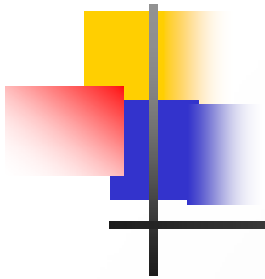
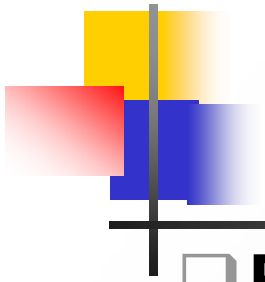


ЗАЩИТА ОТ СЕТЕВЫХ АТАК С ПОМОЩЬЮ МЕХАНИЗМОВ АНАЛИЗА ТРАФИКА

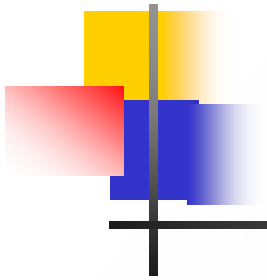
Чечулин А.А.
ЦСС,
Санкт-Петербургский институт информатики и автоматизации РАН

РусКрипто-2010, 1-4 апреля 2010, Москва, Россия



Содержание

- **Введение**
- **Методы анализа трафика и реагирования на атаки**
  - Фильтрация некорректных пакетов
  - Нормализация пакетов
  - Фильтрация на основе данных о сессиях
  - Фильтрация на основе сбора статистики
  - Методы Data Mining для обнаружения сетевых атак
- **Возможные улучшения механизмов**
- **Заключение**



Введение

- Проблемы сетевой безопасности:
  - С помощью ошибок в обработке некорректных пакетов производятся атаки DoS
  - Используя разницу в формировании пакетов, производится сбор информации
  - Растет количество сетевых эпидемий
  - Из-за увеличения объемов трафика растет требуемая мощность оборудования для его анализа

Цели работы

- Разработка комплексного механизма фильтрации и нормализации трафика
  - Классификация атак, основанных на использовании стека протоколов TCP/IP
  - Разработка механизмов фильтрации и нормализации против каждого класса атак
  - Проведение экспериментов
  - Анализ результатов

Область применения механизмов защиты, основанных на анализе трафика

- Задачи, предполагающие применение данных механизмов
  - Защита отдельного компьютера
  - Защита локальной сети путем установки механизмов фильтрации и нормализации на сетевом оборудовании
  - Снижение нагрузки на межсетевые экраны

Обзор существующих работ

- Handley M., Paxson V. Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics // AT&T Center for Internet research at ICSI (ACIRI International Computer Science Institute)
  - Описаны принципы нормализации трафика сетевого и транспортного уровней стека TCP/IP
  - Приведены примеры правил нормализации

Обзор существующих работ

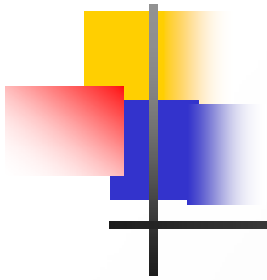
- M.Williamson. Throttling Viruses: Restricting propagation to defeat malicious mobile code // In Proceedings of ACSAC Security Conference, Las Vegas, Nevada. 2002
  - Предложен новый подход к обнаружению сканирования - Virus Throttling
  - Приведены примеры алгоритмов

Атаки на основе протоколов TCP/IP

- Атаки, основанные на ошибках в обработке некорректных пакетов
- Сбор информации, основанный на разнице в обработке некорректных или “нестандартных” пакетов
- Сканирование, основанное на использовании ошибок в обработке сессий
- Сканирование, основанное на корректном установлении соединений

Виды фильтрации и нормализации трафика

- Основанные на анализе отдельных пакетов
  - Фильтрация некорректных пакетов
  - Нормализация пакетов
- Основанные на анализе последовательности пакетов
  - Фильтрация на основе данных о сессиях
  - “Virus Throttling” для реализации на свитче
  - “Virus Throttling” для реализации на свитче на основе метода CUSUM

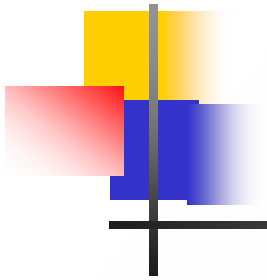


Фильтрация некорректных пакетов

- Проблема: из-за разницы в обработке некорректных пактов разными системами становятся возможными сбор информации и сокрытие и проведение атак
- Решение: фильтрация пакетов, имеющих некорректные заголовки
- Пример: Microsoft (MS09-048) Vulnerabilities in Windows TCP/IP

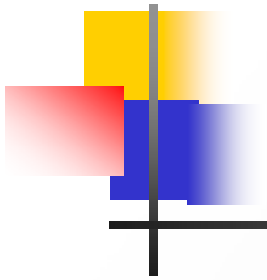
Достоинства фильтрации некорректных пакетов

- Уменьшение нагрузки на межсетевой экран
- Высокая скорость работы
- Надежность
- Возможность работы механизма на сетевом оборудовании
- Защита не от конкретных атак, а от класса атак, использующих ошибки в реализации протоколов



Недостатки фильтрации некорректных пакетов

- Отсутствие дефрагментации пакетов
- Уязвимость к атакам DoS - при слишком большом трафике пакеты либо задерживаются, либо пропускаются без обработки
- Пропуск атак, основанных на корректном сетевом взаимодействии

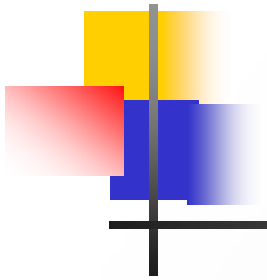


Нормализация пакетов

- Проблема: из-за разницы в обработке корректных пактов разными системами становятся возможными сбор информации и сокрытие атак
- Решение: необходимо привести поля заголовков к стандартным величинам
- Пример: изменить значение поля TTL-протокола IP на 128, это приведет к невозможности использования tracert при сканировании

Достоинства нормализации пакетов

- Высокая скорость работы
- Надежность
- Возможность работы механизма на сетевом оборудовании
- Защита не от конкретных атак, а от класса атак, использующих ошибки в реализации протоколов.



Недостатки нормализации пакетов

- Отсутствие дефрагментации пакетов
- Уязвимость к DoS атакам - при слишком большом трафике пакеты либо задерживаются, либо пропускаются без обработки
- Пропуск атак, основанных на корректном сетевом взаимодействии

Фильтрация на основе данных о сессиях

- Проблема: сбор информации и сокрытие атаки с помощью TCP пакетов, относящихся к несуществующим сессиям
- Решение: фильтрация подобного рода пакетов
- Пример: сканирование Stealth FIN – отправка пакетов TCP с установленным флагом FIN для получения списка закрытых портов

Достоинства фильтрации на основе данных о сессиях

- Уменьшение нагрузки на межсетевой экран
- Возможность работы механизма на сетевом оборудовании
- Защита не от конкретных атак, а от класса атак, использующих ошибки в реализации работы с сессиями

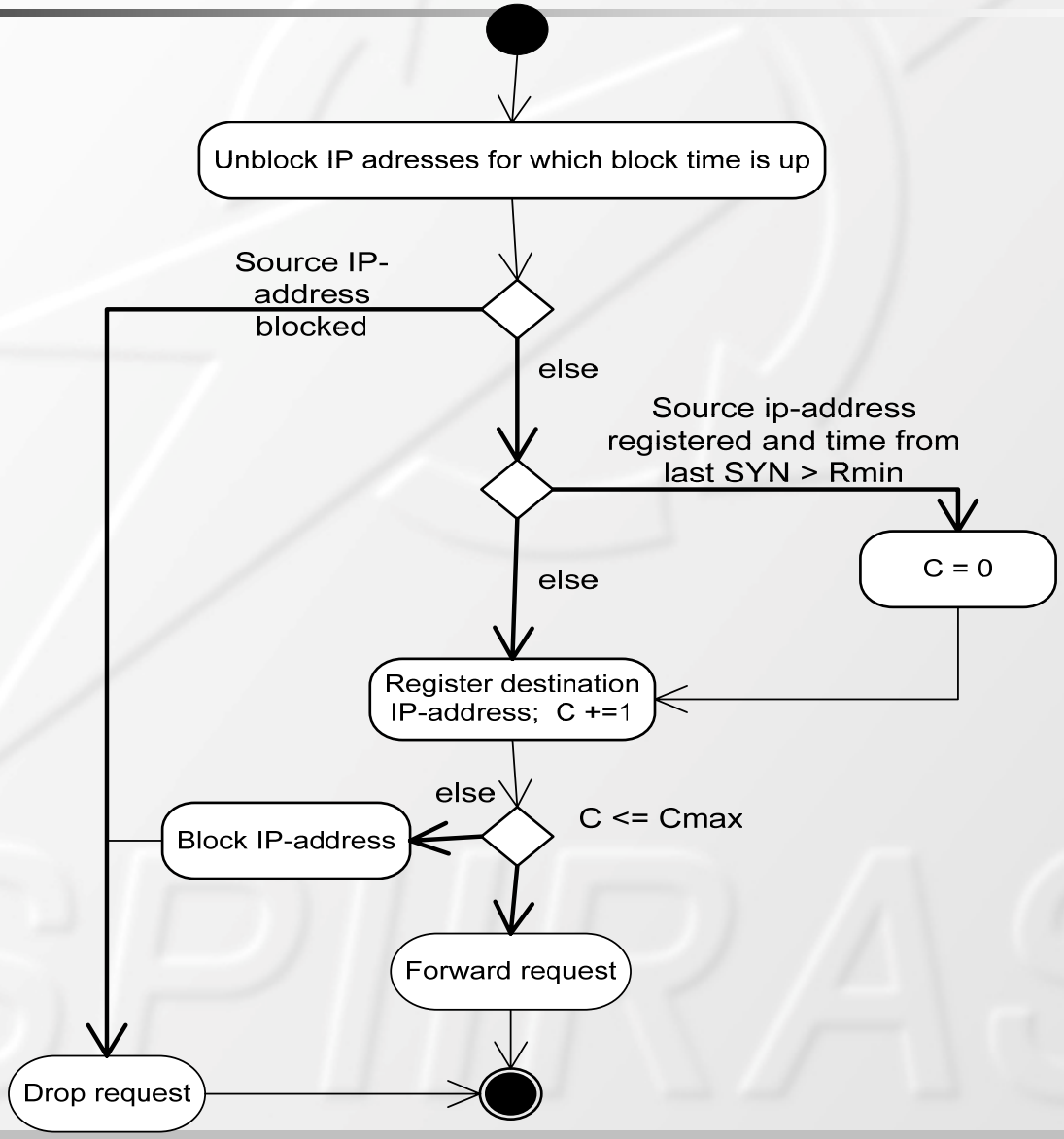
Недостатки фильтрации на основе данных о сессиях

- Сложность установки механизма на сетевом оборудовании
- Уязвимость к DoS атакам - при слишком большом трафике может переполниться таблица сессий и скорость работы механизма заметно снизится
- Пропуск атак, основанных на корректном создании сессий

Методы, базирующиеся на методике “Virus Throttling”

- Механизмы фильтрации, базирующиеся на методике “Virus Throttling”:
  - Базовый “Virus Throttling” для реализации на свитче
  - Модификация “Virus Throttling” для реализации на свитче (на основе метода CUSUM)

Модификация “Virus Throttling” для реализации на свитче (на основе метода CUSUM)



Блок схема метода “Virus Throttling” для реализации на свитче

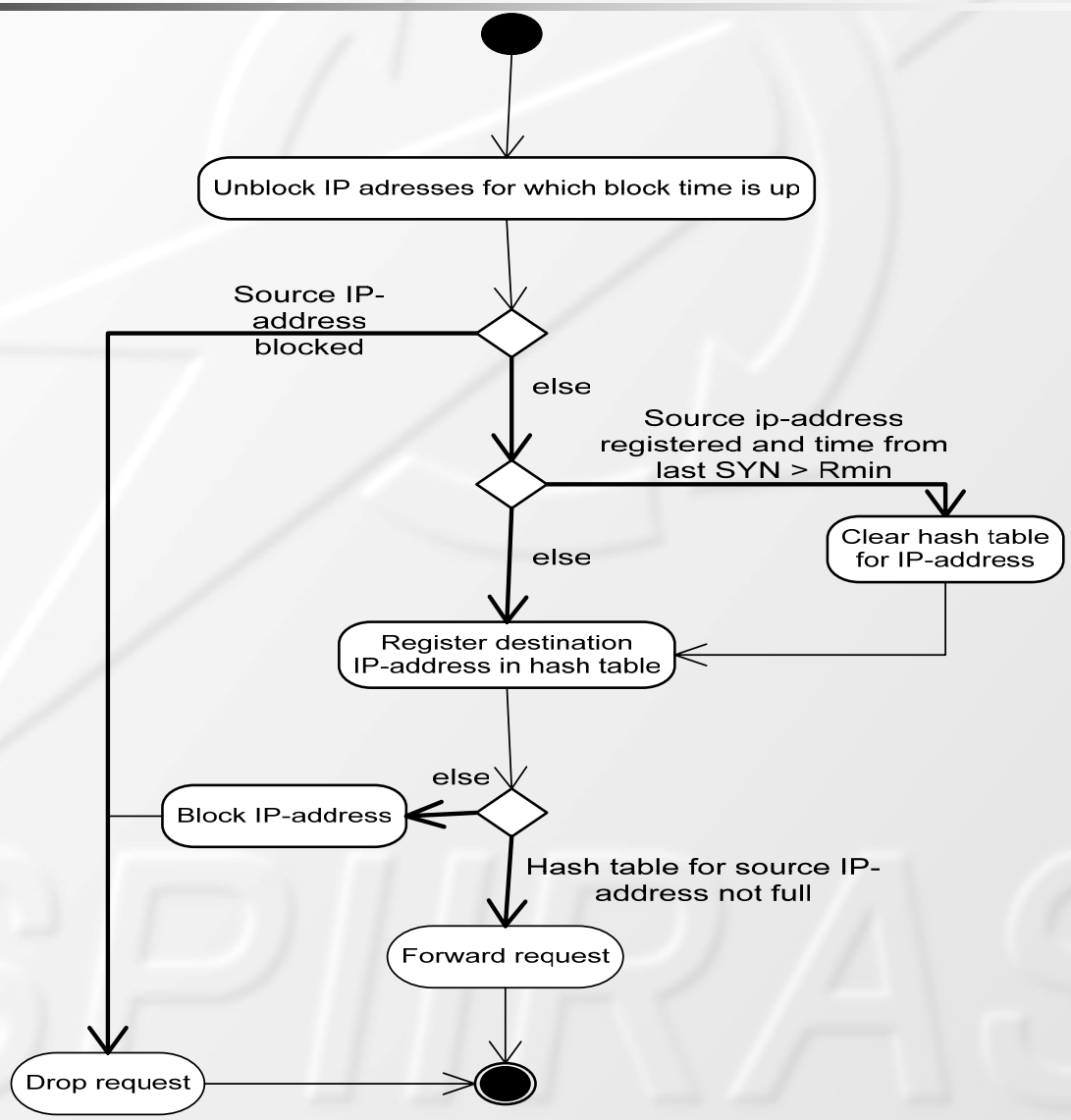
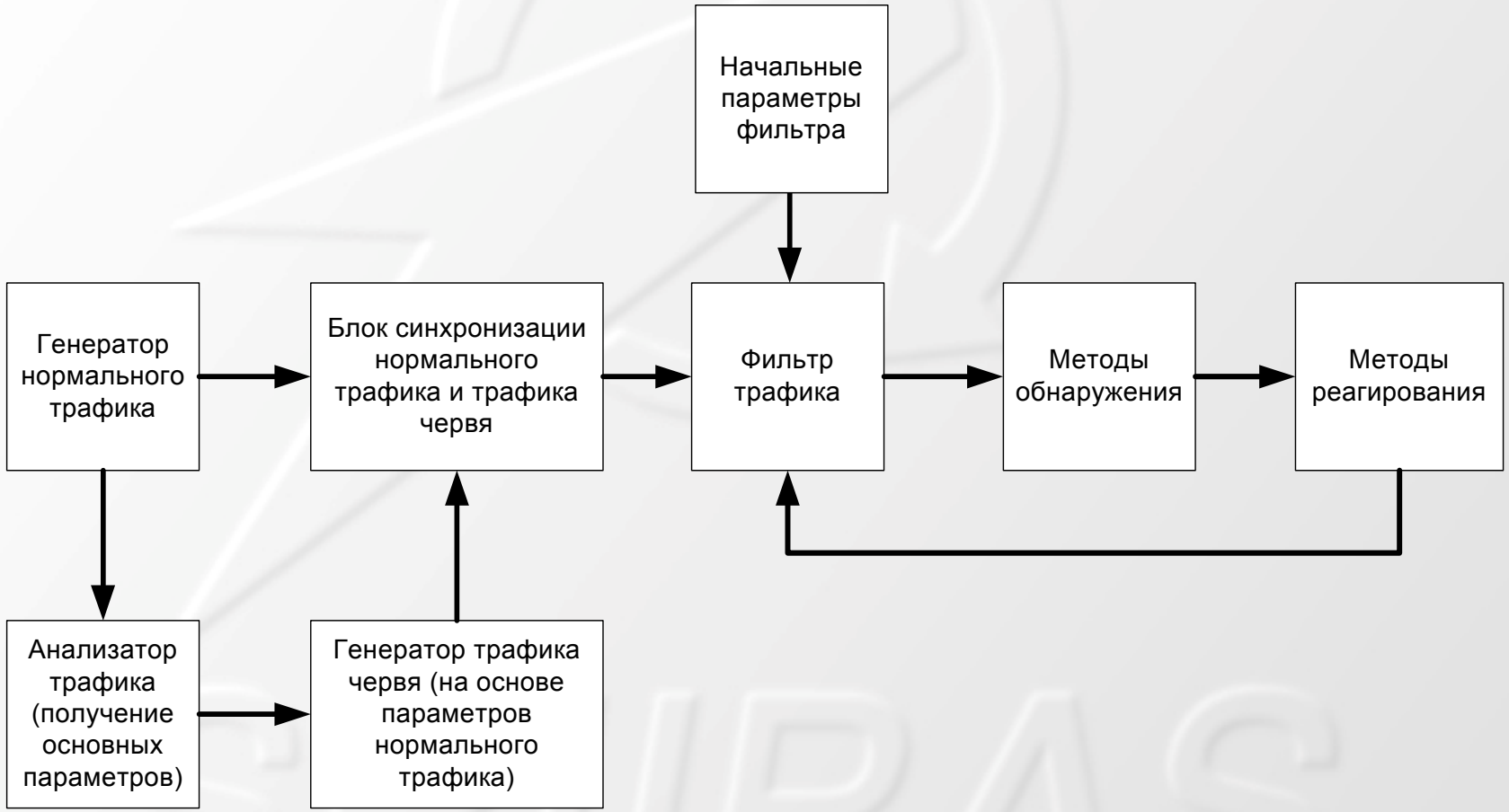


Схема работы генератора

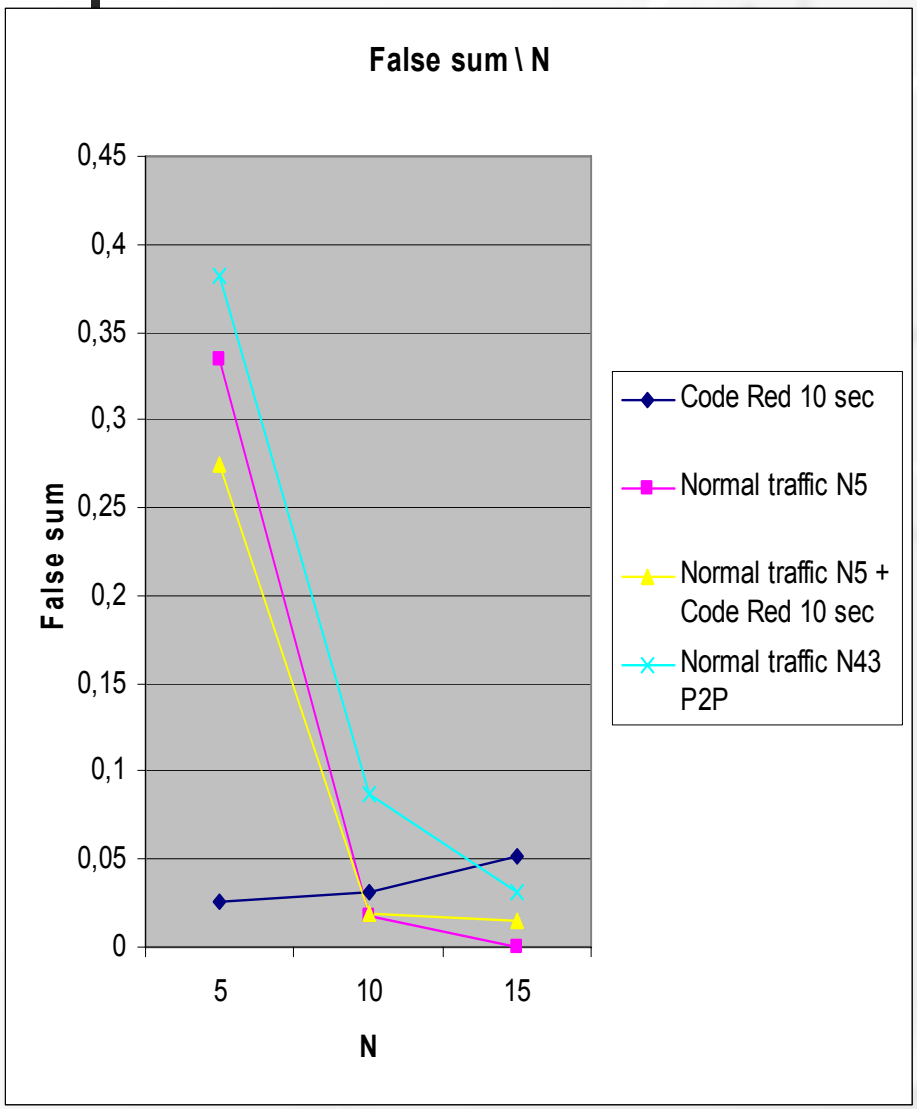


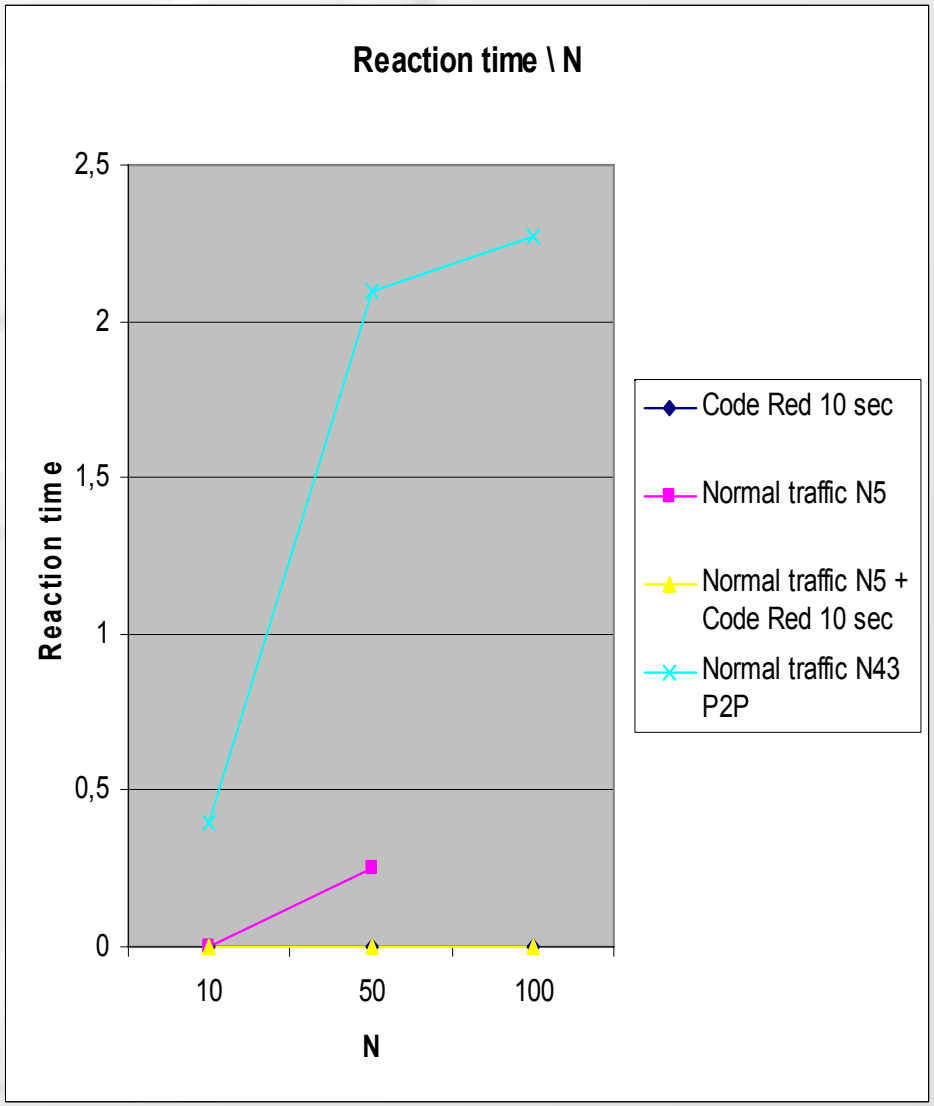
Моделирование известных червей

Code Red II:

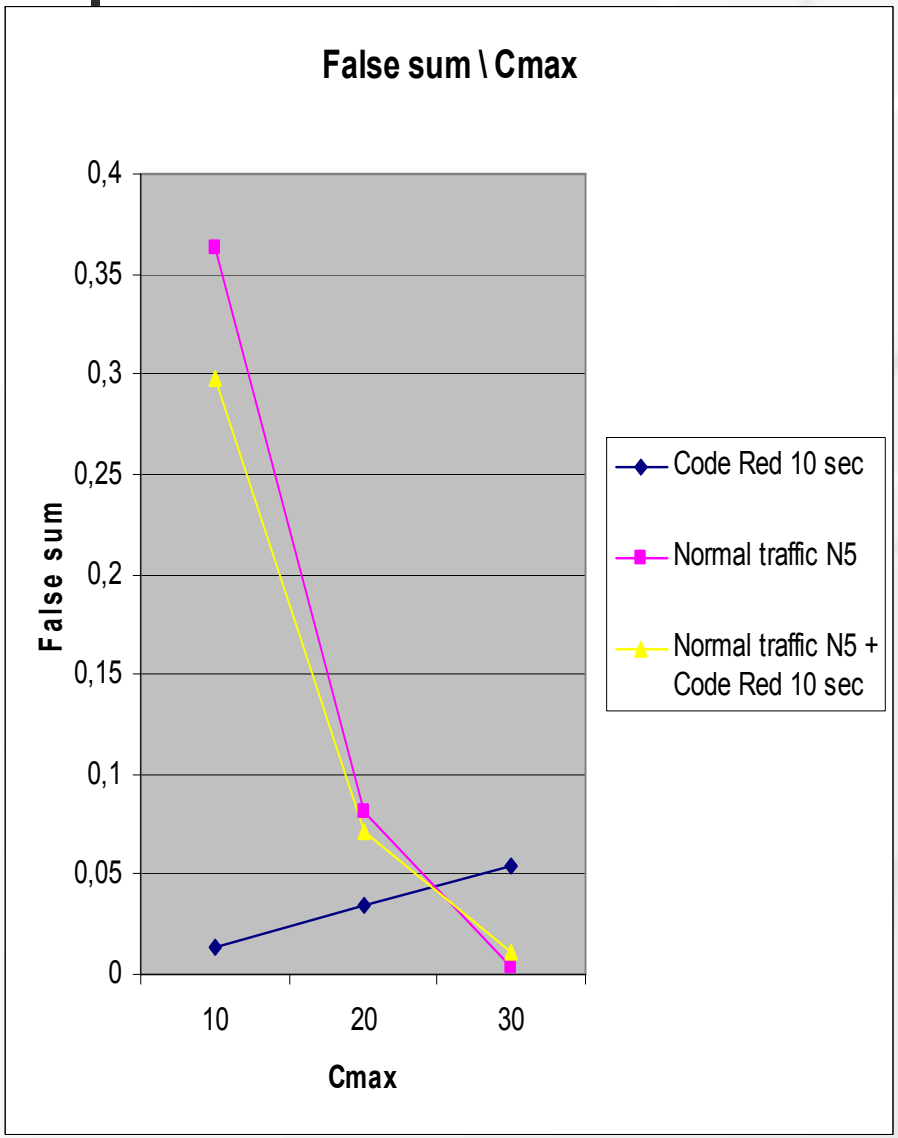
- Генерация пакета TCP-SYN на порт 80 с адресом получателя в соответствии со способом выбора Code Red II (1/8 времени – случайные адреса, 1/2 времени – в той же /8 подсети (X.*.*.*), 3/8 времени – в той же /16 подсети (X.Y.*.*)) с частотой 5.65 в секунду

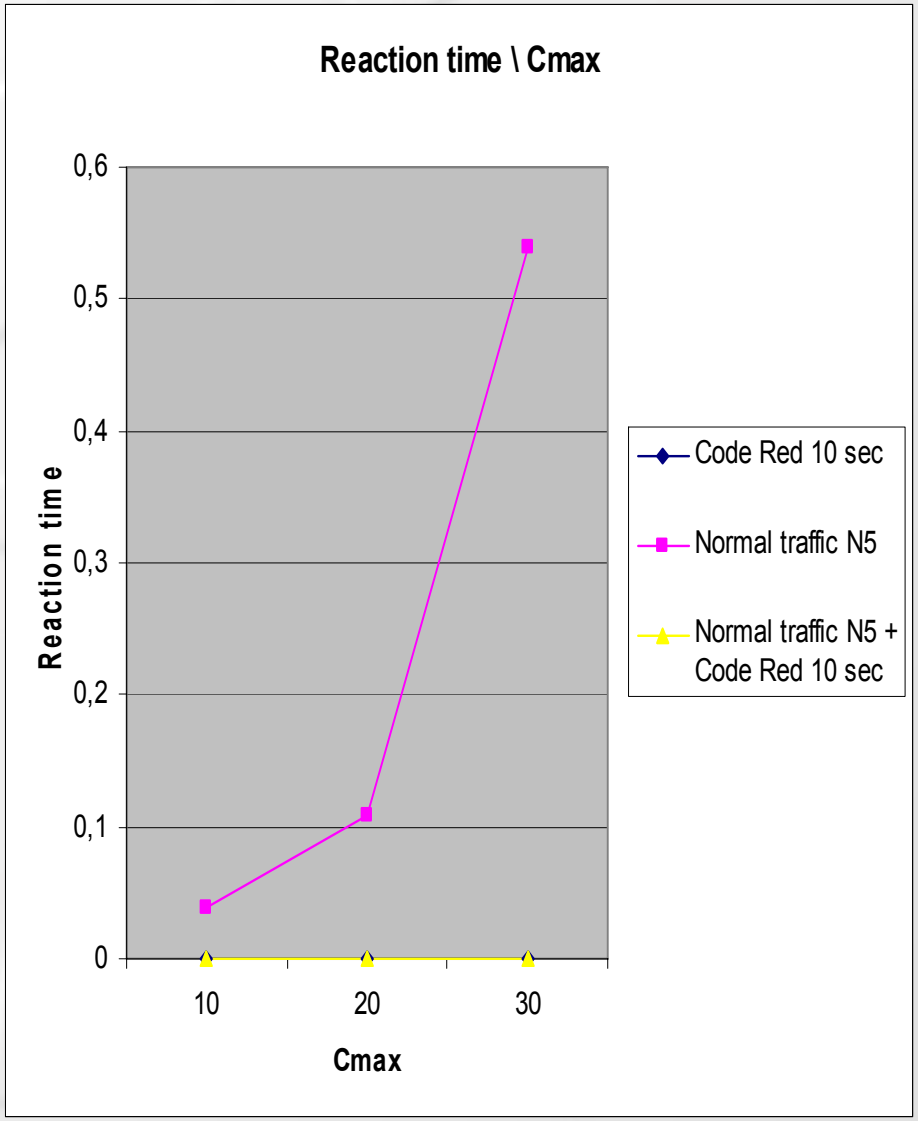
Результаты по VT-S

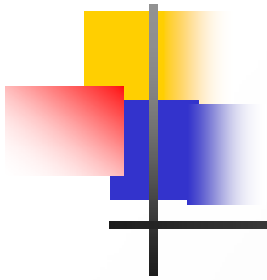




Результаты по VT-Cusum







Достоинства методов “Virus Throttling”

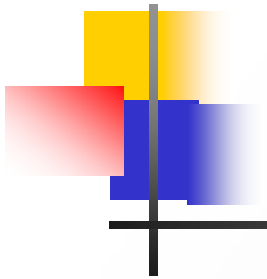
- Простота реализации
- Эффективное обнаружение быстрого сканирования при условии “медленных” легитимных приложений
- Адаптивность – происходит регистрация наиболее часто используемых адресов

Недостатки методов “Virus Throttling”

- Блокируются хосты, на которых установлены приложения, генерирующие много запросов на соединение (web-браузеры, менеджеры закачки, P2P и т.д.)
- Невозможно обнаружить медленное сканирование
- Не учитывается результат установления соединений
- Невозможно обнаружить сканирование, основанное на протоколе UDP

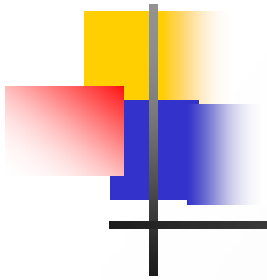
Возможные улучшения методов “Virus Throttling”

- Анализ UDP протокола. Отдельный пакет представляется как запрос на соединение
- Обработка ответов на запросы (TCP SYN-ACK)
- Использование для анализа не только IP-адресов, но и других полей пакета



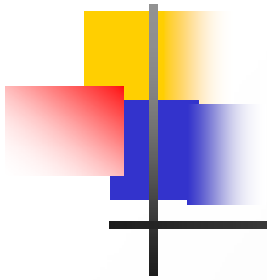
Методы Data Mining для обнаружения сетевых атак

- Обнаружение аномального поведения
  - Не может служить основанием для принятия решений, за исключением “параноидальных” систем
- Обучение методов Data Mining на конкретных сетевых атаках
  - Часто оказывается хуже сигнатурных методов обнаружения



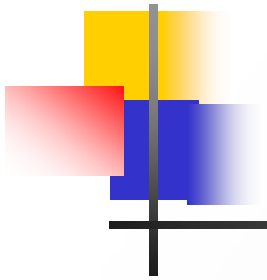
Возможные улучшения механизмов анализа трафика

- Оптимизация механизмов для возможности их работы на сетевом оборудовании
- Создание механизмов фильтрации для работы в сетях с P2P трафиком
- Разработка системы фильтрации и нормализации протоколов верхнего уровня стека TCP/IP



Методы комбинирования

- Метод простого голосования
- Метод взвешенного голосования
  - Учитывает предварительно рассчитанную точность методов
- Метод комбинирования по Байесу
  - Может учитывать изменения характеристик сети



Применимость методов комбинирования

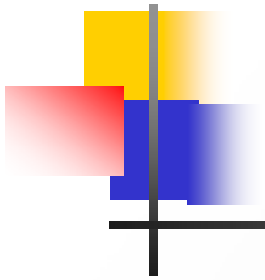
- Для определения вредоносности трафика
  - Используется информация от статистических методов и методов Data Mining
- Для определения вредоносности хоста
  - Используется информация от всех методов анализа трафика

Заключение

- Рассмотрены атаки, основанные на протоколах TCP/IP
- Разработаны механизмы анализа трафика
- Разработан стенд для анализа, механизмов защиты основанных на анализе трафика
- Частично получены и проанализированы результаты работы механизмов защиты

План дальнейшей работы

- Анализ работы механизмов защиты на основе методов Data Mining
- Нахождение оптимальных параметров для существующих механизмов
- Разработка новых механизмов фильтрации и нормализации трафика
- Разработка системы комбинирования методов



Контактная информация

Чечулин Андрей Алексеевич (СПИИРАН)
chechulin@comsec.spb.ru
http://comsec.spb.ru/Chechulin

Вопросы?