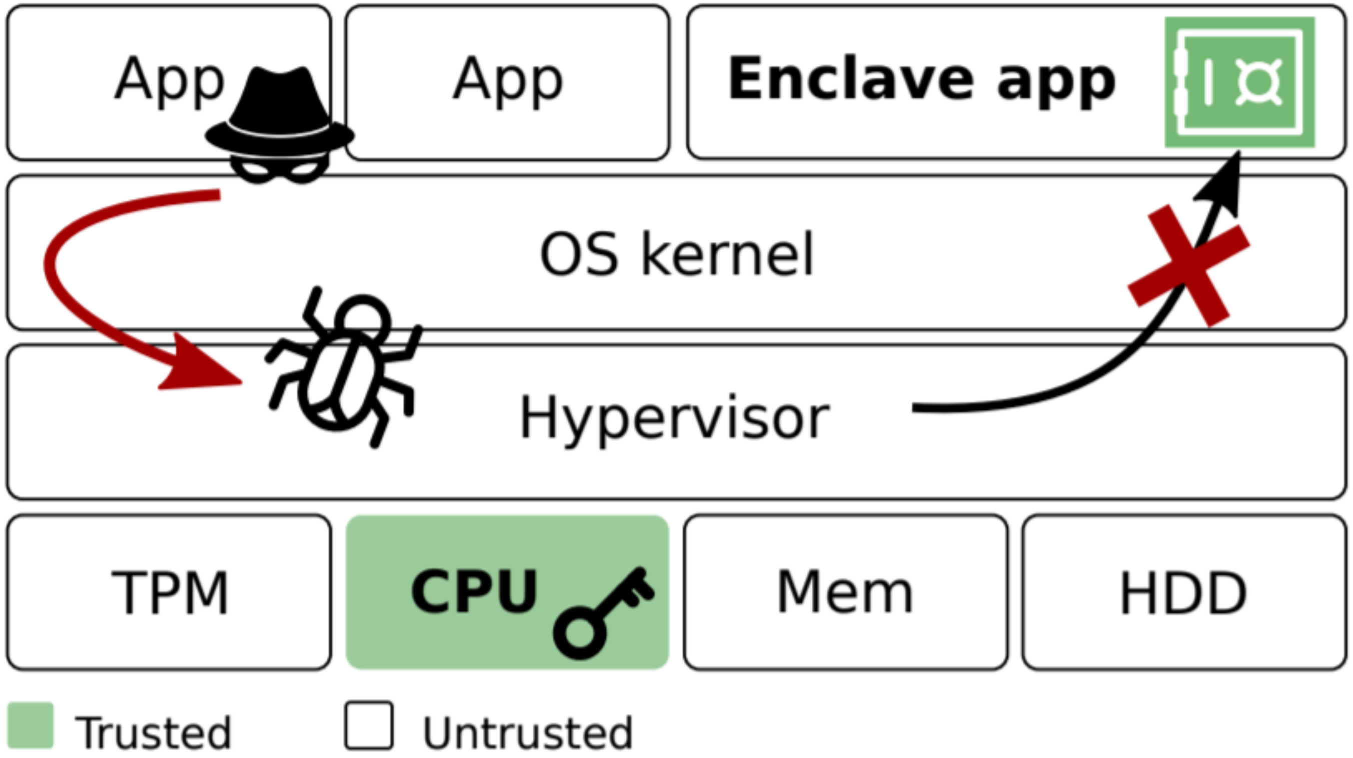
- Intel SGX
- Controlled channel attack
- SG^{XL}
- Results

Intel SGX in the cloud

- Intel Software Guard Extensions (SGX) aims to secure users' code and data in the cloud
- Provides hardware rooted guarantees



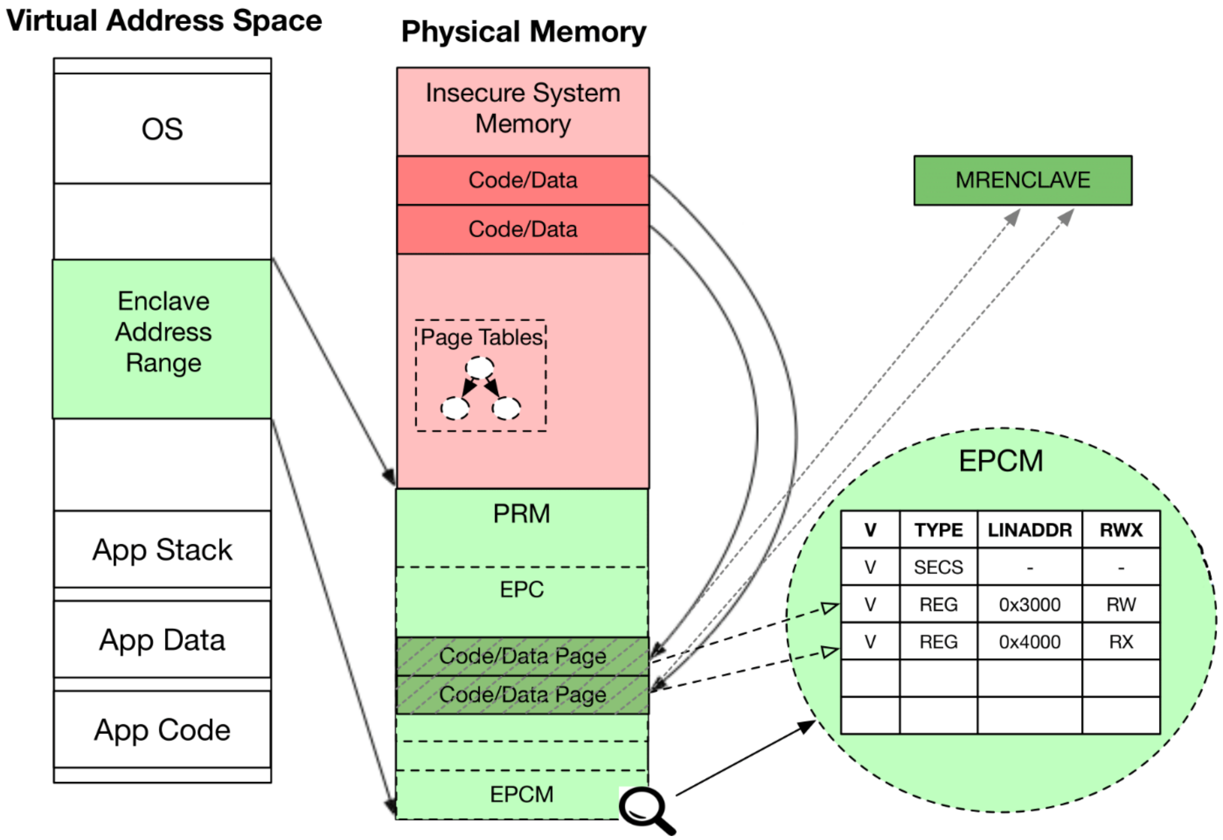
SGX TCB and threat model



- Threat model:
  - Unprivileged software
  - System software
  - Bus snooping attacks

- Trusted Computing Base (TCB):
  - Hardware

Intel SGX: EPC and EPCM



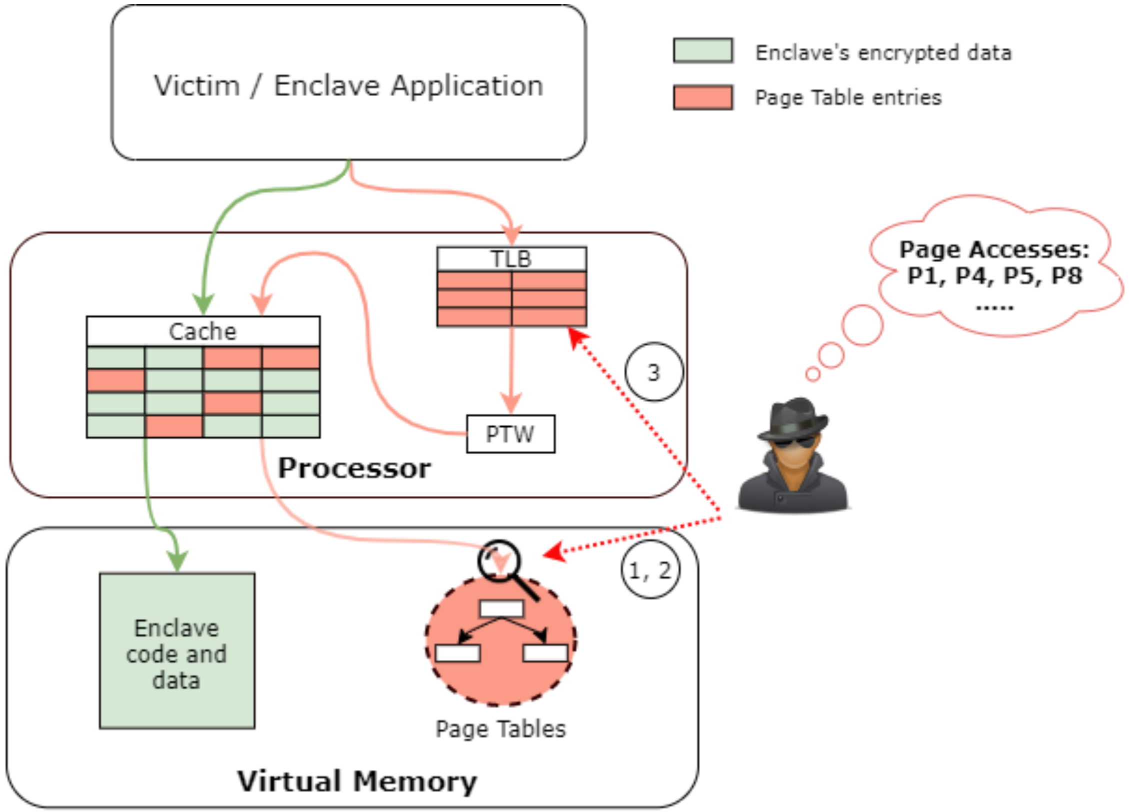
V	TYPE	LINADDR	RWX
V	SECS	-	-
V	REG	0x3000	RW
V	REG	0x4000	RX

- Enclave Page Cache (EPC): physical memory reserved for enclaves
- EPCM: EPC Metadata
- Enclaves rely on untrusted OS for enclave page management

Page-address side channel

Malicious system software can capture victim’s page accesses by

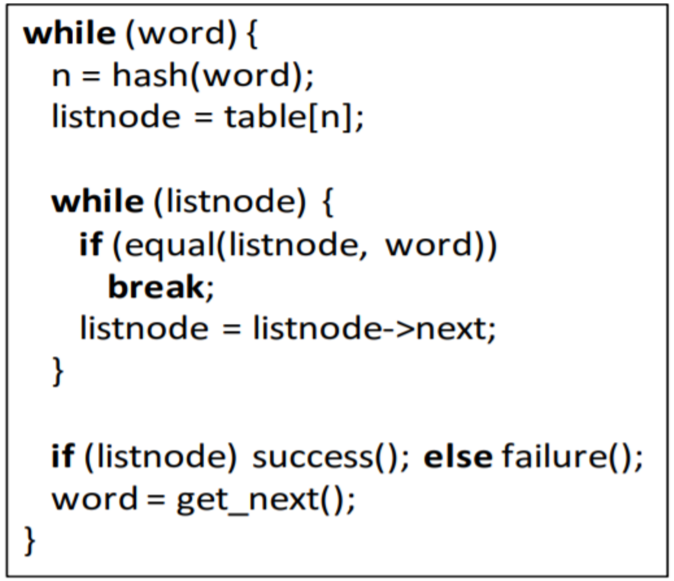
1. Modifying page tables to induce page faults[1]
2. Monitoring Accessed (A) and Dirty (D) bits[2]
3. Using a timing side-channel against TLB[3]



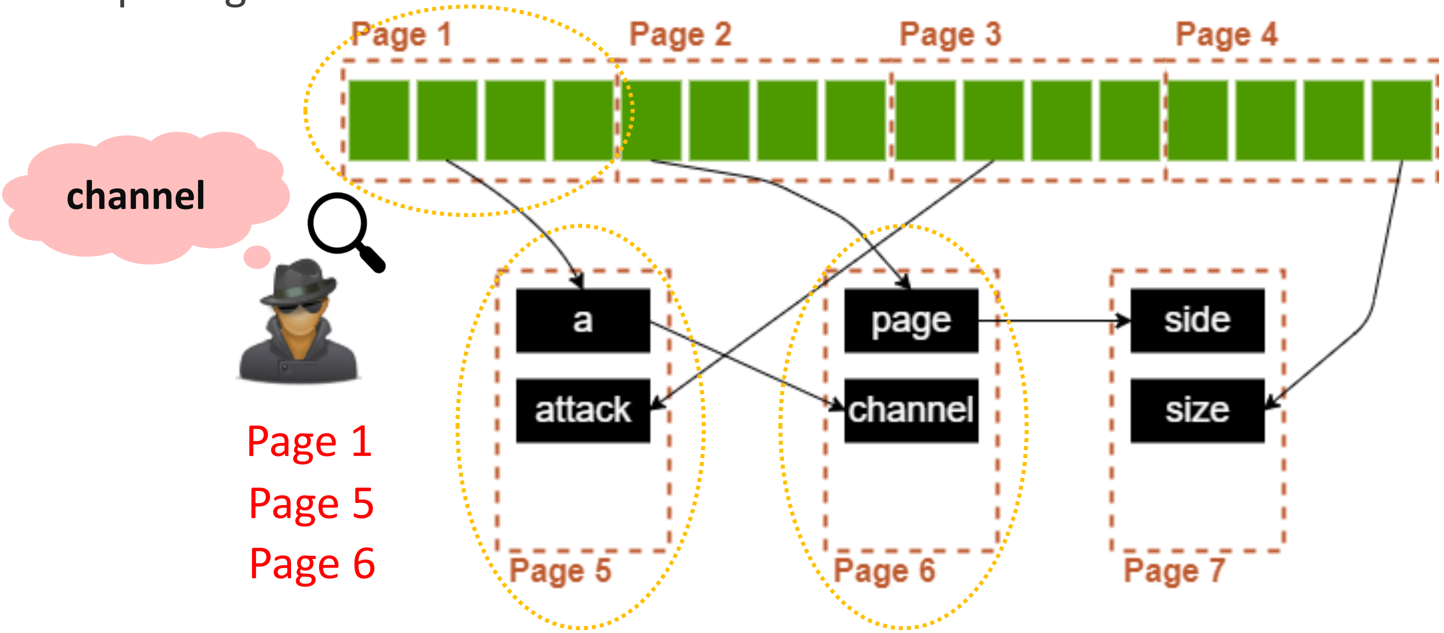
[1] Xu et.al. "Controlled-channel attacks: Deterministic side channels for untrusted operating systems." *2015 IEEE Symposium on Security and Privacy*
[2] J. Van Bulck et.al. “Telling your secrets without page faults: Stealthy page table-based attacks on enclaved execution”. *2017 USENIX Security Symposium*
[3] B. Gras et.al. “Translation leak-aside buffer: Defeating cache side-channel protections with TLB attacks.” *2018 USENIX Security Symposium*

Controlled channel attack[1]

- Infer secrets from page access sequences
- Example:
  - Hunspell is a spell checker library stores words in a dictionary using hashes
  - It traverses a linked list to check the spelling



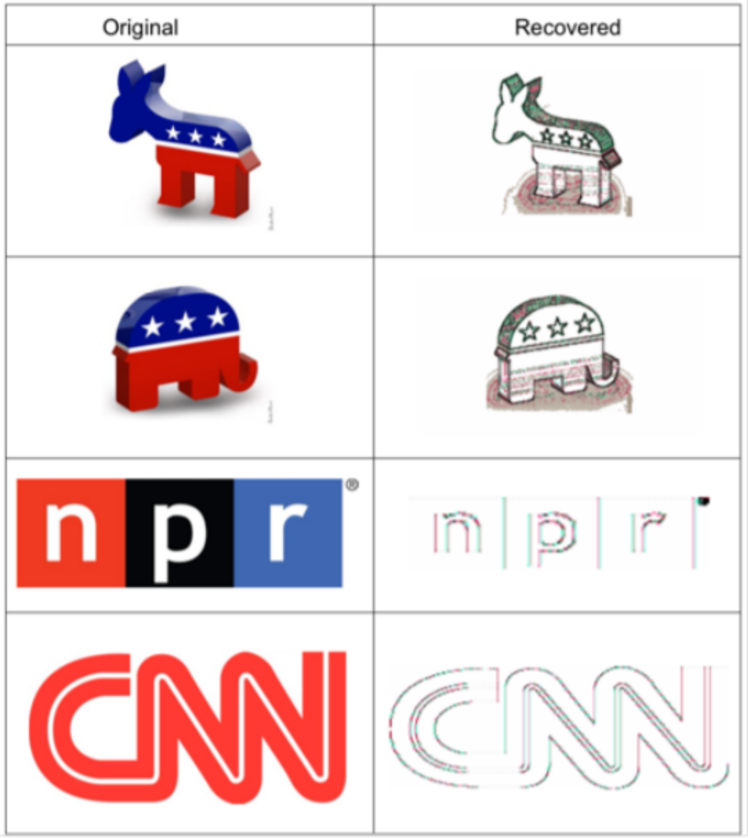
```
while (word) {
  n = hash(word);
  listnode = table[n];

  while (listnode) {
    if (equal(listnode, word))
      break;
    listnode = listnode->next;
  }

  if (listnode) success(); else failure();
  word = get_next();
}
```

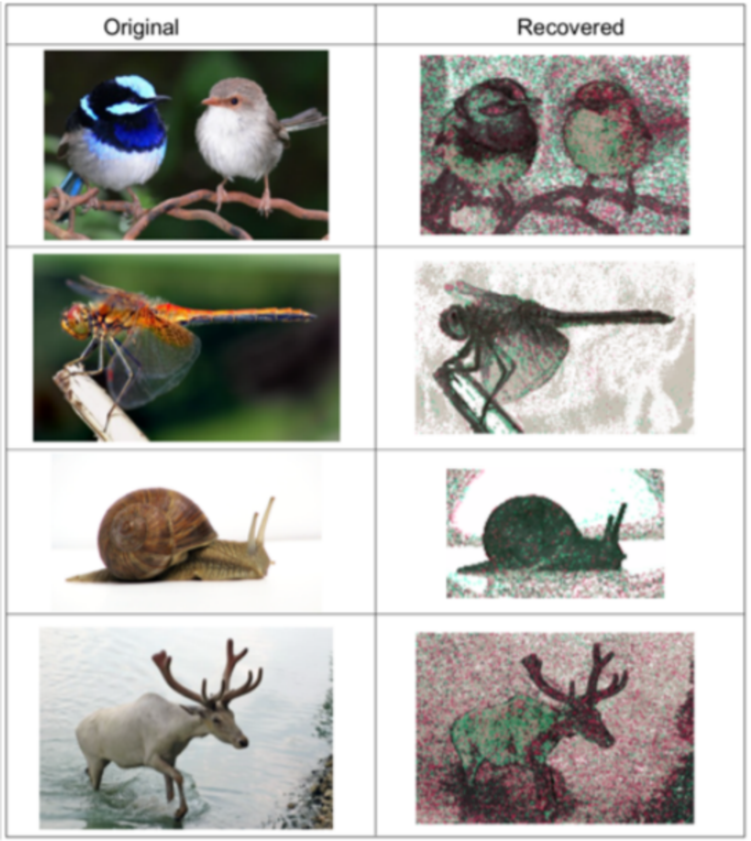


Page 1
Page 5
Page 6

[1] Xu, Yuanzhong, Weidong Cui, and Marcus Peinado. "Controlled-channel attacks: Deterministic side channels for untrusted operating systems." *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015

Example: libJpeg

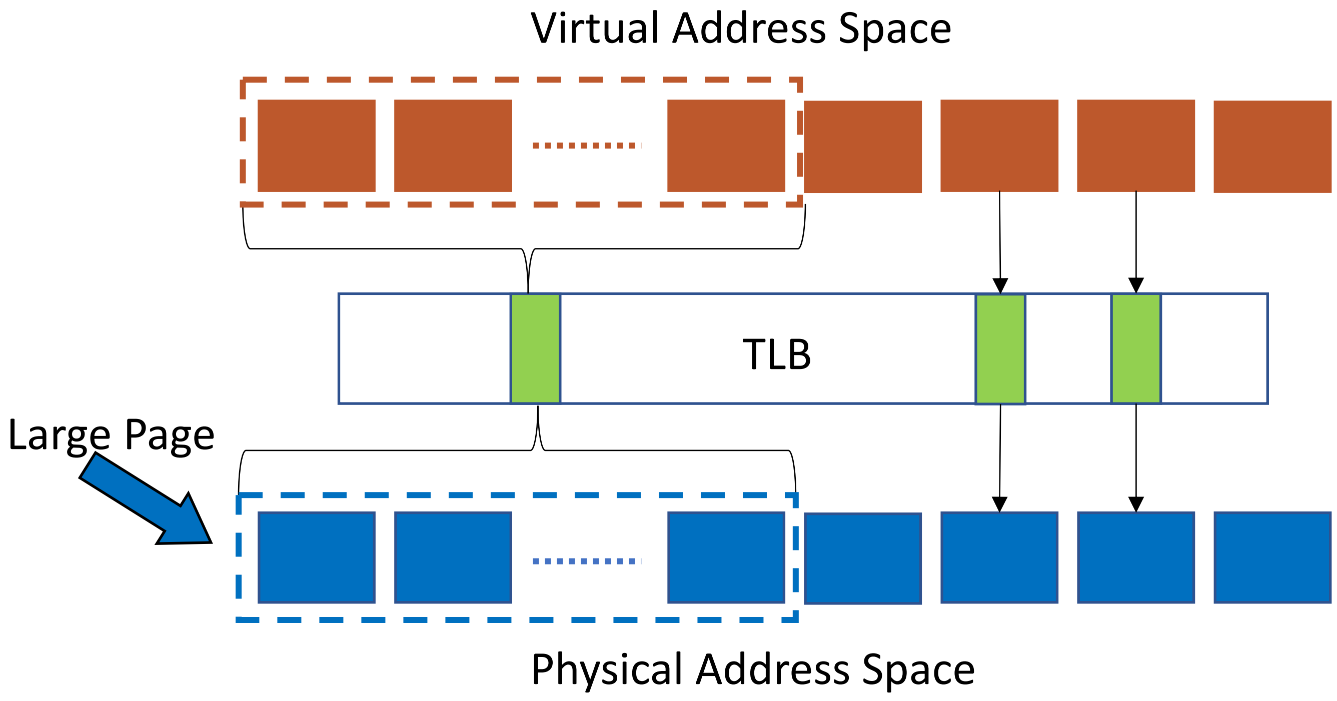




Proposed Defenses

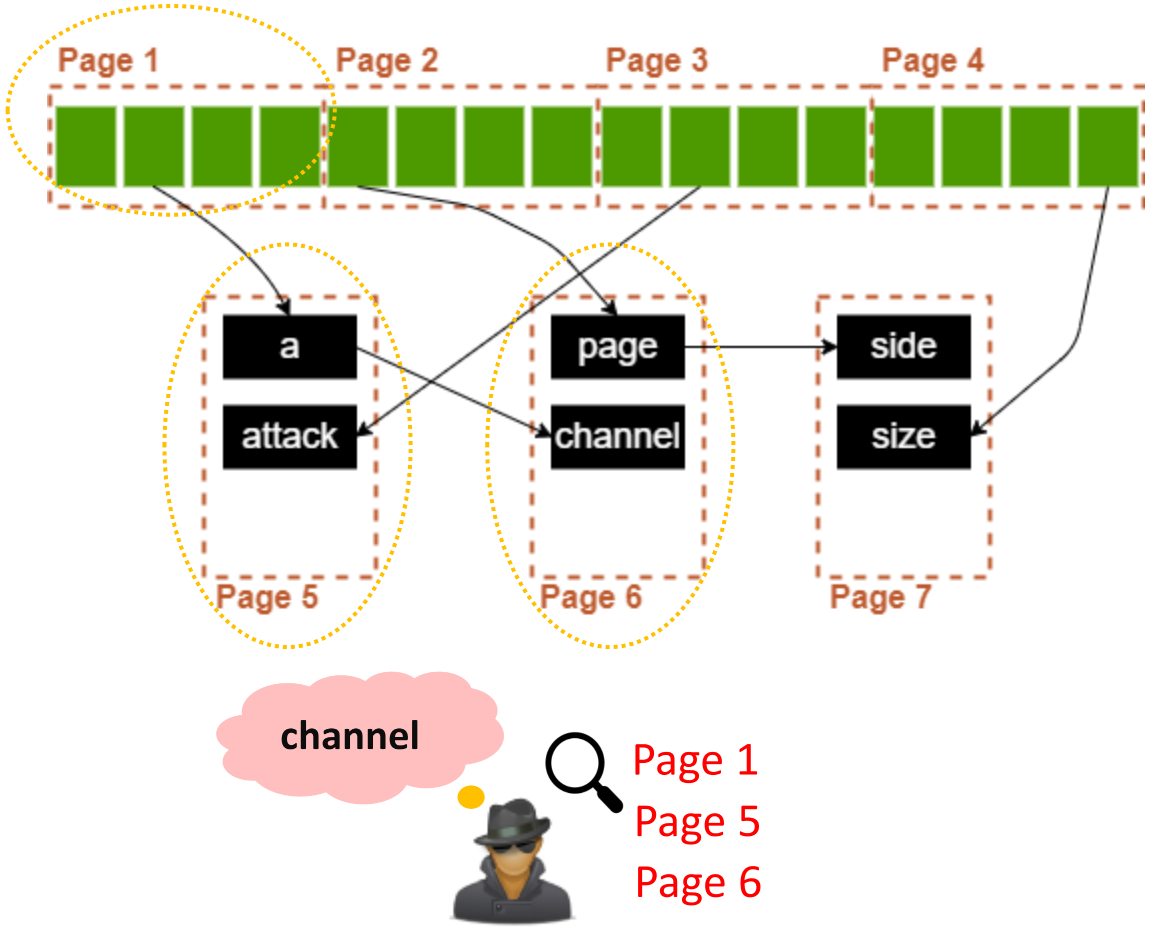
	Page faults	**PTE monitoring**	**TLB tapping**	**Legacy support**
T-SGX	✓	✗	✗	✗
DejaVu	✓	✗	✗	✗
SGX-LAPD	✓	✗	✗	✓
InvisiPage	✓	✓	✗	✓
PAO-compiler	✓	✓	✓	✗
SG^{XL}	✓	✓	✓	✓

SG^{XL}: Large Pages within SGX

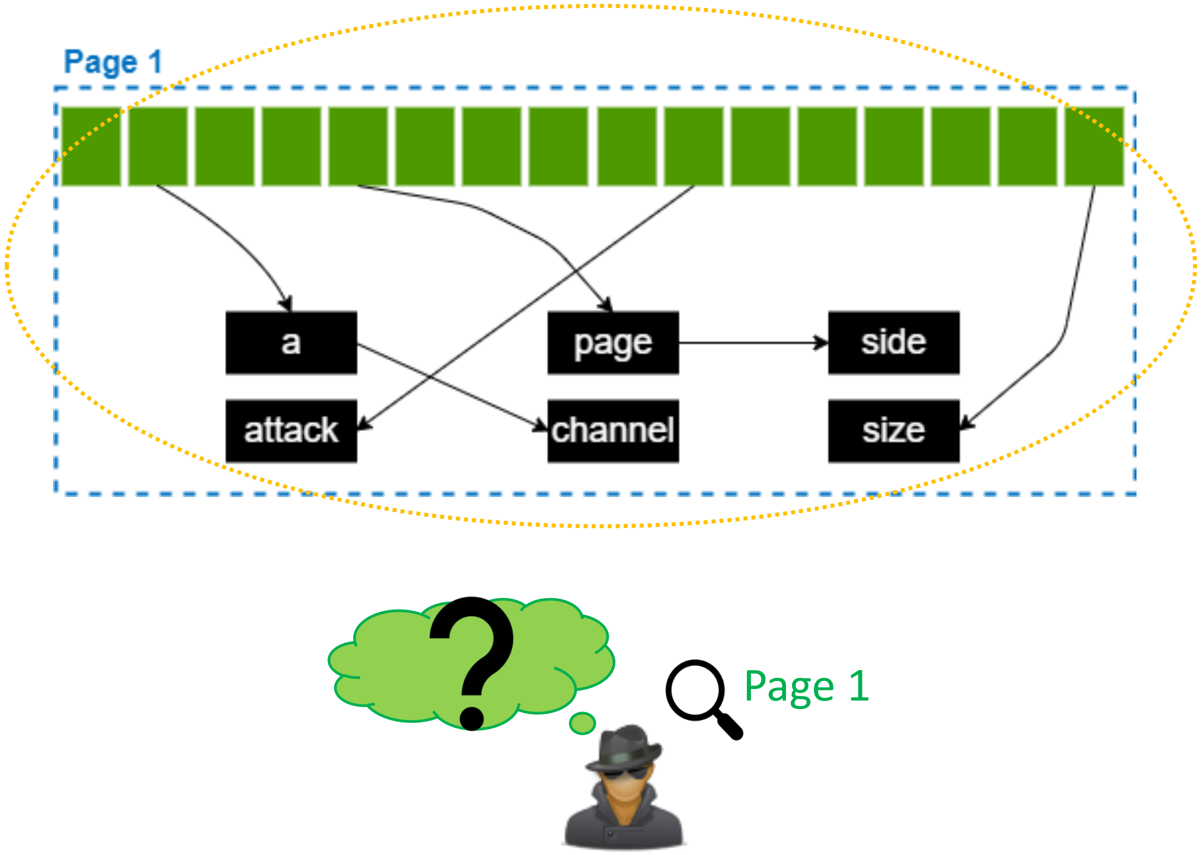


- Regular page size: 4KB
- Large page size: 2MB
  - Combines 512 consecutive 4KB pages
  - Large pages reduce translation overheads
- Large pages reduce the resolution of page address stream

SG^{XL}: Example



SGX with regular (4KB) pages



SG^{XL}

SG^{XL}: Operation

- SG^{XL} still relies on system software for page management. Malicious OS can lie about large pages.

- SG^{XL} needs to ensure that
  - Large pages are provided to the enclave during creation
  - Large page mappings are not changed during execution

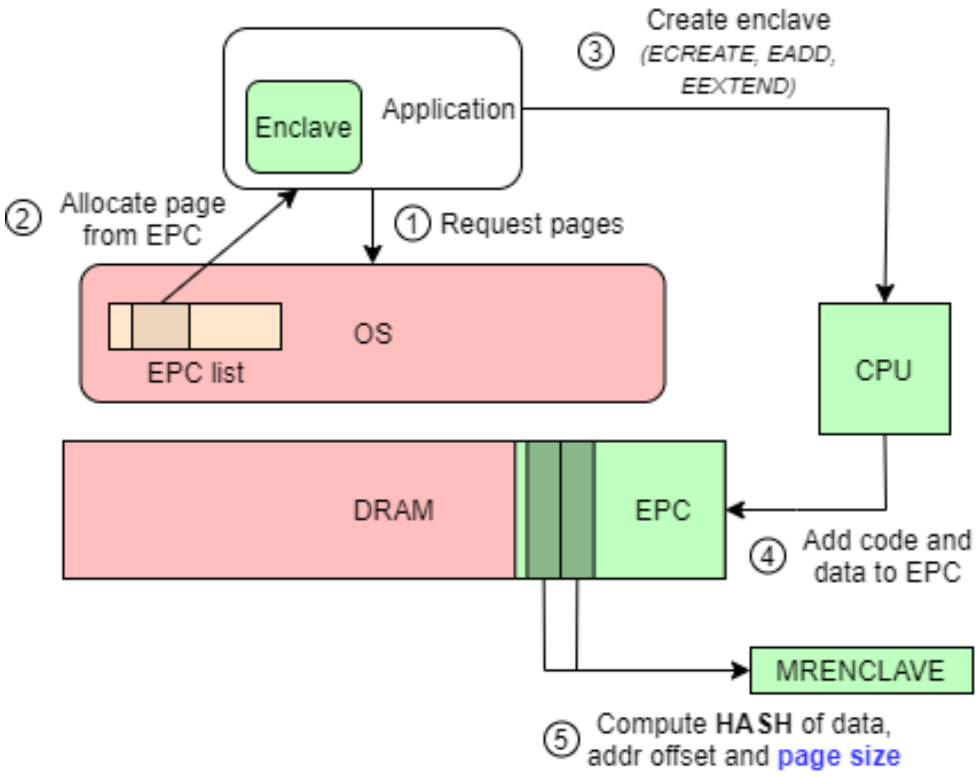
SG^{XL}: Operation

- SG^{XL} still relies on system software for page management. Malicious OS can lie about large pages.

- SG^{XL} needs to ensure that
  - Large pages are provided to the enclave during creation

    Solution: Enclave Measurement
  - Large page mappings are not changed during execution

SG^{XL}: Enclave Measurement



Create enclave
③ (ECREATE, EADD, EEXTEND)
Enclave
Application
② Allocate page from EPC
① Request pages
OS
EPC list
CPU
DRAM
EPC
④ Add code and data to EPC
MRENCLAVE
⑤ Compute HASH of data, addr offset and page size

- In SGX, enclave creation is measured (hash computation) before execution
- The hash primarily includes the data and address offset
- Hardware computes the hash and compares it to hash computed on the client side
- In SG^{XL}, the page size is included in the hash computation

SG^{XL}: Operation

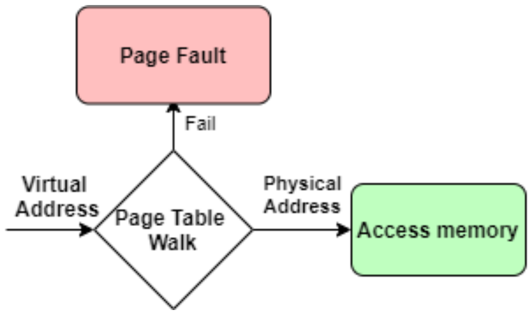
- SG^{XL} still relies on system software for page management. Malicious OS can lie about large pages.

- SG^{XL} needs to ensure that
  - Large pages are provided to the enclave during creation

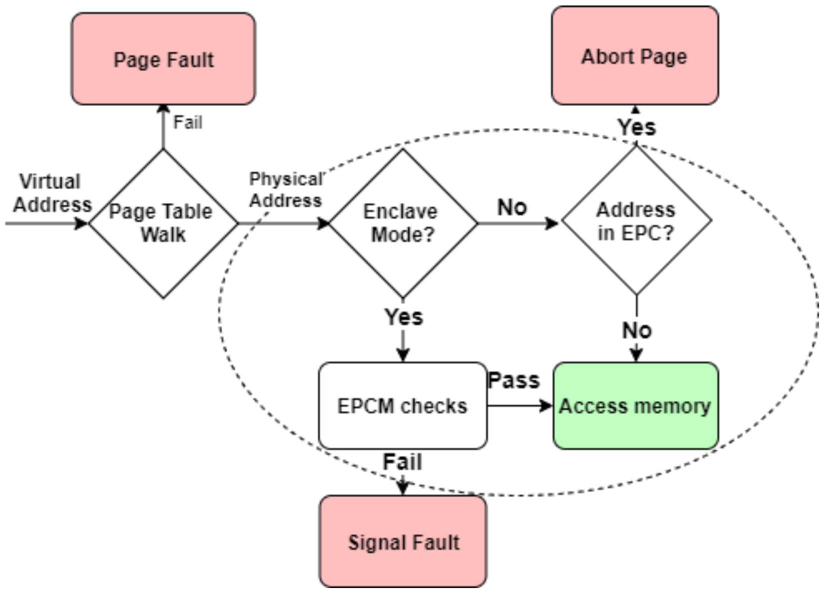
    Solution: Enclave Measurement
  - Large page mappings are not changed during execution

    Solution: Enhanced Access Checks

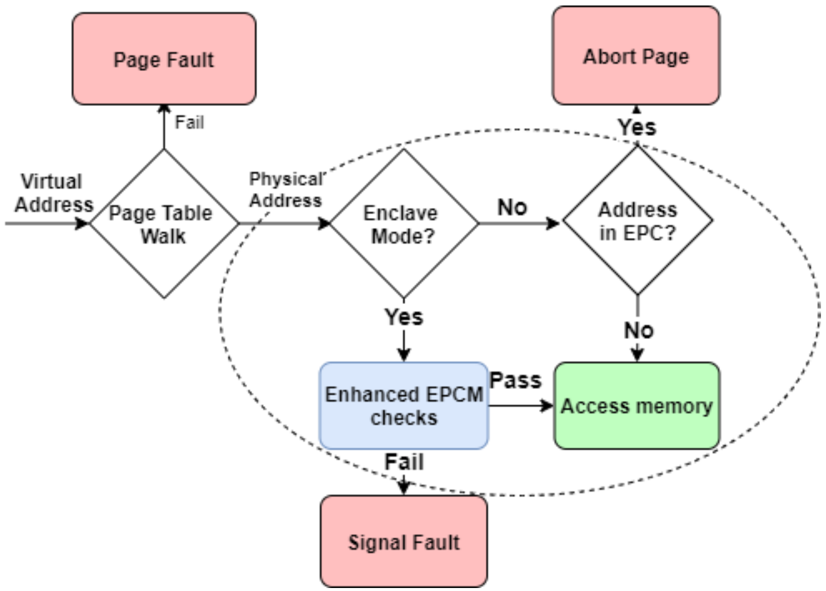
SG^{XL}: Enhanced Access Checks



Traditional systems



SGX



SG^{XL}

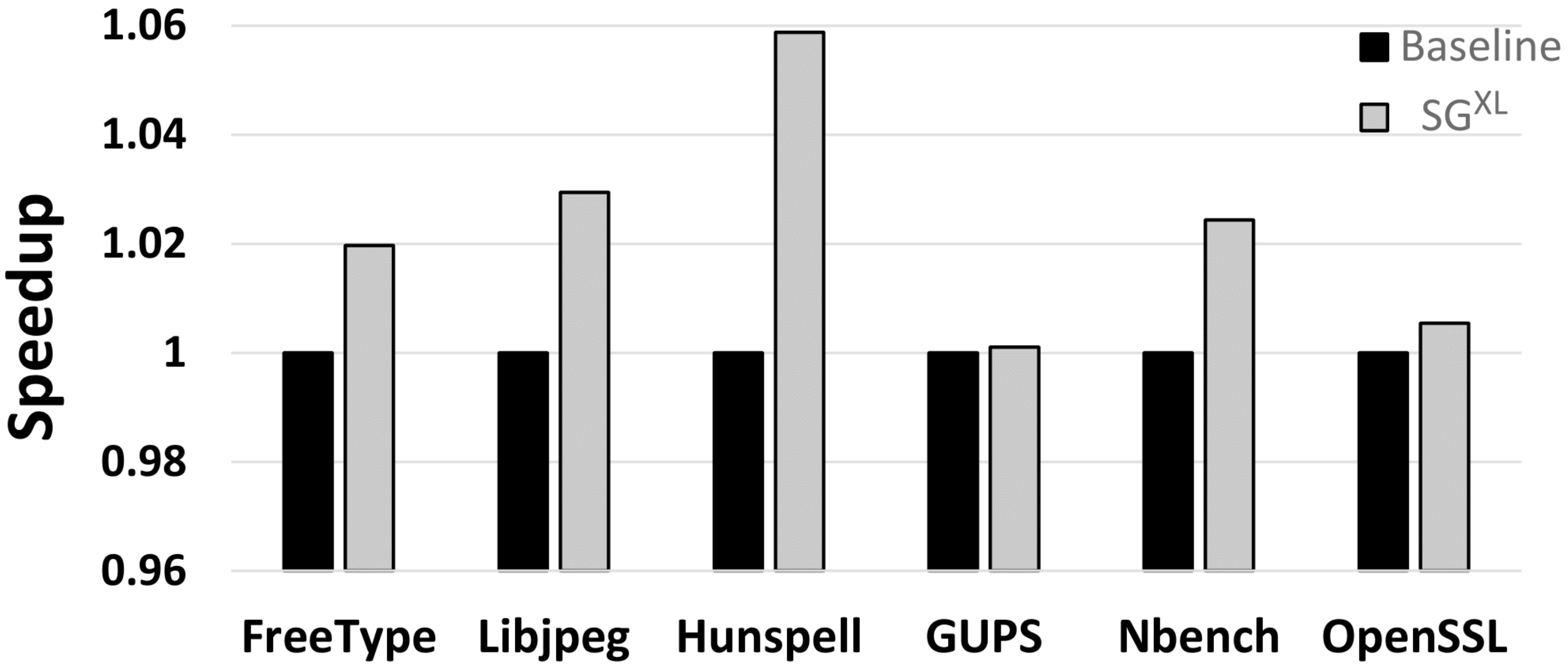
- EPCM stores page size along with offset and permissions
- Page size in EPCM compared to the page table entry size

Evaluation: Security

- We quantize the number of unique sequences that an attacker can identify using bigrams.
- A bigram is a pair of page addresses that appear in the page fault stream.

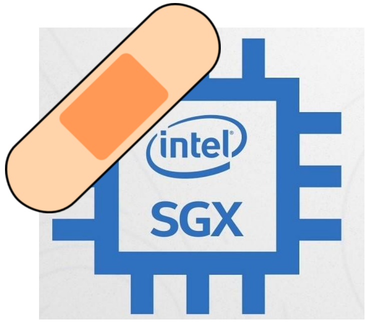
Number of unique bigrams			
Application	Baseline	SG^{XL}	% reduction
FreeType	506	0	100%
Libjpeg	15727	18	99.72%
Hunspell	22869	8	99.97%
GUPS	2825638	421	99.98%
NBench	182	5	97.25%
OpenSSL	1203	0	100%

Evaluation: Performance



Summary

- SGX is vulnerable to page address-based side channel attacks
- SG^{XL} uses large pages to reduce the resolution of page access stream significantly
- SG^{XL} proposes minor modifications to the hardware to guarantee the use of large pages in the presence of an adversarial OS
- SG^{XL} enhances security while improving the overall performance



Thank you!

https://github.com/csl-iisc/SGXL.git

sujayyadalam@cs.wisc.edu