

Методы автоматизированного порождения поисковых эвристик по предметной области «информационная безопасность»

Тян Алексей

20 июня 2013 г.

Цель

На базе метапиосковой системы «виртуальный каталог»
реализовать поиск Интернет ресурсов определённого типа
для любой выбранной рубрики.

Задачи

- ① Изучение основных принципов работы виртуального каталога.
- ② Исследование методов автоматического порождения эвристик для виртуального каталога.
- ③ Реализация возможности порождения эвристик для пар рубрика-тип ресурса.
- ④ Порождение эвристик.
- ⑤ Создание рубрикатора для предметной области «информационная безопасность».

Определения

Релевантность - это соответствие полученной в результате поиска информации информационному запросу.

Пертинентность - это соответствие полученной в результате поиска информации информационной потребности.

Точность - это отношение числа найденных релевантных ресурсов к общему количеству найденных ресурсов.

Полнота - это отношение числа найденных релевантных ресурсов к общему количеству релевантных ресурсов в сети.

- ❶ Потребность пользователя в информации.
- ❷ Формализованный запрос. Представленный в виде с которым работает поисковая система, и отображающий потребность пользователя в информации.
- ❸ Ответ на запрос.

Плюсы

- 1 Высокая релевантность.
- 2 Полнота.
- 3 Количество ресурсов, по которым ведётся поиск.
- 4 Точность.

Минусы

Необходимо выразить информационную потребность в виде 2-3 ключевых слов.

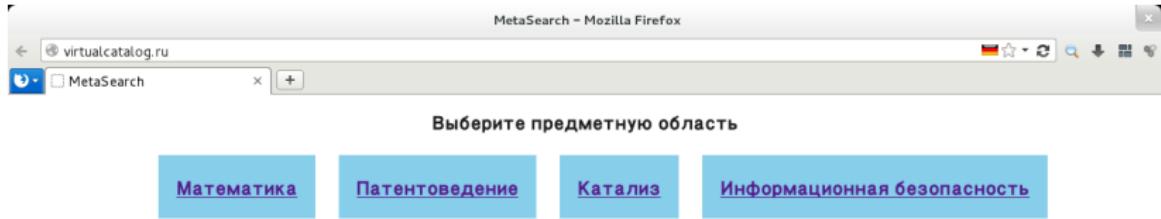
Плюсы

Интерфейс позволяет точно выразить информационную потребность.

Минусы

- ① Низкая полнота.
- ② В сравнении с поисковыми системами, мало ресурсов по которым ведётся поиск.
- ③ Отсутствие свежей информации.

Виртуальный каталог



Виртуальный каталог - синтез Интернет-каталога и поисковой системы.

Интерфейс - аналогичен интерфейсу Интернет-каталога.

Виртуальный каталог в отличие от Интернет-каталога, не хранит ссылки на ресурсы, а составляется запрос к поисковой системе.

- ❶ Управление доступом.
- ❷ Законодательство.
- ❸ Криптография.
- ❹ ПО.
- ❺ Стандарты.
- ❻ Уязвимости.
- ❼ Атаки.
- ❽ Прочее.

Виртуальный каталог: Атаки

- Вредоносные программы.
 - Эксплоиты.
 - Вирусы.
 - Стелс-вирус.
 - Полиморфные вирусы.
 - Троянская программа.
 - Руткиты.
- Инъекции.
 - SQL-инъекция.
 - PHP-инъекция.
 - XSS.
- Отказ в обслуживании.
 - Переполнение буфера.
 - DoS-атака.
 - DDoS-атака.
 - Флуд.
- MITM-атака.
- IP-спуфинг.

Виртуальный каталог: информационная безопасность

The screenshot shows the metasearch.ru search interface. The search term 'атака' is entered in the search bar. The search results are displayed in a grid format.

Рубрика	Описание
Управление доступом	Переполнение буфера
Законодательство	
Криптография	
Программное обеспечение	
Стандарты	
уязвимости	
Нарушения безопасности доступа к памяти	<ul style="list-style-type: none">• Переполнение буфера• Висящие указатели
Ошибки проверки вводимых данных	
Составные гонки	
Ошибка пути/направлений	
Эскалация привилегий	
Прочее	<ul style="list-style-type: none">• Безопасность• Деятельность• Компании• Персоналии

Переполнение буфера — Википедия
ru.wikipedia.org/wiki/Переполнение_буфера - Сохраненная копия · Похожие
Переполнение буфера обычно возникает из-за неправильной работы с в

Статьи:ANDR : Атаки на переполнение буфера - ошибки и ...
securityvulns.ru/articles/fb.asp - Сохраненная копия · Похожие
Атаки на переполнение буфера. Переполнение буфера (buffer overflows) -

Переполнение буфера - CodeNet
www.codenet.ru/program/asm/overflow.php - Сохраненная копия · Похожие
Несмотря на то, что принципы использования **переполнения буфера** ... Итак,

Технология атаки на переполнение буфера

1 Обучение.

Выбрать пертинентные и не пертинентные тексты.

2 Генерация эвристик.

- Получить множество M_1 (лексем из пертинентных текстов).
- Получить множество M_2 (лексем из не пертинентных текстов).
- Составить всевозможные конъюнкции из элементов M_1 .
- Удаление конъюнкций состоящих из элементов M_2 .

3 Проверка результатов.

Сравнение

	google	yandex	виртуальный каталог
инъекции	50%	60%	80%
вирус	20%	40%	60%
автентификация	70%	60%	90%
законодательство	0	0	40%
троянский конь	30%	40%	50%

В таблице сравниваются результаты поиска статей.

Тут пертинентность считается как отношение найденных ресурсов соответствующей тематики ко всем найденным ресурсам.

Результаты

- ① Создана рубрика в виртуальном каталоге по предметной области «информационная безопасность».
- ② Реализован выбор типа ресурса при поиске в виртуальном каталоге.
- ③ Автоматизировано порождение эвристик для пар рубрика-тип ресурса.

- Тян А.Ю. Виртуальный каталог по предметной области информационная безопасность // Материалы 51 Международной Научной Студенческой Конференции «Студент и научно-технический прогресс»: Информационные технологии / Новосиб. гос. ун-т, Новосибирск, 2013, С. 125.
- Тян А.Ю. Виртуальный каталог по предметной области «информационная безопасность» // Современные инновации в науке и технике. Материалы III Международной научно-практической конференции / Юго-Западный гос. ун-т, Курск, 2013, С. 185-192.

Спасибо за внимание.