ПОСТРОЕНИЕ ГРАФОВ АТАК ДЛЯ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

Чечулин А.А., Котенко И.В.

Лаборатория проблем компьютерной безопасности Санкт-Петербургского Института Информатики и Автоматизации РАН

Санкт-Петербург, Россия

РусКрипто'2013, 28-31 марта 2013 г.

Введение (1/2)

- Причины нарушения безопасности в КС:
  - Ошибки политики безопасности
  - Уязвимости
  - Неправильные конфигурации ПО
  - …
- Система постоянно изменяется:
  - Появление новых уязвимостей
  - Обновление ПО
  - Изменение политик безопасности
  - Появление новых элементов сети
  - …

Введение (2/2)

- Аналитическое моделирование позволяет оценить защищенность системы на разных стадиях
  - Во время проектирования системы
  - В момент выбора контрмер
  - К определенной модели нарушителя
  - В зависимости от событий в сети
- Так же на основе полученных данных возможно
  - Определять наиболее вероятные модели нарушителей в соответствии с происходящими в сети событиями
  - Определять наиболее опасные потенциально возможные уязвимости (0-day)
  - Определять наиболее вероятные сценарии атак
  - Рекомендовать наиболее эффективные контрмеры
  - ...

Постановка задачи

- Основные проблемы моделирования
  - Временные затраты на формирование моделей (система должна поддерживать работу в режиме близком к реальному времени)
  - Изменчивость системы (модели приходится перестраивать)
- Дополнительные требования
  - Построенные модели должны учитывать множество моделей нарушителей
  - Модели атак должны позволять производить корреляцию событий безопасности для выявления наиболее вероятных моделей нарушителей
  - Для построения моделей должны использоваться общепринятые стандарты

Этапы работы системы моделирования

- Этап разработки и ввода в эксплуатацию (не real-time)
  - Определение слабых мест в сети
  - Формирование базовых графов атак
  - Расчет метрик безопасности защищаемой сети
  - Наиболее опасные возможные уязвимости нулевого дня
  - …
- Этап эксплуатации (real-time)
  - Обновление хранимых графов атак для соответствия изменениям происходящим в сети
  - Оценка возможных мероприятий по увеличению уровня защиты
  - Предсказание действий нарушителя
  - Обратный анализ действий нарушителя
  - …

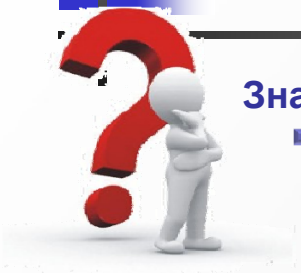
Релевантные работы

- Теоретические подходы
  - T. S. Christey, C. Harris. “Introduction to Vulnerability”. October 29, 2009
  - N. Kheir and J. Viinikka. Comments on analytical attack modeling, 2011
  - P.K. Manadhata and J.M. Wing “A Formal Model for a System's Attack Surface”, Springer, 2011
  - J. Wang, J.N. Whitley, R.C.W. Phan, and D.J. Parish. “Unified Parametrizable Attack Tree”, 2011
  - L.Wang, S.Jajodia, A.Singhal, and S.Noel. “k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks”, 2010
- Прототипы
  - Система стохастического дискретного событийного моделирования COMNET III разработанной компанией CACI Products Company (http://www.caciasl.com/)
  - Система анализа безопасности OpenSKE (Open Security Knowledge Engineered, https://github.com/maherg/openske)
  - Система использующая деревья атак для анализа защищенности Amenaza SecurITree (http://www.amenaza.com/)

Методика

- Подготовительный этап
  - Матрица потенциально возможных атакующих действий. Для каждого хоста строится 3-х мерная матрица по следующим данным:
    - класс атак (сбор данных, подготовительные действия, повышение привилегий, выполнение цели атаки)
    - необходимый тип доступа (удаленный источник без прав доступа, удаленный пользователь системы, локальный пользователь системы, администратор)
    - уровень знаний нарушителя (типы уязвимостей, которые нарушитель может реализовывать)
  - Формирование моделей нарушителей
    - Точки доступа в сети
    - Возможности (уровень знаний и т.д.)
    - Цели
  - Построение графов и расчет метрик защищенности
- Этап анализа событий
  - Корреляция событий безопасности и построенных графов атак

Режимы работы прототипа



Не real-time режим

Знания оператора

Модель сети

Спецификация

Расчет базовых метрик

Уязвимости

Деревья атак

Результаты моделирования

Базовые метрики

Режим anytime

События в реальном времени

Обновленные деревья атак

Деревья атак

Расчет метрик защищенности

Режим real-time

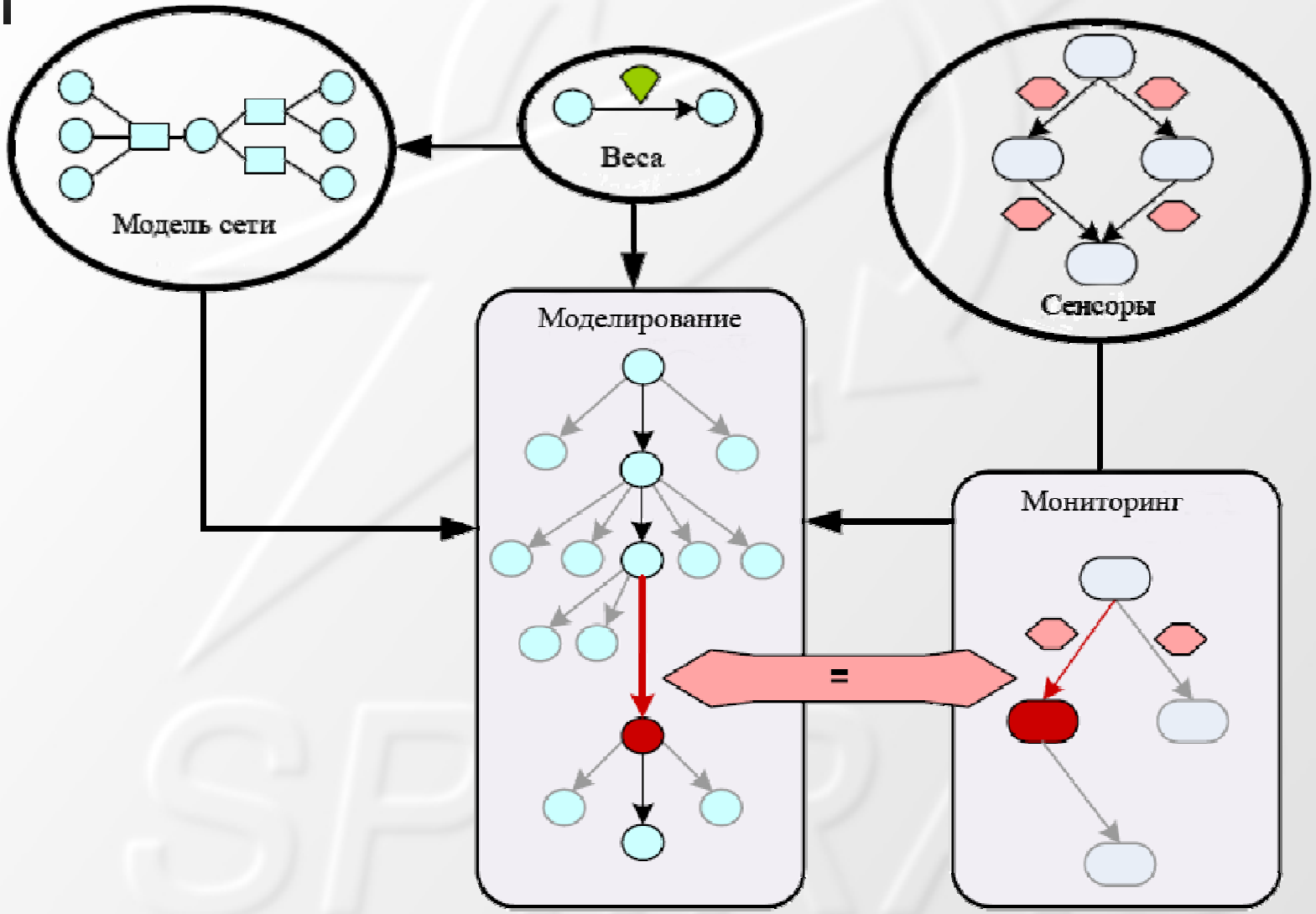
Сценарии

События в реальном времени

Определение сценариев атак

Рекомендации

Анализ событий



Заключение

- Рассмотрены основные проблемы моделирования сетевых атак
- Рассмотрены необходимые исходные данные для моделирования атак
- Описан подход, позволяющий использовать моделирование атак в системах, работающих в режиме близком к реальному времени
- Применение данного подхода позволит повысить уровень защищенности существующих компьютерных сетей

Контактная информация

Чечулин Андрей Алексеевич
chechulin@comsec.spb.ru
http://comsec.spb.ru/chechulin

Котенко Игорь Витальевич
ivkote@comsec.spb.ru
http://comsec.spb.ru/kotenko

Благодарности

Работа выполняется при финансовой поддержке РФФИ, программы фундаментальных исследований ОНИТ РАН, государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.