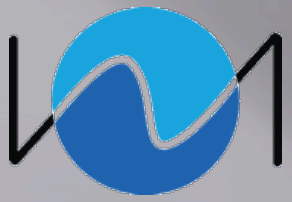


11-Я МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «ИНТЕЛЛЕКТУАЛИЗАЦИЯ ОБРАБОТКИ ИНФОРМАЦИИ»

АНАЛИЗ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ БЕСПРИЗНАКОВОГО РАСПОЗНАВАНИЯ ОБРАЗОВ

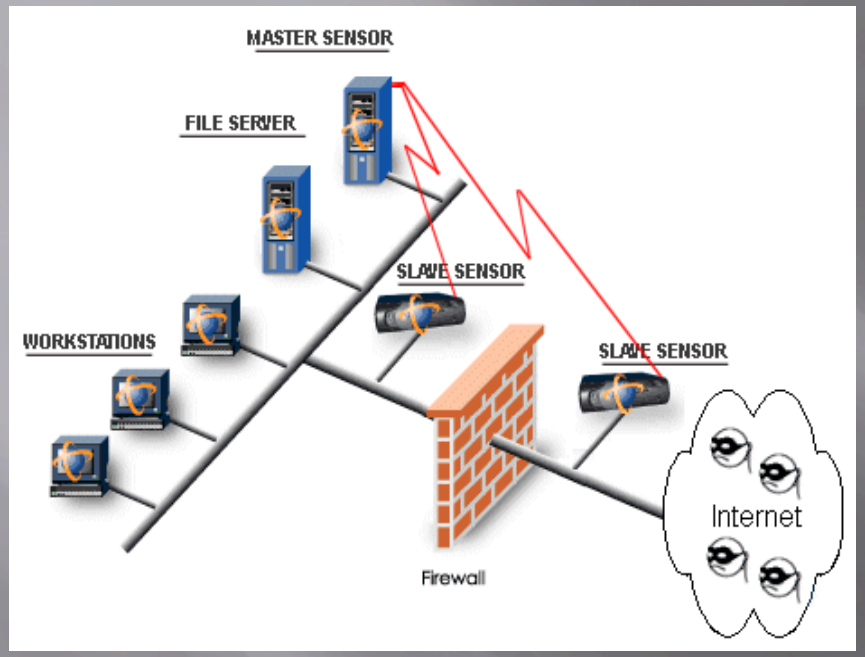
Сычугов Алексей Алексеевич xru2003@list.ru
Руднев Дмитрий Олегович
Тула, ФГБОУ ВО «Тульский государственный университет»,
Кафедра «Информационная безопасность»

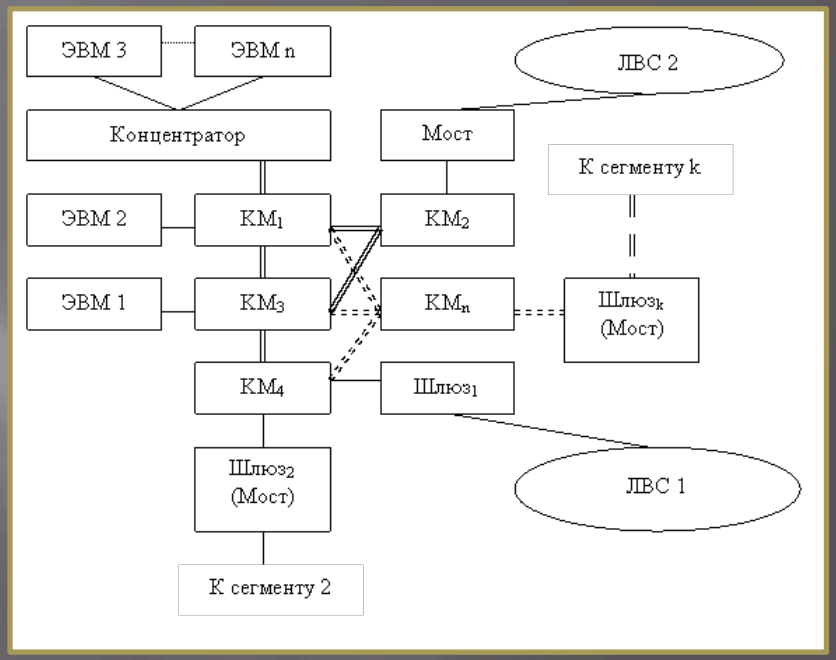
Барселона, Испания

Вводные замечания

- Технологии распределённых вычислений постоянно развиваются
- Основные преимущества: производительность, отказоустойчивость и масштабируемость
- Постоянно увеличивается объем обрабатываемой информации
- Актуальность решения задачи обеспечения информационной безопасности РИС увеличивается

Традиционные ИС и РИС





- В традиционных информационных системах владелец информации может контролировать средства защиты
- В РИС невозможно управление и мониторинг средств безопасности со стороны владельца информации

Задача

Владелец информации может принимать решение только о передаче информации на конкретный узел РИС для вычислений и не может контролировать безопасность информации во время обработки на узле

Разработка методов, позволяющих **оценить** владельцем информации элемент РИС с точки зрения безопасности и одновременно **сохранить конфиденциальность сведений** о средствах защиты и состоянии элемента РИС

Понятие доверия

- Доверие*) – это субъективная вероятность со стороны А выполнения действия стороной В, которое А не может наблюдать и контролировать, при этом, действия В повлияют на благосостояние А, его выгоду.
- В РИС понятие «доверие» можно сформулировать как вероятность того, что данные, переданные на узел РИС и результаты вычислений не будут скомпрометированы и искажены, иными словами, за время обработки информации не будут нарушены её конфиденциальность, целостность и доступность

---

*) Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation // System Sciences. 2002. P. 2431-2439

Модель доверия

$\Omega = \{\Omega_0, \Omega_1, \ldots, \Omega_N\}$ – множество всех узлов РИС

Каждый элемент $\Omega_i \in \Omega$ в момент времени $t_j \in T$ находится в состоянии $s_i^j \in S$

Где S - множество всех возможных состояний элемента РИС, которые определяют величину доверия к данному узлу в текущий момент времени и описываются некоторым набором признаков, обладающих свойством метрики

Для каждого элемента $\Omega_i \in \Omega$ величина доверия p_i в момент времени $t_j \in T$ определяется множеством возможных состояний системы: $p_i = P(s_i^0, s_i^1, \ldots, s_i^j)$

Можно утверждать, что величина доверия зависит от состояния элемента РИС во время наблюдения. Для анализа состояния элемента РИС, не нарушая при этом конфиденциальность сведений о нем, предлагается анализировать не множество значений признаков, описывающих состояние элемента РИС, а меру его похожести на заранее заданный базис, определяющий состояние элемента с известным значением доверия.

Модель доверия

Множество базисных объектов:

$$B = \{b_0, b_1, \ldots, b_M\}$$

Функция похожести состояний элементов РИС:

$$r_{i,j} = \rho(s_i^t, s_j^t)$$

Тогда состояние элемента Ω_i в момент времени t можно описать вектором:

$$s_i^t = \{\rho(s_i^t, b_0), \rho(s_i^t, b_1), \ldots \rho(s_i^t, b_M)\}$$

Таким образом, доверие определяется

$$p_i = P(s_i^0, s_i^1, \ldots, s_i^K)$$

К предлагаемому подходу можно применить математический аппарат, известный в машинном обучении как беспризнаковое распознавание образов.

Преимущества и недостатки

- Переход от непосредственного анализа состояний элементов РИС к анализу метрик похожести решает проблему безопасности периметра РИС.
- Возможно описывать состояние элемента РИС объектами произвольной природы, такими как множества или временные ряды

- Сложность выбора вида функции доверия P, в основу построения которой предлагается заложить следующие принципы:
  - существует период времени, для которого известны значения доверия;
  - доверие выше к тому элементу, чьи состояния повторяются во времени, чье будущее состояние более предсказуемо.

Постановка эксперимента

Задача: сохранив конфиденциальность работы узлов системы, выявить атаки, проводимые на эти узлы. Предполагается, что атака на элемент системы изменит его поведение.

Требования к исходным данным:

1. Данные должны содержать информацию о работе конкретных узлов распределённой информационной системы и их взаимодействии.
2. Данные должны охватывать временной промежуток в несколько недель. Так как в работе информационных систем наблюдаются недельные периоды, то для обучения алгоритма необходимо несколько примеров каждого из дней недели.
3. Данные должны быть размечены. То есть в данных должны присутствовать отметки начала и конца атаки.

Описание данных

Используются данные о работе компьютерной сети Лос-Аламосской национальной лаборатории*), которые удовлетворяют предъявляемым требованиям. Данные представляют собой журналы событий, описывающие работу компьютерной сети за 58 дней и представлены в виде 4 типов журналов событий: журнал событий авторизации, журнал событий сетевого взаимодействия, журнал работы DNS сервера и журнал процессов, запущенных на компьютерах.

Так же данные содержат журнал активности, так называемой, red team – условных злоумышленников, совершающих атаки на компьютеры в сети. В журнале событий red team, содержатся метки времени начала атаки и идентификаторы компьютеров, на которые были направлены атаки. Однако в данных не содержится прямого указания типа атаки и была ли она успешной.

Для эксперимента были взяты данные из журнала сетевого взаимодействия, каждая запись которого содержит следующие поля: метка времени, длительность соединения, сетевой адрес и порт отправителя и получателя, размер пакета. Для сокращения количества обрабатываемых данных был выбран временной промежуток в 3 недели, как оптимальный вариант между количеством исходных данных и ожидаемым результатом.

---

*) A. D. Kent, “Comprehensive, Multi-Source Cybersecurity Events,” Los Alamos National Laboratory, http://dx.doi.org/10.17021/1179829, 2015

Подготовка данных

Для эксперимента были взяты данные из журнала сетевого взаимодействия, каждая запись которого содержит следующие поля:

- метка времени;
- длительность соединения;
- сетевой адрес;
- порт отправителя и получателя;
- размер пакета.

На первом шаге журнал сетевого взаимодействия был разбит на несколько независимых журналов, каждый из которых соответствует журналу одного компьютера. Таким образом, была промоделирована ситуация, когда каждый элемент имеет собственный периметр защиты и информация о сетевом взаимодействии на каждом компьютере не передается за пределы данного компьютера. Затем в каждом журнале данные были сагрегированы по 10 минут.

Состояние элемента РИС определяется следующим набором признаков: $s_i^t = \{v_{i,1}^t, v_{i,2}^t\}$

$v_{i,1}^t$ определяет количество взаимодействий элемента система с другими элементами;

$v_{i,2}^t$ количество используемых портов.

Функция сравнения элементов: $\rho(s_i^t, s_j^t) = d(v_{i,1}^t, v_{j,1}^t) + d(v_{i,2}^t, v_{j,2}^t) + d(v_{i,3}^t, v_{j,3}^t)$

В качестве базиса в эксперименте были взяты состояния случайных элементов РИС в начальный момент времени

Вычислительный эксперимент

В качестве функции доверия P использована средняя абсолютная ошибка в процентах прогнозирования временного ряда:

$$P_i = 1 - \frac{1}{j}\sum_{t=0}^{j}\frac{\rho(s_i^t, b_0) - \rho`(s_i^t, b_0)}{\rho(s_i^t, b_0)}$$

где ρ – фактические значение похожести текущего состояния элемента на базис, $\rho`$ – спрогнозированное значение похожести текущего состояния элемента на базис. Чем выше ошибка прогнозирования, тем ниже доверие к данному элементу в данный момент времени.

Все исходные данные были разделены на две выборки: тренировочная и тестовая по две и одну неделю соответственно. Затем на тренировочной выборке была обучена рекуррентная нейронная сеть. В качестве нейронной сети была выбрана следующая структура: входной слой, слой с Long short-term memory(LSTM)[5] элементами и выходной слой. Нейронные сети с такой архитектурой показывают высокие результаты в задаче обнаружения вторжений и не требуют настройки множества параметров алгоритма.

Основные результаты

- Для большинства элементов РИС атаки не влияют на сетевое взаимодействие самих элементов. *)
- Только по сетевому взаимодействию нельзя делать вывод о происходящей атаке
- Необходимо уточнение исходных данных для эксперимента или создания новых, так как в них отмечаются одновременные изменения поведений в различных группах элементов.
- Одним из направлений дальнейших исследований является разработка алгоритма выбора оптимального базиса.

---

*) Melissa J. M. Turcotte, Nicholas A. Heard, Alexander D. Kent. Modelling user behavior in a network using computer event logs. Dynamic Networks and Cyber-Security. Chapter 3. 2016.

СПАСИБО ЗА ВНИМАНИЕ

Сычугов Алексей Алексеевич
К.т.н., доцент, зав. каф. «Информационная безопасность»
ФГБОУ ВО «Тульский государственный университет»
xru2003@list.ru
Контактный телефон: 8-960-594-88-53

11-я Международная конференция «Интеллектуализация обработки информации»
10-14 октября 2016 г., Барселона, Испания