D. S. Chernyavskiy

Methods for Selection of Network Security Systems in accordance with Information Security Policies

Key words: information security policy, network security system

Selection of network security systems (NSS) that are sufficient for implementation of information security (IS) policies is one of the major steps of IS policy management process. The paper describes existing methods for selection of NSS, outlines their peculiarities and drawbacks, and presents a method for selection of NSSs, which takes into account their cost.

Д. С. Чернявский

МЕТОДИКИ ВЫБОРА СЕТЕВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СООТВЕТСТВИИ С ПОЛИТИКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Выбор средств защиты информации, необходимых для реализации политик информационной безопасности (далее — политик), является одним из этапов процесса управления политиками [1]. В силу большого числа политик для информационно-телекоммуникационных сетей (далее — сетей) в организациях [2], с ростом числа сетевых средств защиты информации (ССЗИ), а также сложностью ССЗИ и ограниченностью ресурсов [3], проблема выбора ССЗИ для реализации политик является актуальной. Однако методики выбора ССЗИ, соответствующих политикам, представлены не так широко в литературе, как языки задания политик (одно из исследований языков представлено в [4]). Рассмотрим те из них, что представлены в [5, 6].

Методика [5] применяется для нахождения в сети ССЗИ, которые могут применяться для реализации политики. Если в сети не присутствуют ССЗИ, обладающие требуемой для реализации политики функциональностью, то в сети ищутся ССЗИ с «почти эквивалентной» функциональностью, позволяющей частично реализовать политику. При этом среди почти эквивалентных ССЗИ выбираются такие, при применении которых риск, связанный с неполной реализацией политики, минимален. Недостатками данной методики являются отсутствие формального критерия нахождения почти эквивалентных ССЗИ, а также рассмотрение только тех ССЗИ, которые уже размещены в сети.

В [6] представлена методика, позволяющая разместить ССЗИ в сети таким образом, чтобы обеспечить максимальный уровень защищенности сервисов в сети при соблюдении ограничений на стоимость ССЗИ и на доступность сервисов. ССЗИ в рамках методики разделены на четыре класса, среди которых производится выбор: осуществляющие фильтрацию сетевого трафика (межсетевые экраны), проверку содержимого трафика (системы обнаружения вторжений), доверенное взаимодействие (виртуальные частные сети) и переадресацию трафика (прокси-серверы). Недостаток методики— рассмотрение только данных четырех классов ССЗИ.

Далее представлен способ нахождения оптимального ССЗИ, обладающего функциональными возможностями для реализации политик, учитывающий стоимость ССЗИ.

Пусть ССЗИ задано как одно или совокупность нескольких простых ССЗИ. Простое ССЗИ, в свою очередь, является абстрактным вычислительным устройством (автоматом), преобразующим входной сетевой трафик в выходной сетевой трафик и вспомогательную информацию (записи журналов регистрации событий, сообщения о нарушениях политик в сети) с учетом заданных политик. Пусть множество простых ССЗИ разбито на классы эквивалентности

таким образом, что все простые ССЗИ в рамках класса производят одинаковые выходы при одинаковых входах в соответствии с некоторыми политиками (формальное описание модели ССЗИ и классификации выходит за рамки данной статьи). Простые ССЗИ по сути определяют функциональные возможности ССЗИ (далее простые ССЗИ называются функциями). Таким образом, каждое ССЗИ включает в себя одну или несколько функций, каждая из которых принадлежит некоторому классу эквивалентности.

Классификация позволяет назначить каждому ССЗИ $F \in \mathcal{F}$ (где $\mathcal{F}$ — множество всех ССЗИ) следующий рейтинг R: $R_F = \sum_i W_{F_i} I^F_{F_i}$, где $W_{F_i} > 0$ — весовой коэффициент функции из класса эквивалентности F_i (все функции, принадлежащие одному классу эквивалентности, имеют одинаковый весовой коэффициент), который может быть вычислен методом экспертных оценок; $I^F_{F_i} \in \{0,1\}$ — индикатор, который показывает, включена ли в состав ССЗИ F функция из класса F_i. Весовой коэффициент определяет значимость конкретной функции, его значение прямо пропорционально количеству уязвимостей, которые позволяет устранить данная функция, и критичности каждой из уязвимостей: $W_{F_i} = \sum_j V^{F_i}_j S_j$, где $V^{F_i}_j \in \{0,1\}$ — индикатор, указывающий на то, что F_i устраняет j-ую уязвимость, S_j — степень критичности j-й уязвимости.

Классификация простых ССЗИ позволяет выбрать ССЗИ с требуемыми функциями. Например, если для реализации политики на границе сети или сегмента сети необходимы функций из классов F_{i_1}, F_{i_2}, ..., F_{i_k}, то с этой целью выбираетсято ССЗИ,которое включает в себя функции из данныхклассов. Если таких ССЗИ несколько, то оптимальным может являться то из них, которое имеет максимальное значение отношения рейтинга к цене, тоесть целевая функция задается следующим образом: $\frac{R_F}{C_F} \to \max$, где C_F — стоимость ССЗИ F. При этом ограничение имеет вид: $C_F \le C_{limit}$, $F \in \{F: \forall F_l \in \{F_{i_1}, F_{i_2}, ..., F_{i_k}\}, I^F_{F_l} = 1\} \subseteq \mathcal{F}$, где C_{limit} — выделенный бюджет.

С применением данной классификации могут быть сформулированы и другие задачи оптимизации. Пусть для реализации политики необходимо ССЗИ с тем же набором функций, что и в предыдущем случае. Оптимальным может считаться то ССЗИ, которое имеет максимальный рейтинг и при этом его стоимость не выходит за рамки выделенного бюджета (C_{limit}). В таком случае целевая функция задается следующим образом: $R_F \to max$, ограничения имеют вид: $C_F \le C_{limit}$, $F \in \{F: \forall F_l \in \{F_{i_1}, F_{i_2}, ..., F_{i_k}\}, I^F_{F_l} = 1\} \subseteq \mathcal{F}$. Пусть теперь требуется найти ССЗИ с минимальной стоимостью, тогда целевая функция и ограничения имеют вид: $F \in \{F: \forall F_l \in \{F_{i_1}, F_{i_2}, ..., F_{i_k}\}, I^F_{F_l} = 1\} \subseteq \mathcal{F}$.

Если не существует ССЗИ, включающих все требуемые функции, то представленные выше задачи формулируются с учетом выбора комбинаций ССЗИ, включающих требуемые функции. В данном случае целевая функция первой задачи задается с учетом суммарных рейтингов для каждой комбинации ССЗИ: $\sum_j \frac{R_{Fj}}{C_{Fj}} \to \max$,где $j \in \{j_1, j_2, ..., j_m\}$,$\{F^{j_1}, F^{j_2}, ..., F^{j_m}\} \subseteq \mathcal{F}$ — множество ССЗИ, входящих в комбинацию. Ограничения задаются следующим образом: $C_F \le C_{limit}$, $\forall F_l \in \{F_{i_1}, F_{i_2}, ..., F_{i_k}\}$, $\exists F^t \in \{F^{j_1}, F^{j_2}, ..., F^{j_m}\}: I^{F^t}_{F_l} = 1$. Аналогично задаются целевые функции и ограничения для двух других задач.

СПИСОКЛИТЕРАТУРЫ:

1. *Rees J., Bandyopadhyay S., Spafford E.H.* PFIRES: A Policy Framework for Information Security // Communications of the ACM. 2003. Vol. 46. Issue 7. P. 101–106.

2. *Chapple M.J., D'Arcy J., Striegel A.* An Analysis of Firewall Rulebase (Mis)Management Practices // ISSA Journal. February. 2009. P. 12–18.

3. Ponemon Institute. Perceptions about Network Security. Survey of IT & IT security practitioners in the U.S. 2011.

4. *Han W., Lei C.* A Survey on Policy Languages in Network and Security Management // Computer Networks. 2012. № 56. P. 477–489.
5. *Preda S., Cuppens-Boulahia N., Cuppens F., Toutain L.* Architecture-Aware Adaptive Deployment of Contextual Security Policies// Proceedings of International Conference on Availability, Reliability, and Security. 2010. P. 87–95.
6. *Rahman M., Al-Shaer E.* A Formal Framework for Network Security Design Synthesis // Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems. 2013. P. 560–570.

REFERENCES:

1. *Rees J., Bandyopadhyay S., Spafford E. H.* PFIRES: A Policy Framework for Information Security // Communications of the ACM. 2003. Vol. 46. Issue 7. P. 101–106.
2. *Chapple M. J., D'Arcy J., Striegel A.* An Analysis of Firewall Rulebase (Mis)Management Practices // ISSA Journal. February. 2009. P. 12–18.
3. Ponemon Institute. Perceptions about Network Security. Survey of IT & IT security practitioners in the U.S. 2011.
4. *Han W., Lei C.* A Survey on Policy Languages in Network and Security Management // Computer Networks. 2012. № 56. P. 477–489.
5. *Preda S., Cuppens-Boulahia N., Cuppens F., Toutain L.* Architecture-Aware Adaptive Deployment of Contextual Security Policies// Proceedings of International Conference on Availability, Reliability, and Security. 2010. P. 87–95.
6. *Rahman M., Al-Shaer E.* A Formal Framework for Network Security Design Synthesis // Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems. 2013. P. 560–570.

A. V. Iuzbashev

Detecting System of Nested Hardware Virtual Machine Monitor

Key words: hypervisor, hardware virtual machine monitor, Intel Vt-x

Method of nested hardware virtual machine monitor detection was proposed in this work. The method is based on HVM timing attack. In case of HVM presence in system, the number of different instruction sequences execution time values will increase. We used this property as indicator in our detection system.

А. В. Юзбашев

СПОСОБ ОБНАРУЖЕНИЯ ВЛОЖЕННЫХ МОНИТОРОВ ВИРТУАЛЬНЫХ МАШИН

Технология аппаратной виртуализации за последние годы получила широкое распространение. Большинство выпускаемых процессоров компаний Intel и AMD поддерживают данную технологию [1].

Монитор виртуальных машин (МВМ) представляет собой программную прослойку, работающую между аппаратной частью и ядром операционной системы (ОС) и контролирующую все ресурсы операционной системы. Стоит отметить, что не существует штатных средств обнаружения МВМ. Также важным моментом является то, что угроза внедрения МВМ может исходить как от поставщиков оборудования, так и от поставщиков программного обеспечения. Основной особенностью внедрения МВМ является тот факт, что возможна установка без изменения микропрограммы BIOS и загрузочной записи жесткого диска, посредством установки драйвера ОС, который позволяет перевести систему в гостевой режим работы [2].