УДК 621.391

Лівенцев С.П., Сторчак А.С.

ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ МЕТОДІВ ІНДУКТИВНОГО ПРОГНОЗУВАННЯ СТАНІВ

Анотація:

Розглядається задача виявлення комп'ютерних атак на ІТС. Показано, що вона зводиться до вирішення комбінаторних завдань, пов'язаних з розгалуженням вирішальних процесів, з перебором варіантів, число яких швидко зростає при ускладненні системи закономірностей.

Аннотация:

Рассматривается задача обнаружения компьютерных атак на ИТС. Показано, что она сводится к решению комбинаторных задач, связанных с ветвлением решающих процессов, с перебором вариантов, число которых быстро растет при усложнении системы закономерностей.

Abstract:

The problem of acquisition of computer attacks is considered. It is demonstrated that it is a solution of combinatorial problems, and their solution is bound to fork of solving processes, with search of alternatives that grows fast at thickening of system of regularities.

Вступ

Національна безпека держави значним чином залежить від забезпечення інформаційної безпеки. При цьому, актуальність створення надійних систем виявлення комп'ютерних атак на інформаційно-телекомунікаційні системи (ІТС) та протидії комп'ютерному нападу випливає з Закону України "Про основи національної безпеки", Доктрини інформаційної безпеки України та вимог інших нормативних документів [1-4].

Виявлення комп'ютерних атак на ІТС є одним із завдань, вирішення якого дозволить підвищити захищеність ІТС в процесі їх функціонування і розвитку.

Розв'язанню загальних проблем виявлення комп'ютерних атак присвячено роботи вітчизняних та зарубіжних авторів, таких як М.П. Комар, К.Е. Бєлов, В.С. Цимбалюк, В.И. Городецький, Д. Денніг, Д. Андерсон та інших.

Методики, методи та алгоритми виявлення комп'ютерних атак на ІТС, що використовуються в даний час не повною мірою вирішують протиріччя між збільшенням часу на виявлення комп'ютерних атак існуючими методами за рахунок збільшення часу аналізу ознак атак з одного боку, і збільшенням часу, який відводиться на аналіз ознак атак, що призводить до зростання ймовірності пропуску атаки з іншого боку [5].

Метою статті є обґрунтування методу індуктивного прогнозування станів для виявлення комп'ютерних атак на ІТС.

Основна частина

Атакою є спроба реалізації загрози [3]. Комп'ютерної атакою на ІТС вважаються дії, спрямовані на реалізацію загроз несанкціонованого доступу до інформації, впливу на неї або на ресурси ІТС із застосуванням програмних або технічних засобів.

Здійснення комп'ютерної атаки відбувається при наявності точок несанкціонованого доступу до інформаційних ресурсів та комунікаційного обладнання ІТС або при наявності потенційного внутрішнього порушника з повноваженнями штатного оператора в територіально-розподіленій обчислювальній мережі.

Наслідками впливів комп'ютерних атак можуть стати блокування керуючої інформації та впровадження неправдивої інформації, порушення встановлених правил збору, обробки і передачі інформації в комплексах засобів автоматизації, відмови і збої в роботі ІТС, а також компрометація одержуваної споживачами інформації [7].

Процес виявлення комп'ютерних атак починається зі збору даних, необхідних для визначення факту атаки на ІТС [7]. Зокрема, можна аналізувати відомості про пакети даних, що надходять в ІТС, продуктивність програмно-апаратних засобів (обчислювальне навантаження на хости, завантаженість оперативної пам'яті, швидкість роботи прикладного ПЗ), відомості про доступ до певних файлів системи тощо.

Для збору вихідної інформації традиційно використовують спеціалізовані датчики, що розміщуються на різних елементах ІТС. Існують два типи таких датчиків – мережеві та хостові. Аналіз даних, зібраних мережевими і хостовими датчиками, проводиться в ІТС з використанням спеціальних методів виявлення атак.

Ефективність виявлення комп'ютерних атак багато в чому залежить від застосовуваних методів отримання інформації. У перших системах виявлення комп'ютерних атак, розроблених у 80-х роках, використовувалися статистичні методи виявлення атак. На цей час до статистичного аналізу додався ряд нових методик застосування інтелектуальних систем виявлення атак, в яких використовуються нейронні мережі, системи нечіткої логіки та експертні системи [7].

Процес навчання із застосуванням нейромережних технологій починається з пред'явлення системі набору навчальних прикладів, що складаються з вхідних і вихідних сигналів. Потім нейронна мережа автоматично підлаштовує свої синоптичні ваги таким чином, що при подальшому пред'явленні вхідних сигналів на виході з’являються необхідні сигнали. Недоліками даного підходу є: складність побудови; труднощі підбору навчальної вибірки, що адекватно описує предметну область; тривалий період навчання; незрозумілість результатів; нестача адекватного навчального матеріалу [8].

Зазначені недоліки відсутні в системах на основі баз знань, що використовують для навчання логічний висновок (ЛВ). При цьому під здатністю до навчання розуміється можливість створення бази знань, а також поповнення і модифікація правил в базі знань під впливом знову отриманої інформації [9].

Більшість сучасних інтелектуальних систем, що використовують ЛВ, дозволяє модифікувати базу знань тільки в ручному режимі. Відомі методи формування знань (або методи машинного навчання), що дозволяють автоматично змінювати базу знань, засновані на застосуванні індуктивного ЛВ [9]. Індукція передбачає наявність достатньо представницької вибірки навчальних прикладів, що узагальнюється за допомогою згенерованих правил.

Перспективним методом виявлення комп'ютерних атак на ІТС є технологія виявлення комп'ютерних атак на основі методу індуктивного прогнозування станів [6].

У [9] пропонується процес розпізнавання ознак об'єкта розділити на два етапи: навчання та власне розпізнавання. Перший етап – індуктивний, другий – дедуктивний. На першому з них обробляються дані численних спостережень над досліджуваним класом об'єктів і на основі отриманих результатів будується деяке вирішальне правило. На другому етапі описане правило застосовується для розпізнавання властивостей інших об'єктів цього ж класу, які цікавлять нас, але безпосередньо не вимірюються.

Розглянемо множину об'єктів і позначимо її через U, вважаючи, що вона складається з окремих елементів, що позначаються через u_2: $U=\{u_1, u_2, \ldots, u_m\}$.Множину всіх ознак, що використовуються при описі цих об'єктів, позначимо через $S=\{s_1, s_2, \ldots, s_m\}$. Множину всіх об'єктів, що володіють деякою конкретною ознакою s_j, позначимо через U_j, називаючи її класом з ознакою s_j, а її доповнення, тобто безліч всіх об'єктів, що не володіють ознакою s_j, – через $\overline{U_j}$.

Наприклад, U може представляти адреси джерела IP-датаграми, що збираються мережевими датчиками для аудиту, $s_1, s_2, \ldots, s_m$ – такі ознаки, як октети діапазону адрес: 192.168.1.16. U_3 – множина всіх дозволених адрес джерела IP-датаграми, що містяться в третьому октеті, $\overline{U_3}$ – безліч не дозволених адрес джерела IP-датаграми, що містяться в третьому октеті.

При дослідженні реальних об'єктів потужність множини U, тобто число елементів у ній, виявляється зазвичай дуже великим, і, як правило, відома лише мала його частина. Припустимо, що нам доступна вся інформація про цю множину і вдалося описати кожен її елемент, перерахувавши ознаки, якими останній володіє, наприклад, у вигляді u_1 - (s_1, s_2, s_4). Це означає, що об'єкт являє собою комбінацію ознак s_1, s_2, і s_4, тобто володіє цими ознаками і ніякими іншими. Доступну інформацію можна уявити інакше – рядком з нулів та одиниць – булевим вектором. Символи рядка відповідають ознакам $s_1, s_2, \ldots$ і виходить, що, якщо об'єкт ознаки має – «1», не має – «0».

Наприклад, опис u_1 - (s_1, s_2, s_4) можна замінити на вектор: [1101] (в даному випадку число ознак обмежено чотирма; при більшому їх числі вектор доповнюється нулями).

Користуючись такими засобами, можна представити множину U в цілому. Для цього слід розташувати один під одним булеві вектори; представляючи послідовно об'єкти u_1, u_2 і т. д., отримати булеву (з нулів і одиниць) матрицю. Позначимо її через R. Матриця містить у зручній для огляду формі інформацію про ставлення приналежності ознак об'єктів: якщо об'єкт U_j має ознаку s_j, то на перетині i-го рядка і j-го стовпця ставиться «1», в іншому випадку – «0».

При великих обмеженнях на вимірювальні засоби індивідуальність об'єктів може бути втрачена. Тоді окремі рядки матриці R будуть служити вже не моделями якихось одиничних об'єктів, а представляти їх цілими групами, кажучи про те, що в множині U існують об'єкти із заданими комбінаціями ознак:

$$R = \begin{matrix} a & b & c & d & \\ \end{matrix} \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \end{matrix}.$$

Рядками матриці є групи об'єктів, нерозпізнаних в даній системі ознак. Стовпці задають класи.

Множина всіх таких комбінацій булевих векторів утворює так званий булевий простір M. Множина U допустимих комбінацій є підмножиною з $U \subseteq M$. Назвемо цю підмножину областю існування об'єктів досліджуваного класу, а її доповнення $\overline{U} = M \setminus U$ – областю заборони, оскільки дана множина утворюється забороненими ознаками.

Таким чином, знання навіть одного елемента множини заборони $\overline{U}$, тобто інформація про те, що деякий об'єкт не існує, дозволяє іноді вирішити задачу

розпізнавання, в той час, як аналогічні відомості про існування деякого об'єкту виявляються недостатніми для цього. Тому формулювання закономірностей, що дозволяють вирішити завдання розпізнавання ознак комп'ютерних атак, будемо пов'язувати із заборонами, тобто забороною на деякі комбінації ознак, що дозволить здійснювати не весь перебір можливих ознак атак в базі даних, а обмежитися скороченим перебором.

При використанні методу індуктивного прогнозування станів комп'ютерна атака розглядається як послідовність дій, що призводять систему з початкового стану в скомпрометований (кінцевий) стан. Таким чином, атака моделюється як множина станів і переходів між ними. Стан системи розглядається як набір змінних, що описують об'єкти, представлених в сигнатурі атаки. Початковий стан асоціюється зі станом до виконання атаки, а скомпрометований стан відповідає стану після закінчення атаки. Переходи із стану в стан асоціюються з новими подіями в системі, що впливають на виконання сценарію атаки. Типи допустимих подій (станів системи) зберігаються в базі даних. Між початковим і скомпрометованим станами існує безліч переходів.

Такий спосіб дозволяє:

описати атаку більш абстрактно, ніж на рівні системних викликів, і більш точно, ніж з використанням неформального текстового опису;

виділити основні події в ході виконання атаки.

Ключові фактори застосовності методу індуктивного прогнозування станів – такі:

у зв'язку зі збільшенням кількості параметрів (ознак) атаки, що враховуються в моделі аналізу станів, використовується метод індуктивного виводу, заснований на розпізнаванні ознак атак, пов'язаних із заборонами, тобто забороною на деякі комбінації ознак, що дозволить здійснювати не весь перебір можливих ознак атак в базі даних, а обмежитися скороченим перебором;

індукція передбачає наявність досить представницької вибірки навчальних прикладів, які узагальнюється за допомогою згенерованих правил, що дозволяє модифікувати базу знань системи виявлення атак на ІТС в автоматичному режимі та формувати нові правила і видаляти старі;

скомпрометований стан має бути розпізнано без використання зовнішніх знань про наміри порушника.

Висновок

Таким чином, завдання виявлення комп'ютерних атак на ІТС зводяться до вирішення комбінаторних завдань, пов'язаних з розгалуженням вирішальних процесів, з перебором варіантів, число яких швидко зростає при ускладненні системи закономірностей. Такий перебір неминучий, але його можна скорочувати до прийнятної величини, що дозволяє вирішувати завдання виявлення комп'ютерних атак на ІТС. Застосування індуктивного прогнозування станів дозволить модифікувати базу знань системи виявлення атак на ІТС в автоматичному режимі, формувати нові правила і видаляти старі.

Література:

1. *Закон України* “Про основи національної безпеки” [Електронний ресурс]. – Режим доступу : http:// www.rada.gov.ua.

2. *Указ Президента України* № 514/2009 “Про Доктрину інформаційної безпеки України” [Електронний ресурс]. – Режим доступу : http:// www.rada.gov.ua.

3. *НД ТЗІ 1.1-003-9* Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua

4. *НД ТЗІ 2.5-004-99* Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: http://www.dstszi.gov.ua

5. *Анализ* существующих методов обнаружения удаленных сетевых атак. Перспективы развития средств и комплексов связи. Подготовка специалистов связи : Материалы межвузовской научной конференции. В 2 ч. Ч. 2 / Новочеркасское высшее военное командное училище связи. – Новочеркасск, 2009. – С. 56-61.

6. *Шангин В.Ф.* Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шангин – М.: ДМК Пресс, 2010. – 544 с.

7. *Лаптев В.Н.* Применение метода индуктивного прогнозирования состояний для обнаружения компьютерных атак в информационно-телекоммуникационных системах / Лаптев В.Н., Сидельников О.В., Шарай В.А. // Научный журнал КубГАУ. – 2011. –№ 72(08).

8. *Котельников Е.В.* Абдуктивный метод модификации посылок в исчислении высказываний / Е.В. Котельников // Вестник Вятского научного центра Верхне-Волжского отделения Академии технологических наук Российской Федерации. Серия: Проблемы обработки информации. – 2006. – № 1. – С. 18-28.

9. *Закревский А.Д.* Логика распознавания. / А.Д. Закревский. – М. : Эдиториал УРСС, 2003. – 200. – 144 с.