ИСП РАН

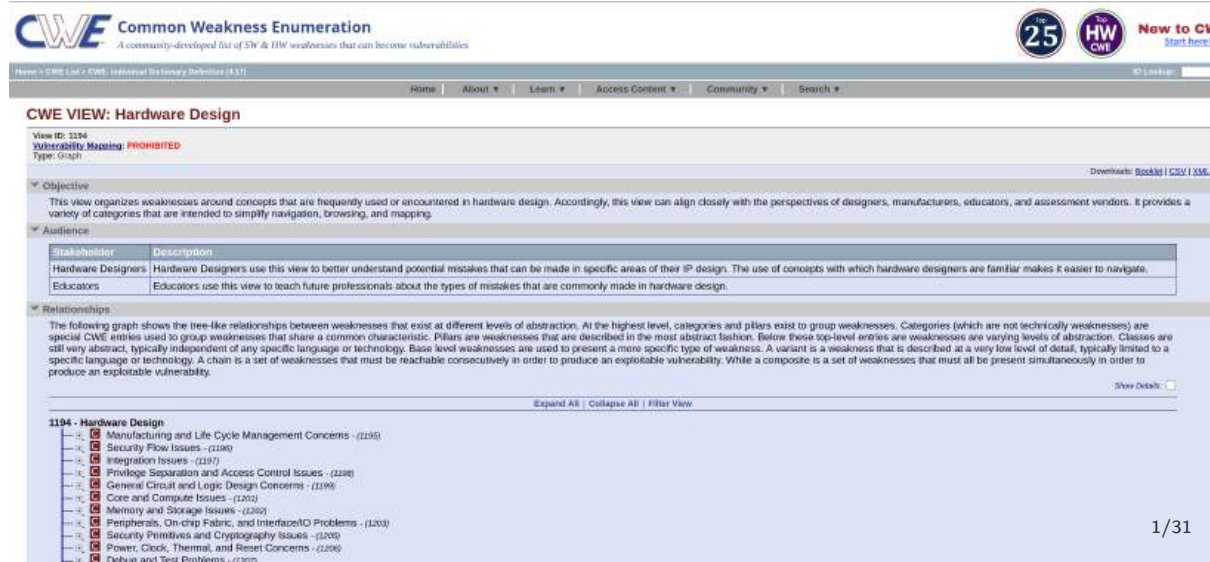
Обзор актуальных аппаратных уязвимостей

М. Ю. Кричанов <krichanov@ispras.ru>

19 июня 2025 г.

ИСП РАН

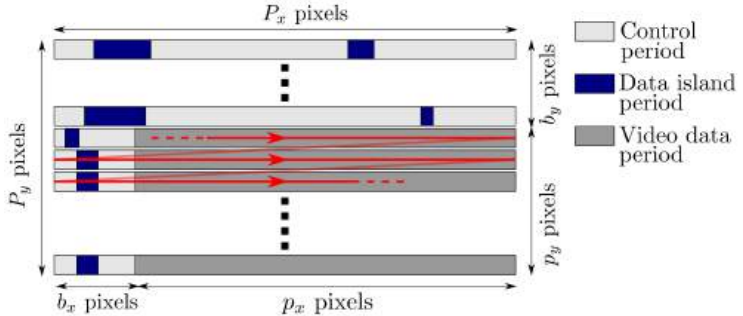
База данных аппаратных уязвимостей



Электромагнитное излучение: VGA и DVI

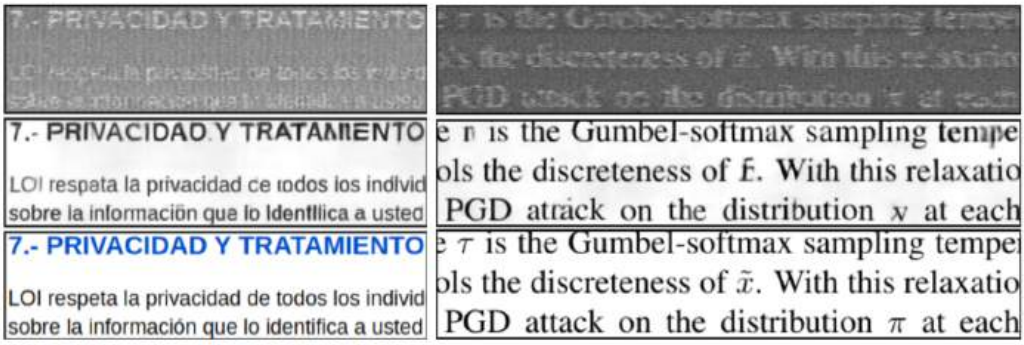
Wim van Eck: ***Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*** Computers & Security, Vol. 4, pp. 269–286, 1985.

Электромагнитное излучение: HDMI



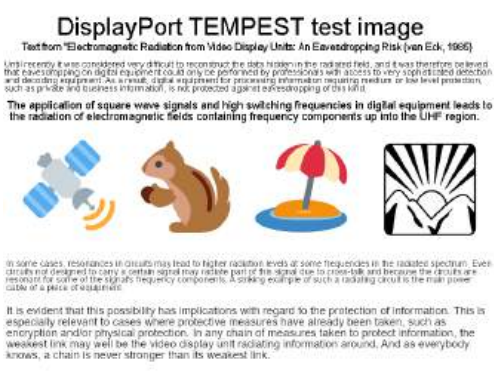
Santiago Fernández, et. al.: ***Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations.***

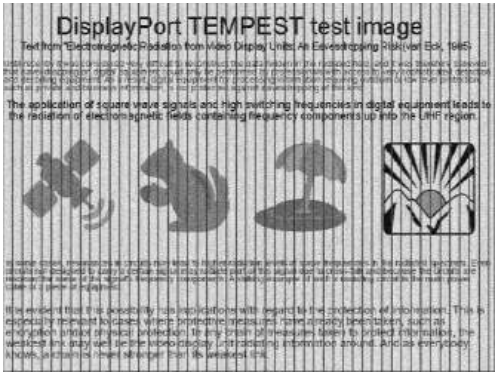
Электромагнитное излучение: HDMI



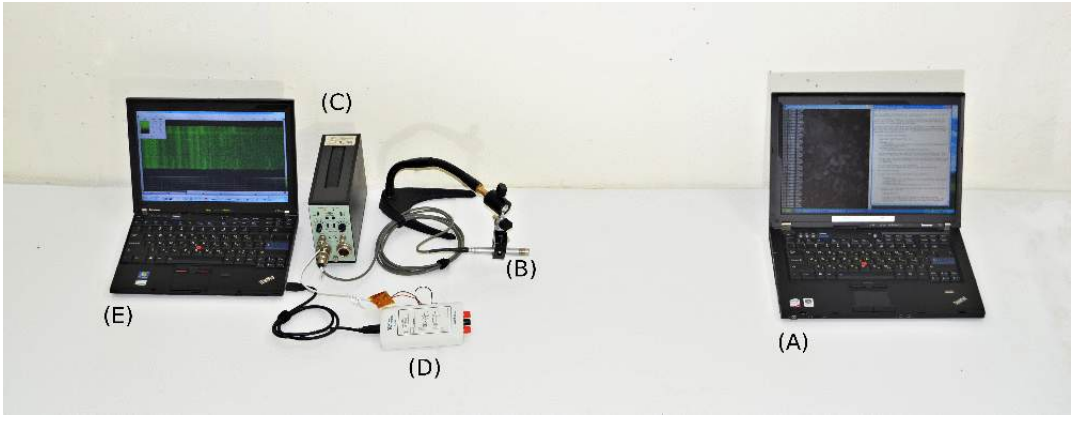
Santiago Fernández, et. al.: ***Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations.***

Электромагнитное излучение: DisplayPort





Акустические колебания



A – атакуемая машина. B – микрофон. C – источник питания и усилитель. D – АЦП. E – компьютер злоумышленника.

Daniel Genkin, et. al.: ***RSA key extraction via low-bandwidth acoustic cryptanalysis.*** IACR Cryptology ePrint Archive, 2013:857, 2013.

Акустические колебания: RSA, криптоанализ

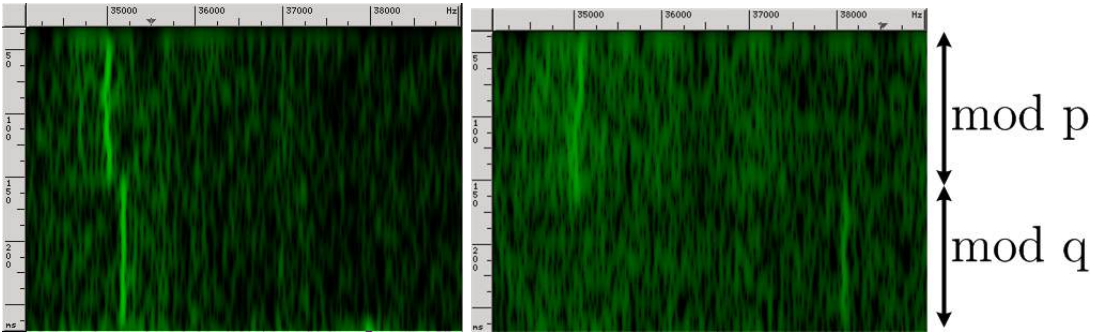
$$M = C^d \bmod N,\ N = p \times q$$

- Атака на основе специальным образом подобранных шифротекстов.
- Извлекает по одному биту секретного ключа за сообщение.
- Оптимизаций №1 – китайская теорема об остатках: mod $N \rightarrow$ mod p, mod q.
- Оптимизаций №2 – разные алгоритмы умножения в зависимости от размера множителя (в байтах).
- Разные шифротексты $\rightarrow$ разные потоки управления $\rightarrow$ разное энергопотребление ЦП.

Daniel Genkin, et. al.: ***RSA key extraction via low-bandwidth acoustic cryptanalysis.*** IACR Cryptology ePrint Archive, 2013:857, 2013.

Акустические колебания: RSA, спектральный анализ

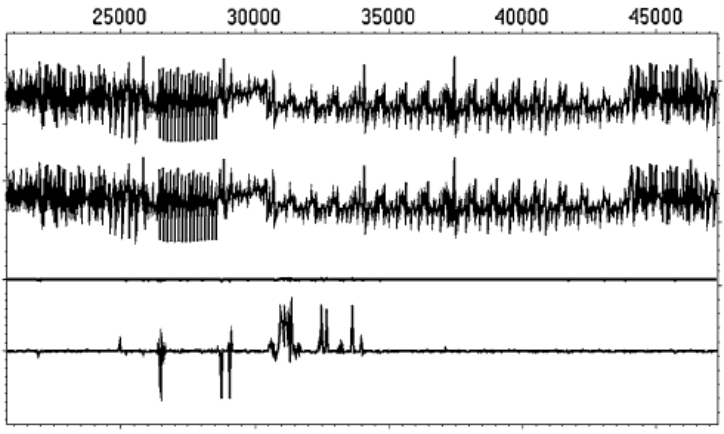
$$M = C^d \bmod N,\ N = p \times q$$



$q_i = 0$ $q_i = 1$

Daniel Genkin, et. al.: ***RSA key extraction via low-bandwidth acoustic cryptanalysis.*** IACR Cryptology ePrint Archive, 2013:857, 2013.

Анализ энергопотребления: измерение напряжения

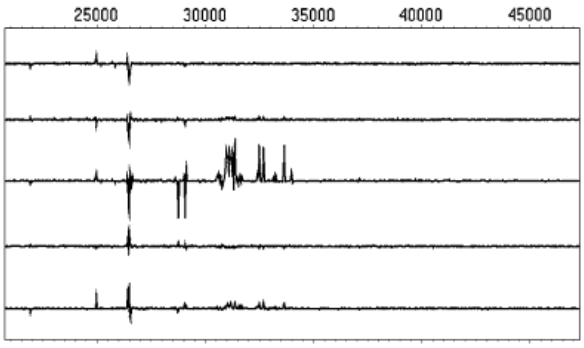


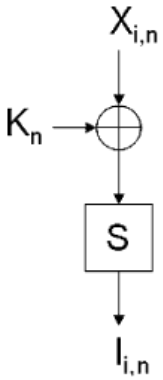
Дифференциальный анализ:

1. Сбор трасс.
2. Разбиение на 2 множества.
3. Усреднение множеств.
4. Вычитание усреднённых трасс.

Paul Kocher, et. al.: ***Introduction to differential power analysis.*** Journal of Cryptographic Engineering, Volume 1, pages 5–27 (2011).

Анализ энергопотребления: AES-128





- X – открытый текст
- K – секретный ключ
- i – номер трассы
- n – номер байта
- S – таблица замен
- I – результат подстановки
- $I_{i,0}(X_{i,0})[0]$ – функция разбиения
- 256 возможных значений K_0

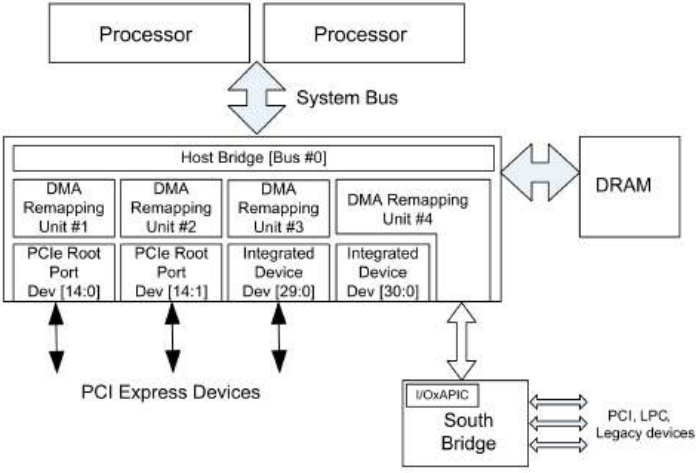
Paul Kocher, et. al.: ***Introduction to differential power analysis.*** Journal of Cryptographic Engineering, Volume 1, pages 5–27 (2011).

Периферийные устройства

1. Нет криптографии, есть обновление.
2. Сетевую карту можно взломать удалённо.
3. PCI Express позволяет устройствам взаимодействовать в обход ЦП.
4. BIOS должен правильно настроить Access Control Services (PCIe ACS).

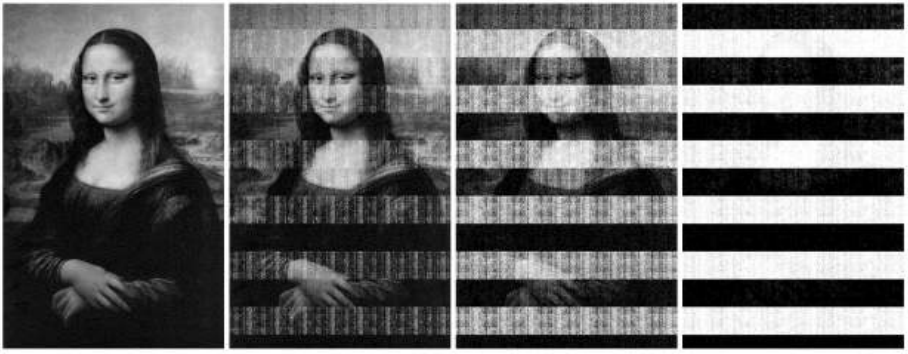
1. K. Chen: ***Reversing and exploiting an Apple firmware update.***
2. Loïc Duflot, et. al.: ***Can you still trust your network card?***
3. Arrigo Triulzi: ***Project Maux Mk.II.***

Периферийные устройства: DMA



Rafal Wojtczuk, et. al.: ***Another Way to Circumvent Intel Trusted Execution Technology. Tricking SENTER into misconfiguring VT-d via SINIT bug exploitation.***

Оперативная память: постепенное стекание заряда



Отсутствие заряда может интерпретироваться платой памяти как 0 или 1 для разных блоков адресов.

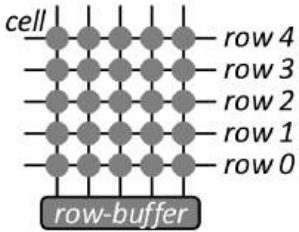
J. Alex Halderman, et. al.: ***Lest We Remember: Cold Boot Attacks on Encryption Keys.*** Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA.

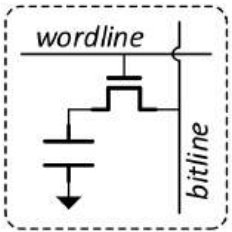
Оперативная память: AES-128

- В оперативной памяти хранятся закрытый ключ и производные от него ключи.
- Выкрасть включённый ноутбук → охладить плату → вставить в свою машину → сканировать.

J. Alex Halderman, et. al.: ***Lest We Remember: Cold Boot Attacks on Encryption Keys.*** Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA.

Оперативная память: ускорение разрядки битов

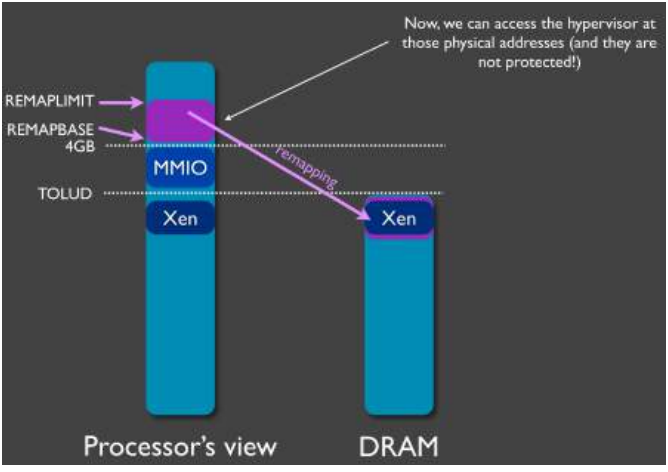




- Рост объёма памяти → рост плотности ячеек на кристале → усиление взаимных влияний.
- Частые активации одного ряда → ускорение разрядки ячеек соседних неактивных рядов.
- Близкие ряды, но далёкие физические адреса.
- DDR5 Per-Row Activation Counting (PRAC) устраняет проблему.

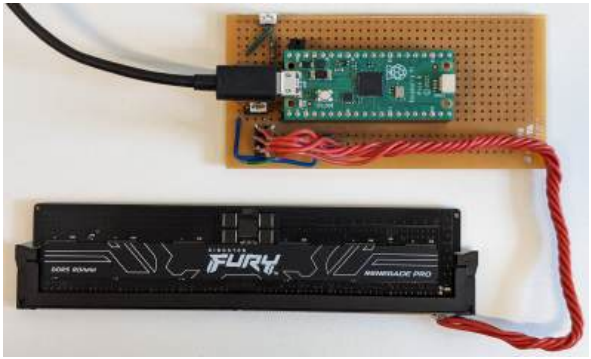
Yoongu Kim, et. al.: ***Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors.*** 2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA), Minneapolis, MN, USA, 2014, pp. 361-372.

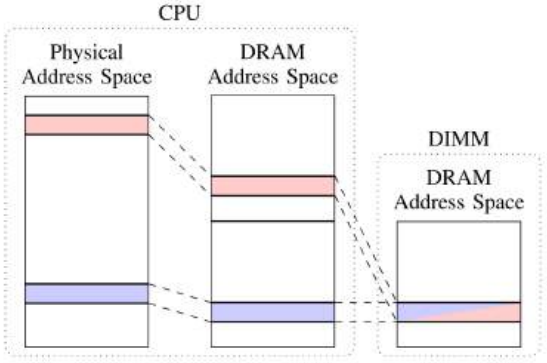
Оперативная память: изменение отображения, контроллер памяти



Joanna Rutkowska, et. al.: ***Preventing and Detecting Xen Hypervisor Subversions.***

Оперативная память: изменение отображения, модуль памяти



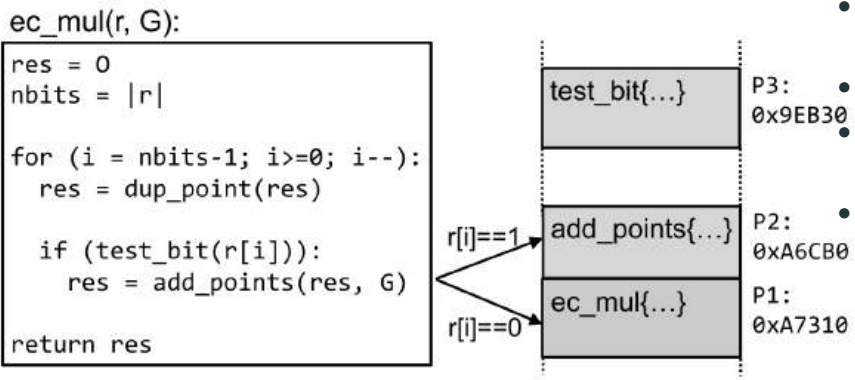


Jesse De Meulemeester, et. al.: ***BadRAM: Practical Memory Aliasing Attacks on Trusted Execution Environments.*** In 2025 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2025, pp. 4117-4135.

Аппаратное шифрование: SATA

Tilo Müller, et. al.: ***Self-encrypting disks pose self-decrypting risks. How to break Hardware-based Full Disk Encryption.*** In 29th Chaos Communinication Congress, Hamburg, Germany, December 2012.

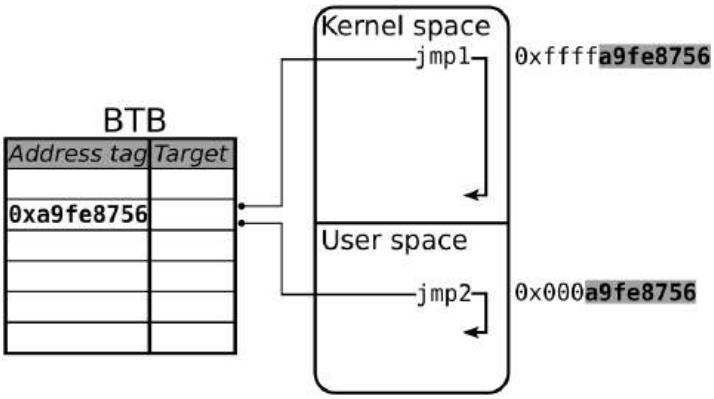
Аппаратное шифрование: SGX, Page Fault



- Оперативная память зашифрована.
- ОС скомпрометирована.
- У процесса только 3 страницы (rip, src, dst).
- Очерёдностью вызываемых страниц выдаёт секретный ключ.

Shweta Shinde, et. al.: ***Preventing Page Faults from Telling Your Secrets.*** In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 2016, pp. 317-328.

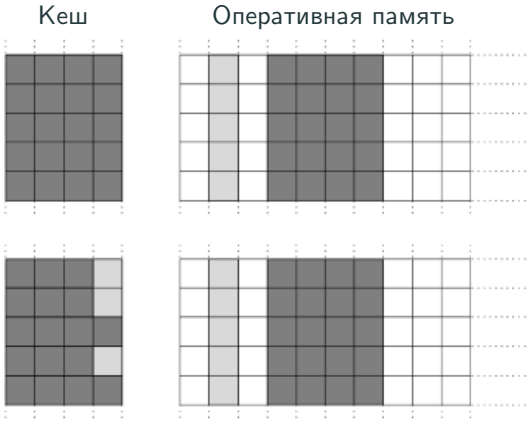
Аппаратное шифрование: SGX, Branch Target Buffer



- BTB кеширует информацию о недавних jmp.
- BTB хранит младшие биты адреса инструкции → коллизии → медленнее jmp.
- ОС скомпрометирована.
- ОС вызывает коллизии там, где jmp зависит от секретного ключа.
- Время исполнения jmp выдаёт значение секретного бита.

Sangho Lee, et. al.: ***Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing.*** In 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, August 2017, pp. 557-574.

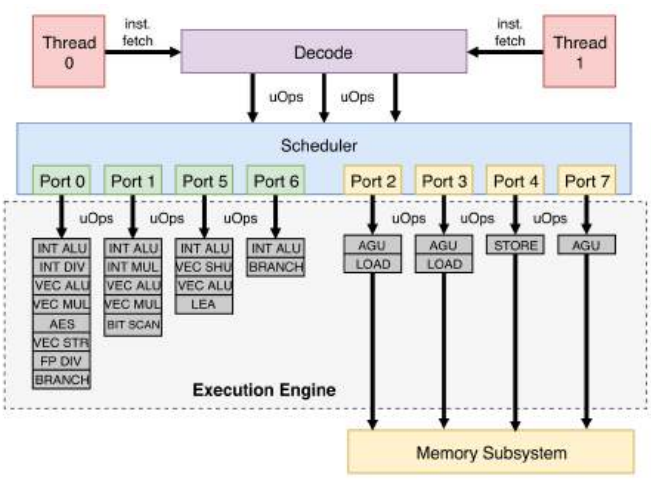
Разделяемые ресурсы как сторонние каналы: кеш, AES-128



- Один квадрат – одна строка кеша.
- Одна строка кеша – 16 элементов таблицы замен S .
- $S[X_n \oplus K_n]$, $n \in \{0, ..., 15\}$, X – открытый текст, K – секретный ключ.
- Одна строка кеша – 4 старших бита индекса $X_n \oplus K_n \rightarrow$ старшая половина байта K_n.
- Младшая половина байта K_n во 2-м раунде.

Dag Arne Osvik, et. al.: ***Cache Attacks and Countermeasures: the Case of AES.*** In Topics in Cryptology–CT-RSA 2006: The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 2005. Proceedings, pp. 1-20. Springer Berlin Heidelberg.

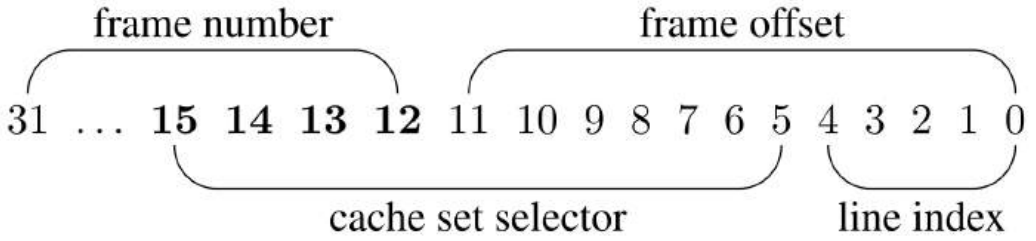
Разделяемые ресурсы как сторонние каналы: АЛУ



- У нитей исполнения одного ядра общее АЛУ.
- Время исполнения специального набора инструкций позволяет оценить текущий уровень загрузки каждой из подсистем (Port 0 – 7) $\rightarrow$ какие инструкции в данный момент времени исполняются в соседней нити.
- Характерные микрооперации выдают секретные биты.

Alejandro Cabrera Aldaya, et. al.: ***Port Contention for Fun and Profit.*** In 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2019, pp. 870-887.

Разделяемые ресурсы как сторонние каналы: раскрашивание кеша



- Устранение общих ресурсов.
- Отдельные вычислительные ядра.
- Виртуальный адрес строки кеша определяет её принадлежность к множеству.
- Разные нити $\rightarrow$ разные страницы $\rightarrow$ разные множества кеша.
- Раскрашивание кеша: цвета $\in \{15, ..., 12\}$, всего $2^4 = 16$.

Qian Ge, et. al.: ***A Survey of Microarchitectural Timing Attacks and Countermeasures on Contemporary Hardware.*** Journal of Cryptographic Engineering (2018), Volume 8, pp. 1-27.

Спекулятивное исполнение: кеш – сторонний канал

```
1  ;rcx = kernel address
2  ;rbx = probe array
3  ;Read forbidden memory
4  ;-> Page Fault
5  mov al, byte [rcx]
6  ;Speculative execution
7  ;Convert byte value into
8  ;page address
9  shl rax, 0xc
10 ;Save secret value in cache
11 mov rbx, qword [rbx + rax]
```

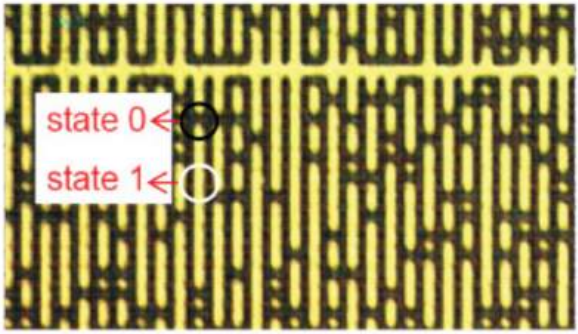
1. Аллоцировать область памяти размером в 256 страниц.
2. Сбросить из кеша начальные строки каждой страницы.
3. Прочитать один байт данных из недоступной области памяти. (стр. 5)
4. Спекулятивно преобразовать значение этого байта в адрес начала страницы. (стр. 9-11)
5. Спекулятивно прочитать несколько байт из начала этой страницы. (стр. 11)
6. Измерить время обращения к началу каждой из 256 страниц.

Номер страницы с t_{min} = значению байта недоступной памяти.

Moritz Lipp, et. al.: ***Meltdown: Reading Kernel Memory from User Space.*** In 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, August 2018, pp. 973-990.

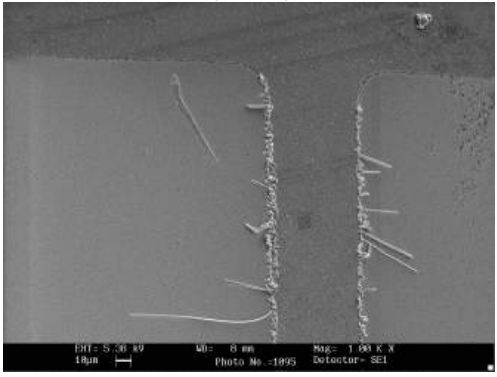
Побочные эффекты на микроуровне: ROM

Обратная инженерия



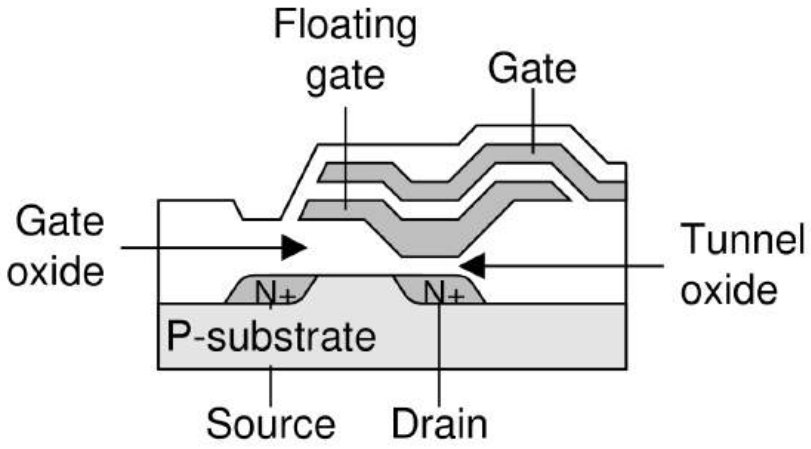
Shahed E. Quadir, et. al.: ***A survey on chip to system reverse engineering.*** ACM Journal on Emerging Technologies in Computing Systems, Vol. 13, No. 1, Article 6, April 2016.

Электромиграция



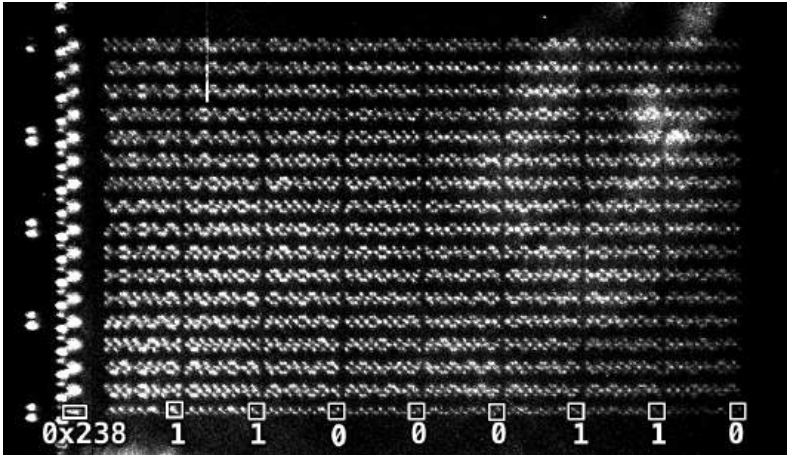
Peter Gutmann: ***Data Remanence in Semiconductor Devices.*** In Proceedings of the 10th USENIX Security Symposium, Washington, D.C., USA, August 2001, pp. 39–54.

Побочные эффекты на микроуровне: Flash



Peter Gutmann: ***Data Remanence in Semiconductor Devices.*** In Proceedings of the 10th USENIX Security Symposium, Washington, D.C., USA, August 2001, pp. 39–54.

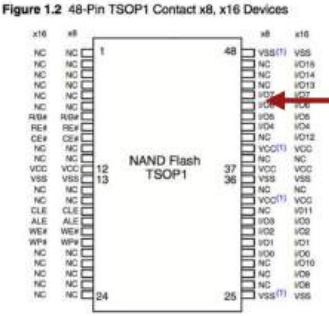
Побочные эффекты на микроуровне: ближний инфракрасный диапазон



- Содержимое оперативной памяти можно увидеть в ближнем инфракрасном диапазоне.
- AES-128 → найти таблицу замен → наблюдать за обращениями → извлечь секретный ключ.

Alexander Schlösser, et. al.: ***Simple Photonic Emission Analysis of AES. Photonic side channel analysis for the rest of us.*** In Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 2012. Proceedings 14, pp. 41-57. Springer Berlin Heidelberg.

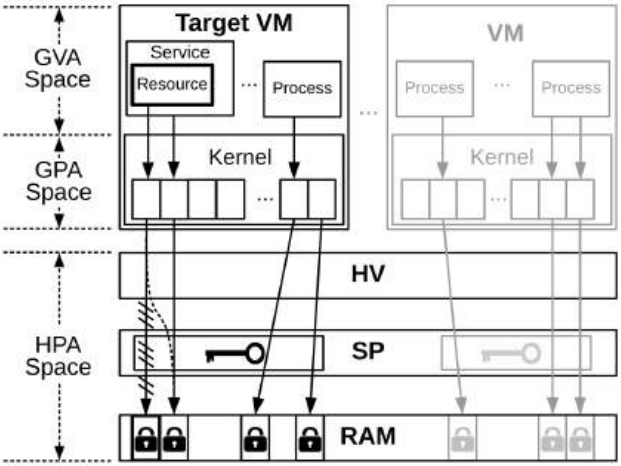
Внедрение ошибок



1. Замыкание адресного и контрольного контактов Flash памяти → переход в командную строку.
2. Заземлить LRESET# контакт TPM → повторно инициализировать TPM → обмануть удалённую аттестацию.

1. Brad Dixon: ***How to Root an Embedded Linux Box with a Sewing Needle.***
2. Bernhard Kauer: ***OSLO: Improving the security of Trusted Computing.*** In Proceedings of 16th USENIX Security Symposium (SS'07), Boston, MA, USA, August 2007, pp. 229-237.

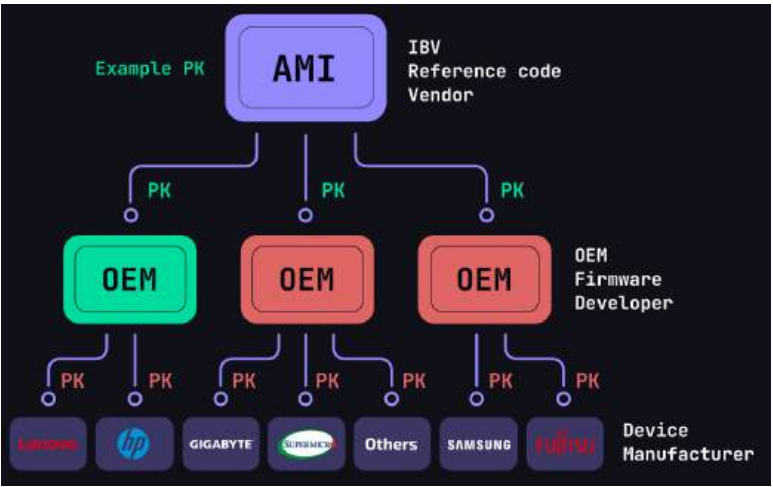
Trusted Execution Environment: конструктивная безопасность?



- Формальный подход к безопасности.
- Недоверенная аппаратура, но доверенная среда исполнения?
- Модуль для безопасности, для остального недоверенное окружение?
- Компьютерная безопасность – это конечный результат суммы дизайнерских решений на протяжении всего жизненного цикла программно-аппаратного комплекса.

Mathias Morbitzer, et. al.: ***SEVered: Subverting AMD's Virtual Machine Encryption.*** In EuroSec'18: 11th European Workshop on Systems Security, Porto, Portugal, April 2018, pp. 1-6.

Basic Input/Output System: конструктивная безопасность?



- BIOS инициализирует независимые компоненты.
- UEFI регламентирует архитектуру BIOS.
- UEFI Secure Boot фрагментирует BIOS.
- Монолитный BIOS упростит архитектуру.
- Неконтролируемые части BIOS должны исполняться с наименьшими привилегиями.

Binarly REsearch Team: ***PKfail: Untrusted Platform Keys Undermine Secure Boot on UEFI Ecosystem.***

Выводы: не повторять ошибки

Вектор атаки	Противодействие
Электромагнитное излучение	Шифрование
Акустические колебания	Контроль периметра
Анализ энергопотребления	Контроль периметра
Периферийные устройства	Правильная настройка BIOS
Оперативная память	DDR5
Разделяемые ресурсы	Исключение общих ресурсов
Спекулятивное исполнение	Изменение настроек ЦП
Микроуровень	Контроль периметра
Внедрение ошибок	Контроль периметра

Спасибо за внимание!