NON SIGNATURE-BASED METHODS FOR ANOMALY DETECTION

P.Osipovs, A.Borisovs

Keywords: Intrusion Detection, Statistical Model, Agents, Markov Models

Рассмотрены различные подходы к задаче обнаружения аномального поведения в рамках систем обнаружения вторжений с использованием методов не использующих шаблоны. В основу каждого рассмотренного алгоритма положены различные модели, но все они показывают эффективные результаты в задачах оценки наличия противоправности в действиях авторизованного пользователя информационной системы.

Рассмотрены подходы использующие Марковские цепи, иерархические скрытые Марковские модели, применение алгоритмов фильтрации шумов в сигнале к данной задаче, методы, основанные на онтологиях и агентах. В заключение рассмотрена экспериментальная система разрабатываемая в колумбийском университете Калдас.

Введение

В современном информационном обществе задача обеспечения безопасности информации является одной из важнейших. Существует целый класс систем обнаружения вторжений (СОВ), зачастую использующих весьма изощрённые алгоритмы для обнаружения и предотвращения вторжений в информационные системы [1,2,3].

В [4] приведено несколько видов классификаций вторжений, в частности, по уровням анализируемых данных. Выделены 4 уровня, на которых нужно анализировать активность на предмет её аномальности: *сетевой*, *операционной системы*, *приложения* и *данных*. Большинство подобных систем анализируют данные на всех уровнях обмена информацией, от сетевого до уровня приложения. Однако чем выше уровень, тем больше построенные модели зависят от специфики приложения. К примеру, если на сетевом уровне достаточно анализировать TCP (Transmission Control Protocol) пакеты, то на уровне приложения требуется учитывать контекст взаимодействия пользователя с системой.

Кроме уровней анализа данных СОВ делятся по принципу анализа деятельности пользователя. Существуют методы обнаружения злоупотреблений (Misuse Detection) [5] и обнаружения аномальной деятельности (Anomaly Detection). В обоих случаях речь идёт об обнаружении нелегитимной деятельности авторизованного в системе пользователя. В случае систем обнаружения злоупотреблений используется подход, основанный на шаблонах известных атак (Signature-Based systems), в то время как в системах обнаружения аномальной деятельности строится статистическая модель поведения пользователя (Statistical-Based Intrusion Detection Systems (SBIDS), на основе которой производится анализ его действий.

Одним из наибольших недостатков первого подхода является затруднённое обнаружение новых типов атак и трудность в обновлении параметров модели. В свою очередь, второй подход позволяет хорошо персонифицировать модель и анализировать не подготовленную базу атак, а само поведение пользователя. Однако такой подход намного сложнее в реализации ввиду его трудной формализуемости и неопределённости на этапах настройки, обучения и использования.

Постановка задачи

В данной статье рассматриваются основанные не на шаблонах методы обнаружения аномальной деятельности как более гибкие и потенциально более эффективные [6]. Большинство методов, используемых при построении такого рода систем, ~~имеют в своей основе некую статистическую модель пользователя, которая~~ позволяет оценивать степень аномальности его поведения.

В настоящее время существует большое разнообразие методов построения модели и оценки её эффективности. Основной задачей данной статьи является обзор наиболее часто используемых подходов.

Рассмотрены следующие подходы:

- Трактовка поведения пользователя как сигнала; в таком случае обычное его поведение можно отфильтровать как шум, а аномальное считать сигналом [9].
- Обнаружение вторжений, основанное на использовании агентов [7].
- Обнаружение с использованием онтологий [8].
- Использование иерархических скрытых моделей Маркова [10].
- Построение классификатора действий пользователя на основе моделей Маркова [11].

- Экспериментальная система совмещающая несколько подходов с целью повышения итоговой эффективности обнаружения вторжений.

Поведение пользователя как сигнал

При использовании методов анализа временных рядов в задаче обнаружения аномалий нормальное поведение пользователя трактуется как шум, а аномальное как сигнал (см. рис. 1). Затем используются алгоритмы фильтрации для измерения силы сигнала (аномального поведения). Если уровень сигнала выше некоторой пороговой величины, то соответствующее ему действие объявляется аномальным.

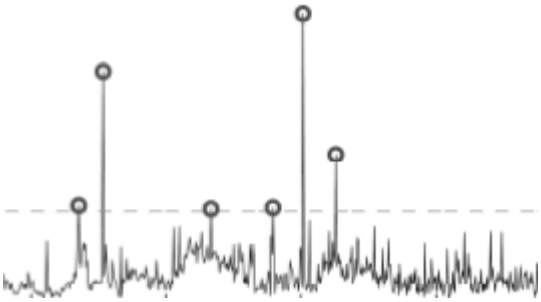

Рис. 1. Аномальное поведение как сигнал

Данный подход позволяет уменьшать количество ложных срабатываний СОВ, так как «нормальное» поведение отфильтровывается и не используется при оценке.

Рассмотренный в [9] алгоритм представляет модель поведения пользователя в виде цепи Маркова (МЦ). Сессия взаимодействия пользователя с системой, состоящая из атомарных действий (шагов), анализируется не целиком, а только её часть – скользящее окно размером ω символов (атомарных транзакций пользователя в системе). Происходит сравнение с уже имеющейся базой примеров нормального поведения. Для каждой транзакции пользователя вычисляется минимальное расстояние Хемминга для всех шагов из базы данных.

Модель поведения пользователя представлена в виде МЦ $M = (S, p)$, для каждого шага вычисляется значение метрики $\alpha \in [0,1]$, обозначающее наличие (или отсутствие) аномалий в поведении. В таком случае стохастическая модель процесса представлена в виде (H, A), где H ω - вектор истории предыдущих шагов, A - значения аномальности. Тогда фильтрация заключается в удалении A из H.

На данный момент показана возможность использования подобного подхода для обнаружения аномальной деятельности. Оценку эффективности и сравнительный анализ авторы планируют провести в будущем.

Иерархические скрытые модели Маркова

Скрытые модели Маркова (СММ) [12] представляет собой Марковскую модель, но имеющую набор неизвестных параметров. В этом случае требуется определить значения неизвестных параметров (вероятностей переходов), основываясь на известных переменных. Подобные структуры часто используются в задачах машинного обучения, к примеру, в распознавании образов.

Иерархическая СММ (ИСММ) является расширением идеи СММ для представления моделей, имеющих иерархическую структуру. ИСММ являются структурированным многоуровневым стохастическим процессом (structured multi-level stochastic process). ИСММ используются для распознавания рукописного ввода [13], визуального распознавания действий [14].

Для более формального определения ИСММ введём следующие термины:

e - конечный набор состояний.

e^* - всевозможные комбинации e.

$q_i^d (d \in \{1,..,D\})$ - состояние с индексом i на уровне d.

$|q_i^d|$: - количество дочерних состояний, для корня можно писать q^d.

В ИСММ переход между состояниями на одном уровне называется горизонтальной транзакцией, между разными - вертикальной транзакцией.

$A^{q^d} = (a_{ij}^{q^d}) : a_{ij}^{q^d} = P(q_j^{d+1} \mid q_i^{d+1})$ - вероятность горизонтальной транзакции из состояния i в j для подмножества узлов q^d.

$\Pi^{q^d} = \{\pi^{q^d}(q_i^{d+1})\} = \{P(q_i^{d+1} \mid q^d)\}$ - вектор начальных вероятностей для подмножества q^d.

$B^{q^D} = \{b^{q^D}(k)\} : b^{q^D}(k) = P(\sigma_k \mid q^D)$ - вероятность того, что состояние q^D выдаст символ $\sigma_k \in e$.

Основываясь на этом, ИСММ можно описать в следующем виде:

$$\lambda = \{\lambda^{q^d}\}_{d \in \{1,..,D\}} = \{\{A^{q^d}\}_{d \in \{1,..,D-1\}}, \{\Pi^{q^d}\}_{d \in \{1,..,D\}}, \{B^{q^D}\}\}$$

На каждом уровне (кроме корневого) существует конечное состояние, после которого процесс переходит в родительское для данного подмножества состояние. Это условие позволяет использовать рекурсивные алгоритмы над ИСММ.

Пример топологии ИСММ приведён на рис. 2.

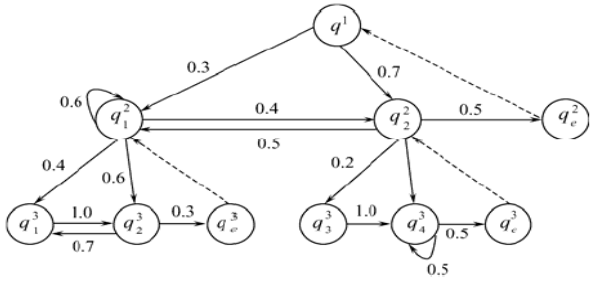

Рис. 2. Топология простой ИСММ

Обнаружение аномалий можно трактовать как задачу иерархического характера. Используемые программы распределены по типу их функциональности, сами программы используют вызовы системных функций с различных уровней.

Важнейшей составляющей алгоритмов, использующих СММ, является вычисление неизвестных характеристик модели, для этого используется алгоритм Баума-Вельша (Baum-Welch) [16].

В [10] показано, что в результате накладываемых на ИСММ ограничений временная сложность для вычисления аномалий на такой сети равняется $O(NT^3)$, где N – количество состояний, T – количество рассматриваемых транзактов на каждом шаге. В то же время подобный алгоритм на СММ имеет сложность $O(N^2T)$.

В качестве примера применения данного подхода к задаче обнаружения вторжений в [12] рассмотрено использование трёхуровневой ИСММ на статистике реальных данных системных вызовов UNIX – сервера университета Нью Мексико (UNM).

На этапе тренировки, используя алгоритм Баума-Вельша, вычисляются значения скрытых параметров модели. Затем, строится база системных вызовов для анализа. На третьем этапе производится тестирование, по тестовым данным проходит скользящее окно – анализатор, возвращающий последовательности данных и вычисляющий для каждой последовательности сходство с тестовой последовательностью O. Вероятность аномалии $P(O|\lambda)$ вычисляется в зависимости от желаемой точности.

По тем же тестовым данным был создан классификатор, использующий простую СММ, и точность анализа сравнивалась с результатами ИСММ. Для того чтобы можно было сравнивать численные данные, была высчитана общая характеристика receiver operating characteristic (ROC).

На рис. 3 представлен график точности определения аномальной деятельности для обоих методов.

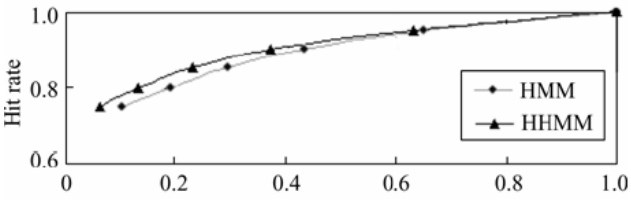

Рис. 3. Сравнение точности СММ и ИСММ

Чем ближе результат к верхнему левому углу графика, тем он точнее. Видно, что на рассматриваемых тестовых данных метод, использующий ИСММ, показал несколько лучшие результаты.

Онтологии в задачах обнаружения аномалий

Большинство попыток классификации типов вторжений в информационные системы создают как результат таксономию атак, распределённых по некоторым признакам. Полученные в итоге таксономии затруднительно использовать в других системах, отличных от той, для которой она была разработана. Данное ограничение нельзя просто обойти, используя таксономии для хранения информации о взаимодействии элементов.

Для предотвращения однотипных разработок по классификации методов и признаков вторжений следует использовать более гибкий инструмент описания, и это *онтологии* [17]. Создание онтологии признаков вторжения позволит использовать её в различных программах (разделение логики системы обнаружения вторжений (СОВ) и модели данных) машинного взаимодействия в автоматическом режиме, то есть программы смогут оперировать терминами этой предметной области без специфической настройки и привлечения экспертов. Также это позволяет создавать распределённые СОВ, когда используется центральная онтология и запросы к ней.

В [4] описана попытка создания подобной онтологии и тестирование её эффективности.

Онтология создана на основе предыдущих исследований, ставящих целью классификацию признаков вторжений. Также использованы язык описания онтологий DARPA [18] и инструменты для работы с построенной моделью DAML-JessKB [19].

При создании рассмотренной онтологии было проанализировано около 4000 различных типов атак на информационные системы. Также были рассмотрены существующие исследования, и некоторые из них включены в качестве составных частей итоговой онтологии.

Основные атрибуты созданной онтологии приведены на рис. 4.

Главными категориями модели являются:

- Системные компоненты (наиболее часто атакуемые). Включают в себя стек сетевых протоколов, операционную систему и приложения.
- Суть атак. Состоит из ошибок валидации введённой информации, переполнения буфера, ошибки обработки граничных значений данных и подобного ввода неожиданной информации.
- Последствия атаки. Как результат атаки отказ в обслуживании, неавторизованный доступ, потеря конфиденциальности данных.
- Положение атаки. Разделение на *внешнее*, *локальное* и *внешне*/*локальное*.

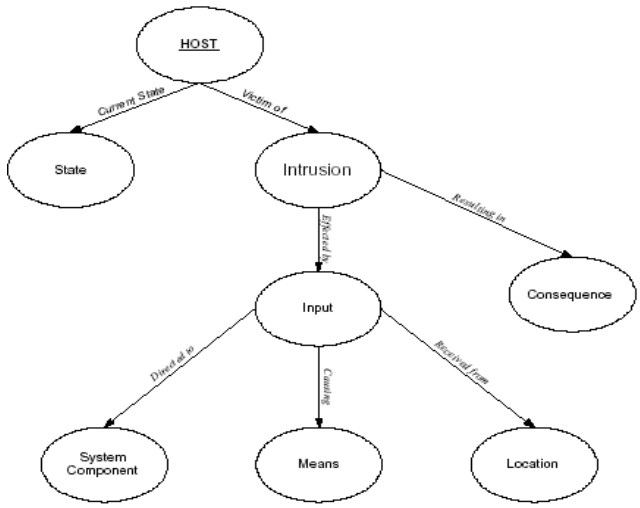

Рис. 4. Верхний уровень абстракции онтологии

Более низкие уровни абстракции содержат всё более детализированное описание его компонент. К примеру, класс Deny of Service имеет дочерние узлы Syn Floods, Mailstorms, Pings of Death, и все остальные основные виды атак типа «Отказ в обслуживании».

В качестве примера используется знаменитая «атака Митника» [20]. Она состоит из нескольких атак на различных уровнях и не может быть комплексно воспринята типичными СОВ, только составляющие. Однако при использовании центральной онтологии используемой СОВ, производящей мониторинг различных уровней, последовательность тревожных сообщений можно объединить в одно специализированное правило для именно такого типа атак.

Агентный подход для обнаружения вторжений

В [7] описан метод обнаружения вторжений в информационную систему, основанный на использовании агентов. Общая структура подхода отображена на рис. 5.

Рассматриваемая система построена на основе открытого инструментария для создания мультиагентных среда COUGAAR [21]. Использование COUGAAR позволило авторам сосредоточиться на основной логике системы, облегчив техническую реализацию агентов и протоколы их взаимодействия.

В основу системы положено взаимодействие 4 агентов, расположенных на различных уровнях системы и совместно выполняющих мониторинг происходящих событий.

- Агент менеджер – является координатором действий остальных агентов. Его основной задачей является управление задачами и потоками данных между остальными агентами. Также, в случае использования распределённой среды, агент менеджер осуществляет общение с агент менеджерами в других узлах.
- Агент решений – несёт ответственность за принятие решений об уровне аномальности текущей анализируемой деятельности. Содержит в себе различные модули анализа, такие как модуль нечёткой логики, классификаторы, база данных. Модуль нечёткой логики используется ввиду того, что зачастую разница между «нормальным» и «подозрительным» поведением не имеет чётких границ и методы работы с нечёткой логикой позволяют значительно уменьшить количество ложных срабатываний.

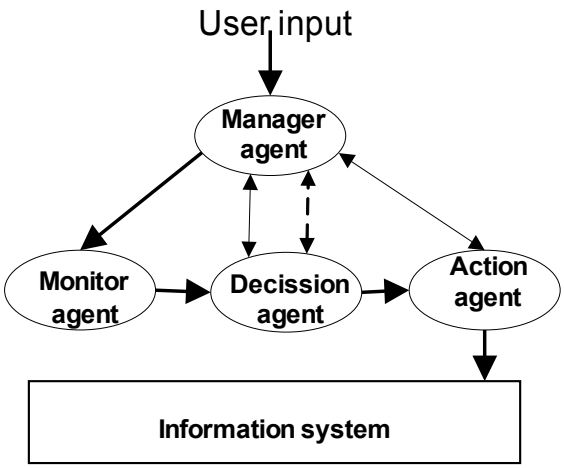

Рис. 5. Общая структура взаимодействия агентов

- Агент действий – сообщает о статусе анализируемой системы с использованием специализированного языка обмена сообщений СОВ (IDMEF – Intrusion Detection Message Exchange Format). Дополнительно агент действий выдаёт свои рекомендации о возможных дальнейших действиях (к примеру, завершить процесс, запретить доступ пользователя к системе, сообщить администрации).
- Агент мониторинга – собирает всю необходимую для анализа агентом решений информацию. Функционирует на всех уровнях

анализируемой системы. Для увеличения эффективности данный агент может использовать специализированный модуль описания текущей предметной области.

Пример использования системы.

1. Пользователь запрашивает некоторую информацию, агент менеджер отсылает её агенту мониторинга на анализ.
2. Агент анализа начинает собирать текущую информацию со всех доступных уровней и анализировать её на предмет наличия в ней отклонения от нормы.
3. Если зафиксировано отклонение от нормы, весь контекст отсылается агенту решений.
4. Агент решений задействует свои модули анализа, такие как модуль нечёткой логики, другие классификаторы для выявления уровня аномальности контекста.
5. Результат анализа отсылается агенту действий, который отсылает своё заключение менеджеру агентов в формате объекта IDMEF.

Данная система была успешно протестирована на нескольких типах тестовых атак и показала хорошие результаты, обнаружив в некоторых тестовых случаях 100% вторжений.

Комплексное применение рассмотренных методов

Дополнительно к рассмотренным выше методам существует интересный пример совместного использования различных технологий интеллектуальной обработки данных [22] в области СОВ.

В рамках создания собственной СОВ (OntoIDPSMA - Ontological Intrusion Detection System and Prevention Multi-agent system) разработчики из колумбийского университета Калдас решили использовать различные технологии на разных этапах анализа текущей ситуации.

Общая структура OntoIDPSMA представлена на Рис. 6. Каждый поступивший TCP пакет проходит несколько стадий анализа с использований различных технологий, и в итоге СОВ выдаёт заключение о возможности его допуска во внутреннюю целевую информационную систему.

Основная часть анализа производится с использования агентного подхода, сходного с рассмотренным выше. Агенты обмениваются информацией в формате IDMEF. Для представления знания о признаках атак и рекомендуемых соответствующих ответных действиях используются онтологии. Общение агентов с онтологиями осуществляются с использованием языка OWL (Web Ontology Language [23]).

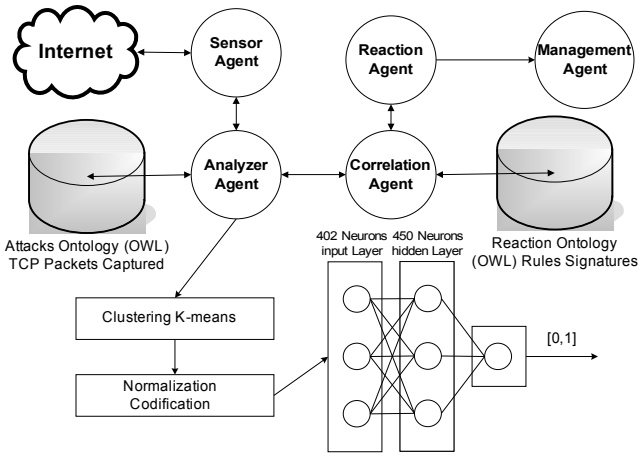

Рисунок 6 Общая структура взаимодействия молулей OntoIDPSMA.

Каждый тип входных данных (заголовки пакетов IP (Internet Protocol), запрошенные порты, данные, типы протоколов и пр.) дополнительно классифицируется с использованием метода К-средних, результат классификации по всем параметрам нормализуется и подаётся на вход нейронной сети, которая окончательно выдаёт результат о наличии аномальности в анализируемом запросе.

Авторы заявляют, что благодаря использованию комплексного подхода подобной структуры эффективность итоговой системы выше, чем у обычных СОВ.

Заключение

В настоящее время темпы роста информационных систем делают всё более затруднительным описательный подход к обнаружению вторжений. Слишком разнообразные возможности воздействия на систему имеют современные программы.

В результате всё более актуальным становится статистический подход к обнаружению вторжений, который позволяет обнаруживать новые типы атак.

Разработаны различные методы построения статистических моделей для анализа состояния системы и поведения пользователя. Однако, ввиду трудной формализуемости данной задачи, не создано подхода, который имел бы явное преимущество над другими и мог использоваться в системах уровня предприятия.

В данной работе рассмотрены некоторые такие методы. Каждый значительно отличается от остальных, имеет свои преимущества и недостатки.

References

1. Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International.
2. Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988.
3. Kohlenberg, Toby (Ed.), Alder, Raven, Carter, Dr. Everett F. (Skip), Jr., Esler, Joel., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, "Snort IDS and IPS Toolkit," Syngress, 2007, ISBN 978-1-59749-099-3.
4. J.Undercoffer, J.Pinkston, A.Joshi, T. Finin. A Target-Centric Ontology for Intrusion Detection // IJCAI-03 Workshop on Ontologies and Distributed Systems, Acapulco, August 9th.
5. Warrender. C, Forrest. S and Pearlmutter. B.: Detecting Intrusion Using System Calls: Alternative Data Models. IEEE Symposium on Security and Privacy, May (1999)
6. G.J.Mun, Y.M.Kim, D.K.Kim, B.N.Noh, Network Intrusion Detection Using Statistical Probability Distribution. M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3981, pp. 340 – 348, 2006.© Springer-Verlag Berlin Heidelberg 2006
7. D.Dasgupta, F.Gonsalez, K.Yallapu, J.Gomez, R.Yarramstetti. CIDS: An agent-based intrusion detection system. Computers & Security, 2005, 24:387- 398.
8. G.Isaza, A.Castillo, M.López, L.Castillo. Towards Ontology-Based Intelligent Model for Intrusion Detection and Prevention. "Computational Intelligence in Security for Information Systems", Springer Berlin Heidelberg - Berlin, Heidelberg, 2009
9. S.Jha, L.Kruger, T.Kurtz, Y.Lee, A.Smith. A Filtering Approach To Anomaly Detection and Masquerade Detection. Technical report, Univ of Wisconsin, Madison.
10. J.Chunfu, Y.Feng. An Intrusion Detection Method Based on Hierarchical Hidden Markov Models. Wuhan University Jornual of Natural Sciences. Vol. 12 No. 1 2007 135-128
11. S. Jha, K. Tan, R.A. Maxion. Markov Chains, Classifiers and Intrusion Detection //Computer Security Foundations Workshop (CSFW), June 2001.
12. L. E. Baum and T. Petrie, "Statistical inference for probabilistic functions of finte state Markov chains," Annls of Mathematical Statistics , 37:1554-1563, 1966.
13. Fine S, Singer Y, Tishby N. The Hierarchical Hidden Markov Model: Analysis and Applications[J]. Machine Learning, 1998, 32(1):41-62.
14. Ivanov Y, Bobick A. Recognition of Visual Activities and Interactions by Stochastic Parsing[J]. IEEE Trans on Pattern Analysis and Machine Intelligence, 2000, 22(8):852-872.
15. Fine S, Singer Y, Tishby N. The Hierarchical Hidden
16. Markov Model: Analysis and Applications[J]. Machine Learning, 1998, 32(1):41-62.
17. Marvin Minsky. Representation: Structuring Knowledge & Data in AI Programs. Association for the Advancement of Artificial Intelligence (AAAI). http://www.aaai.org/AITopics/pmwiki/pmwiki.php/AITopics/Representation
18. DARPA Agent Markup Language+Ontology Interface Layer. http://www.daml.org/2001/03/daml+oil-index 2001.
19. Joe Kopena. DAMLJessKB. http://edge.mcs.drexel.edu/assemblies/software/damljesskb/articles/DAMLJessKB-2002.pdf, October 2002.
20. The Mitnick Case: How Bayes Could Have Helped. IFIP International Federation for Information Processing, 2005, Volume 194/2005, 91-104, DOI: 10.1007/0-387-31163-7_8
21. J. Zinky, R. Shapiro, S. Siracuse and T. Wright. Experience with Dynamic Crosscutting in Cougaar. Lecture Notes in Computer Science, 2010, Volume 4803/2010, 595-612, DOI: 10.1007/978-3-540-76848-7_41
22. Gustavo Isaza, Andrés Castillo, Manuel López and Luis Castillo. Towards Ontology-Based Intelligent Model for Intrusion Detection and Prevention. Advances in Soft Computing, 2009, Volume 63/2009, 109-116, DOI: 10.1007/978-3-642-04091-7_14
23. Grigoris Antoniou and Frank van Harmelen. Web Ontology Language: OWL. Department of Computer Science, University of Crete

About the autors

Pavel Osipov Mg.Sc.Ing. Ph.d. student, Institute of Information Technology, Riga Technical University. He received his masters diploma in Transport and Telecommunications Institute, Riga. His research interests include web data mining, machine learning and knowledge extraction.

Arkady Borisov, Dr.habil.sc.comp.,Professor, Institute of Information Technology, Riga Technical University, 1 Kalku Street, Riga LV-1658 Latvija, e-mail: arkadijs.borisovs@cs.rtu.lv.

Павел Осипов, Аркадий Борисов. Альтернативные основанным на шаблонах методы обнаружения аномального поведения.

В статье рассмотрены основные методы, используемые в задачах обнаружения вторжений в информационные системы. Актуальность именно альтернативных шаблонным методов обусловлена значительным усложнением современной информационной среды, которое не позволяет и дальше эффективно использовать описательный подход к обнаружению вторжений и аномального поведения.
Используя новые интеллектуальные методики, с элементами самообучения и искусственного интеллекта появляется возможность в режиме реального времени отслеживать и реагировать на новые типы атак.
Рассмотрен подход, трактующий нормальное поведение пользователя как шум, а аномальное как сигнал. В таком случае появляется возможность использовать хорошо исследованные алгоритмы обработки и фильтрации сигнала применительно к предметной области обнаружения вторжений.
Рассмотрен подход использующий Скрытые Иерархические Модели Маркова для представления шаблона нормального поведения пользователя. Имея такую модель возможно в дальнейшем использовать её для анализа наличия аномальности для каждого последующего действия пользователя в системе.
Также рассмотрен опыт построения онтологии признаков вторжений, которая позволит автоматизировать обмен знаниями между различными интеллектуальными системами безопасности в будущем.
Кроме этого рассмотрена возможность использования агентного подхода для обнаружения вторжений, приведена общая модель взаимодействия агентов.
В заключении приведён пример создания экспериментальной системы совмещающей на различном уровне мониторинга разные подходы: агентный, онтологии, искусственные нейронные сети и методы классификации.