Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Воробьев Антон Александрович
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Факультет компьютерных технологий,
каф. Информационной безопасности автоматизированных систем (ИБАС)
Аспирант каф. ИБАС
Vorobev Anton Alexandrovich
«Komsomolsk-on-Amur state technical University», faculty of computer technologies
Post-graduate student of Department of information security of automated systems
E-Mail: zeromem@mail.ru

Анализ уязвимостей вычислительных систем на основе алгебраических структур и потоков данных National Vulnerability Database

Vulnerability analysis of computer systems based on algebraic structures and National Vulnerability Database data flows

Аннотация: Данная работа является продолжением исследований в области анализа уязвимостей вычислительных систем. В ней применен аппарат булевых алгебр с целью разработки математической модели описания уязвимостей из элементов источника данных NVD при использовании классификации на основе концепции измерений. Для разработанной булевой алгебры уязвимости предложена квазимера, доказано, что она является мерой с точки зрения теории меры. Показано, что предлагаемая алгебраическая структура также является алгеброй событий.

Abstract: This work is a sequel of the studies in the analysis of vulnerabilities in computer systems. It applied boolean algebras to develop a mathematical model describing the exploits of the NVD data source when using the classification based on the concept of measurement. Quasimeasure has been offered for the boolean algebra, proved that she is a measure from the point of view of measure theory. Shows that the algebraic structure is also algebra of events.

Ключевые слова: Булева алгебра; уязвимость; защита информации; таксономия; мера; квазимера; алгебра событий.

Keywords: Boolean algebra; vulnerability; protection of information; taxonomy; National Vulnerability Database; measure; quasimeasure; algebra of events.

***

Введение

Анализ уязвимостей локальных вычислительных сетей предприятий и их оценка является важнейшим направлением в области защиты информации. При анализе существующих корпоративных сетей, исследователи неизбежно сталкиваются с необходимостью классификации уязвимостей, а также возможных атак с целью разработки математической модели для оценки и контроля показателей защищенности исследуемой сети. Ряд зарубежных исследователей [1,2,3,4,5,6,7] предлагают различные варианты классификаций (таксономий), каждая из которых имеет свои преимущества в определенных условиях. Однако, их сопряжение с существующими открытыми базами данных уязвимостей, таких как National Vulnerability Database(NVD)[8], делают их малопригодными или сложными в прикладном анализе уязвимостей корпоративных сетей. Данная работа предоставляет алгоритм соответствия между открытыми базами данных уязвимостей на примере NVD и совокупностью классификаций, основанных на концепции измерений.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Классификации уязвимостей в концепции измерений

В 1995 году, Бишоп[6] предложил классификацию уязвимостей для UNIX-систем. Отличительной особенностью его работы было создание принципиально новый схемы классификации. Шесть «осей координат» включали в себя[3,6]:

1. Природа уязвимости – описывает природу ошибки в категориях протекционного анализа;
2. Время появления уязвимости;
3. Область применения – что может быть получено через уязвимость;
4. Область воздействия – на что может повлиять уязвимость;
5. Минимальное количество – минимальное количество компонент, необходимых для атаки;
6. Источник – источник идентификации уязвимости.

Интересной особенностью классификации Бишопа было использование подхода на основе концепции измерений, вместо табличных и древовидных классификаций. Располагая на координатных осях классификационные группы, и отсчитывая по первым элементы групп, Бишоп предложил схему, которую именуют схемой классификации уязвимостей в концепции измерений.

Хадсон и Хант, в своей работе о таксономии сетевых и компьютерных атак[3], расширили возможности схемы классификации Бишопа, путем применения следующей методики трансформации древовидной иерархии: элементами оси при древовидной иерархии классификации являются листья дерева.

Алгебра уязвимостей

В работе [9], автором была предоставлена математическая модель описания предложенных классификаций уязвимостей в концепции измерений в виде булевой алгебры[10] уязвимостей.

Пусть $\{X_i\}$ – конечное семейство классов характеристик уязвимостей, откладываемых на координатных осях некоторого пространства $G, i \in [1;n], n \in N.$ Известно, что мощность каждой компоненты $\#X_i = m_i$. Некоторая произвольная уязвимость $a \in G$ описывается как совокупность

$$a = \{\alpha_1, \alpha_2, ..., \alpha_n\}, \alpha_i \subseteq X_i,$$

$$G = 2^{X_1} \times 2^{X_2} \times ... \times 2^{X_n},$$

$$0_G = \{\varnothing, \varnothing, ..., \varnothing\}_n,$$

$$1_G = \{X_1, X_2, ..., X_n\},$$

$$\overline{a} = \{\overline{\alpha_1}, \overline{\alpha_2}, ..., \overline{\alpha_n}\}.$$

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Введем операцию сложения и умножения на множестве *G*:

Сложение: $\forall a \in G \forall b \in G : a \oplus b = \left\{ \alpha_1^{(a)} \cup \alpha_1^{(b)}, \alpha_2^{(a)} \cup \alpha_2^{(b)}, ..., \alpha_n^{(a)} \cup \alpha_n^{(b)} \right\}$.

Умножение: $\forall a \in G \forall b \in G : a \otimes b = \left\{ \alpha_1^{(a)} \cap \alpha_1^{(b)}, \alpha_2^{(a)} \cap \alpha_2^{(b)}, ..., \alpha_n^{(a)} \cap \alpha_n^{(b)} \right\}$.

Теорема 1: Совокупность $\left\langle G, \oplus, \otimes, 0_G, 1_G, \bar{} \right\rangle$ - булева алгебра.

Доказательство в [9].

National Vulnerability Database

National Vulnerability Database [8] – это стандартизированная база данных обнаруженных уязвимостей. Непосредственное взаимодействие с базой данных выполняется по протоколу SCAP (Security Content Automation Protocol). Выделим необходимые компоненты данного протокола:

- CVE (Common Vulnerabilities and Exposures) – система ссылок и обозначений уязвимостей и ошибок;
- CPE (Common Platform Enumeration) – совокупность стандарта и словаря для инвентаризации программно-аппаратного обеспечения;
- CVSS (Common Vulnerabilities Scoring System) – система оценки уязвимостей.

На момент написания данной работы, база данных содержит более 55 тысяч уязвимостей в 70 тысячах программных продуктов.

Основная задача NVD – предоставление доступа к информации об уязвимостях для автоматизации процессов управления уязвимостями, а также оценки и контроля защищенности объектов информатизации.

Компоненты протокола SCAP реализованы в виде набора словарей, каждый из которых представлен одним или несколькими XML(extensible markup language – расширяемый язык разметки) документами. Структура XML документа описана в соответствующих файлах XSD (язык описания структуры XML документа).

Ядро структуры документа CPE представляет тег «*cpe-list*», внутри которого описание каждого программного обеспечения заключено тегом «*cpe-item*». Важнейшим атрибутом тега «*cpe-item*» является атрибут «*name*», однозначно определяющий позицию элемента в словаре. Для примера, приведем описания нескольких элементов данного словаря.

```
<cpe-item name="cpe:/o:conectiva:linux">
<title xml:lang="en-US">Conectiva Linux</title>
<meta:item-metadata modification-date="2007-09-19T16:35:27.380-04:00"
status="DRAFT" nvd-id="68014" />
</cpe-item>
<cpe-item name="cpe:/o:conectiva:linux:1.0.0">
<title xml:lang="en-US">Conectiva Conectiva Linux 1.0.0</title>
<meta:item-metadata modification-date="2008-04-01T10:41:53.323-04:00"
status="DRAFT" nvd-id="22260" />
</cpe-item>
```

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Как видно из примера, атрибут «name» имеет тип, производный от базового типа «*xsd:anyURI*», и, в соответствии со схемой, должен удовлетворять регулярному выражению «*[c][pP][eE]:/[AHOaho]?(:[A-Za-z0-9\._\-~%]*){0,6}*»

Система CVE – представляет справочно-поисковую систему ссылок и обозначений обнаруженных уязвимостей для общественности. Важной составляющей данной системы являются CVE идентификаторы (CVE-IDs), - уникальные идентификаторы, присваиваемые каждой известной уязвимости из области информационной безопасности. Протокол SCAP использует систему идентификаторов CVE с целью обозначения ссылки на отдельную уязвимость.

Система оценки CVSS 2.0 предоставляет повторно воспроизводимый способ единообразного вычисления и выражения рисков, ассоциированных с данной программной уязвимостью (например, с CVE). Совместное использование данной модели количественной оценки предоставляет возможность сравнения уязвимостей в соответствии со шкалой тяжести. CVSS состоит из трех совокупностей метрик, определяющих группы, каждая из которых может использоваться для вычисления значения тяжести заданной уязвимости, а именно:

- Базовые – используют внутренние особенности уязвимости для вычисления универсального значения тяжести;
- Временные – охватывают внешние факторы, которые могут изменяться с течением времени (например, доступность кода эксплоита уязвимости). Для отражения временного значения тяжести, используется преобразование универсального значения тяжести с учетом временных факторов;
- Экзогенные – характеризуют тяжесть уязвимости в контексте операционной среды организации.

Цель проведения оценок по метрикам CVSS в том, чтобы помочь организациям осознать относительную важность различных уязвимостей для эффективной оценки и сдерживания. Вследствие того, что сотни уязвимостей публично анонсируются каждую неделю, крайне важно иметь простой способ определения тех из них, что представляют наибольшую опасность. Значения тяжести по метрикам CVSS измеряются по шкале от 0 до 10 с шагом в одну десятую.

Аналитики NVD вычисляют и публикуют базовые значения тяжести для каждой записи об уязвимости в CVE, а организации, по своему усмотрению, могут дополнительно использовать базовое значение тяжести для определения временных и экзогенных метрик с целью детальной оценки риска относительно специфики своей организации, представляемого некоторой уязвимостью. Аналитика NVD публично доступна на сайте Национального Института Стандартов и Технологий.

Математическая модель уязвимостей на основе потоков данных NVD

В данной работе, математическая модель уязвимостей базируется на булевой алгебре уязвимостей.

Пусть совокупность $CPI = \langle n, t, i, c, w \rangle$ представляет описание некоторой уязвимости из потока данных NVD, где

n - идентификатор программно-аппаратного продукта, удовлетворяющий спецификации CPE, и представленный в виде CPE-URI;

t - дата последней модификации информации о программно-аппаратном продукте;

i - внутренний идентификатор NVD;

c - уникальный идентификатор уязвимости CVE-ID;

w - идентификатор описания вида ошибки для программно-аппаратного продукта CWE-ID в соответствии с классификатором Common Weakness Enumeration.

Тогда множество всех уязвимостей потоков данных NVD представляется множеством $I = \{CPI_i\}$, где $i \in Q$ - индексное множество для анализируемых записей потоков данных NVD. Определим классы характеристик X_i

Пусть классы характеристик X_i, $i \in \overline{1,5}$ определены, как

$$X_1 = \left\{ l \mid \exists k \in I_{i^{(n)}}^{(n)}, k = l \right\} \cup \{\varnothing\},$$

$$X_2 = \left\{ l \mid \exists k \in I_{i^{(c)}}^{(c)}, k = l \right\} \cup \{\varnothing\},$$

$$X_3 = \left\{ l \mid \exists k \in I_{i^{(w)}}^{(w)}, k = l \right\} \cup \{\varnothing\},$$

$$X_4 = \left\{ l \mid \exists k \in I_{i^{(i)}}^{(i)}, k = l \right\} \cup \{\varnothing\},$$

$$X_5 = \left\{ l \mid \exists k \in I_{i^{(t)}}^{(t)}, k = l \right\} \cup \{\varnothing\},$$

где $I_{i^{(p)}}^{(p)}$ - множество всех элементов компоненты $p = \{n,t,i,c,w\}$ совокупности CPI.

Тогда в соответствии с теоремой 1, совокупность $B = \left\langle G, \oplus, \otimes, 0_G, 1_G, \bar{} \right\rangle$ - булева алгебра, где пространство алгебры

$$G = 2^{X_1} \times 2^{X_2} \times 2^{X_3} \times 2^{X_4} \times 2^{X_5}.$$

Введем отношение частичного порядка на множестве I. Отображение

$$S : I \to T = \langle I, \rho \rangle$$

представляет упорядоченную двойку (кортеж) элементов, где

ρ – отношение естественного частичного порядка, такое, что

$$\forall z_1, z_2 \in I : z_1 \rho z_2 \Leftrightarrow z_1^t \le z_2^t.$$

В качестве количественной оценки уязвимости по номеру CVE-ID, примем M - функционал координаты $\mathrm{Pr}_2 T$, такой, что

$$M : \left(\mathrm{Pr}_2 T\right)^c \to [0;\alpha] \in R.$$

Рассмотрим вещественную функцию $\mu(x)$

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

$$\mu(x)=\frac{M[x]}{\#Q}=\frac{M\left[\left\langle\{x_1,x_5,x_4,x_2,x_3\},\rho\right\rangle\right]}{\#Q},$$

где

$$M[x]=0\Leftrightarrow x=0_G,$$

$$Q=\langle X_1,X_2,X_3,X_4,X_5\rangle.$$

Теорема 2. Вещественная функция $\mu(x)$ - квазимера.

Вещественная функция $\mu(x)$, заданная на булевой алгебре B, является квазимерой, если $\mu(x)$ аддитивна и все ее значения неотрицательны.

Вещественная функция $\mu(x)$, заданная на булевой алгебре B, называется аддитивной, если для любой конечной дизъюнктной системы E элементов B выполняется равенство:

$$\mu\left(\underset{x\in E}{\vee}x\right)=\sum_{x\in E}\mu(x). \quad (1)$$

Алгебры вида 2^Q [10] представимы в виде дизъюнктного разложения прямых сумм главных идеалов, которые соответствуют точкам $q\in Q$. Действительно, каждый элемент множества $q\in Q$ вложен в алгебру 2^Q нормально, так как Q непусто и из

$$\forall\alpha\in Q, x\le\alpha\Rightarrow x\in Q,$$

где отношение является отношением частичного порядка по естественному включению, а следовательно

$$Q_u=\left\{\{q_1\},\{q_2\},...,\{q_{\#Q}\},\varnothing\right\}, q_i\in Q$$

является главным идеалом по определению.

Более того, главный идеал Q_u является компонентой, так как по свойствам дизъюнктных дополнений

$$(Q_u)^d=Q_{\neg u},$$

$$\left((Q_u)^d\right)^d=(Q_{\neg u})^d=Q_{\neg\neg u}=Q_u.$$

Зафиксируем произвольное подмножество $E\subset Q_u$ - некоторое дизъюнктное подмножество. Имеем

$$\mu\left(\underset{q\in E}{\vee}q\right)=\sum_{q\in E}\frac{M[q]}{\#Q} \quad (2)$$

Покажем, что (2) является квазимерой относительно формулировки (1).

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

В качестве базиса индукции примем

$$E = \{\{q_1\},\{q_2\}\},$$

$$\mu(\{q_1\} \vee \{q_2\}) = \frac{M[q_1]}{\#Q} + \frac{M[q_2]}{\#Q} .$$

Предположим, что утверждение верно для

$$E = \{\{q_1\},\{q_2\},...,\{q_n\}\}.$$

Покажем, что утверждение верно и для

$$E = \{\{q_1\},\{q_2\},...,\{q_n\},\{q_{n+1}\}\}.$$

Действительно,

$$\mu\left(\underset{q\in E}{\vee} q\right) = \frac{M[q_1]}{\#Q} + \frac{M[q_2]}{\#Q} + ... + \frac{M[q_n]}{\#Q} + \frac{M[q_{n+1}]}{\#Q} = \sum_{q\in E}\frac{M[q]}{\#Q},$$

что и требовалось доказать.

Покажем, что квазимера $\mu(x)$ является счетно-аддитивной существенно положительной на алгебре B.

Утверждение 1. Квазимера $\mu(x)$ счетно-аддитивна.

Действительно, так как множество Q - счетно, следовательно равенство $\mu\left(\underset{x\in E}{\vee} x\right) = \sum_{x\in E}\mu(x)$

выполняется для любого не более чем счетного дизъюнктного множества E, что и требовалось доказать.

Утверждение 2. Квазимера $\mu(x)$ существенно положительна.

Пусть существует некоторое дизъюнктное разложение $E \subset Q_u$, такое, что

$$\mu\left(\underset{q\in E}{\vee} q\right) = 0.$$

Так как $\#Q > 0$, следовательно

$$\sum_{q\in E}\frac{M[q]}{\#Q} = \sum_{q\in E} M[q] = 0. \qquad (3)$$

Заметим, что из (3) следует

$$\sum_{q\in E}\frac{M[q]}{\#Q} = M[0_G] = 0$$

в силу неотрицательности отображения M и построения главного идеала Q_u. Следовательно, квазимера $\mu(x)$ является существенно положительной по определению, что

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

и требовалось доказать.

Более того, так как мерой[11] булевой алгебры B по определению является вполне аддитивная существенно положительная квазимера, то $\mu(x)$ является мерой на B. Действительно, множество Q счетно по построению, из чего следует эквивалентность определений вполне аддитивной и счетно-аддитивной функции на булевой алгебре B.

Известно, что булевые алгебры имеют тесную связь с различными математическими разделами. Покажем, что предлагаемая автором алгебраическая структура является алгеброй событий с пространством элементарных исходов Q. Действительно, на B выполнимы свойства:

1. $Q \in B$. Очевидно, не требует доказательства.
2. $\forall x \in B \Rightarrow \bar{x} \in B.$ Пусть это не так. Следовательно, $\exists y \mid y = \bar{x}, y \notin B.$ Значит булева алгебра B не является решеткой, что невозможно по определению.
3. $\forall x \in B \forall y \in B \Rightarrow x \oplus y \in B.$ Свойство выполнимо исходя из замкнутости алгебраических операций над B.

Таким образом, рассматриваемая алгебраическая структура является алгеброй событий.

Заключение

В данной работе рассмотрены подходы к классификации уязвимостей и атак на основе концепции измерений, предложенной Бишопом в работе о классификации уязвимостей сетей и ОС UNIX. В результате проведенных исследований, получена математическая модель уязвимостей вычислительных систем как формализованный результат ассимиляции существующих потоков данных об уязвимостях из National Vulnerability Database с классификацией на основе концепции измерений. Исследование показало, что предлагаемая математическая модель является алгебраической структурой – булевой алгеброй. С целью количественной оценки рассматриваемых математической моделью уязвимостей, была предложена вещественная функция $\mu(x)$, которая, как доказано в работе, является квазимерой булевой алгебры, а также мерой в понятиях теории меры. Продемонстрирована тесная связь алгебраической структуры с другими разделами математики, в частности показано, что разработанная структура является алгеброй событий, что позволяет вводить вероятностные критерии, оценки, применять аппарат теории вероятностей для изоморфных математических структур.

В области дальнейших исследований, предполагается поиск верхней и нижних мер для предлагаемой структуры с целью поиска на ней меры Лебега. Данная задача считается реализуемой, так как выполнен ряд необходимых условий ее существования, в частности счетная аддитивность предложенной меры $\mu(x)$. Введение меры Лебега позволит применять методы вариационного и функционального анализов для решения задачи оптимизации в области нахождения оптимума критериев защищенности при заданных рисках и ограничениях ресурсов.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

ЛИТЕРАТУРА

1. Lipson H.F. Tracking and tracing cyber-attacks: technical challenges and global policy issues, November 2002 // www.cert.org/archive/pdf/02sr009.pdf.
2. Garshva E. Computer System Attack Classification / N. Paulauskas, E. Garshva // Electronics and Electrical Engineering. – Kaunas: Technology, 2006. – No. 2(66). – P. 84–87.
3. Hansman S.A. taxonomy of network and computer attacks / S. Hansman, R. Hunt // Computer & Security. – 2005. Vol. 24. Issue 1. Pp. 31 – 43.
4. Peter G. Neumann, “Computer System Security Evaluation,” 1978 National Computer Conference Proceedings (AFIPS Conference Proceedings 47), pp. 1087–1095 (June 1978).
5. Alvarez G., Petrovic S. A new taxonomy of web attacks suitable for efficient encoding. // Computers and Security, 22(5): p. 435–449, July 2003.
6. Bishop M. A taxonomy of Unix and network security vulnerabilities. Technical repo rt, Department of Computer Science, University of Cali fornia at Davis, May 1995.
7. Howard J. D. An analysis of security incidents on the Internet, 1989-1995. PhD thesis, Carnegie Mellon University, Department of Engineering and Public Policy, April 1997. // www.cert.org/research/JHThesis/table_of_contents.html
8. NIST Special Publication 800-126 Revision 1 (Second Public Draft). The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 (Draft) // http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf.
9. Воробьев А.А. Алгебраические методы исследования таксономий уязвимостей вычислительных сетей и компьютерных систем / А.А. Воробьев // Доклады ТУСУРа 1(25), часть 2, ISSN 1818-0442, С 12-15.
10. Владимиров Д.А. Булевы алгебры / Д.А. Владимиров. – М.: "НАУКА", 1969. – 320 с. ил.
11. Халмош П. Теория меры / П. Халмош. – М.: Издательство иностранной литературы, 1953. — 282 с.

Рецензент: Д.т.н., помощник ректора по информатизации ФГБОУ ВПО «Комсомольский-на-Амуре Государственный технический университет» С.В. Биленко.