7. Le modèle à maille fine Arome - Météo-France [Электронный ресурс]. – Режим доступа: http://www.meteofrance.fr/prevoir-le-temps/la-prevision-du-temps/le-modele-a-maille-fine-arome. Дата доступа: 22.03.2019.

ИСПОЛЬЗОВАНИЕ МНОГОКРАТНЫХ ТЕСТОВ С ИЗМЕНЯЕМЫМ НАЧАЛЬНЫМ СОСТОЯНИЯМ ДЛЯ ПСЕВДОИСЧЕРПЫВАЮЩЕГО ТЕСТИРОВАНИЯ ОЗУ

Леванцевич В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ярмолик В.Н. – д.т.н., профессор

Исследуется возможность использования многократных вероятностных тестов с изменяемым начальным состоянием ячеек памяти для псевдо-исчерпывающего тестирования ОЗУ. Определено среднее число итераций многократного теста для исчерпывающего тестирования заданного количества ячеек памяти

Одним из эффективных способов определения неисправных ячеек ОЗУ является исчерпывающее тестирование[1]. Однако его применение ограничено сложностью и как следствие значительными временными затратами на реализацию подобного тестирования. Поэтому используют одну из аппроксимаций исчерпывающего тестирования в виде псевдо-исчерпывающих тестов [2].

Псевдо-исчерпывающим тестом является тест $Ts(M,k),$ который для любого заданного количества ячеек k из общего количества ячеек памяти M, при $k < M$, обеспечивает генерирование всех 2^k двоичных разрядов. То есть таким тестом мы можем организовать исчерпывающее тестирование в любых k ячейках памяти.

В качестве примера псевдо-исчерпывающего теста можно привести тест для шести ячеек памяти $Ts(6,2) = \{000000, 000011, 011100, 101101, 110110, 111011\}$. Можно заметить, что в данном тесте для любых двух ячеек памяти присутствуют возможные 2^2=4 двоичные комбинации. При этом некоторые комбинации присутствуют более, чем по одному разу. На рисунке 1 приведены примеры псевдо-исчерпывающих тестов для различного количества ячеек памяти.

T(3, 2)	*T*(4, 2)	*T*(4, 3)	*T*(5, 2)	*T*(5, 3)
0 0 0	0 0 0 0	0 0 0 0	1 1 1 1 1	1 0 0 0 0
0 1 1	0 1 1 1	0 0 1 1	1 0 0 0 0	0 1 0 0 0
1 0 1	1 0 1 1	0 1 1 0	0 1 0 0 0	0 0 1 0 0
1 1 0	1 1 0 1	0 1 0 1	0 0 1 0 0	0 0 0 1 0
	1 1 1 0	1 1 0 0	0 0 0 1 0	0 0 0 0 1
		1 1 1 1	0 0 0 0 1	0 1 1 1 1
		1 0 1 0		1 0 1 1 1
		1 0 0 1		1 1 0 1 1
				1 1 1 0 1
				1 1 1 1 0

Рисунок 1 – Примеры псевдо-исчерпывающих тестов

Одним из недостатков псевдо-исчерпывающих тестов, является сложность вычисления тестовых наборов, входящих в псевдо-исчерпывающий тест. Поэтому на практике для формирования подобных тестов используют многократные вероятностные тесты.

Классический однократный маршевый для тестирования *k* произвольных ячеек можно представить как совокупность двоичных векторов, разрядностью *k,* которая называется орбитой. [3]. Конкретный набор векторов, входящих в орбиту, зависит от трех основных факторов: правила формирования орбиты, очередности формирования адресов ячеек памяти и исходного содержимого ячеек памяти (рисунок 1).

Орбиты	O_0	O_1	O_2	O_3
Начальное состояние P_0	000…00	000…00	111…11	111…11
Последовательность адресов	Прямая (↑)	Обратная (↓)	Прямая (↑)	Обратная (↓)
P_0	000…00	000…00	111…11	111…11
P_1	000…01	100…00	111…10	011…11
P_2	000…11	110…00	111…00	001…11
…	…	…	…	…
P_{k-2}	001…11	111…00	110…00	000…11
P_{k-1}	011…11	111…10	100…00	000…01
P_k	111…11	111…11	000…00	000…00

Рисунок 2 – Четыре орбиты классического маршевого теста

Можно выделить четыре орбиты для классического маршевого теста, который имеет прямую и обратную очередность формирования адресов и два исходных содержимых ячеек памяти.

Анализ таблицы показывает, что каждая орбита, при тестировании произвольных k ячеек памяти, содержит k +1 двоичные вектора P_0, P_1, ..., P_k, разрядностью k.

Для повышения эффективности многократных тестов используется методы их формирования в которых на каждом шаге многократного теста изменяется начальное содержимое ячеек памяти, что позволяет существенно повысить покрывающую способность тестов [3].

Рассмотрим ОЗУ, которое содержит $M = 2^n$ однобитных ячеек и каждую ячейку можно адресовать с помощью уникального n-разрядного адреса. Для любых k ячеек ОЗУ, где k больше единицы и меньше 2^n существует 2^k исходных состояний P_0 для которых классический маршевый тест формирует 2^k оригинальных орбит для фиксированной очередности следования адресов ячеек памяти [3].

Как показано в [3] для определенного k и фиксированной очередности следования адресов существуют $2^k - (k^2 + k)/2 - 1$ орбит O_n с разным исходным состоянием ОЗУ, в состав которых входят вектора , не водящие в орбиту O_o, а также количество орбит, равное $(k^2 + k)/2$ в состав которых входят два вектора, из орбиты O_o.

Для определения среднего количества итераций O_s многократного теста с изменяемым исходным состоянием памяти и фиксированным порядком следования адресов ячеек памяти предположим, что они формируются случайным образом и их значения равномерно распределены с вероятностью 2^k. Тогда для определения среднего количества итераций при реализации псевдо-исчерпывающего тестирования k ячеек ОЗУ, можно применить классическую задачу «Coupon Collector's Problem», где в качестве очередного купона служит орбита с новым исходным состоянием памяти [4]:

$$O_s = 1 + \frac{2^k}{2^k - 1} + \frac{2^k}{2^k - 2} + \ldots + \frac{2^k}{2} + 2^k = 2^k \sum_{n=1}^{2^k} \frac{1}{n}. \quad (1)$$

Используя выражение 1 среднее значение количества итераций O_s для формирования всех 2^k двоичных векторов многократных тестов типа $MATS++$ равно $O_s(MATS++) = O_s / k + 1$. Для тестов $MarchC-$ это значение определяется выражением $O_s(MarchC-) = O_s / 2k$ [3].

На рисунке 3 изображены данные сравнительного анализа среднего количества итераций многократных тестов $MATS++$ и $MarchC-$ полученные экспериментально и теоретически.

Экспериментальные и теоретические значения O_s для теста $MATS++$ и $MarchC-$

k	2	3	4	5	6	7	8	9	10
2^k	4	8	16	32	64	128	256	512	1024
Теор. Os	2,77	5,44	10,82	21,64	43,37	86,93	174,20	349,00	699,03
Эксп. Os	–	4,44	9,42	19,54	40,90	83,57	170,36	341,10	680,86

k	2	3	4	5	6	7	8	9	10
2^k	4	8	16	32	64	128	256	512	1024
Теор. O_S	2,77	3,62	6,76	12,98	25,30	49,67	97,98	193,89	384,47
Эксп. O_S	–	2,33	4,42	9,34	19,55	40,55	82,62	169,32	339,48

Рисунок 3 – Сравнительный анализ средней кратности тестов (MATS ++) и *March C−*

Анализ эксперимента показывает, что значения среднего количества итераций O_S являются реализуемыми , поэтому можно сделать вывод о применимости многократных вероятностных тестов с изменяемыми исходными состояниями для псевдо исчерпывающего тестирования ОЗУ.

Список использованных источников:

1. Barzilai, Z. Exhaustive Generation of Bit Pattern with Application to VLSI Self–Testing / Z. Barzilai, D. Coppersmith, A. Rozenberg // IEEE Transactions on Computers. –1983. – Vol. C–31, № 2. – P.190–194.
2. Nicolaidis, M. Theory of transparent BIST for RAMs // IEEE Transactions on Computers. – 1996. – Vol. 45, № 10. – P. 114.
3. Ярмолик, В.Н. Псевдоисчерпывающее тестирование ОЗУ / В.Н. Ярмолик, И. Мрозек, В.А. Леванцевич// Информатика. – 2017. – №2(54). – С.58–69.
4. Д. Кнут Устойчивые паросочетания и другие комбинаторные задачи / Д.Э.Кнут / МЦМНО. 2014, с 26-28

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ЗАЩИТЫ ПРИВАТНОСТИ И ФИЛЬТРАЦИИ НЕЖЕЛАТЕЛЬНЫХ ПИСЕМ В ЭЛЕКТРОННОЙ ПОЧТЕ

Литвинко П.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лапицкая Н.В. – к.т.н.,доцент

В настоящей работе предлагается новый подход к решению проблемы фильтрации спама за счёт распознавания массовых рассылок и дополнительной проверки отправителя при обнаружении сообщений личного характера. Проверка осуществляется при помощи автоматизированного теста Тьюринга. Разработанная модель позволяет добиться высокой точности распознавания (98.81%) и эффективно осуществлять фильтрацию писем, а также защиту от утечек личной информации.

Электронная почта остаётся неотъемлемой частью социального взаимодействия и повсеместным средством коммуникации. По данным исследования Radicati Group, число активных пользователей электронной почты составляет 3,9 млрд на 2019 год [1]. По прогнозам, общее количество отправляемых и получаемых электронных писем в день к концу 2023 года вырастет до 347 миллиардов, а число пользователей - до 4,3 миллиардов.

По мере того, как число пользователей и объём пересылаемых сообщений неуклонно растёт с годами, несанкционированное использование электронной почты в маркетинговых и мошеннических целях, распространения вредоносного ПО и кражи личной информации становится одной из самых серьёзных проблем в почтовых службах. По оценкам, в 2010 году более 97% писем были классифицированы как спам [2]. При этом становится всё более распространённым феномен «перегрузки электронной почтой», впервые описанный ещё в 1996 году [3]. Именно поэтому многие исследования, изучающие или анализирующие электронные письма, сосредоточены на аспекте категоризации электронных писем, а также поиске эффективных инструментов управления почтой и снижения информационной перегрузки. Однако борьба между спамерами и инструментами защиты от спама продолжается, поскольку каждая сторона пытается создать новые способы преодоления методов, разработанных другой.

Традиционные методы определения спама включают применение байесовского классификатора [4], системы оценки на основе правил [5], проверку DNS MX-записей и обратный поиск по адресу [6], ведение чёрных списков IP и DNS (DNSBL) [7]. Однако каждый из приведённых объективных методов классификации при достижении заданного предела точности приводит к ложным положительным или неверным отрицательным срабатываниям. Идеальное решение не может быть найдено, поскольку каждая сторона использует уязвимости прежних алгоритмов для разработки новых способов доставки писем.

Принципиальная сложность разработки эффективных систем фильтрации спама заключается в том, само определение спама является субъективным и получателем электронных писем также является субъект. В то же время общей характеристикой спама является массовый характер рассылок, поскольку отправитель рассчитывает лишь на заданный процент доставки и открытия электронных писем, что является уже объективным критерием.