УДК 004.076:004.056

УЯЗВИМОСТИ ДИНАМИЧЕСКОЙ ОПЕРАТИВНОЙ ПАМЯТИ

Маковецкий Иван Юрьевич, Галушко Светлана Алексеевна
ГВУЗ «Национальный Горный Университет», http://bit.nmu.org.ua, miha_a@ua.fm

В этой статье речь идет о возможности извлечения информации из оперативной памяти динамического типа, с целью получения несанкционированного доступа к зашифрованной информации.

Ключевые слова – оперативная память; безопасность информации; доступ.

ВВЕДЕНИЕ

Несмотря на, казалось бы, всем известные факты, ОЗУ, используемые почти во всех современных компьютерах сохраняют свое содержимое в течении нескольких секунд после отключения питания. И это приводит к тому, что при учете некоторых потерь данных, содержимое ОЗУ после отключения питания остается доступным на время, достаточное для атаки с извлечением содержимого, в том числе ключей шифрования.

Как правило, цель злоумышленника – взлом зашифрованного содержимого жесткого диска. Однако существует и ряд других уязвимостей.

ТЕОРЕТИЧСКИЕ СВЕДЕНИЯ

Регенерация памяти – это процесс периодического считывания информации из определенной области компьютерной памяти, и мгновенной перезаписи информации в ту же область без модификации. Регенерация памяти незаменима в полупроводниковой динамической памяти с произвольным доступом (Dynamic Random Access Memory, DRAM), и фактически является основной определяющей характеристикой этого типа памяти.

В противовес мнению, что DRAM память теряет данные, если периодически не выполнять регенерацию, было экспериментально установлено, что многие из доступных DRAM модулей сохраняют достаточно много информации без регенерации, даже без питания, на периоды, длящиеся более чем несколько тысяч циклов регенерации.

ЭКСПЕРИМЕНТАЛЬНЫЕ ДАННЫЕ

Используя специальное программное обеспечение для наблюдения за памятью, используемые для опыта модули памяти были заполнены псевдослучайными числовыми последовательностями.

Информацию с модулей памяти считывали через определенные промежутки времени без обновления. Уровень ошибок вычисляется количеством ошибочных бит на общее количество считанных бит. Так как при исследовании использовалась псевдослучайная последовательность, то память с максимальной потерей информации будет иметь уровень ошибок приблизительно в 50%.

Экспериментально были получены графики кривых, которые позволяют приблизительно оценить количество ущерба, нанесенного информации в модуле памяти в зависимости от времени, которое модуль памяти был отключен от питания. Также, графики для разных производителей и моделей памяти похожи по форме – сначала короткий период, когда ошибки в памяти незначительны (от 0% до 5%), за которым следует период резкого увеличения количества ошибок до 40-45%, и после плавное увеличение количества ошибок до финальной отметки около 50%.

ОПЫТЫ ПРИ НИЗКИХ ТЕМПЕРАТУРАХ

Модули памяти, как и в предыдущем опыте, были загружены псевдослучайной числовой последовательностью. Во время работы машины, модули памяти были охлаждены приблизительно до -50^{o}C. После выключения машины, температура поддерживалась на том же уровне до снятия показаний в различные моменты времени.

Как и ожидалось, можно наблюдать намного уменьшенный уровень ошибок при низких температурах, т. е. на всех образцах модулей памяти уровень ошибок настолько низок, что противник, отключив модуль памяти на 1 минуту может прочитать 99,9% бит верно.

Также был проделан экстремальный эксперимент – модуль памяти охладили до -50^{o}C во время работы машины, и после этого, его отключили от питания и погрузили в канистру с жидким азотом на 60 минут. Измерив уровень ошибок, было установлено, что в секторах размером 1 МБ – в среднем 14’000 бит содержало ошибки, что соответствует 0,17% уровню ошибок. Отсюда можно сделать вывод, что даже в современных модулях памяти, при достаточном охлаждении, информацию можно считать и восстановить через много часов и даже дней после извлечения модуля памяти.

Наблюдая за ростом уровня ошибок, можно заметить, что некоторые сектора памяти держат заряд дольше, а некоторые – меньше. Более того, распределение этих секторов строго закономерно, и отличается на разных моделях модулей памяти.

МЕРЫ ПРОТИВОДЕЙСТВИЯ

1. Удаление или перезапись криптографических ключей после их использования.
2. Периодическая очистка памяти.
3. Ограничение загрузки машин с переносных устройств и по сети.
4. Избегать предварительных расчетов в криптографических системах.
5. Использование сенсорных систем.

ВЫВОДЫ

На самом деле, все меры, описанные выше являются скорее «ампутацией», а не «лечением». Риск подобных атак является наивысшим для ноутбуков, смартфонов и лэптопов. Фактически, это означает, что память DRAM следует считать небезопасной, и следует избегать обработки каких либо данных на таких машинах. И это будет так, пока разработчики памяти не введут какие-либо серьезные архитектурные изменения, и программное обеспечение сможет хранить криптографические ключи в каком-либо действительно безопасном месте.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Википедия: свободная общедоступная мультиязычная универсальная интернет-энциклопедия (Електрон. ресурс) / Способ доступа: URL: http:// www.wikipedia.org/

2. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, Edward W. Felten
Lest We Remember: Cold Boot Attacks on Encryption Keys Princeton University, February 21, 2008