A Survey on SGX Enclave Cache-miss Based Side-Channel Attacks

AMIN FALLAHI, Syracuse University, USA

Side-channel attacks targeting programs which are executed on Intel SGX processors are of common vulnerabilities in this platform. The security of code and data in the cloud is provided by execution of the program in the SGX enclave, but it is subject to side-channel attacks which target the enclave and retrieve data by controlling page-faults, cache-misses, TLB flushes, etc. In this report, we review and discuss common attacks on SGX enclaves, the protection which is needed and currently trending in research. In our study, we have observed and examined several researches done in this area and compared them with each other. Another importance in this area, is the performance loss caused by protection techniques which we also discuss in this report.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Security and privacy** → **Hardware-based security protocols**; **Side-channel analysis and countermeasures**; *Distributed systems security*; • **Computer systems organization** → *Processors and memory architectures*;

Additional Key Words and Phrases: Side-Channel Attack, Software Guard Extension, Page-Monitoring Attack

1 INTRODUCTION

One of the present challenges in cybersecurity systems is to outsource programs to be executed in the cloud and at the same time maintaining the privacy of the owner and the security of data. The program code has to be protected alongside the data which is being used inside it. Even in a securely encrypted code, the low-level instructions are visible when they are being executed by the CPU and a malicious operating system kernel can tamper with them. Several attacks are possible by reverse engineering the instructions, including code reuse, data injection, copyright violation, and recovery of classified data. Intel SGX (Software Guard eXtensions) [5] is a novel architecture introduced with Intel Skylake micro-architecture [8] that protects the code and the data inside an encrypted enclave that is a portion of memory which is protected by the support of hardware. The enclave is secure against direct eavesdropping by the adversary, but there are several successful attacking methods using side-channel information which is visible to the adversary [20]. The problem with this hardware extension is that the memory layout is still visible to the operating system kernel and a malicious OS in the cloud can recover useful information by observing the occurrences of page faults. As a result, this side-channel attack can be successful on recovering the data by clearing the page table and causing page faults and observing them for different inputs. In the same scenario, cache-misses are a point for side-channel attacks. The pattern of cache-miss occurrences can be used by a malicious operating system to attack the enclave program.

Several theoretical and practical attacks based on SGX side channels discussed and experimented to be practical and effective. The points of interest during the execution of a program inside enclave for the adversary are cache and whatever is missed and retrieved from the memory, page-faults, and page-table which is attacked by making use of accessed and modified bits.

Author's address: Amin Fallahi, Syracuse University, 111 College Pl 4-294, Syracuse, NY, 13244, USA, afallahi@syr.edu.

In response to the development of attacks, several defense mechanisms are designed which have been effective in some cases and conditions. These defense methods usually sacrifice performance or accuracy while improving the security against side-channel attacks.

In this report, we study the possible attacks which are possible using SGX side-channel information and their points of success. Then, we discuss possible defenses which have been proposed by the researchers and study their methods and compare the defenses and their effectiveness under different conditions and scenarios.

In summary, the main points of study in this work are:

- Examining SGX enclave points of attacks.
- Discussing the past work which have been done on defending the SGX enclave against side-channel attacks.
- Comparing and analyzing the defense methods and their effectiveness.

Outline In the remainder of this report, we discuss basic background knowledge required for studying this work in section 2. Then, we review and analyze the attacks which are possible to be launched against SGX enclave using side-channel information in section 3. In section 4, we introduce several defenses which have been proposed by past researches and in section 5 we analyze and compare the effectiveness of these defense methods in terms of security and performance. At last, we conclude the research in section 6.

2 BACKGROUND

In this section, we provide detailed background on side-channel attacks targeting enclaved applications, tools, and terms we use in this report.

2.1 Intel SGX

Protecting the data inside a shield has been a major interest for improving security and privacy in distributed systems and several software-based and hardware-based solutions have been proposed for this purpose.

Intel introduced a new hardware-based technique in its new Skylake micro-architecture [8] line of processors called Software Guard eXtensions (SGX) [5]. The main function of it is assigning a portion of main memory to a program and protect it from being read and written by other processes. The effectiveness of this technique scales up to preventing the operating system kernel itself from accessing the shielded memory which is called enclave. Intel SGX API [6] uses two main kinds of specialized function calls to work with enclave. ECALLs are functions which run inside the enclave and can be called from outside and OCALLs are useful for using system functions and other operations which are possible to be done outside enclave [4].

One of the major problems with running applications inside the cloud is the leakage of data and code instructions. Even with encryption, the CPU can only execute unencrypted instructions which can be eavesdropped and reverse engineered to useful code. Only with hardware modifications and adding SGX support to the hardware, it is possible to improve security and privacy in this term.

2.2 Storage Structure

In the common hardware architectures used in cloud computing environments today, data is transferred through several buses using multiple protocols to be used. The encrypted data is stored on the hard drive and will be transferred into enclaved memory. The encrypted data in the main memory will be cached using multiple levels of cache for performance

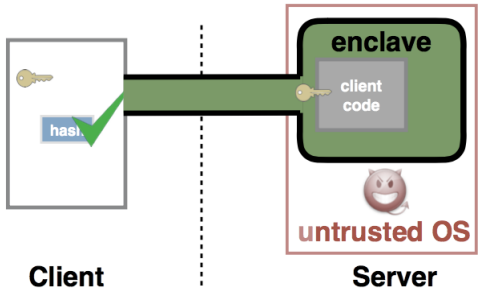

Fig. 1. Overview of remote attestation available in Intel SGX [19].

optimization. Also, page mappings between virtual and physical addresses of data are kept in the main memory and a transaction look-aside buffer (TLB) is used to cache the mappings in the page-table for better performance.

Each data transfer can be a point of side-channel attack. While the data is encrypted, the patterns of reads and writes, cache-misses, page-faults, and other interrupts and exceptions can be used by the adversary for launching attacks and recovering useful information.

2.3 Side-Channel Attacks on the Enclave

Multiple effective attacks and defenses on the enclave have been proposed by past research. Most of the attacks make use of the side-channel information that can be leaked and accessed by a modified malicious kernel. In these attacks, the malicious kernel retrieves useful information about the code and the data by changing the behavior of program execution or analyzing the page-faults and other possible points of data leakage.

One of the major points of attacks is targeting exceptions caused by the program. Since the exceptions are first acknowledged by the kernel before the program, a malicious OS can use them to infer activities and the behavior of the program according to the inputs which leads to recovering the actual data and code of the program.

Another kind of attack that can be triggered by a malicious OS is an interrupt-based attack. The kernel can trigger interrupts to control the execution of program.

Other attacks such as Stealthy Page Monitoring (SPM) attacks [18, 20] can also be effective. For a typical page-fault attack, the attacker can make all the page table entries invalid and restrict enclave programs access to all the pages and by causing page-faults, view the pattern of memory reads and writes by the program. This action will cause a lot of page-faults which lead to a high overhead which leads to attack detection by the victim, so the attacker is interested to retrieve this information and view the pattern without causing unwanted page-faults by the victim. In page monitoring attacks, the attacker monitors the bits representing the validity and whether a page is accessed or modified. The attacker is also able to clear these bits and view them again frequently. So, the pattern of accesses can be visible to the attacker without causing page-faults [18, 20].

2.4 Intel TSX

One of the technologies which have been came into notice for making benefit in defense against side-channel attacks is Intel TSX [9]. This technology has been introduced by Intel since Haswell mirco-architecture [3] for critical sections management and monitoring serialization. Intel TSX provides two frameworks to add transaction support to the processor.

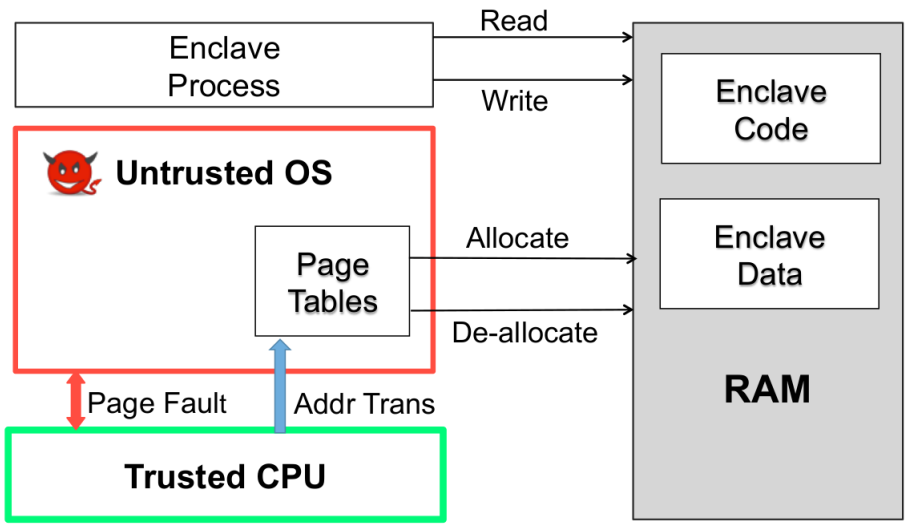

Fig. 2. Problem Setting. Process executing in an enclave on untrusted OS [16].

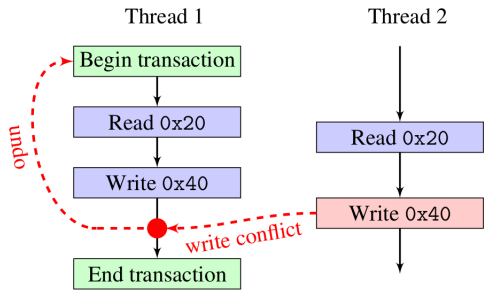

Fig. 3. HTM ensures that no concurrent modifications influence the transaction, either by preserving the old value or by aborting and reverting the transaction. [10].

Both frameworks intoduce new instructions for region specification, backward compatiblity, and flexiblity [9]. We use RTM (Restricted Transactional Memory) [7] for implementing our defenses in this work.

RTM has been used by previous researches like T-SGX [15] to isolate instructions and Cloak [10] to pin sensitive code and data to the caches which is not supported by current hardware instructions.

3 ATTACKS

Several side-channel attacks on the enclave have been proposed by the past research. Focusing on the thorough work done by Wang et al. [20] we focus on summarizing the attacks and the points of attacks in this section.

ALGORITHM 1: Prime+Probe branching side-channel sample code [10, 18]

```
if (secret)
{
    ;
}
else
{
    ;
}
```

3.1 Attack Model

In our attack scenario, the enclave is protected by Intel SGX, so no one except the main program running inside enclave has the key to access the enclave. The operating system kernel which runs on top of a hypervisor can view and manage tasks queue, exceptions and interrupts. The hypervisor kernel is also capable of viewing data transfer between memories and caches while Intel SGX prevents it from accessing the enclave data. It is considered that other tenants executing on the same hypervisor are not able to control the resources assigned to the main machine by the hypervisor.

3.2 Points of Attack

Several weaknesses in SGX architecture have been proposed to be points for launching attacks against the enclave.

TLB, as an address translation cache, can be one point of attack. While TLB is shared between enclave and non-enclave programs when hyper-threading is enabled, it can create side-channels which can be used for retrieving useful information [20].

Also, during AEX (Asynchronous EXit), TLB and paging-structure caches will be flushed and let the adversary know the flushed entries at context switch [20].

Another point of attack is the use of page table entry flags. The accessed and dirty bits which are set and unset for page table entries upon accesses and modifications, are used for launching attacks. So, the code in non-enclave mode can observe page-table updates and the memory write pattern to recover useful data [18, 20].

Other than TLBs, CPU caches are shared between the enclave and non-enclave code resulting in the possiblity of cache side-channel attacks [20].

3.3 Prime+Probe

Prime+Probe is composed of two stages. Considering an L1 cache of 64 sets, each containing 8 cache lines which are each 64 bytes, in the prime stage, the attacker executes conflicting cache lines to make page fault possible for the victim who branches on a secret. In the probe step, the attacker executes all the cache lines and measures the execution time of each, and if a cache line execution takes longer, it can be revealed that the secret has been zero [10, 13, 17].

3.4 Flush+Reload

By making use of page sharing between enclave and non-enclave code, the attacker can find out if a certain page is removed from the cache. More precisely, the attacker flushes the target memory line from the cache and waits for the victim to access it. The wait time can

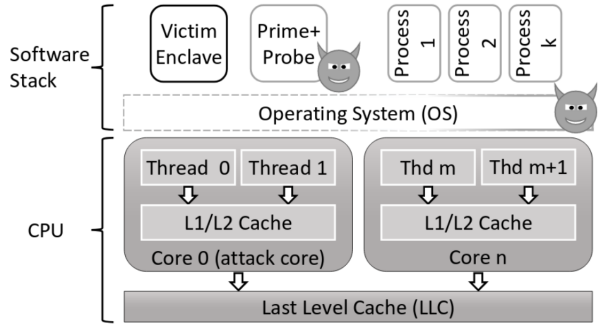

Fig. 4. High-level view of our attack; victim and attackers Prime+Probe code run in parallel on a dedicated core. The malicious OS ensures that no other code shares that core minimizing noise in L1/L2 cache [1].

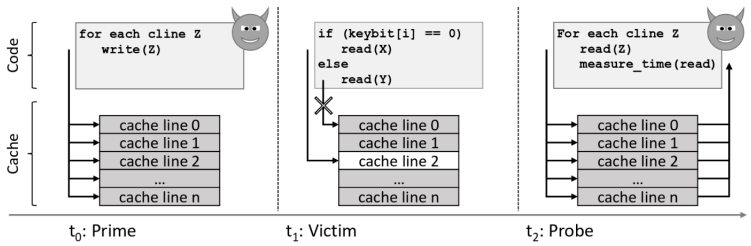

Fig. 5. Prime+Probe side-channel attack technique; first the attacker primes the cache, next the victim executes and occupies some of the cache, afterwards the attacker probes to identify which cache lines have been used by the victim. This information allows the attacker to draw conclusion on secret data processed by the victim process [1].

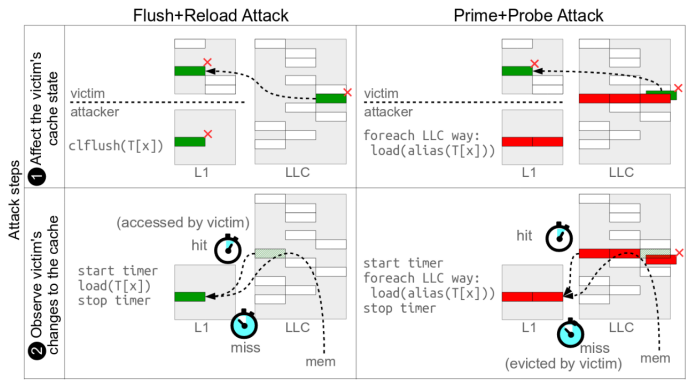

Fig. 6. Prime+Probe vs Flush+Reload Attacks [12].

be fixed to either a random value or a value that is experimented to be good for the attack success. Then, the attacker will request to access the page, and measures the time it takes for the page to be fetched. Judging based on the time, the attacker can say if the page is

already cached or fetched from the memory. In the case that it takes longer than a certain amount of time for the page to be retrieved, the attacker can conclude that it has not been fetched or touched by the victim [21].

3.5 Stealthy Page Table-Based Attacks

Since the emerging of various page-fault based side-channel attacks, it is important to come out with a method for retrieving information without causing page-faults. Intended page-faults are possible to protect, and also cause a lot of overhead which leads to attack detection.

Van Bulck et al. [18] have confirmed that accessed and dirty flags are set and unset for page table entries in both enclave mode and non-enclave mode. Monitoring these attacks can lead to page-fault detection on protected memory region without the need to induce intended page-faults [18].

3.6 Sneaky Page-Monitoring Attacks

Wang et al. [20] introduce three kinds of attacks for monitoring page-table entries with the consideration of the performance slowdown caused by inducing intentional page-faults. In the case that a page-fault is induced for each memory access by the victim, the number of page-faults and performance slowdown can be a point for attack detection.

3.6.1 Accessed flags monitoring. Accessed and dirty flags of page table entries, as discussed earlier, can be used to trigger attacks without causing page-faults. In this attack, the attacker monitors the set-unset pattern of the flags for page table entries and recovers information about the program running inside the enclave and encrypted data which is being accessed in the protected memory. A problem with this attack is that after address translations are cached in TLB, the flags are no longer updated in the page-table, but are updated in the TLB. Thus, it is needed to force the victim to walk its page-tables in order for the flags to be updated. In this attack, the attacker flushes the TLB by initiating an inter-processor interrupt which causes TLB shootdown. Thus, the flags will need to be updated in the page-table before being cached in the TLB [18, 20].

3.6.2 Timing enhancement. High number of accesses to a page-table entry for a certain input, can result in lots of interrupt requests in accessed flags monitoring attack which can be detected by monitoring interrupt requests by the victim. To prevent this, by finding out two pages which are accessed by the victim repetitively, and measuring the time between these two page accesses, the input can be recovered. Thus, instead of multiple interrupts, one interrupt after each cycle is enough for clearing the TLB and successful attack.

3.6.3 TLB flushing through Hyper-Threading. To further remove the interrupts which are needed by the two aforementioned attacks, it is possible to make use of the fact that the TLB is shared between two threads which are being executed on the same core. Thus, by running the attacker program in the same core with the victim program, it is possible to invalidate TLB entries outside the enclave and without initiating interrupts.

3.7 DRAMA Attacks

With caching disabled to prevent cache-based side-channel attacks, the attacker allocates two memory lines in the same memory bank which map to different virtual addresses but have common physical addresses. Then the attacker starts to regularly access on of the memory lines. In case the victim accesses the other memory line, a row conflict will cause

the next fetch of the attacker to take more time. By measuring these times the attacker can recover the sensitive memory access which is done by the victim [14, 20].

3.8 Cache-DRAM Attacks

Using two threads for launching the Prime+Probe attack [13, 17] and DRAMA attacks [14] together, Prime+Probe can cause conflicts in the cache which leads to fetching the data from DRAM, making DRAMA attack possible in the case caching is disabled [20]. Therefore, launching this attack, the slowdown caused by disabling cache in DRAMA attacks is avoided.

3.9 Flush+Flush

Using the *clflush* instruction, it is possible to flush a cache line and if the cache line is already empty, the instruction will abort. Considering that the abort takes less time than the flush, it is possible to use this delay to recover information about the content of the cache. By observing the existence of data inside the cache line, it is possibe to find out which memory address have been accessed by the victim. Running the *clflush* instruction repetitively and measuring its execution time, the attacker retrieves this information [11].

4 DEFENSES

4.1 Cache-based attacks

It is known that in a multicore system, there are three levels of cache: L3 is shared between all physical cores, L2 is shared between each cores threads and L1 shares data and code separately between the hyperthreads. In a typical environment, it is not visible to the enclave program running in one thread, what is being run in the other thread on the same core. So, if the other hyperthread is trusted (assuming there are two hyperthreads running in each core) it is only needed to care about the L3 cache. In the SGX environment, the hyperthreads cannot trust each other, thus, L2 and L1 caches are also of importance when it comes to the case of cache side-channel attacks, because attacks like Prime+Probe will be possible in this case [10].

The obvious approach to confront cache-based side-channel attacks including Prime+Probe [13, 17] and eliminate the leakage is to pin sensitive code and data into caches so no conflict and cache-miss be possible to happen, but it is not possible to pin data into caches in the current hardware/software environment. So, there is a need to introduce a hack for indirectly doing this that has been implemented using Intel TSX by Gruss et al. [10]. TSX works like making use of semaphores to prevent interrupts but performs faster.

By studying the in-depth architecture of TSX instructions, it is found out that TSX uses a write set and a read set and interrupts to these sets cause the transaction to abort. The write set is always the 32kb L1 and the read set is the 8mb sized L3. So, if a cache line in L1 is modified and made dirty, the transaction aborts. The same happens when some cache line in L3 is removed due to a conflict. Also, it is observed that code, which is read-only, can only be a part of the read set L1. This has the benefit of detecting external code evictions by other cores which share the same L3 cache [10].

After explaining the indirect effect of using TSX for pinning data to cache it is needed to load the data and code into the cache inside a TSX transaction. After that, each cache conflict which leads to making cache access pattern to be visible will cause the transaction to abort. So, the sensitive code and data will be preloaded and the program will start to run inside the transaction. Then, the victim does not experience cache misses and there is nothing for the attacker to measure, so the enclave is protected against malicious OS [10].

ALGORITHM 2: Cloak sample code [10]

```
xbegin();
preload all sensitive data/code;
run algorithm;
xend();
```

For preloading, if the attacker targets L1, the code should be preloaded into L1-I by execution. Also, all the data should be loaded into the write set. For the attackers targeting L3, code and read-only data should be loaded into read set, while the data which will possibly be touched again should be loaded into the write set [10].

4.1.1 Analysis. There will still be some leakage remaining which this research does not handle. Overall execution time can leak information. Also, aborts do not cause the concurrent memory accesses to be canceled. Branch predictor is influenced due to the cache pinning and other micro-architecture effects can be possible due to the modifications to the execution behavior.

The strength of the research is to introduce a new software-based way for pinning data into cache lines which has not been done before. Making use of Intel TSX instructions for this purpose is a novel idea that can be used in various areas other than enclave side channel attack protection. There is also an opportunity for later research on optimization and performance improvement and architectural study for reducing faults.

4.2 Dj Vu

Chen et al. [2] focus on detecting SGX side-channel attacks performed by privileged attackers (OS, etc.). They make use of Intel TSX to embed a clock inside the enclave. The use of TSX is for detecting any interrupts to the clock itself if occurred. When the execution time of the program inside the enclave exceeds a fixed amount of time as the threshold, it is considered that the code has been interrupted by some external factor and an AEX (asynchronous enclave exit) will be detected. Thus, the research claims to detect attacks to a good degree and the evaluation results show little performance overhead and good precision in detecting the attacks.

The implemented clock should be hidden from the OS in terms of reading and modification and it should not be decreased under any condition. These can be assured by implementation inside SGX enclave. Also, the clock should not be stopped or interrupted by the OS. This feature is addressed by using Intel transactional memory. For protecting the clock to be read by the OS, a random value will be generated in a transaction and will be added to the global timer variable. This will run in a thread parallel to the main program which is targeted to be executed inside the enclave.

For measuring the threshold for program interruption detection by the attacker, the system needs to be trained with execution to learn the execution time without AEXs and the minimum time of an AEX execution.

The security evaluation has been done by running attacks on the clock for stopping it, triggering page-faults for tracing the execution, and slowing the clock by modifying CPU cores' working frequency.

4.2.1 Strengths and Weaknesses. The problem with this method is that it only considers enclave exits as points of attacks and possible attacks that may have been occurred during the execution which do not cause AEX have been excluded. So, attacks like B-SPM and

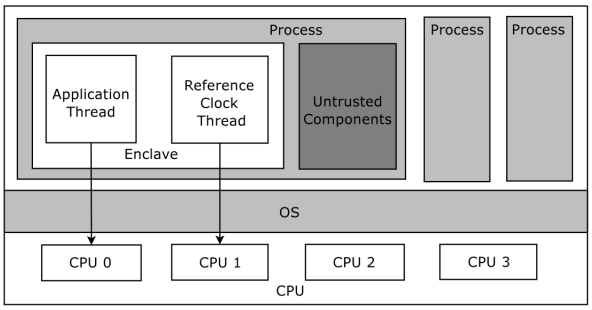

Fig. 7. System architecture of Dj Vu. Blocks in gray are untrusted, which include the untrusted components of the processes and the entire OS kernel [2].

HT-SPM (sneaky page monitoring attacks in general) which do not rely on AEX can still be effective in the presence of Dj Vu.

4.3 Pigeonhole attacks

Shinde et al. [16] study the possible side-channel attacks which make use of page-faults. Firstly, they do a statistical study on the percent of leakage, vulnerability, and the possibility and effectiveness of page-fault based attacks which they call pigeonhole attacks. Then, they study the possible ways of eliminating page-fault side-channels. The paper claims that for lowering the overheads, there is a need for hardware changes. It defines pigeonhole attack as an attack that is performed when a page table walk is done. Moving data between physical memory and virtual memory from different pages sequentially causes page-faults on every single page when the virtual memory is already full, holding all the other pages. When the first page is fetched, the next page will be removed from the page table and when the next page is to be fetched, a page fault will occur.

The solution of the paper is based on the fact that the malicious OS cannot differentiate accesses which are occurred in a single page. Thus, by mapping all the input dependent data into a single page, the program will access the same pattern of the pages independent of the input and makes it page fault oblivious. The page containing the input dependent data is called data staging page and the page containing the code is called code staging page. By creating a decision tree of the program instructions, it is understood that in each stage of the program which is being executed, there is a page-fault sequence dependent on the data, which can be mapped to a staging page. So for each stage, we consider a staging page.

This technique will create a big overhead, thus the paper also works on optimizing the method they have implemented. The optimizations are:

- Eliminating copy operations by skipping saving the read-only data
- Merge small data blocks into single pages to reduce the number of fetches
- Merge levels of execution and reduce the number of stages
- Removing the mux based on the input to reduce the possibility of branch conditions
- Remove the dependence of code on the data, Ex. CAS obliviousness

The idea of the paper has been implemented as an LLVM compiler pass.

4.4 Stealthy

This paper introduces a new group of side-channel attacks named stealthy page table-based attacks which are not dependent on page faults and can recover useful information from

the data which is being accessed by the program running inside the enclave without page faults being occurred. While current defenses are all based on preventing page faults from happening, there is little effort to prevent attacks which do not depend on page faults.

One of the attack vectors discussed by this paper is pages accessed and dirty bits. Suppose a program is being executed in the enclave which branches based on a secret. If the branch occurs one page will be retrieved and thus its accessed flag will be set, otherwise the same happens for another page. By observing the accessed bit for these two page tables, the secret is revealed. Doing this sequentially can reveal all the secrets which lead to EdDSA session key to be revealed gradually.

The evaluation of this research is done by writing a microbenchmark for measuring interrupts frequency and latency and launching attacks against Libgcrypt EdDSA for extracting private session keys. The results show that it is possible to recover the same session keys which are possible by attacking using page faults without incurring page faults.

4.4.1 Strengths and Weaknesses. Does not work on performance optimization but only to attack and recover information without the use of page faults.

5 SGX-SHIELD

6 CONCLUSIONS

In this article, we develop the first multifrequency MAC protocol for WSN applications in which each device adopts a single radio transceiver. The different MAC design requirements for WSNs and general wireless ad-hoc networks are compared, and a complete WSN multifrequency MAC design (MMSN) is put forth. During the MMSN design, we analyze and evaluate different choices for frequency assignments and also discuss the nonuniform back-off algorithms for the slotted media access design.

7 TYPICAL REFERENCES IN NEW ACM REFERENCE FORMAT

A paginated journal article [**?**], an enumerated journal article [**?**], a reference to an entire issue [**?**], a monograph (whole book) [**?**], a monograph/whole book in a series (see 2a in spec. document) [**?**], a divisible-book such as an anthology or compilation [**?**] followed by the same example, however we only output the series if the volume number is given [**?**] (so Editor00a's series should NOT be present since it has no vol. no.), a chapter in a divisible book [**?**], a chapter in a divisible book in a series [**?**], a multi-volume work as book [**?**], an article in a proceedings (of a conference, symposium, workshop for example) (paginated proceedings article) [**?**], a proceedings article with all possible elements [**?**], an example of an enumerated proceedings article [**?**], an informally published work [**?**], a doctoral dissertation [**?**], a master's thesis: [**?**], an online document / world wide web resource [**? ? ?**], a video game (Case 1) [**?**] and (Case 2) [**?**] and [**?**] and (Case 3) a patent [**?**], work accepted for publication [**?**], 'YYYYb'-test for prolific author [**?**] and [**?**]. Other cites might contain 'duplicate' DOI and URLs (some SIAM articles) [**?**]. Boris / Barbara Beeton: multi-volume works as books [**?**] and [**?**].

A couple of citations with DOIs: [**? ?**].

Online citations: [**? ? ?**].

A SWITCHING TIMES

In this appendix, we measure the channel switching time of Micaz [**?**] sensor devices. In our experiments, one mote alternatingly switches between Channels 11 and 12. Every time after the node switches to a channel, it sends out a packet immediately and then changes to a new

channel as soon as the transmission is finished. We measure the number of packets the test mote can send in 10 seconds, denoted as N_1. In contrast, we also measure the same value of the test mote without switching channels, denoted as N_2. We calculate the channel-switching time s as

$$s = \frac{10}{N_1} - \frac{10}{N_2}.$$

By repeating the experiments 100 times, we get the average channel-switching time of Micaz motes: 24.3 μs.

B SUPPLEMENTARY MATERIALS

B.1 This is an Example of Appendix Subsection Head

Channel-switching time is measured as the time length it takes for motes to successfully switch from one channel to another. This parameter impacts the maximum network throughput, because motes cannot receive or send any packet during this period of time, and it also affects the efficiency of toggle snooping in MMSN, where motes need to sense through channels rapidly.

By repeating experiments 100 times, we get the average channel-switching time of Micaz motes: 24.3 μs. We then conduct the same experiments with different Micaz motes, as well as experiments with the transmitter switching from Channel 11 to other channels. In both scenarios, the channel-switching time does not have obvious changes. (In our experiments, all values are in the range of 23.6 μs to 24.9 μs.)

B.2 Appendix Subsection Head

The primary consumer of energy in WSNs is idle listening. The key to reduce idle listening is executing low duty-cycle on nodes. Two primary approaches are considered in controlling duty-cycles in the MAC layer.

ACKNOWLEDGMENTS

The authors would like to thank Dr. Maura Turolla of Telecom Italia for providing specifications about the application scenario.

The work is supported by the National Natural Science Foundation of China under Grant No.: 61273304_a and Young Scientists' Support Program (http://www.nnsf.cn/youngscientists).

REFERENCES

[1] Ferdinand Brasser, Urs Müller, Alexandra Dmitrienko, Kari Kostiainen, Srdjan Capkun, and Ahmad-Reza Sadeghi. 2017. Software grand exposure: SGX cache attacks are practical. *arXiv preprint arXiv:1702.07521* (2017), 33.

[2] Sanchuan Chen, Xiaokuan Zhang, Michael K Reiter, and Yinqian Zhang. 2017. Detecting privileged side-channel attacks in shielded execution with Déjá Vu. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM, 7–18.

[3] Intel Corporation. [n. d.]. 4th Generation Intel Core Processor. Retrieved April 12, 2018 from https://software.intel.com/en-us/node/524022

[4] Intel Corporation. [n. d.]. ECALL/OCALL Functions. Retrieved April 12, 2018 from https://software.intel.com/en-us/node/709001

[5] Intel Corporation. [n. d.]. Intel Software Guard Extensions (Intel SGX). Retrieved April 12, 2018 from https://software.intel.com/en-us/sgx

[6] Intel Corporation. [n. d.]. Intel Software Guard Extensions (Intel SGX) SDK. Retrieved April 12, 2018 from https://software.intel.com/en-us/sgx-sdk

[7] Intel Corporation. [n. d.]. Restricted Transactional Memory Overview. Retrieved April 12, 2018 from https://software.intel.com/en-us/node/524022
[8] Intel Corporation. 2017. 6th Generation Intel Processor Family. Retrieved April 12, 2018 from https://www.intel.com/content/www/us/en/processors/core/desktop-6th-gen-core-family-spec-update.html
[9] Intel Corporation. 2017. Intel Transactional Synchronization Extensions (Intel TSX) Overview. Retrieved April 12, 2018 from https://software.intel.com/en-us/node/524022
[10] Daniel Gruss, Julian Lettner, Felix Schuster, Olya Ohrimenko, Istvan Haller, and Manuel Costa. 2017. Strong and efficient cache side-channel protection using hardware transactional memory. In *USENIX Security Symposium*.
[11] Daniel Gruss, Clémentine Maurice, Klaus Wagner, and Stefan Mangard. 2016. Flush+ Flush: a fast and stealthy cache attack. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 279–299.
[12] Mehmet Kayaalp, Nael Abu-Ghazaleh, Dmitry Ponomarev, and Aamer Jaleel. 2016. A high-resolution side-channel attack on last-level cache. In *Proceedings of the 53rd Annual Design Automation Conference*. ACM, 72.
[13] Dag Arne Osvik, Adi Shamir, and Eran Tromer. 2006. Cache attacks and countermeasures: the case of AES. In *Cryptographers Track at the RSA Conference*. Springer, 1–20.
[14] Peter Pessl, Daniel Gruss, Clémentine Maurice, Michael Schwarz, and Stefan Mangard. 2016. DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks.. In *USENIX Security Symposium*. 565–581.
[15] Ming-Wei Shih, Sangho Lee, Taesoo Kim, and Marcus Peinado. 2017. T-SGX: Eradicating controlled-channel attacks against enclave programs. In *Proceedings of the 2017 Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA*.
[16] Shweta Shinde, Zheng Leong Chua, Viswesh Narayanan, and Prateek Saxena. 2015. Preventing your faults from telling your secrets: Defenses against pigeonhole attacks. *arXiv preprint arXiv:1506.04832* (2015).
[17] Eran Tromer, Dag Arne Osvik, and Adi Shamir. 2010. Efficient cache attacks on AES, and countermeasures. *Journal of Cryptology* 23, 1 (2010), 37–71.
[18] Jo Van Bulck, Nico Weichbrodt, Rüdiger Kapitza, Frank Piessens, and Raoul Strackx. 2017. Telling your secrets without page faults: Stealthy page table-based attacks on enclaved execution. In *Proceedings of the 26th USENIX Security Symposium*. USENIX Association.
[19] Frank Wang. 2017. Opaque: An Oblivious and Encrypted Distributed Analytics Platform. https://medium.com/mit-security-seminar/opaque-an-oblivious-and-encrypted-distributed-analytics-platform-4109a0e70bcf
[20] Wenhao Wang, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, Xiaofeng Wang, Vincent Bindschaedler, Haixu Tang, and Carl A. Gunter. 2017. Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX. 2421–2434.
[21] Yuval Yarom and Katrina Falkner. 2014. FLUSH+ RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack.. In *USENIX Security Symposium*. 719–732.