М. Ю. Чекмарев

ПРИНЦИПЫ И ПОСЛЕДОВАТЕЛЬНОСТЬ ОРГАНИЗАЦИИ ДОВЕРЕННОГО СЕАНСА СВЯЗИ

Базовой идеей доверенного сеанса связи (ДСС) является рассмотрение решения задач обеспечения информационной безопасности взаимодействия пользователя с удаленным информационным ресурсом (ИР) с явным учетом временной последовательности событий и анализа длительности каждого из этапов жизненного цикла доверенной среды.

Возникающая потребность в защите информации в рамках эпизодических, относительно малых по времени процессов в настоящее время удовлетворяется, как правило, путем создания на персональном компьютере пользователя доверенной среды на все время использования этого компьютера. Такой подход обусловлен в первую очередь исторически сложившейся практикой, но никак не является чем-то объективно обоснованным. Большинство требований к доверенной среде описывают ее существование только в привязке к решению той или иной задачи, то есть в случае с взаимодействием с внешним ИР, к отрезку времени, связанному с работой пользователя по информационному обмену с ИР. Доверенная среда становится необходимой незадолго до начала сеанса связи и теряет практическую ценность незамедлительно после его завершения. Только в последнее время появились публикации, трактующие организацию доверенной среды как короткую преамбулу сеанса связи с корректным завершением ее функционирования после исчезновения непосредственной необходимости [1].

Анализ изменений, вносимых таким подходом, можно провести в рамках развития мультипликативной парадигмы информационной безопасности с применением вероятностной модели угроз и атак.

Сравнение воздействия на систему защиты в рамках простой модели равновероятных и почти равномерно распределенных по времени атак показывает, что вследствие роста интегрального воздействия на постоянно существующую доверенную среду и в рамках мультипликативной модели с течением времени модельная вероятность успешного отражения очередной атаки снижается, поскольку вероятности отражения каждой атаки независимы при неизменности характеристик и условий существования доверенной среды.

Процесс работы системы защиты можно с хорошей степенью точности считать Марковским только тогда, когда состояние системы не изменяется под действием атак, что в общем случае неверно, поскольку

1) время реакции на атаки является конечным и уже при относительно небольшой интенсивности предшествующие события влияют на способности системы защиты отражать атаки в настоящий момент времени;

2) успешная атака является событием с хотя и малой, но конечной вероятностью, что при рассмотрении систем с большим количеством пользователей неизбежно приводит к нарушению определения Марковского характера процесса — несрабатывание защиты хотя бы для одного из множества пользователей в какой-то момент в прошлом оказывает влияние на пространство состояний системы в будущем, несмотря на успешность работы защиты во всех последующих атаках.

Таким образом, процесс, при котором вероятность нахождения системы пользователь — информационный ресурс (в дальнейшем — системы) в любом из возможных состояний зависит только от вероятности предшествующего состояния, будет Марковским. В Марковском процессе с непрерывным параметром (временем) переходы системы из состояния в состояние задаются интенсивностями переходов.

Свойства Марковского процесса с непрерывным параметром (временем) определяются потоком событий, под воздействием которого система может переходить в различные состояния в случайные моменты времени. К таким потокам относятся пуассоновские потоки, простейшим из которых является стационарный пуассоновский поток.

Обозначим постоянную интенсивность простейшего потока событий как l_{ij} — интенсивность перехода системы из состояния x_i в состояние x_j.

Воздействие атаки на систему является случайным событием, возникающим в произвольный момент времени. Все возможные атаки образуют случайное множество {i},i =1,n.

Множество {i} атак содержит два подмножества: множество парированных атак и множество успешных атак.

Обозначим вероятности указанных исходов соответственно через $P_i(t)$ и $Q_i(t)$.

События из множества событий {i} в момент времени t являются зависимыми событиями и подчиняются теореме сложения вероятностей:

$$P(t) = \overset{m}{P_0}(t) + \sum P_i(t)$$
$$Q(t) = \sum_{i=1}^{m} Q_i(t), \quad (1)$$

где $P_0(t)$ — вероятность исходного состояния системы; m — количество возможных зависимых событий.

Для определения вероятностей $P_0(t)$, $P_i(t)$, $Q_i(t)$ воспользуемся моделью Марковского процесса со счетным множеством состояний и непрерывным временем.

Допустим, что:

- в момент времени t = 0 ситуация исходная;
- последовательность воздействия i-х атак является простейшим потоком с интенсивностью l_i;
- поток благополучных исходов от воздействия на систему i-х атак является простейшим с интенсивностью, равной $l_i r_i$, где r_i — вероятность парирования i-й атаки;
- потоки неблагополучных исходов от воздействия на систему i-х атак являются простейшими с интенсивностью, равной $l_i q_i$, где q_i — вероятность непарирования i-й атаки.

Предположим, как указывалось выше, что события атак, их парирования и восстановления системы происходят одновременно.

Граф состояний переходов в такой модели приведен на рис. 1.

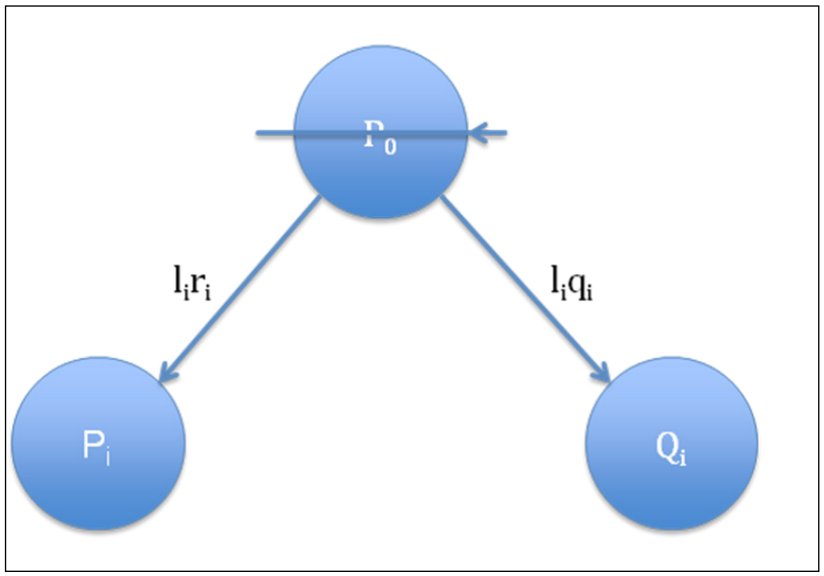

Рис. 1. Граф состояний системы с учетом атак

В узлах графа обозначаются состояния системы после воздействия на нее i-й угрозы. Вершине графа (состояние «0») соответствует состояние системы до воздействия на нее i-й угрозы. На ребрах графа указаны интенсивности перехода системы из исходного состояния в последующее.

В соответствии с графом состояния дифференциальные уравнения имеют следующий вид [2]:

- для вероятности исходного состояния системы

$$d\rho_0/dt = -l_0\rho_0; \quad (2)$$

- для вероятности состояния первого уровня

$$d\rho_i/dt = l_i r_i (1-S_i)\rho_0, \quad (3)$$

$$dQ_i/dt = l_i q_i \rho_0, \quad (4)$$

где

$$l_0 = \sum_{i=1}^{n} l_i r_i (1-S_i) q_i = = \sum l_i (1-S_i r_i);$$

S_i — вероятность восстановления системы после i-й атаки.

Из уравнений (2)—(4) получим выражения для определения ρ_0, ρ_i, Q_i.

$$P_0(t) = \exp_{i=1}^{n} \{-\sum l_i (1-S_i r_i) t\} \quad (5)$$

$$P_i(t) = \{l_i r_i (1-S_i) / \sum_{i=1}^{n} l_i (1-S_i r_i)\} [1 - \exp\{-\sum l_i (1-S_i r_i) t\}] \quad (6)$$

$$Q_i(t) = \{l_i q_i / \sum_{i=1}^{n} l_i (1-S_i r_i)\} [1 - \exp\{-\sum l_i (1-S_i r_i) t\}] \quad (7)$$

Формулы (5)—(7) дают вероятности перехода системы из нулевого (начального) состояния в последующие.

При воздействии на систему случайного множества атак в предельном случае, когда S_i = 1,0 (i=1,n), т. е. когда система полностью парирует i-ю атаку без ущерба для себя, выражения (5), (6), (7) будут иметь вид:

$$P_0(t) = \exp_{i=1}^{n} \{-\sum l_i (1-r_i) t\} = \exp\{-\sum l_i q_i t\}; \quad (8)$$

$$P_i(t) = 0; \quad (9)$$

$$Q_i(t) = \{l_i q_i / \sum_{i=1}^{n} l_i q_i\} [1 - \exp\{-\sum l_i q_i t\}]. \quad (10)$$

Таким образом, вероятность существования состояния, обеспечивающего безопасность информации, дается формулой (8), в которой $l_i q_i$ — поток i-х атак; t — суммарное время атак за период существования системы.

Отчетливо видно, что для доверенного сеанса связи время t будет существенно меньше, чем аналогичный параметр для постоянно действующей доверенной среды, поскольку в суммарное время атак не войдут атаки, происходящие вне времени функционирования ДСС. С учетом экспоненциального характера зависимости для случаев относительно редкого взаимодействия пользователя с информационным ресурсом выигрыш по данному критерию безопасности может быть весьма существенным.

«Физический» смысл сказанного выше состоит в том, что предположение об отсутствии влияния прошлого на будущее при фиксированном настоящем включает в себя, при рассмотрении постоянно функционирующей доверенной среды, экстремально сильное предположение о ее абсолютной надежности в течение всего предыдущего периода времени, на длительность которого не накладывается никаких ограничений, что, в свою очередь, противоречит предполагаемому как условие вероятностному характеру результата работы защиты.

Вместе с тем в рамках той же модели формирование доверенной среды на ограниченное время приводит к исчезновению эффекта «накопления» вероятности несрабатывания защиты.

При этом время формирования ДСС не должно быть неприемлемо большим по сравнению с продолжительностью самого ДСС, что позволит сохранить показатели эффективности работы пользователя аналогичными постоянно действующей доверенной среде.

Разработанная математическая модель жизненного цикла ДСС обеспечивает формальный метод построения и функционирования ДСС в соответствии с требованиями высокой мобильности;

Отсутствие общих (зависимых) для разных ДСС ресурсов позволяет обеспечить заданный уровень информационной безопасности в соответствии с заданными критериями и практически осуществить динамическое управление разграничением доступа в каждом отдельном ДСС.

Из сказанного выше вытекают принципиальные требования к технологической реализации средства формирования ДСС:

- наличие активного внутреннего процессора,
- наличие защищенной от НСД памяти,
- программные средства для встраивания функционала СКЗИ во внешние (по отношению к средству создания ДСС) программные комплексы,
- наличие внутренней энергонезависимой памяти достаточного размера и размещение в ней набора программных компонент, необходимых для всех этапов работы пользователя с внешним ИР (операционной системы, браузера и т. п.),
- наличие высокоскоростного интерфейса к персональному компьютеру, позволяющего провести загрузку доверенной операционной системы и формирование доверенной среды за приемлемое для пользователя время.

Методы реализации ДСС, отвечающие указанным выше требованиям, инвариантны относительно используемых технологий и конфигураций средств вычислительной техники и расширяют общепринятый подход к обеспечению безопасности информации за счет динамического формирования доверенной вычислительной среды путем использования операционной среды и функционального программного обеспечения в течение ограниченного времени сеанса взаимодействия пользователя с информационным ресурсом.

Другим результатом создания такого средства и отказа от поддержания доверенной среды в течение времени невостребованности пользователем защищаемого взаимодействия является исчезновение «привязанности» пользователя и средств обеспечения информационной безопасности к конкретной рабочей станции.

СПИСОК ЛИТЕРАТУРЫ:

1. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ! // Комплексная защита информации. Материалы XV Международной научно-практической конференции (Иркутск (Россия), 1–4 июня 2010 г.). М., 2010. С. 166–169; URL: http://www.accord.ru/konyavskiy_2010_1.html.

2. *Росенко А. П.* Научно-теоретические основы исследования влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированных информационных системах // Известия ТРТУ. Материалы VII научно-практической конференции «Информационная безопасность». Таганрог: ТРТУ, 2005. С. 19–30.