УДК 681.3.06

О.Е. МАЗУЛЕВСКИЙ

Полтавский военный институт связи, Украина

МЕТОДИКА ОРГАНИЗАЦИИ КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ

В статье рассмотрена методика организации контроля защищенности компьютерной сети автоматизированной системы управления на основе использования экспертной информации. Основной целью методики является организации такого порядка проведения контроля, при котором уменьшается общее время затрачиваемое на контроль, а также временя обнаружения критических уязвимостей на наиболее важных узлах компьютерной сети.

контроль, анализ защищенности, компьютерная сеть, уязвимость

Введение

Информация, компьютерные сети являются одними из важнейших факторов, определяющих жизнедеятельность и развитие современного общества. В связи с этим большое значение приобретает задача обеспечения необходимого уровня защищенности компьютерной сети. Первым шагом в решении данной задачи является выявление уязвимостей – слабых мест в системах и приложениях, использование которых злоумышленником может привести к реализации той или иной угрозы. Для поиска уязвимостей администратор безопасности компьютерной сети использует различные системы анализа защищенности (САЗ).

Особенности использования современных САЗ, среди которых наибольшее распространение получили сканеры безопасности, обуславливают низкую эффективность проводимого контроля защищенности компьютерной сети, а также приводят к снижению оперативности принятия решения администратором безопасности [1, 2].

Преодоление указанных недостатков возможно на основе организации автоматического адаптивного контроля защищенности компьютерной сети и устранения ручных подготовительных операций [3, 4]. Сущность данных операций заключается в определении администратором безопасности порядка проведения контроля: какие узлы проверять, в какой очередности, какие проверки использовать, в какой последовательности, какова должна быть периодичность контроля и т.д.

В работе [5] представлен возможный вариант решения задачи организации контроля защищенности компьютерной сети. Данная задача формулируется как многокритериальная и для ее решения используется лексикографический метод в нечеткой постановке. Для обеспечения минимума среднего времени обнаружения наиболее критичных уязвимостей на узлах сети используется ранжирование проверок. Критерием ранжирования является отношение значения важности проверки к среднему времени её выполнения.

Однако данный подход имеет следующие недостатки: в связи с поочередным, последовательным проведением анализа узлов на наличие уязвимостей общее время, затрачиваемое на контроль защищенности всей сети, может быть достаточно большим, как следствие, увеличивается время обнаружения критических уязвимостей на наиболее важных узлах.

В данной статье представлена методика, которая позволяет значительно уменьшить общее время контроля защищенности сети, а также уменьшить время

обнаружения критических уязвимостей на наиболее важных узлах.

Исходные данные и постановка задачи. Пусть $S = \{s_i\}$ – множество узлов компьютерной сети, $i = \overline{1,I}$, $E = \{e_r\}$ – множество линий связи компьютерной сети, $r = \overline{1,R}$. Каждый узел $s_i \in S$ и линия связи $e_r \in E$ характеризуется загрузкой ρ_{S_i} и ρ_{e_r} соответственно. Для контроля защищенности узлов компьютерной сети используется множество проверок $P = \{p_j\}$, $j = \overline{1,J}$. Обозначим через W эффективность контроля защищенности, тогда задачу организации контроля защищенности можно сформулировать следующим образом: необходимо выбрать вариант реализации контроля защищенности, обеспечивающий максимум эффективности при допустимом уровне загрузке линий связи компьютерной сети.

Формальная постановка задачи имеет вид:

$$T^0 = \arg\max W(T),$$

найти $T^0 \in T^+$ при ограничениях:

$$\begin{cases} \rho_{s_i} \le \rho_{s.доп}; \\ \max(\rho_{e_1},...,\rho_{e_r}) \le \rho_{e.доп}, \end{cases};$$

где T^o – оптимальный в некотором смысле вариант проведения контроля защищенности; T^+– допустимые варианты проведения контроля, $\rho_{s.доп}$ – допустимый уровень загрузки узла, $\rho_{e.доп}$ – допустимый уровень загрузки линии связи.

Осуществим выбор показателей качества оценки эффективности контроля защищенности компьютерной сети. Очевидно, что эффективность контроля будет тем выше, чем меньше будет времени затрачиваться на контроль всей сети и чем меньше будет время обнаружения наиболее критичных уязвимостей на наиболее важных узлах компьютерной сети.

Таким образом, критериями для оценки эффективности контроля защищенности будут $t_{k\Sigma}$ – общее время контроля защищенности сети и $t_{обн.кр}$ – время обнаружения наиболее критичных уязвимостей на наиболее важных узлах компьютерной сети.

Поскольку при организации контроля защищенности администратор учитывает параметры узлов, проверок и топологию сети, то порядок проведения контроля должен зависеть от параметров узлов компьютерной сети, от параметров проверок и от топологии сети.

Введем следующие обозначения: $H = \{h_m\}$, $m = \overline{1,M}$ – множество параметров, характеризующих узел сети; $G = \{g_n\}$, $n = \overline{1,N}$ – множество параметров, характеризующих проверку. Тогда выражение для варианта порядка проведения контроля будет иметь следующий вид:

$$T = f(H,G,E).$$

Этапами решения задачи организации контроля будут:

– сбор и обработка экспертной информации о параметрах узлов сети и определение обобщенного показателя влияния узла на защищенность компьютерной сети;

– сбор и обработка экспертной информации о параметрах уязвимостей, обнаруживаемых соответствующими проверками, и определение обобщенного показателя влияния уязвимости на защищенность сети;

– определение интегрального показателя влияния каждой уязвимости, обнаруживаемой проверками на каждом узле, на общую картину защищенности компьютерной сети;

– расчет последовательности проведения контроля; определение возможности одновременного выполнения проверок.

Успешное решение данной задачи возможно на основе использования знаний и опыта грамотного администратора безопасности, т.е. на основе экспертной информации.

Рассмотрим этапы методики.

Этап 1 – определение обобщенного показателя влияния узла на защищенность компьютерной сети на основе экспертной информации. Каждый узел сети будем характеризовать следующими показателями: h_1 – «важность узла», h_2 – «подверженность узла атакам» (зависит от местоположения узла: на периметре сети или внутри её), h_3 – «степень подверженности атакам операционной системы», h_4 – «степень подверженности атакам установленного программного обеспечения», h_5 – «автономность узла» (возможность изменения настроек пользователем узла). Пусть q_i – обобщенный показатель влияния некоторого узла s_i на защищенность компьютерной сети. Для учета степени влияния частных показателей целесообразно использовать аддитивный показатель, который представляет собой сумму взвешенных частных показателей.

Числовые значения частных показателей оцениваются числами, лежащими на интервале (0, 1]. Таким образом, зная значения частных показателей, можно определить аддитивный показатель для каждого узла следующим образом:

$$q_i = \sum_{m=1}^{M} h_{im}\mu_m , \qquad (1)$$

где q_i – значения аддитивного показателя для i-го узла, h_{im} – значения m-х частных показателей i-го для узла, μ_m – весовые коэффициенты m-х частных показателей.

Этап 2 – определение обобщенного показателя влияния уязвимости, обнаруживаемой соответствующей проверкой на защищенность компьютерной сети на основе экспертной информации. Введем следующие показатели для проверок, обнаруживаемых уязвимости: g_1 – «степень опасности уязвимости обнаруживаемой проверкой»; g_2 – «простота реализации атаки с использованием уязвимости обнаруживаемой проверкой»; g_3 – «популярность (частота) использования уязвимости обнаруживаемой проверкой».

Обобщенный показатель влияния уязвимости, обнаруживаемой j-й проверкой на защищенность компьютерной сети, также может определяться с помощью аддитивного показателя:

$$c_j = \sum_{n=1}^{N} g_{jn}\mu_n , \qquad (2)$$

где c_j – значения аддитивного показателя для j-й проверки; g_{jn} – значения n-х частных показателей для j-й проверки; μ_n – весовые коэффициенты n-х частных показателей.

Весовой коэффициент имеет тем большую величину, чем большее влияние он оказывает на важность показателя, при этом:

$$\sum_{m=1}^{M}\mu_m = 1;\ \mu_m > 0;\ m = \overline{1, M},$$

$$\sum_{n=1}^{N}\mu_n = 1;\ \mu_n > 0;\ n = \overline{1, N}.$$

Определение весовых коэффициентов для частных показателей может производиться различными методами, например, методом парных сравнений (метод Саати) [6] либо методами, представленными в [7].

Этап 3. Определение интегрального показателя. Введем матрицу $\Theta \equiv [\theta_{ij}]$ соответствия проверок узлам, которую сформируем по следующему правилу:

$$\theta_{ij} = \begin{cases} 1, \text{ если } j \text{ - я проверка используется} \\ \qquad\qquad \text{для } i \text{ - го узла;} \\ 0, \text{ если } j \text{ - я проверка не используется} \\ \qquad\qquad \text{для } i \text{ - го узла.} \end{cases}$$

Для определения интегрального показателя составим перекрестную объединенную прямоугольную матрицу $Z \equiv [z_{ij}]$, в которой каждый элемент определятся по формуле

$$z_{ij} = q_i \times c_j \times \theta_{ij} . \qquad (3)$$

Числовые значения элементов матрицы Z дают нам представление об общем весе предпочтений для проведения контроля i-го узла j-й проверкой.

Рассмотренные пункты методики могут быть выполнены на этапе проектирования сети с последующим уточнением результатов в ходе её эксплуатации, поэтому назовём данную часть методики статической.

Следующие пункты методики соответствуют динамической части, в ходе выполнения которой непосредственно решается задача организации контроля компьютерной сети автоматизированной системы управления.

Этап 4. Для организации контроля составим прямоугольную матрицу $V \equiv [v_{ij}]$, в которой каждый элемент определятся по формуле:

$$v_{ij} = (z_{ij} + u) \times \theta_{ij},$$

где u – полученный с помощью экспертного опроса интервал отсрочки проведения контроля. Возможно динамическое изменение значения u на основе логико-лингвистической аппроксимации с учетом текущей загрузки узлов и линий связи, а также предыдущих этапов проведения контроля.

На основе сформированной матрицы V контроль защищенности узлов сети будем проводить по следующему алгоритму.

1. Сравниваем все элементы матрицы v_{ij} с единицей, и, если $v_{ij} \geq 1$, тогда принимаем решение о необходимости проведения контроля i-го узла j-й проверкой, а элементу присваиваем значение z_{ij}.

2. Производим пересчет всех элементов матрицы по формуле

$$v_{ij} = (v_{ij} + u) \times \theta_{ij}.$$

3. Возвращаемся к шагу 1.

В ходе работы алгоритма может возникнуть ситуация, когда некоторые элементы матрицы V будут иметь одинаковые значения.

Тогда очередность назначения их для проведения контроля целесообразно решать с помощью метода прямого ранжирования [8], учитывая значение их обобщенных показателей, элементы матрицы Z.

Во время работы сети узлы могут включаться и выключаться, подключаться новые узлы. При включении узла в сеть его необходимо, в первую очередь, проверить всеми допустимыми проверками, аналогично при поступлении новой проверки, контроль с ее помощью необходимо провести для всех допустимых для нее узлов. Для этого элементам соответствующей строки или столбца матрицы V необходимо присвоить значение единицы, кроме элементов, равных нулю.

Особенность работы алгоритма заключается в более тщательном контроле за наиболее критичными уязвимостями на наиболее важных узлах. Это достигается периодическим повторением данных проверок, что в целом приводит к увеличению времени контроля защищенности всей сети. Однако исследование данного алгоритма с помощью имитационного моделирования для различного числа узлов в сети и различного количества проверок показало, что в среднем количество проводимых проверок увеличивается не больше, чем на 5% (рис. 1).

Рис. 1. Среднее значение увеличения количества проводимых проверок

Устранение данного недостатка может быть реализовано за счет одновременного выполнения сразу нескольких проверок на различных узлах сети, т.е. за счет распараллеливания процесса проведения контроля защищенности.

Решение данной задачи является сущностью следующего этапа методики.

Этап 5. Результат работы алгоритма организации контроля, рассмотренного на предыдущем этапе,

можно представить в виде множества $\Omega' = \{\omega_\psi\}$, $\psi = \overline{1,\Psi}$, состоящего из элементов матрицы *Z*. Причем элементы данного множества будут повторяться в определенной последовательности вследствие работы алгоритма.

Сформируем из элементов множества Ω' подмножество Ω, элементами которого будут элементы множества Ω' до первого повторяющегося элемента. Для каждого элемента множества Ω известны величина трафика, создаваемого соответствующей проверкой ρ_{ω_ψ}, а также $L^\psi = \{l_b^\psi\}$, $b = \overline{1,B}$ – множество линий связи, через которые проходит трафик проверки до соответствующего узла. Будем считать, что можно начать одновременное выполнение всех проверок, включенных в множество Ω, если суммарный трафик, создаваемый проверками для любой общей линии связи не превышает некоторого заданного значения, т.е.

$$\rho_\Omega \le \rho_{don}, \qquad (4)$$

где ρ_Ω – суммарный трафик, создаваемый проверками, включенными в множество Ω; ρ_{don} – допустимое значение загрузки линии связи.

В случае, если условие (4) не выполняется, множество Ω необходимо разбить на группы (подмножества) таким образом, чтобы для проверок, включенных в группу, условие (4) выполнялось.

Введем в рассмотрение множество $A = \{A_1,...,A_\chi\}$ возможных вариантов разбиения множества Ω на группы. Будем полагать, что если выбран вариант разбиения A_α, $\alpha = 1,...,\chi$, то множество Ω подразделяется на m_α групп, т.е.:

$$A_\alpha : \Omega_k^{A_\alpha} \bigcap \Omega_g^{A_\alpha} = \varnothing,$$

$$\bigcup_{i=1}^{m_\alpha} \Omega_i^{A_\alpha} = \Omega;\ k,g = 1,...,m_\alpha;\ k \ne g.$$

В зависимости от используемого типа среды передачи (разделяемая или коммутируемая) возможны различные варианты разбиения множества Ω на группы. Рассмотрим их.

Вариант 1: использование общей разделяемой среды передачи данных.

Для включения некоторого элемента ω_ψ в группу $\Omega_k^{A_\alpha}$ необходимо выполнение следующего условия:

$$\rho_{\omega_\psi} + \rho_{\Omega_k^{A_\alpha}} \le \rho_{don}, \qquad (5)$$

где $\rho_{\Omega_k^{A_\alpha}}$ – суммарная нагрузка на сеть, создаваемая трафиками проверок, уже включенных в группу. Если условие (5) выполняется, то элемент ω_ψ включается в $\Omega_k^{A_\alpha}$:

$$\Omega_k^{A_\alpha} := \Omega_k^{A_\alpha} \bigcup \omega_\psi.$$

Величина ρ_{don} может быть задана фиксированной или изменяться динамически на основе постоянно собираемой статистики о работе сети.

Вариант 2: использование коммутируемой среды передачи данных. Особенность данной среды передачи состоит в том, что компьютерная сеть с помощью коммутаторов разбивается на несколько доменов коллизий, либо производится более глубокое сегментирование сети – микросегментация, при которой каждому узлу сети выделяется своя коммутируемая линия, что исключает возникновение коллизий и позволяет организовать двунаправленный обмен между узлами [9].

В данном случае условие (5) о включении узла в группу имеет смысл только в том случае, если у узла, включаемого в группу, с одним из узлов, уже включенных в группу, имеется одна или несколько общих линий связи, т.е.:

$$L^k \bigcap L^q \ne \varnothing;\ k,q = \overline{1,\psi};\ k \ne q.$$

Условие (5) для коммутируемой среды можно записать следующим образом:

$$\forall l_k : \rho_{don} \ge \rho_{\Omega_k^{A_\alpha}} + \rho_{\omega_\psi},$$

т.е. для любой линии связи любого элемента, уже

включенного в группу, суммарный трафик проверок и трафик проверки, которую предполагается включить в группу, не должен превышать заданного порогового значения.

Таким образом, в данном случае на количество одновременно проводимых проверок влияет топология сети, особенно связи между устройствами, образующими сетевую магистраль.

Выводы

В статье представлена методика организации контроля защищенности компьютерной сети АСУ. Методика обеспечивает реализацию наиболее рационального варианта проведения контроля защищенности за счет учета влияния параметров узлов сети и уязвимостей, обнаруживаемых соответствующими проверками на защищенность сети в целом. За счет распараллеливания процесса контроля методика позволяет уменьшить общее время проведения контроля защищенности компьютерной сети, время обнаружения критических уязвимостей, а также обеспечивает более тщательный контроль за критическими уязвимостями. Кроме того, методика обеспечивает возможность организации контроля защищенности в автоматическом режиме, что исключает необходимость выполнения администратором безопасности ручных операций.

Литература

1. Шохін Б.П., Юдін О.М., Мазулевський О.Є. Вдосконалення контролю за станом захищеності комп'ютерної мережі на основі адаптивного моніторингу // Зб. наук. пр. ВІТІ НТУУ «КПІ». – К.: ВІТІ НТУУ «КПІ», 2004. – № 4. – С. 208-217.

2. Юдін О.М., Мазулевський О.Є. Експериментально-теоретичне дослідження засобів аналізу захищеності комп'ютерної мережі // Зб. наук. пр. «Труди академії». – К.: НАОУ, 2005. – № 57. – С 139-145.

3. Мазулевський О. Є. Методика адаптивного контролю захищеності комп'ютерної мережі // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки – К.: «Київський університет», 2005. – № 10-11. – С. 69-72.

4. Юдин А.Н., Сомов С.В., Мазулевский О.Е. Система адаптивного контроля защищенности. // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУ ПС, 2005. – № 5. – С. 102-105.

5. Юдін О.М. Вибір стратегії і тактики контролю захищеності вузлів комп'ютерної мережі на основі нечіткої логіки // Зб. наук. пр. ВІТІ НТУУ «КПІ» – К.: ВІТІ НТУУ «КПІ», 2005. – № 1. – С. 172-177.

6. Герасимов Б.М., Дивизинюк М.М., Субач И.Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. – Севастополь: Издательский центр СНИЯЭиП, 2004. – 320 с.

7. Анохин А.М., Глотов В.А., Павельев В.В., Черкашин А.М. Методы определения коэффициентов важности критериев // Автоматика и телемеханика. – 1997. – № 8. – С. 3-35.

8. Варфоломеев В.И., Воробьев С.Н. Принятие управленческих решений: Учеб. пособие для вузов. – М.: КУДИЦ-ОБРАЗ, 2001. – 288 с.

9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. – С.-Пб.: Питер, 2003. – 867 с.

Поступила в редакцию 23.02.2006

Рецензент: д-р техн. наук, проф. Б.П. Шохин, Военный институт телекоммуникаций и информатизации НТУУ "КПИ, Киев.