УДК 621.391

ПОКАЗАТЕЛИ УСТОЙЧИВОСТИ ЭЛЕМЕНТОВ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ К СЕТЕВЫМ АТАКАМ

В.В. КОЗЛОВСКИЙ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки 6, Минск 220013, Беларусь

Поступила в редакцию 16 октября 2009

Рассматриваются показатели устойчивости элементов инфраструктуры открытых ключей к сетевым атакам.

Ключевые слова: инфраструктура открытых ключей, показатели устойчивости, сетевые атаки.

Введение

В современных системах телекоммуникации для обеспечения информационной безопасности электронных документов и обмена транзакциями применяется технология на основе инфраструктуры открытых ключей (ИОК). Элементы ИОК, включающие в свой состав комплексы программных и аппаратных средств функционирующих в сетевом окружении в соответствии с установленными политиками и процедурами, так же подвергаются различным атакам, в частности – сетевым.

Методы сетевых атак

Анализ существующих классификаций методов и алгоритмов сетевых атак позволяет выделить следующие методы их проведения:

- подмена доверенного объекта ИОК;
- внедрение в ИОК ложного объекта за счет навязывания ложного маршрута;
- отказ в обслуживании за счет создания аппаратного/программного сбоя, уничтожения или изменения информации управления, использования ресурсов.
- передача управления враждебному коду, внедренному в программное обеспечение элемента ИОК (прикладное или системное) [1];

Оценка устойчивости элементов ИОК

Для оценки устойчивости элементов ИОК к сетевым атакам необходимо построить модель системы анализа устойчивости (САУ), описывающую совокупность воздействия на ИОК во время проведения исследований. В модели САУ для ИОК определяем следующие критерии устойчивости:

$P(T)$ – показатель устойчивости элемента ИОК;

$H(T)$ – показатель эффективности конфигурации средств обеспечения устойчивости элемента ИОК;

Метрики для вычисления количественных значений показателей устойчивости:

1) значение показателя устойчивости ИОК при воздействии сетевых атак вычисляется следующим образом

$$P(T) = 1 - D(T) / K, \quad (1)$$

где $D(T), K$ – положительные действительные числа;

$D(T)$ – количество экспериментов, в которых в течение времени T не была восстановлена устойчивость ИОК, нарушенная в результате сетевой атаки;

K – общее количество экспериментов, в ходе которых сетевые атаки приводили к нарушению устойчивости ИОК;

2) значение показателя эффективности конфигурации средств обеспечения устойчивости ИОК вычисляется следующим образом

$$H(T) = 1 - \sum_{i \in V} p_i(t), \qquad t \le T, \tag{2}$$

где T – максимально допустимое время восстановления, измеренное на последовательности интервалов наблюдения;

V – множество невозвратных состояний, т.е. эксперименты, в которых не была восстановлена устойчивость;

$p_i(t)$ – статистическая оценка показателей устойчивости.

Для определения меры устойчивости элемента ИОК к воздействию сетевых атак дополняем существующие критерии оценки устойчивости программных средств по ГОСТ 28195-99 параметром времени T. Таким образом, в формуле (1) для метрики показателя устойчивости элемента ИОК к воздействию сетевых атак время восстановления введено как важный параметр. Допустим, атакующему для осуществления своей цели необходимо в течение времени t нарушить доступность элемента ИОК, для чего он генерирует поток запросов, вызывающий отказ в обслуживании (или сбой). Однако, если за время $T < t$ доступность элемента ИОК восстанавливается, т.е. возвращается в устойчивое состояние, то нарушитель своей цели не достигает [2, 3].

Таким образом, формула (1) определяет показатель P(T) – устойчивости восстановления элемента ИОК при воздействии сетевой атаки, характеризует его способность обеспечивать восстановление работы в заданных режимах и имеет смысл вероятности восстановления устойчивости за время наблюдения $T_н$.

Для определения показателя H(T2) – эффективности конфигурации средств обеспечения устойчивости, – по формуле (2) необходимо наличие большой статистики по показателю устойчивости восстановления. В то же время об эффективности конфигурации средств обеспечения устойчивости ИОК можно судить по показателю эффективности восстановления элемента ИОК при воздействии сетевых атак по отношению к параметру среднее время восстановления T2.

Под нарушением устойчивости понимается временная приостановка выполнения запроса или отказ в выполнении запроса. Чтобы зафиксировать нарушение устойчивости необходимо знать параметр среднее время обработки запроса T1, который либо задается в программной документации на элемент ИОК или вычисляется по формуле

$$T1 = \frac{1}{m} \sum_{j=1}^{m} T_j, \tag{3}$$

где T_j, m – действительные положительные числа;

T_j – время обработки j-го запроса;

m – количество экспериментов меньшее N, т.е. количество запросов в потоке, в которых запросы обслуживались без нарушений;

N – общее количество экспериментов, т.е. запросов в потоке, подаваемых с высокой интенсивностью на исследуемый элемент ИОК.

Зная параметр среднего времени обработки запроса T1 можно вычислить следующие параметры:

K – количество экспериментов, которые завершились с нарушением устойчивости, т.е. когда время ответа на запрос превышает среднее время обработки T1;

T2 – среднее время восстановления на последовательности в N экспериментов.

Среднее время восстановления вычисляется по формуле

$$T2 = \frac{1}{n} \sum_{i=1}^{n} T_i, \tag{4}$$

где T_i, n – действительные положительные числа;

T_i – время восстановления после i-го нарушения устойчивости;

n – количество экспериментов, которые завершились с восстановлением устойчивости.

Тогда метрика определения показателя H(T2) – эффективности средств обеспечения устойчивости, – зависит от параметра среднего времени восстановления T2 и описывается следующей формулой

$$H(T2) = \frac{B(T2)}{K - D(T)}, \tag{5}$$

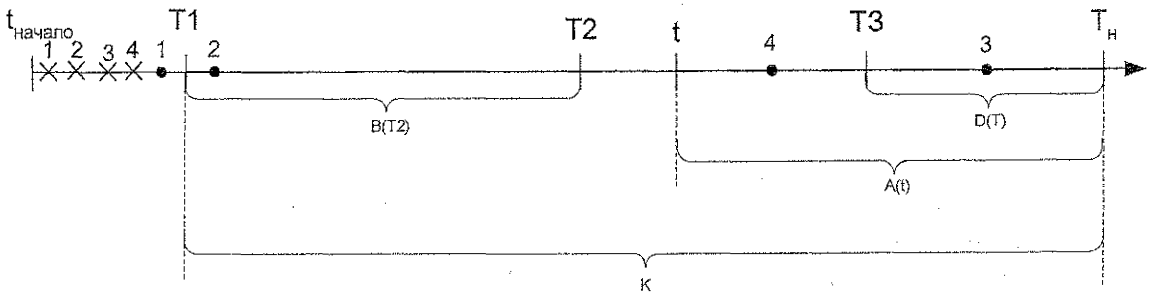
где $B(T2)$, K, $D(T)$ – действительные положительные числа;

$B(T2)$ – количество экспериментов, в которых восстановление устойчивости происходило за среднее время восстановления T2;

K – количество экспериментов, которые завершились с нарушением устойчивости;

$D(T)$ – количество экспериментов, в которых воздействие сетевых атак приводило к отказу, т.е. ответ на запрос не пришел или пришел с кодом отказа за время наблюдения $T_н$.

Для облегчения понимания на рисунке приведена временная диаграмма проведения N экспериментов.



Временная диаграмма проведения N экспериментов

Таким образом, показатель H(T2) характеризует способность элемента ИОК за среднее время восстановления после отклонений, вызванных воздействием сетевых атак, восстанавливать устойчивую работу и имеет смысл вероятности восстановления устойчивой работы за среднее время восстановления.

Для определения меры устойчивости элемента ИОК к воздействию сетевых атак необходимо ввести дополнительные показатели оценки:

- R(T) – показатель устойчивого функционирования при воздействии сетевых атак;
- G(T) – показатель безотказности работы;
- M(T) – показатель успешности восстановления;

Метрика определения показателя R(T) – устойчивого функционирования при воздействии сетевых атак, – также зависит от параметра времени и описывается следующей формулой

$$R(T) = 1 - \frac{K - D(T)}{N}, \tag{6}$$

где K, $D(T)$, N – действительные положительные числа;

$K - D(T)$ – количество экспериментов, в которых восстановлена устойчивость за время наблюдения $T_н$;

N – количество экспериментов, т.е. количество запросов в потоке.

Показатель R(T) характеризует способность элемента ИОК обеспечивать устойчивую работу без возникновения отклонений, вызванных воздействием сетевых атак, и имеет смысл вероятности выполнения работы без нарушения.

Метрика определения показателя G(T) – безотказности работы, – также зависит от параметра времени и описывается следующей формулой

$$G(T) = 1 - \frac{D(T)}{N}, \tag{7}$$

где $D(T)$, N – действительные положительные числа;

$D(T)$ – количество экспериментов, в которых воздействие удаленных активных атак приводило к отказу;

N – количество экспериментов.

Показатель G(T) характеризует способность элемента ИОК при воздействии сетевых атак обеспечивать выполнение всех запросов за время наблюдения $T_н$ (т.е. обеспечивать продолжения работы без отказов) и имеет смысл вероятности безотказной работы.

Метрика определения показателя M(T) – успешности восстановления, –также зависит от параметра времени и описывается следующей формулой

$$M(T) = \frac{K - A(t)}{K - D(T)}, \tag{8}$$

где K, $A(t)$, $D(T)$ – действительные положительные числа;

K - $A(t)$ – количество экспериментов, в которых восстановлена устойчивость за время t;

K - $D(T)$ – количество экспериментов, в которых восстановлена устойчивость за время наблюдения $T_н$;

$A(t)$ – количество экспериментов, в которых нарушения устойчивости не восстановлены за время t;

t – время наблюдения на интервале $T2 < t < T3$, т.е. большее среднего времени восстановления, но меньшее времени отказа.

Показатель M(T) характеризует способность элемента ИОК при воздействии сетевых атак обеспечивать восстановление времени работы за время большее среднего времени восстановления и имеет смысл вероятности выполнения восстановления за время t.

Перечень показателей устойчивости элементов ИОК к воздействию сетевых атак

Критерий устойчивости	Обозначение	Свойство
Устойчивость восстановления при воздействии сетевых атак	P(T)	Способность элемента ИОК при возникновении отклонений, вызванных воздействием сетевых атак, обеспечивать восстановление своей работы в заданных режимах
Устойчивость функционирования при воздействии сетевых атак	R(T)	Способность элемента ИОК обеспечивать устойчивую работу без возникновения отклонений, вызванных воздействием сетевых атак
Эффективность средств обеспечения устойчивости	H(T2)	Способность элемента ИОК за среднее время восстановления после отклонений, вызванных воздействием сетевых атак, восстанавливать устойчивую работу
Безотказность работы	G(T)	Способность элемента ИОК обеспечивать продолжение работы без отказов после возникновения отклонений, вызванных воздействием сетевых атак
Успешность восстановления	M(T)	Способность элемента ИОК после отклонений, вызванных воздействием сетевых атак, обеспечивать восстановление своей работы в заданных режимах за время большее среднего времени восстановления

Заключение

Проведенные исследования показали необходимость выбора показателей устойчивости, которые поддаются измерению при испытаниях элементов ИОК. При оценке испытуемых элементов ИОК должны быть учтены особенности и ограничения по их функционированию.

INDICATORS OF THE SUSTAINABILITY OF THE ELEMENTS OF PUBLIC KEY INFRASTRUCTURE FOR NETWORK ATTACKS

V.V. KOZLOVSKI

Abstract

Discusses the indicators of the sustainability of the elements of public key infrastructure for network attacks.

Литература

1. *Горбатов В.С., Полянская О.Ю.* Основы технологии PKI, М., 2004.
2. *Громов Ю.Ю., Драчев В.О.* Синтез и анализ живучести сетевых систем. М., 2007.
3. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах. М., 2005.