уровнях иерархии, повторно анализируются в среднем и высшем уровнях иерархии. В результате проведенных анализов обработки статистических данных, создаётся план повышения квалификации инженеров-специалистов на новый служебный год, с каждого гидрометаллургического завода. И принимается решение о планировании повышения квалификации, связанные с вопросами какое количество инженеров-специалистов, на какой срок нужно направить на повышение квалификации.

Для формирования элементов информационных матриц целесообразно проведение вычислительных экспериментов статистических данных в низких уровнях (в заводском уровнях) иерархии в следующей последовательности:

-заполняется информационная матрица и данные сохраняются в базе данных;

-создаётся организация времени проведения тестирования инженера-специалиста (ИТР) по каким предметам(специалистам), на какой срок и этот план оформляется соответствующим приказом управления кадров горно-металлургического комбината;

-по всем специальностям гидродметаллургического завода, группами экспертов готовятся задания тестирования(тесты);

-решаются задачи анализа с помощью информационной матрицы, созданной (сформированной) результатом тестирования специалистов-инженеров;

-эксперты классифицирует(или группирует) по результатам анализа итогов тестирования по знаниям и навыком инженеров-специалистов.

После проведения выше приведенных последовательностей по определенным планам, эксперты передают информацию в горно-металлуригический комбинат, об отправлении специалиста-инженера в курсы повышения квалификации.

Приведенный последовательности формирования элементов информационных матриц с помощью вычислительных экспериментов можно принменят в большинстве производственных отраслях в частности горнодобывающей промышленности.

Руководитель гидрометаллургического завода принимает решение о повышении квалификации инженеров-специалистов на служебный год и подготовленные статистические данные передаются в управление кадров горно-металлуригического комбината.

Разрабатываемая система управления повышения квалификации специалистов отраслей (применительно к горно-металлургическим промышленностям) является открытой системой, так как структуры системы непрерывно можно дополнять дополнительными элементами и регулировать для применения другим классам производственных и социальных объектов управления, где требуется повышения квалификации специалистов (или сотрудников).

Литература

[1] Buslenko N.S. Slozhnyx system-M "Nauka" -1981-470p.

[2] Suvonov O.O. One task of optimal management of learning processes in the education system is the International Scientific Conference - “Infocommunication and Computational Technologies in Science, Engineering and Education” of the Institute of Applied Social Sciences of the Republic of Uzbekistan. Tashkent 2004- 35-39 pp.

[3] Suvonov O.O. Mathematical modeling of management processes in the education system – Tashkent Journal "Educational Technologies" №1 -2015- 45-47 pp.

[4] Suvonov O.O., Hasanova X.M., Kuchkarova S.S. As the object of educational process management, Tashkent. Journal "Educational Technologies" №2 2017, - 68-71pp.

Журакулов Толиб Тохирович

преподаватель кафедры «Методика преподавания информатики» Навоийского государственного педагогического институт

Тел.: +998 (93) 314-41-15

Эл. почта: jurakulov89@inbox.ru

T.T. Jurakulov

Mathematical model and algorithm of calculation of processes of management of improving the qualification of experts in the mining and extractive industry

Annotation. In this article will be considered the managinand teaching processes of applied task in example of public education. Treated the mathematical models of task with implementing of system approach principles of management theory and elements of set theory. It was created the computational task algorithm and presented results of computational experiment and given practical recommendation.

Keywords: management theory, system, system approach, production, industry, learning process, professional development skill, object, subject, teacher, mathematical model, set, subset, corner, union, information matrix, algorithm and computational experiment.

УДК 004.056.53

Рахманов А.Т., Керимов К.Ф., Камалов Ш.К.

Алгоритм автоматического обнаружения уязвимости вида SQL инъекции

Аннотация. В данной статье разрабатывается алгоритм обнаружения атаки по инъекции SQL с помощью функции извлечения одного символа, и оценку эффективности предложенного алгоритма с помощью искусственных данных.

Ключевые слова: SQL инъекция, уязвимость, обнаружение атак, определение угроз, использование специальных символов и строк, алгоритм.

Математическое моделирование и идентификация информационных объектов играет важную роль при решении задач распознования образов. Одним из таких задач является обнаружение атак или нормальных запросов на веб приложения. Исследования, посвящённые изучению обнаружения атак или нормальных запросов на веб приложения начались сравнительно недавно. Но тем не менее существует много исследований в этом направлении[1-11]. Применение математических методов в решении таких задач в основном велись японскими учеными [1,2,6]. Например в работе [1] предложено 2 способа обнаружения атак SQL инъекций основанных на свойстве распределения символов при построении атак SQL инъекций. В работе [2] предложена моделирование

атак и нормальных запросов и их идентификация с помощью некоторой функции, нижняя граница которой зависит от длины входной строки и вообще говоря неограниченна снизу. В нашей работе предлагается математический способ идентификации атак SQL инъекций с помощью ограниченной снизу функции, которая зависит от входной строки. Для построения такой функции мы использовали специальные знаки и ключевые слова, которые часто встречаются в построении атак злоумышленников.

Часто в построении атак SQL инъекций используются специальные символы и специальные ключевые слова, которые приведены в следующих таблицах.

Таблица 1 (специальных символов).

Переменная	Символ
u_1	Пробел
u_2	Точка-запятая(;)
u_3	Апостроф(’)
u_4	Правая скобка())
u_5	Левая скобка(()
u_6	Правая фигурная скобка (})
u_7	Левая фигурная скобка ({)
u_8	Правая квадратная скобка (])
u_9	Левая квадратная скобка([)
u_{10}	Диез(#)
u_{11}	Процент (%)
u_{12}	Кавычка (”)
u_{13}	Амперсанд (&)
u_{14}	Обратная косая (\)
u_{15}	Вертикальная линия (|)
u_{16}	Знак равенства (=)
u_{17}	Больше чем (>)
u_{18}	Меньше чем (<)
u_{19}	Звездочка (*)
u_{20}	Косая черта (/)

Для определения SQL инъекции вводим характеристики атак SQL инъекций с помощью специальных символов из таблицы 1 и специальных ключевых слов из таблицы 2.

Таблица 2 (специальных ключевых слов).

Переменная	Ключевые слова
u_{21}	and
u_{22}	or
u_{23}	union
u_{24}	where
u_{25}	limit
u_{26}	group by
u_{27}	select
u_{28}	\'
u_{29}	hex
u_{30}	substr

Пусть наблюдается некоторая входная строка L и пусть $x_1, x_2, ..., x_{20}$ частота появления в L специальных знаков из таблицы 1 и пусть $x_{21}, x_{22}, ..., x_{30}$ являются частотой появления специальных ключевых слов из таблицы 2 , x_{31} частота появления всех остальных знаков и чисел 0,1,2,...,9 в строке L. С точки зрения определения атак SQL инъекций обычные символы $a, b, ..., z$ и числа 0, 1, … , 9 не играют важную роль. По этому в данной работе мы всегда считаем что частота появления всех этих символов и чисел в наблюдаемой строке L равно 1, т.е. $x_{31} = 1$. Таким образом, любую строку L можно определить с помощью характеристик следующим образом: $L = (x_1, x_2, ..., x_{20}, x_{21}, ..., x_{30}, x_{31})$, как элемент некоторого фазового пространства X.

Метод определения

Из определения L видно, что любой элемент L из построенного пространства X лежит на гиперплоскости $\Gamma = \{L = (x_1, x_2, ..., x_{20}, ..., x_{30}, x_{31}) : x_{31} = 1\}$. Используя данное уравнения гиперплоскости, можно предположит, что чем больше частота появления специальных знаков и ключевых слов во входной строке, тем очевиднее становится близость входной строки L к атакам SQL инъекций. Поэтому, функция определения атаки должна быть возрастающей по переменным $x_1, x_2, ..., x_{20}, x_{21}, ..., x_{30}$, и убывающей по переменной x_{31}. Исходя из этого предлагаем следующую возрастающую по $x_1, x_2, ..., x_{20}, x_{21}, ..., x_{30}$ функцию:

$$f(L) = f(x_1, x_2, ..., x_{20}, x_{21}, ..., x_{31}) = \frac{\sum_{i=1}^{30} x_i}{\sum_{i=1}^{30} x_i + x_{31}}$$

для определения атак SQL инъекций. Так как в данной работе мы всегда считаем, что частота появления всех остальных знаков и чисел 0,1, 2,..., 9 в строке L равно 1, то из последнего равенства получим:

$$f(L) = f(x_1, x_2, ..., x_{20}, x_{21}, ..., x_{31}) = \frac{\sum_{i=1}^{30} x_i}{\sum_{i=1}^{30} x_i + 1} \quad (1)$$

Данная функция имеет следующие свойства: 1) $0 \le f(L) < 1$ для всех $L \in \Gamma$.

2) для атак SQL инъекций минимальное значение функции снизу ограничена числом 1/2.

Таким образом, если входная строка L является атакой SQL инъекции то это строка по крайней мере должна содержать один специальный символ из таблицы №1 или одно ключевое слово из таблицы №2. Поэтому $\sum_{i=1}^{30} x_i \ge 1$ и так как функция $f(L)$ является возрастающей по каждому из переменных x_i её минимум при $\sum_{i=1}^{30} x_i \ge 1$ достигается в точке L_0 для которого

$$\sum_{i=1}^{30} x_i = 1.$$

Таким образом, если L произвольная строка и $f(L) \geq 1/2$, то L возможно является атакой SQL инъекции, или же $f(L) < 1/2$ то тогда входная строка возможно является нормальной, если при построении атак SQL инъекций используются специальные ключевые слова из таблицы 2. Поэтому функцию (1) можно использовать для распознавания нормальных строк и атак SQL инъекций, построенных с помощью специальных символов и ключевых слов .

Таким образом, если L произвольная строка, содержащая минимум 2 специальных символов из таблицы 1, то $f(L) \geq 2/3$, и L возможно является атакой SQL инъекции, или же $f(L) < 2/3$ то тогда входная строка возможно является нормальной, если при построении атак SQL инъекций используются только специальные символы из таблицы 1. Поэтому функцию (1) можно использовать для распознавания нормальных строк и атак SQL инъекций, построенных с помощью специальных символов из таблицы 1 и специальных ключевых слов из таблицы 2.

Образцы строк по инъекции SQL

Таблица 3

Номер	Строки атаки
1	id=1'
2	AlexanderPHP'
3	AlexanderPHP'%20--%20habrahabr
4	1 UNION SELECT 1,2
5	1 UNION SELECT 1,2,3
6	1 UNION SELECT 1,2,3,4,5
7	1 GROUP BY 2
8	1 GROUP BY 8
9	-1 UNION SELECT 1,2,3,4,5
10	-1 UNION SELECT 1,2,3,4,5 FROM users WHERE id=1
11	-1 UNION SELECT name,2,pass,4,5 FROM users WHERE id=1
12	-1' UNION SELECT name,2,pass,4,5 FROM users WHERE id=1 --%20
13	-1' UNION SELECT 1,'<?php eval($_GET[1]) ?>',3,4,5 INTO OUTFILE '1.php' --%20
14	-1' UNION SELECT 1,2,3,4,5 INTO OUTFILE '1.php' --%20
15	-1' UNION SELECT 1,LOAD_FILE('1.php'),3,4,5 --%20
16	4+OR+1
17	4+--
18	4+UNION+SELECT+*+FROM+news+WHERE +id=4
19	admin' --
20	admin' #
21	admin'/*
22	' or 1=1--
23	' or 1=1#
24	' or 1=1/*
25	') or '1'='1--
26	') or ('1'='1—
27	' HAVING 1=1 --
28	' GROUP BY table.columnfromerror1 HAVING 1=1 --
29	' GROUP BY table.columnfromerror1, columnfromerror2 HAVING 1=1 --
30	' GROUP BY table.columnfromerror1 columnfromerror2, columnfromerror3 HAVING
31	10 UNION SELECT TOP 1 password FROM admin_login where login_name='neo'--
32	10 UNION SELECT TOP 1 password FROM admin_login where login_name='trinity'--
33	10 UNION SELECT TOP 1 convert(int, password%2b'%20morpheus') FROM admin_login where login_name='trinity'--
34	10; UPDATE 'admin_login' SET 'password' = 'newpas5' WHERE login_name='neo--
35	10; INSERT INTO 'admin_login' ('login_id', 'login_name', 'password', 'details') VALUES (635,'neo2','newpas5','NA')--
36	hi' or 1=1—
37	food' or 1=1—
38	10 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES--
39	10 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME NOT IN ('table1')--

В обеих случаях используя функцию (1) мы имеем критерий качества для определения угроз. Похожая к (1) функция была построена и использована в работе [*], но там значение функции зависит от длины входной строки L и минимум такой функции для любой строки L не существует. Поэтому в работах [*] для определения границы разпознающей функции строятся дополнительные усредненные критерии качества, решая соответствующую оптимизационную задачу, используя дополнительные математические аппараты.

В нашем случае границей разпознающей функции (1) является рациональное число 1/2. Таким образом, если

строка L содержить хотя бы один специальный знак или же одно ключевое слово, то условие $f(L) \geq 1/2$ достаточно для определения угрозы.

Образцы нормальных строк

Номер	Нормальные строки
1	test
2	password
3	kamil@
4	@kamil
5	{(1%2)+(3/4)}/5}
6	&temptest(URL){ width,height }

Определение степени важности специальных символов по данному алгоритму: результаты эксперимента

	степени важности для y
=	0.4872
%	0.2051
‘	0.6923
*	0.0769
/	0.0513
]	0.0256
[	0.0257
{	0
}	0
&	0
\	0
#	0.0513
“	0
!	0
<	0.0256
>	0.0255
(	0.1538
)	0.1795
;	0
пробел	0.7949

Заключение

В данной работе мы предложили алгоритм обнаружения атаки по инъекции SQL с помощью определенной функции, и оценку эффективности предложенного алгоритма с помощью искусственных данных.

В предлагаемом алгоритме, мы определили примерный набор символов, который сочетается как с атакой, так и с нормальными обнаружениями, и с ранее известным порогом, используя примерные данные атакующих и нормальных строк. Согласно нашим экспериментам с искусственными данными, набор содержит пробел, точку с запятой, и правая скобка хорошо зарекомендовал себя для большего диапазона веса для атаки и нормальной строки. Важным моментом, однако, является гибкий выбор лучшего набора в зависимости от наблюдаемых данных.

Проблемой в предлагаемом алгоритме является сбор естественных атак из серверов веб-приложений в эксплуатации и нормальных строк и их генерация.

Литература

[1] Michio Sonoda, Takeshi Matsuda, On Automatic Detection of SQL Injection Attacks by the Feature Extraction of the Single Character, Proceeding of 2011 IEEE International Conference on Systems.

[2] Takeshi Matsuda, Daiki Koizumi, Michio Sonoda, and Shigeichi Hirasawa, “On Predictive Errors of SQL Injection Attack Detection by the Feature of the Single Character,” Proceeding of 2011 IEEE International Conference on Systems, Man, and Cybernetics (to appear).

[3] G. T. Buehrer, B. W. Weide, P. A. G. Sivilotti, *Using Parse Tree Validation to Prevent SQL Injection Attacks*, SEM 2005

[4] W. G. Halfond, A. Orso, *Combining Static Analysis & Runtime Monitoring to Counter SQL-Injection Attacks*, WODA 2005

[5] W. G. Halfond, A. Orso, *AMNESIA: Analysis and Monitoring for NEutralizing SQL Injection Attacks*, ASE 2005

[6] Tsunoda Naoki, Yasui Hiroyuki, and Matsuyama Minoru, Detection for SQL Injection with Anomaly Detection Method, The 71th National Convention of ISPJ collection of papers (3), pp.379–380, 2009.

[7] William Robertson, Giovanni Vigna, Christopher Kruegel, and Richard A. Kemmerer, “Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks,” in Proceeding of the Network and Distributed System Security (NDSS) Symposium, San Diego, CA, February, 2006.

[8] Justin Clarke, SQL Injection Attacks And Defense, Syngress Publishing Inc., 2009.

[9] Ke Wei, M. Muthuprasanna, S. Kothari, *Eliminating SQL Injection Attacks in Stored Procedures*, pp. 191-198, IEEE ASWEC, 2006

[10] W. R. Cook, S. Rai, *Safe Query Objects: Statically Typed Objects as Remotely Executable Queries*, ICSE 2005

[11] R. McClure, I. Kruger, *SQL DOM: Compile Time Checking of Dynamic SQL Statements*, ICSE 2005

Рахманов Аскар Таджибаевич
т.ф.н., Муҳаммад ал-Хоразмий номидаги ТАТУ ТАД кафедраси доценти.
Тел.: +998 (97) 763-59-63
Эл. почта: domack@gmail.com
Керимов Камиль Фикратович
т.ф.н., Муҳаммад ал-Хоразмий номидаги ТАТУ ТАД кафедраси доценти
Тел.: +998 (90) 909-70-01
Эл. почта: domack@gmail.com
Камалов Шухрат Камалович
Муҳаммад ал-Хоразмий номидаги ТАТУ ТАД кафедраси в.в.б. доценти
Тел.: +998 (97) 776-33-50
Эл. почта: kamalov.shukhrat@gmail.com

Rahmanov A.T., Kerimov K. F., Kamalov Sh.K.
Algorithm for automatic detection of vulnerability of the form of SQL injection

The article presents an algorithm for detecting attacks on SQL injection using the function of extracting one character, and evaluating the effectiveness of the proposed algorithm using artificial data.

Keywords: SQL injection, vulnerability, attack detection, threat detection, use of special characters and strings, algorithm.

Rahmanov A.T., Kerimov K. F., Kamalov Sh.K.
SQL in'ektsiyasi shaklining zaifligini avtomatik aniqlash algoritmi

Maqolada bir belgini chiqarish funktsiyasidan foydalangan holda SQL in'ektsiyalariga qarshi hujumlarni aniqlash bo'yicha algoritm ishlab chiqadi va sun'iy ma'lumotlardan taklif qilingan algoritmning samaradorligini baholaydi.

Kalit so'zlar: SQL in'ektsiyasi, zaiflik, hujumni aniqlash, tahdidlarni aniqlash, maxsus belgilar va satrlarni ishlatish, algoritm.

УДК 621.395.019.3

Якубова М.З., Якубов Б.М., Куликов А.А., Оразалиева С.К., Садикова Г.

Имитационное моделирование концепции производительности технологии протоколов маршрутизации EIGRP и OSPF с использованием пакета прикладных программ Opnet modeler v.14.5

Аннотация. В статье проанализированы и проведены исследования некоторых характеристик технологии использования протоколов маршрутизации OSPF и IEGRP при имитационном моделировании на основе использования пакета прикладных программ Opnet modeler v.14.5 в телекоммуникационных сетях.

Ключевые слова. ZigBee, 6LoWPAN, PANA, сенсорные сети, координатор, маршрутизатор, инновационная интегрированная сеть.

Известно, что пользовательские данные при передаче разбивают на пакеты определенной продолжительности по длине. Каждый пакет обеспечивается кодами начала и конца в пакете, местопребыванием отправляющего и получающего, номером пакета в оповещении, уведомлением для проверки верности представляемых сообщений в промежутках узлов связи и в месте предназначения.

Являясь, самостоятельными частицами информации, пакеты, относящиеся к единой и той же информации, передаются сразу по разнообразным направлениям или маршрутам в числе блока, как информации, передаваемой протоколом через сеть связи без предварительного установления соединения и создания виртуального канала.

При помощи компьютеров, выполняющих роль центров коммутации пакетов в узлах связи происходит управление передачей и обработкой пакетов. Продолжительное хранение пакетов не предусматривается, по этой причине пакеты препровождаются, в место предназначения с наименьшим запозданием, где из них образуется завершающая информация [1].

Концепция коммутации пакетов выражается мультиплексированием, при проведении деления времени применения того же канала большим количеством клиентами, что увеличивает производительность деятельности телекоммуникационных систем.

На современном этапе пакетная коммутация считается базой для трансляции предоставленной информации.

Рассмотрим, цели и методы маршрутизации. Маршруты или же маршрутизация**,** задачи в выборе маршрута для передачи информации от отправителя к получателю являющейся маршрутизацией. Она обладает значимостью в сетях, где не только необходимо, но и возможен выбор наилучшего или приемлемого направления. В нынешних сетях с перемешанной технологией (звездной, кольцевой, шинной, когда много сегментов) действительно заслуживает принятие решения задачи выбора направлений для трансляции кадров, для чего используют надлежащее оборудование, к примеру маршрутизаторы.

Маршрутизации - правила предопределения выходной линии связи предоставленного узла связи телекоммуникационной системы для трансляции пакета, основывающегося на оповещении, включающего в заглавия пакета (адресата отправляющего и получающего), и сообщений о нагрузке данного узла и, вероятно телекоммуникационных систем, в целом.

Различают следующие способы маршрутизации: централизованная маршрутизация, распределенная маршрутизация и смешанная маршрутизация

Обычно маршрутизатор использует разные сетевые протоколы и протоколы маршрутизации.

Последние устанавливают технологию сети и содержат сообщения о ней в маршрутной таблице. Когда маршрутизатор не использует протокол маршрутизации, он сохраняет так называемые статические маршруты или применяет раздельный протокол на любом порту. Как правило маршрутизаторы используют один протокол маршрутизации.

Сообщения о маршрутизации сохраняют метрические данные, это мера периода или дистанции, и некоторые отметки о периоде времени. Данные о передаче содержат в себе информацию о выходном порте и местоназначения, которое является следующей системой по линии.

Известно, что маршрутизаторы сохраняют информацию о различных всевозможных последующих маршрутизаторах в едином перечне таблицы.

Обычно протоколы маршрутизации используют 2 самые важные технологии

Первое**,** при их работе устанавливаются наилучшие то есть оптимальные пути трансляции пакета по сети.

Как правило, выбирается линия, снабжающая наименьшее время доставки при наибольшей надежности.

Протокол маршрутизации выполняет стабильный сбор данных о состоянии маршрутов и обновление таблиц маршрутизации при изменении структуре топологии сети, в результате несогласий или перегрузок. Поэтому, таблицы маршрутизации постоянно имеют достоверные данные о структуре сети.

Во-вторых, деятельность протоколов маршрутизации выражается в трансляции пакетов по сети. Принимая следующий пакет, маршрутизатор узнает место предназначения из заглавия пакета и предопределяет, в которой направленности то-есть сквозь какой узел необходимо передавать следующий пакет. Для осуществления такой проблемы применяется данные из таблицы маршрутизации.

Протоколы, применяемые при организации таблицы маршрутизации, разделяются на 3 категории:

- протоколы размаха вектора дистанции;
- протоколы ситуации в канале;
- протоколы ориентации трассировки