УДК 004.056.5
ББК 31

МНОЖЕСТВО МИРОВ МНОГОАГЕНТНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК

А.В. Никишова

Предложена многоагентная система обнаружения атак. Внешний мир разбит на множество миров, и агенты разделены на группы, чье представление о внешнем мире ограничено определенным миром из множества.

Ключевые слова: *система обнаружения атак, многоагентная система, агент, множественность миров, совместное решение.*

Как показывает анализ современных свободно распространяемых систем обнаружения атак (СОА), их развитие направлено на сбор данных для анализа из нескольких источников, но при этом в большинстве СОА не учитывается взаимосвязь этих данных. Предлагается модель СОА – многоагентная система (МАС), позволяющая не только анализировать множество источников данных, но и принимать решение на основании всего множества собранных данных о состоянии информационной системы (ИС) в целом.

В.Б. Тарасов дает формализованное определение МАС, не детализируя содержание входящих в формулу составляющих [1]:

$$MAS = (A, E), \qquad (1)$$

где MAS – многоагентная система, A – множество агентов, E – множество миров, находящихся в определенных отношениях и взаимодействующих друг с другом, формирующих некоторую организацию, включая возможные коммуникативные действия.

Был проведен анализ типовой ИС и выделены следующие источники сведений о событиях, происходящих в ИС, подлежащих анализу для задачи обнаружения атак: сведения о событиях маршрутизаторов, сведения о сетевых пакетах, сведения о событиях операционной системы серверов, сведения о события операционных систем рабочих станций. Каждому из этих источников данных соответствует свой тип агента. Было сформировано множество агентов, решающих задачу обнаружения атак:

1) агенты рабочей станции $A_W = \{A_W^L, A_W^R, A_W^P\}$,
   - анализирующие события, отражающиеся в журнале безопасности, A_W^L;
   - анализирующие события, отражающиеся в реестре, A_W^R;
   - анализирующие сведения о процессах, выполняемых на рабочей станции, A_W^P;
2) сетевой агент A_N;
3) агент маршрутизатора A_R;
4) агенты сервера (состав зависит от функционального назначения сервера) A_S.

Так как многоагентная СОА содержит большое число агентов, то их взаимодействие каждый с каждым будет иметь существенное влияние на загруженность сети. А потому в модели используется концепция «множественности миров». Все пространство ИС разбивается на миры, которые ограничивают функционирование и взаимодействие агентов. Каждый агент может принадлежать нескольким мирам. В результате анализа было сформулировано следующее множество миров:

- миры $M_W \subset A_W$, включающие в себя агентов рабочей станции. Анализируя события соответствующего источника, агенты рабочей станции $A_W = \{A_W^L, A_W^R, A_W^P\}$

принимают совместное решение о состоянии рабочей станции;

- миры $M_{NS} \subset A'_W$, A_N, включающие в себя агентов сегмента сети. В этот мир имеют доступ по одному агенту с каждой рабочей станции A'_W (он обладает объединенным мнением о состоянии рабочей станции) и сетевой агент A_N соответствующего сегмента сети. Данная группа агентов принимает совместное решение о состоянии сегмента сети;
- миры $M_N \subset A_R$, A_N, включающие в себя агентов подсети. В этот мир имеет доступ агент маршрутизатора A_R и сетевые агенты A_N (они обладают объединенным мнением о состоянии соответствующего сегмента сети), сегмент сети которых соединен с данным маршрутизатором. Данная группа агентов принимает совместное решение о состоянии подсети, ограниченной данным маршрутизатором;
- миры $M_S \subset A_S$, включающие в себя агентов сервера. Анализируя события соответствующего источника, агенты сервера A_S принимают совместное решение о состоянии сервера;
- мир $M_{IS} \subset A'_S$, A_R, в котором принимается окончательное решение о состоянии ИС. Данное решение принимают по одному агенту от каждого сервера A'_S (они обладают объединенным мнением о состоянии соответствующего сервера) и агенты маршрутизаторов A_R (они обладают объединенным мнением о состоянии соответствующей подсети). Они принимают совместное решение об общем состоянии ИС.

Учитывая возможные пути реализации многошаговых и распределенных атак, агенты взаимодействуют между собой внутри определенных миров. Они путем голосования [2] принимают совместное решение о состоянии частей ИС, а в итоге о состоянии ИС в целом, то есть решение о возникновении или невозникновении атаки.

При принятии решения об обнаружении атаки агенты системы в соответствии с настройками, выполненными администратором, могут выполнять некоторые элементарные действия, например разрыв соединения или уничтожение процесса.

СПИСОК ЛИТЕРАТУРЫ

1. Тарасов, В. Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика / В. Б. Тарасов. – М. : Эдиториал УРСС, 2002. – 352 с.

2. Shoham, Y. Multiagent systems. Algorithmic, game-theoretic, and logic foundations / Y. Shoham, K. Leyton-Brown. – N. Y. : Cambridge University Press, 2009. – С. 256–260.

MULTIAGENT INTRUSION DETECTION SYSTEM'S SET OF WORLDS

A.V. Nikishova

Multi-agent intrusion detection system has been suggested. Outside world has been divided into set of worlds, and agents have been divided into groups with their beliefs about outside world limited to certain world of the set.

Key words: *intrusion detection system, multi-agent system, agent, multiplicity of worlds, joint resolution.*