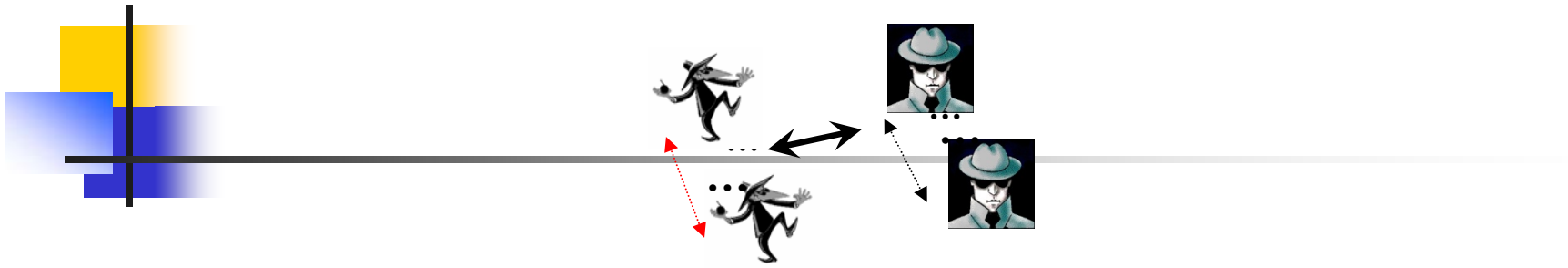


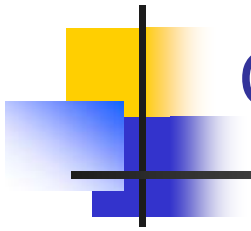
МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ WEB-САЙТОВ НА ОСНОВЕ ОЦЕНОК РЕПУТАЦИИ

Чечулин А.А., Зозуля Ю. В., Котенко И.В., Тишков А.В., Шоров А.В.

ООО "Центр специальной системотехники"
НИГ компьютерной безопасности, Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)

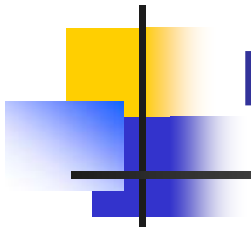
SPIIRAS

РусКрипто'2009, 2-5 апреля 2009 г.



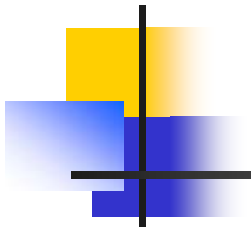
Структура доклада

- Введение
- Методы вычисления репутации
- Источники данных для построения репутации
- Архитектура системы защиты, основанная на репутациях
- Атаки на систему защиты, основанную на репутациях
- Заключение



Введение

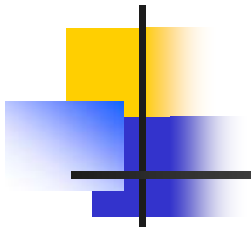
- Необходимость в системе защиты, основанной на репутациях, вызвана рядом причин:
  - резкое сокращение периода активности вредоносного ПО (с полугода до 1-2 недель)
  - резкий рост количества зарегистрированных экземпляров вредоносного ПО
  - ориентация вредоносного ПО на скрытное функционирование
  - использование для распространения типовых способов передачи контента



Существующие решения, использующие Web-репутации

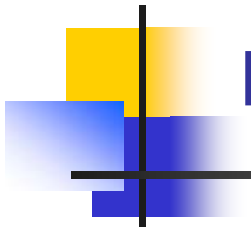
- **Репутация** – это некий набор величин (оценок), характеризующих в числовом виде степени принадлежности объекта к набору контролируемых категорий

  - IronPort - Web Reputation Filters
  - SecureComputing - TrustedSource Reputation
  - Trend Micro - Smart Protection Network



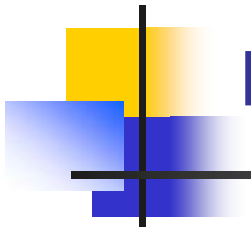
Методы, основанные на подсчете средних значений

- Примеры: eBay, Amazon, Epinions
- Пример оценки (eBay): {-1,0,+1}
- Достоинства:
  - Простота
  - Высокая скорость вычисления
- Недостатки:
  - Равнозначность всех голосов
  - Инертность изменения оценки



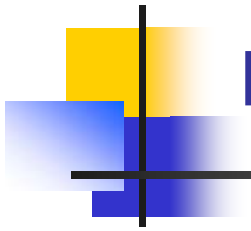
Потоковые модели

- PageRank [1998] и основанные на нем
  - анализируется граф связей между веб-объектами (от страниц до веб блогов и электронной почты)
  - используется рекуррентная формула и соответствующий итеративный алгоритм подсчета рейтингов для узлов сети
  - есть возможность «персонализации» алгоритма: пользователь определяет предпочтительные узлы и рейтинг строится с учетом этих предпочтений
  - известно много разновидностей и приложений для блогов, электронной почты (защиты от спама), пиринговых сетей



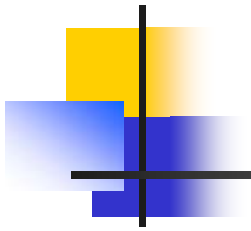
PageRank, развитие идеи (1/2)

- TrustRank [2004]
  - использует мнение экспертов
  - позволяет вычислять рейтинг любых web-страниц в графе связей на основе оценок некоторых из них
- BlogRank [2006]
  - сложная структура узла графа и связей между узлами. Включает совокупность самих постов, пользователей-авторов, комментариев
  - зависимость между узлами обусловлена не только количеством ссылок на посты, но и числом пользователей, общих тем и др.



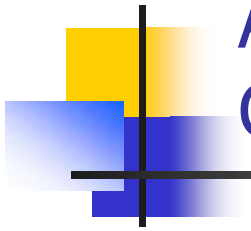
PageRank, развитие идеи (2/2)

- MailRank [2005]
  - граф создается на основе отправленных писем, используется отношение отправитель-получатель
  - используется персонализированный PageRank, где наибольший вес для отправителя имеют получатели, которым письма отправляются чаще
  - алгоритм хорошо работает для разреженных графов, что является принципиальным для электронной почты



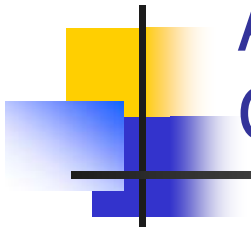
Источники данных для построения репутации

- Автоматические
  - анализ сайта средствами системы
  - анализ внешних источников оценок
- Экспертные
  - оценки, выставленные доверенными пользователями
  - оценки, полученные от обычных пользователей системы



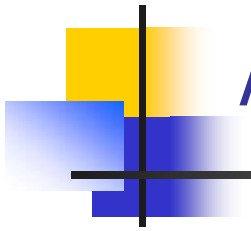
Анализ сайта средствами системы. Собираемые данные (1/2)

- Анализ истории сайта
  - возраст сайта
  - страна, в которой зарегистрирован сайт
  - организация, предоставляющая хостинг сайту
  - история серверов, на которых размещался сайт
- Анализ связей между сайтами
  - анализ репутаций сайтов, на которые ссылается исследуемый сайт
  - анализ репутаций сайтов, ссылающихся на исследуемый сайт



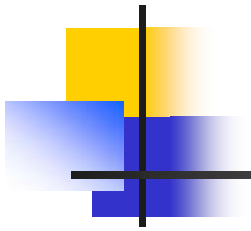
Анализ сайта средствами системы. Собираемые данные (2/2)

- Анализ содержимого сайта на наличие объектов заданных категорий
  - текстовая информация (наличие ключевых слов и фраз)
  - изображения, представленные на сайте
  - файлы, размещенные на сайте
  - структура и внутренние теги сайта
  - анализ новых процессов в системе, появившихся после посещения сайта (sandbox)
  - антивирусный анализ сайта



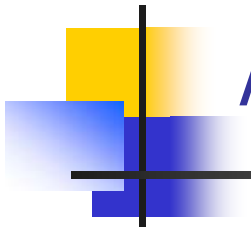
Анализ сайта средствами системы

- Возможная реализация:
  - робот-паук, оценивающий сайты по мере возможности
  - модуль, оценивающий каждую запрашиваемую страницу по запросам от пользователя
- Достоинства:
  - высокая производительность, не требует дополнительных расходов
  - хорошая защита от сайтов, не скрывающих свою принадлежность к какой-либо категории
  - возможность оценки всех запрашиваемых сайтов
- Недостатки:
  - возможность обмана системы
  - ложные срабатывания
  - требуется мощное оборудование при большом количестве запросов к сайтам
  - устаревание оценки



Анализ внешних источников оценок. Собираемые данные

- Информация о вредоносности сайта
  - Google safebrowsing
  - Web Of Trust
- Информация о размещении сайта
  - Сервисы WhoIs
- Наличие сайта в списках по категориям
  - Списки сайтов для систем родительского контроля
  - Тематические каталоги сайтов

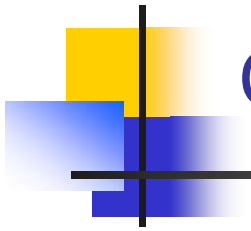


Анализ внешних источников оценок

- Возможная реализация:
  - постоянно обновляемые с внешних источников базы
- Достоинства:
  - высокая точность (особенно коммерческих списков)
  - высокая производительность
- Недостатки:
  - разные критерии оценки
  - противоречивость списков разных источников
  - устаревание оценки
  - желательна проверка качества списков

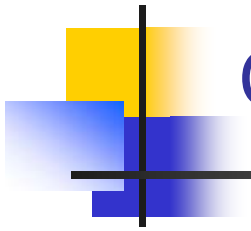
Оценки пользователей

- Собираемые данные:
  - Пользовательские оценки сайта (идентификатор лицензии, адрес сайта, оценки)
  - Информация о пользователях (степень доверия, активность пользователя и т.д.)
- Возможная реализация:
  - Дополнительный модуль в браузере
  - Выставление оценок по истории посещений сайтов (для родительского контроля)
- Способы выставления пользователем оценки репутации ресурса, отличающиеся точностью оценки:
  - запрещение или разрешение обращения к ресурсу (построение черного и белого списков);
  - отнесение ресурса к одной из категорий (построение списка по категориям);
  - выставление оценки ресурса по каждой категории.



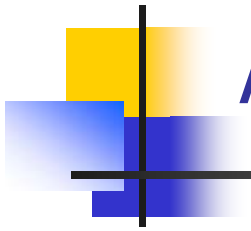
Оценки пользователей

- Достоинства:
  - высокая точность оценки (эксперты)
  - решение спорных вопросов (эксперты)
  - возможность создания своей репутации и правил для разных городов, стран или групп пользователей
  - быстрое внесение в список часто посещаемых сайтов
- Недостатки:
  - низкая производительность
  - небольшое число экспертов
  - разные критерии оценки у разных пользователей
  - устаревание оценки
  - возможны умышленные фальсификации отзывов



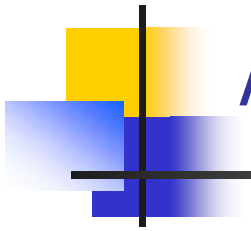
Объединение источников

- Вычисление репутации ресурса по каждой категории учитывает:
  - Оценки пользователей
  - Результаты автоматического анализа
  - Коэффициенты устаревания данных
  - Веса различных источников
  - Прошлые значения репутации
- По вычисленной репутации на локальных компьютерах создаются правила доступа и перенаправления (политики), учитывающие репутацию ресурсов



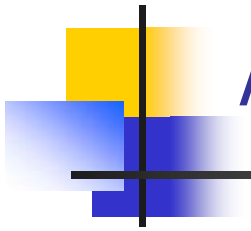
Атаки на систему репутации

- Цель атаки: Подмена оцениваемой информации
- Путь: Перенос сайта на другой хостинг или URL
- Решение: Вычисление процента соответствия между сайтами (требуется большая БД), возможно хранение хэшей текстов, изображений или сайта целиком
- Путь: Подмена информации на уже оцененном сайте
- Решение: хранение хэшей текстов, изображений или сайта целиком



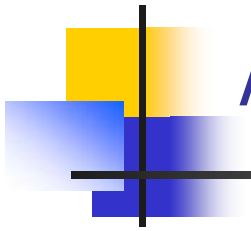
Атаки на клиентское ПО

- Цель атаки: Искажение репутации объектов и субъектов
- Путь: Выставление оценок от имени другого пользователя
- Реализация: Изменение уникального идентификатора лицензии клиентского ПО
- Решение: шифрование кода ПО, контроль целостности и т.д.



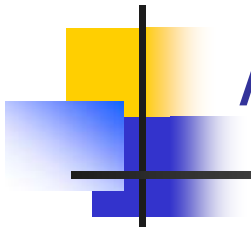
Атаки на промежуточное ПО (1/4)

- Цель атаки: Искажение репутации объектов и субъектов
- Путь: Выставление оценок от имени другого пользователя
- Реализация: Вход в систему под чужим именем
- Решение: Уникальный идентификатор лицензии клиентского ПО используется как идентификатор пользователя



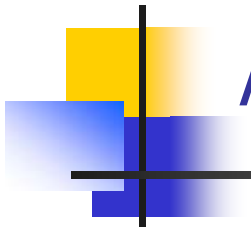
Атаки на промежуточное ПО (2/4)

- Цель атаки: Искажение репутации объектов и субъектов
- Путь: Выставление оценок от имени другого пользователя
- Реализация: Захват идентификатора авторизованной сессии
- Решение: Сессионное шифрование, ограничение продолжительности сессии, привязка к IP



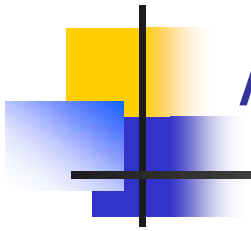
Атаки на промежуточное ПО (3/4)

- Цель атаки: Искажение репутации объектов и субъектов
- Путь: sybil атаки
- Реализация: Создание множества виртуальных пользователей системы
- Решение: Уникальный идентификатор лицензии клиентского ПО не позволяет создавать пользователей без покупки экземпляра клиентского ПО, анализ поведения пользователей, инертность оценок



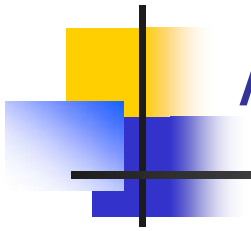
Атаки на промежуточное ПО (4/4)

- Цель атаки: Отказ в обслуживании
- Путь: Паразитные запросы
- Реализация: Создание множества запросов (выставление оценки, запрос оценок) к системе репутации
- Решение: Кэширование данных, анализ поведения пользователей, блокировка пользователей по идентификатору лицензии



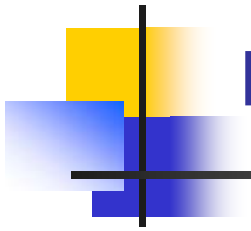
Атаки на базу данных

- Цель атаки: Искажение информации о репутации
- Путь: Несанкционированный доступ к базе данных
- Реализация: Получение прямого доступа к данным хранящимся в БД и их последующая модификация
- Решение: Использование промежуточного ПО, запрет подключений к БД с посторонних IP адресов, контроль целостности данных, репликация БД для возможности восстановления корректных данных



Атаки на базу данных

- Цель атаки: Отказ в обслуживании
- Путь: Программное уничтожение сервера БД, DoS атаки на БД
- Реализация: Получение прямого доступа к данным, хранящимся в БД, и их последующая модификация
- Решение: Использование промежуточного ПО, запрет подключений к БД с посторонних IP адресов, репликация данных БД между независимыми серверами

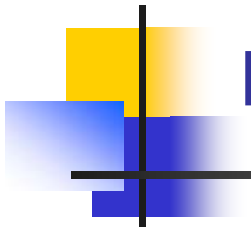


Результаты

- Рассмотрены модели вычисления репутации
- Рассмотрены основные источники информации для построения репутации Web-сайта
- Предложена архитектура системы защиты, основанной на репутациях
- Проанализированы возможные атаки на систему защиты, основанную на репутациях

Направления дальнейших исследований

- Развитие предложенных методов
- Уточнение и оптимизация источников информации
- Совершенствование методов комбинирования оценок для более точного вычисления репутации
- Реализация системы и оценка эффективности



Вопросы

Контактная информация:

Чечулин Андрей Алексеевич (andreych@bk.ru)
Зозуля Юлия Викторовна (yuzozulya@gmail.com)
Котенко Игорь Витальевич (ivkote@comsec.spb.ru)
Тишков Артем Валерьевич (avt@iias.spb.su)
Шоров Андрей Владимирович (ashorov@comsec.spb.ru)

Благодарности:

- РФФИ (проект № 07-01-00547) , ОНИТ РАН