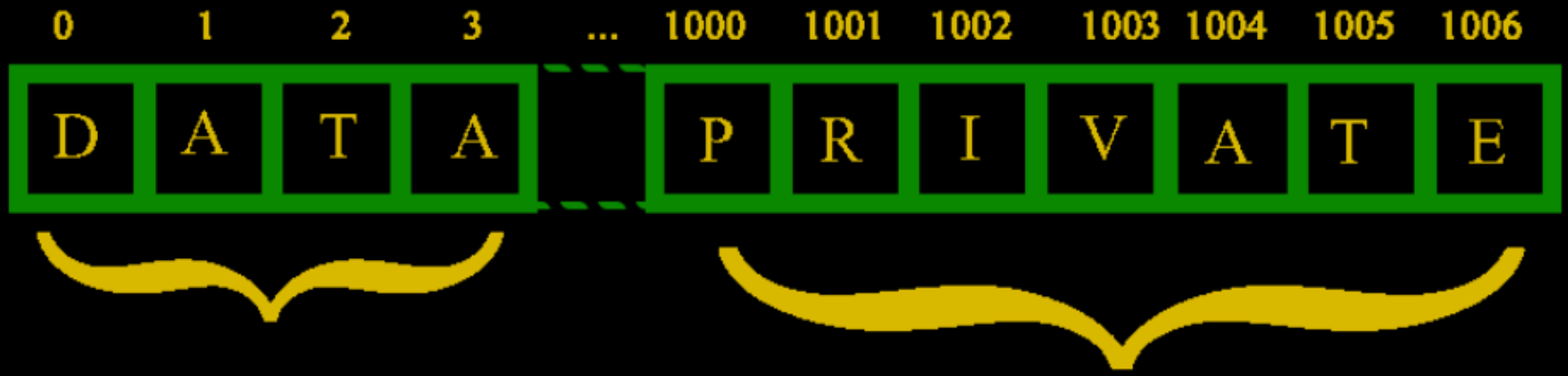
УЯЗВИМОСТИ MELTDOWN И SPECTRE

З.Д. СМИРНОВА
Кафедра защиты информации
Факультет инфокоммуникаций
БГУИР, Минск, Беларусь

Анализ особенностей функционирования процессоров, обеспечивающих эксплуатацию уязвимостей

1) Ядро ОС хранит данные в адресном пространстве процессора

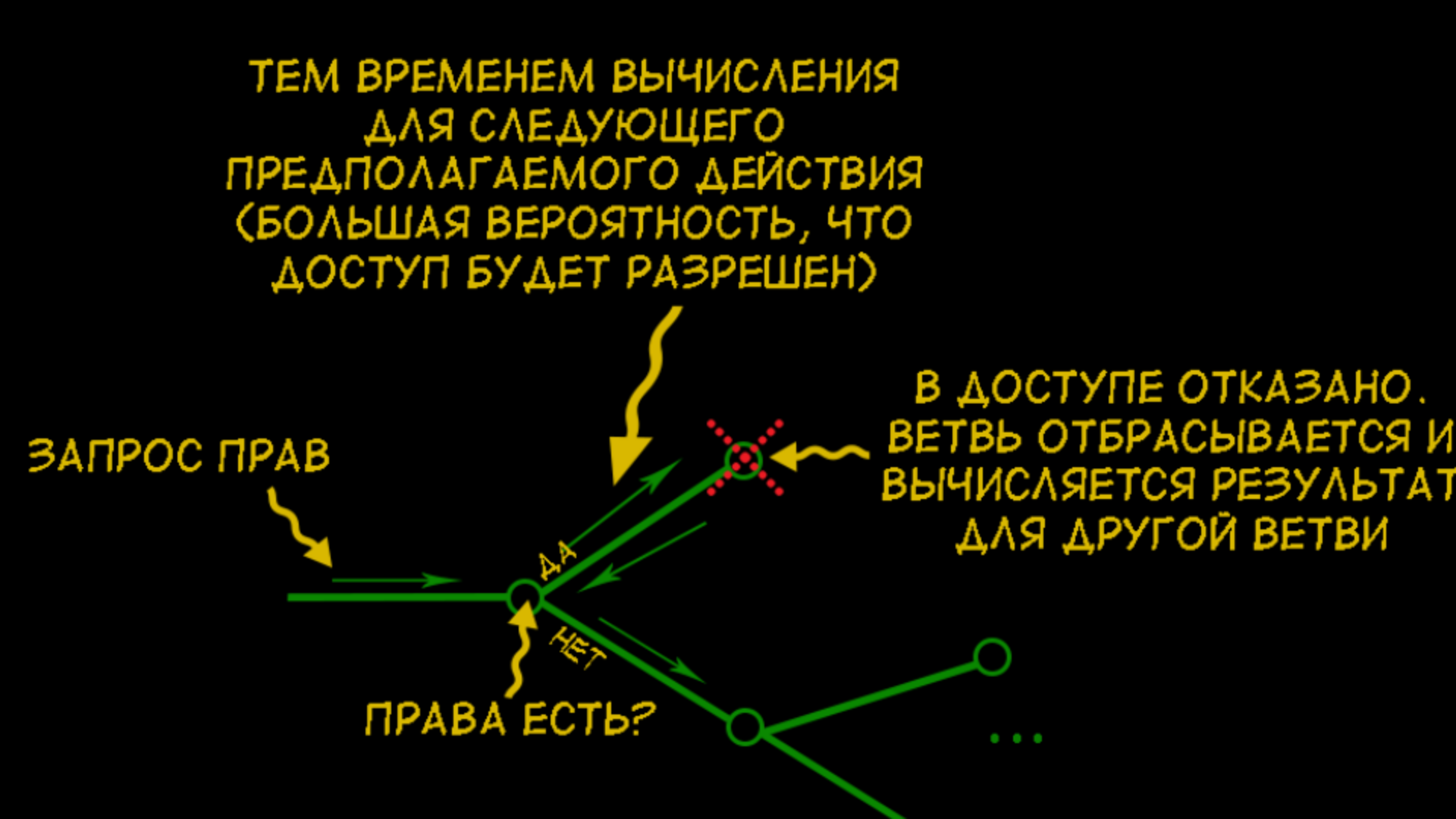
- Доступ к данным обеспечивается за счет реализации механизма привилегий


0 1 2 3 ... 1000 1001 1002 1003 1004 1005 1006
D A T A P R I V A T E
ВАШИ ДАННЫЕ. ЕСТЬ ПРАВО ДОСТУПА.
ЗАЩИЩЕННЫЕ ДАННЫЕ. НЕТ ПРАВА ДОСТУПА.

Анализ особенностей функционирования процессоров, обеспечивающих эксплуатацию уязвимостей

2) Выполнение вычислительных операций процессором происходит без проверки прав процесса получить доступ к данным

- Процессор, в ожидании ответа о праве доступа, выполняет вычисления для следующего предполагаемого действия


ТЕМ ВРЕМЕНЕМ ВЫЧИСЛЕНИЯ ДЛЯ СЛЕДУЮЩЕГО ПРЕДПОЛАГАЕМОГО ДЕЙСТВИЯ (БОЛЬШАЯ ВЕРОЯТНОСТЬ, ЧТО ДОСТУП БУДЕТ РАЗРЕШЕН)
ЗАПРОС ПРАВ
ДА
НЕТ
ПРАВА ЕСТЬ?
В ДОСТУПЕ ОТКАЗАНО. ВЕТВЬ ОТБРАСЫВАЕТСЯ И ВЫЧИСЛЯЕТСЯ РЕЗУЛЬТАТ ДЛЯ ДРУГОЙ ВЕТВИ
...

Анализ особенностей функционирования процессоров, обеспечивающих эксплуатацию уязвимостей

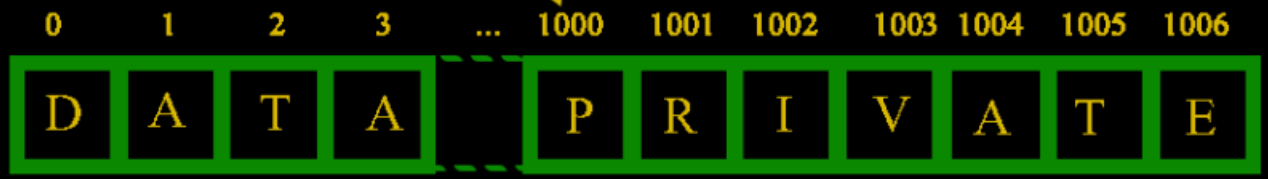
3) Отсутствие процедуры очистки кэша от результатов вычислительных операций над данными в доступе к которым процессу отказано

- Соответственно, можно проанализировать наличие данных в кэше, в зависимости от времени доступа к ним.

1) ОБРАЩЕНИЕ К ЗАЩИЩЕННОЙ ЯЧЕЙКЕ ПАМЯТИ

2) В ДОСТУПЕ ОТКАЗАНО

3) НО ДАННЫЕ ОСТАЛИСЬ В КЭШЕ



4) ПОСЛЕДОВАТЕЛЬНЫЙ ПЕРЕБОР ДАННЫХ (УСЛОВНО - БУКВЫ АЛФАВИТА)

5) БОЛЕЕ БЫСТРЫЙ (ПО СРАВНЕНИЮ С ДРУГИМИ ДАННЫМИ) ОТВЕТ ОЗНАЧАЕТ, ЧТО ДАННЫЕ БЫЛИ В КЭШЕ.

6) ЗНАЧИТ В ЯЧЕЙКЕ 1000 ПАМЯТИ НАХОДЯТСЯ ИМЕННО ЭТИ ДАННЫЕ

7) ПЕРЕХОД К ЯЧЕЙКЕ 1001 И ПОВТОРВСЕХ ДЕЙСТВИЙ.

A? 60мкс

B? 60мкс

C? 60мкс

...

P? 10мкс

Процессоры подверженные уязвимостям

- Intel, выпущенные с 1995 года (кроме Intel Itanium и Intel Atom)
- ARM64: Cortex-R7 / R8, Cortex-A8 / A9 / A15 / A17 / A57 / A72 / A73 / A75
- AMD, IBM System Z, POWER8 и POWER9

Возможные последствия

Нарушение изоляции приложений в облачных сервисах, например:

- Amazon Web Services (AWS),
- Google Cloud Platform,
- Microsoft Azure

Методы защиты

- На стороне сервера
- На стороне клиента

Уровни защиты

- На уровне архитектуры процессора
- На уровне ядра ОС
- На уровне браузера
- На пользовательском уровне

На уровне архитектуры процессора

- Необходима полная переработка архитектуры процессора с удалением или изменением функции проведения вычислений для следующих предполагаемых действий;
- Добавление функции своевременной очистке кэша в случае вычислений в ошибочной ветви событий.

На уровне ядра ОС

- Kernel page-table isolation (KPTI)

То есть разграничение страниц памяти пользовательских процессов и ядра ОС

На уровне браузера

- Ограничение точности таймера до 20 мкс и отключение SharedArrayBuffer в Firefox 57
- Использование функции Site Isolation в Chrome и Opera

На уровне пользователя

- Использование инструмента Spectre browser vulnerability check для проверки
- Отключение JavaScript

Анализ эффективности предложенных средств

- Полная переработка архитектуры процессора может потребовать значительного количества времени и средств
- Изоляция страниц вызывает замедление работы процессоров на 7-30%
- Меры, касающиеся работы с браузером, могут быть причиной незначительного замедления работы и уменьшения удобства его использования

Спасибо за внимание