УДК 681.3.067

Бубнов А.А.

ПРОБЛЕМЫ ОРГАНИЗАЦИИ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

Введение

Распределенные вычислительные системы на основе одноранговых сетей существенно расширяют возможности стандартных вычислительных платформ, обеспечивая скоординированную работу подключенных к сети вычислительных устройств, которые теоретически могут находиться в любых географических точках. Технология распределенных вычислений в одноранговых сетях объединяет вычислительные ресурсы различных систем в единое виртуальное вычислительное пространство, позволяя им работать совместно, несмотря на различия в местоположении, типах аппаратного и программного обеспечения.

На сегодняшний день устранены практически все серьезные препятствия на пути масштабируемости при создании распределенных систем такого типа, однако существует ряд вопросов, связанных с обеспечением безопасности распределенных вычислений. Они связанны со спецификой создаваемых систем – высокой степенью территориальной удаленности и децентрализацией вычислений. Большинство современных масштабных приложений объединяют множество распределенных географически и в сети отдельных сервисов [1]. Простые процедуры аутентификации и авторизации явно недостаточны для организации контроля доступа и принятия решения об объемах и сроках предоставления ресурсов. Необходимость аутентификации пользователя/клиента каждым из приложений при предоставлении комплексных услуг является серьезным ограничением для современного электронного бизнеса [2].

Современные коммерческие и некоммерческие решения основаны на использовании Инфраструктуры Открытых Ключей (PKI) [2], обеспечивающей функцию идентификации пользователя, директорий и интегрирующих их мета-директорий, а так же реализующих, соответственно, функции аутентификации пользователя и интеграции распределенных идентификаторов пользователя. Однако такие решения работают только в иерархических PKI-структурах в пределах одного административного или доверительного домена, и в большинстве случаев только в рамках одного распределенного предприятия. В таких случаях при доступе пользователя к определенным сервисам или ресурсам требуется его аутентификация службой доступа ресурса или сервиса, это часто реализуется как набор мандатов, удостоверяющих личность пользователя [4].

Эффективная реализация сервисов аутентификации и авторизации является важным фактором построения защищенных распределенных информационно-коммуникационных систем.

Анализ моделей сетей с организацией доверительных отношений

Сеть с доверием представляет собой альтернативную модель доверия. Эта концепция была впервые использована в технологии Pretty Good Privacy (PGP). Она заключается в том, что каждый пользователь сертифицирует свой сертификат и передает его известным ассоциированным объектам, которые могут подписать сертификат другого пользователя, так как он известен [4].

В данной модели не существует центрального бюро сертификатов. Если пользователю А требуется верифицировать информацию, поступающую от пользователя В, он запрашивает сертификат пользователя В. Так как пользователь А знает пользователя В, то доверяет сертификату и даже может его подписать.

Рассмотрим ситуацию, в которой А получает информацию от С. Пользователь С не известен пользователю А, но у пользователя С есть сертификат, подписанный пользователем

B. Таким образом, рассматриваемая модель распространяется на всю компьютерную сеть. Единственным решением, которое должно приниматься в процессе работы, является число переходов, которому доверяет пользователь. Как правило, это число равно 3 или 4. Кроме того, может возникнуть ситуация, в которой проблема установления доверия по отношению к другому пользователю может иметь неоднозначное решение. Например, B может использовать два пути установления доверия с пользователем E: один через пользователя C и другой - через пользователя D. Так как оба пользователя C и D сертифицируют пользователя E, пользователь B может быть уверен в сертификате пользователя E.

Главной проблемой, связанной с данной моделью доверия, является недостаток масштабируемости. Так как модель сети состоит из двусторонних взаимоотношений, каждый пользователь должен иметь некоторое число таких взаимосвязей, чтобы пользоваться в сети каким-либо доверием. На практике такие взаимосвязи могут отсутствовать, поскольку большинство пользователей работают с небольшим числом связей и редко выходят на уровень трех или четырех переходов.

В [5] вводится формальная модель доверия, построенная на двух параметрах: «степень доверия» и «точность предсказания». Например, можно представить отношение субъекта A к субъекту B как интервал на отрезке [0,1]. Медиана интервала соответствует степени доверия, а длина интервала — предполагаемому разбросу действительного значения (чем меньше длина, тем больше точность предсказания).

Алгоритмическая модель принятия решений с учётом доверия и риска при поступлении нового отзыва пересчитывать обе характеристики доверия, например, как медиану и среднеквадратичное; при «хорошем» поведении мы получаем сужающийся интервал. Недостаток — модель не чувствительна к динамическому, меняющемуся во времени поведению агента (она не различает «сегодня» и «месяц назад» в той формальной постановке, в которой она представлена).

Экспериментальный подход, описанный в [6], содержит общую формулу вычисления степени доверительности отношений как взвешенную сумму положительных отзывов об участнике от других участников (умноженных на доверительность каждого отзыва и на доверие к тем, кто этот отзыв оставил) и «адаптивного контекста сообщества» рассматриваемого участника.

«Адаптивный контекст сообщества» — это такой модификатор метрики, который служит компенсацией за существующие в системе разного рода деформации мотивов для оставления отзывов (например, получение рейтинга по количеству оставленных отзывов).

Данный подход позволяет получить неплохой результат для «неровного» поведения участников – т.е. выявить колебания в их поведении. Однако данный метод подсчёта, учитывая смену поведения участников, никак не защищает систему от проблемы «повторного входа», т.е. ситуации, когда участник просто очищает свою текущую репутацию и входит в систему заново, с «пустой» историей.

Анализируя изложенные подходы можно сделать вывод, что эффективное решение проблемы множественной идентификации пользователей требует изменения самой парадигмы в построении инфраструктуры безопасности раепределенных сервисов и приложений, по сравнению с традиционной архитектурой безопасности. Также необходимо выполнить исследования вопросов применения отношений доверия при объединении политик безопасности различных узлов децентрализованной распределенной сети.

Децентрализованная индивидуальная модель репутаций

Предлагаемая модель репутаций, используя децентрализованный подход, позволяет частично решить отмеченные недостатки доверительных моделей. Суть предложенного алгоритма можно свести к следующему.

Определим конечный результат диалога между двумя узлами как:

- стартовые условия, определяющие ход действия — и действительный результат такового действия;
- стартовые условия, определяющие формальные условия транзакции — и действительные условия совершившейся транзакции.

Тогда, конечный результат можно представить кортежем r вида

$$r = (a; b; L; X_f; X; t), \tag{1}$$

где a и b — узлы, устанавливающие отношения;

$$L = \{l_1, l_2, ..., l_n\} \tag{2}$$

— набор записей, определяющий состав отношений;

X_f и X — два вектора, содержащие, соответственно, оговорённые и действительные результаты транзакции;

t – время подписания договора.

Определим Q — как множество всех возможных исходов, у него есть подмножество $Q(a,b) \in Q$, касающееся только рассматриваемой пары узлов. Задача модели - отображать непосредственное взаимодействие между узлами. Репутация, которая учитывает это взаимодействие, является наиболее надёжной, потому что апеллирует к непосредственному раннему опыту общения с данным конкретным узлом. Тогда репутацию конечного результата $R_{r(a,b)}(\varphi)$ можно рассчитывать непосредственно исходя из базы данных таких исходов, где φ – тип репутации, подмножество прецедентов исхода, определяется индексом состава отношений и зависит от предметной области.

Определим $S(\varphi)$ как связь между типом репутации и отдельными прецедентами исхода. Каждый прецедент описывается кортежем в форме (l_i, α_i). Первый параметр – это одна из составляющих отношений L, вторая описывает отношение между прецедентом и репутацией с учетом знака (увеличивается ли она в случае появления данного прецедента или нет) и вес данного прецедента при общем подсчёте репутации.

Для подсчёта репутации используем формулу взвешенного среднего:

$$R_{r(a,b)}(\varphi) = \sum_{r_i \in Q(a,b)} \rho(t_i, t) \cdot \sigma(r_i, S(\varphi)), \tag{3}$$

где

$$\rho(t_i, t) = \frac{\frac{t_i}{t}}{\sum_{r_j \in Q(a,b)} \frac{t_j}{t}} \tag{4}$$

временной вес исхода с учётом временного веса всех исходов;

$$\sigma(r_i, S(\varphi)) = \omega(\upsilon(X_S) - \upsilon(X_f)), \tag{5}$$

содержательный вес исхода.

Формула суммирует значения, получаемые для каждого конкретного исхода через произведение указанных двух факторов.

Содержательный вес исхода определяется как разница в ценности транзакции и ценности результата этой транзакции. Выражение считается как функция $\omega(*)$ разности значений функций ценности $\upsilon(X)$ от вектора оговорённого в контракте положения X_f и вектора X_S, получаемого путем замены в векторе X_f ожидаемых значений на фактические для тех позиций, которые затронуты в записях $S(\varphi)$ рассматриваемого типа репутации:

$$X_{S_i} = \begin{cases} X_i, i \in S(\varphi) \\ X_{f_i}, i \notin S(\varphi) \end{cases}. \tag{6}$$

Функция $\sigma(*)$, в свою очередь, учитывает степень и знак изменения результата и предлагается в виде

$$\sigma(x) = \sin(\frac{\pi}{2} \cdot x). \qquad (7)$$

Кроме подсчёта значения репутации важно знать, насколько это значение достоверно. Используя методику, предложенную в [7], нами детально рассмотрены два параметра, позволяющие оценить надёжность подсчитанного значения: количество исходов, принятых во внимание при подсчёте значения и разброс в оценках этих исходов.

Установлено, что на определенном уровне взаимодействия (с достаточно большим числом исходов) узлы попадают в фазу «близких» отношений, когда рост числа исходов более не увеличивает надёжность сформировавшегося мнения. Следует так же отметить, что координаты данной точки в значительной мере зависят от предметной области.

Применение отношений доверия при объединении политик безопасности

Создание модели системы в виде набора строгих математических соотношений, описывающих ее начальное состояние и ограничений на возможные переходы, не нарушающие политику безопасности многокомпонентной системы, что позволило бы путем строгих логических рассуждений доказать справедливость ее выполнения в любых состояниях системы, оказывается весьма сложной задачей. С учетом объективно высокого уровня сложности подобных систем и огромного числа возможных ее состояний в процессе эксплуатации, требуется разработка новых подходов к построению математических моделей гарантированно защищенных распределенных объектов. В качестве примера, подтверждающего перспективность такого подхода, можно указать модель распределенной компьютерной системы, представленной в виде обобщения автоматной модели невлияния Гогена-Месгауэра в случае вероятностного автомата [8]. Такой подход позволяет редуцировать традиционную детерминированную модель с большим числом состояний к вероятностной модели с таким их числом, которое позволяет построить необходимые и достаточные локальные условия, обеспечивающие глобальную безопасность системы.

Выполним анализ различных вариантов объединения основных политик безопасности, приведенных в [3] на основе отношений доверия.

Определим, что информационная система *C* является корректным объединением систем *A* и *B*, если множество объектов системы *C* является объединением множеств объектов систем *A* и *B* и ограничение политики безопасности системы *C* на систему *A* или *B* совпадает, соответственно, с политикой безопасности системы *A* или *B*.

Для ролевой модели разграничения доступа, когда отношения доверия определяются с использованием субъектов систем, необходимы вспомогательные построения:

- каждый субъект *s*, не являющийся пользователем, соотнесен с некоторым сеансом *e*;
- при этом субъекту *s* приписывается подмножество ролей *e*.

Любое корректное объединение ролевых политик, а также политик типа Type Enforcement, безопасности информационных систем *A* и *B* могут быть выражены с помощью пары отношений доверия $T_{A,B}$ и $T_{B,A}$.

Для многоуровневой модели разграничения доступа:

- система *C* может являться корректным объединением систем *A* и *B* только в том случае, если решетки ценностей систем *A* и *B* вложены в решетку ценностей системы *C*;
- система *C* может являться корректным объединением систем *A* и *B*, построенным с помощью отношений доверия только в том случае, если решетки ценностей систем *A* и *B* изоморфны решетке ценностей системы *C*.

В качестве недостатков внедрения простых отношений доверия следует отметить, что на практике один субъект может доверять другому не полностью, совершая от его имени

только некоторые операции. Кроме того простые отношения доверия позволяют объединять не все виды политик безопасности.

Указанные проблемы в значительной мере позволяет решить подход, связанный с использованием ограниченных отношения доверия.

Пусть каждому субъекту b информационной системы B приписана решетка доверия L_b. Ограниченным отношением доверия между системами A и B называется подмножество $T_{A,B}$ прямого произведения множеств $S(A)$ и $S(B)$, в котором каждому элементу (a,b) приписан элемент $l(a,b)$ решетки доверия L_b, называемый уровнем доверия. Каждой операции, которую может выполнять субъект S_B, приписан минимальный уровень доверия. Запрос субъекта S_A выполняется, если уровень доверия S_B к S_A выше минимального уровня доверия для указанного запроса. В этом случае справедливо утверждение, что любое корректное объединение многоуровневых политик безопасности информационных систем A и B может быть выражено с помощью пары ограниченных отношений доверия между системами A и B.

Выводы

Существующие механизмы безопасности, используемые для организации совместных распределенных вычислений, не обладают достаточной гибкостью для удовлетворения требований, связанных с определением степени доверия источнику запросов и ресурсов, не в полной мере решают проблемы расстановки приоритетов. При анализе безопасности распределенных систем требуется идентификация факторов и проблем, влияющих на степень доверия к услугам распределенной системы. Сетевая топология, узловые уровни оценки недостаточны для такого анализа. Такие факторы, как среда безопасности распределенной системы, структура управления и взаимодействие между различными механизмами безопасности в рамках принятой политики могут играть ключевую роль.

Проблемы, возникающие при адаптации концепций защиты отдельных ЭВМ по отношению к безопасности распределенной системы можно решить введением распределенной доверенной вычислительной базы или сети, в которой каждая участвующая узловая сущность доверяет всем остальным, реализующим распределенную систему. В статье предложена математическая модель системы репутаций, использующая децентрализованный подход и позволяющая более эффективно управлять доверием в среде распределенных информационно-коммуникационных систем.

По результатам выполненного анализа методов объединения политик безопасности различных узлов можно сделать вывод, что наиболее перспективными подходами к объединению политик безопасности распределенных систем можно считать системы и модели, основанные на ограниченных отношениях доверия, которые требуют проведения дополнительных исследований.

Список литературы

1. *Кореньков В., Тихоненко Е.* Организация вычислений в научных областях. Открытые системы, № 2, 2001. -С. 29-34.

2. *Черней Г.А.* «Проблемы аутентификации в информационных системах»- Кишинев: Реклама, 2001. – 112 с.

3. *Халатенко А. В.* Реализация многоуровневой политики безопасности в ОС Linux. Информационная безопасность. Инструментальные средства программирования. Микропроцессорные архитектуры. М.: НИИСИ РАН, 2003. -С. 107-125.

4. *U. Maurer.* Modelling a public-key infrastructure. Computer Security –ESORICS '96, LNCS 1146, Springer Verlag, 1996.

5. *V. Cahill, et al.* Using Trust for Secure Collaboration in Uncertain Environments. IEEE Pervasive Computing Magazine, 2003, vol. 2, №3, P. 52-61.

6. PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities, ACM IEEE Volume 16 , Issue 7, 2004. -P. 843 – 857.

7. *G. Zacharia.* Collaborative reputation mechanisms for online communities. Massachusetts Institute of Technology, September 1999.

8. *Goguen J. A., Meseguer J.* Unwinding and Inference Control. 1984, Symposium on Security and Privacy, P. 75-85, IEEE, May 1984.

Поступила 19.10.2006 г.

УДК 004.056.5: 518: 512.624.3 **Кобозева А.А., Маракова И.И.**

МЕТОД ПОВЫШЕНИЯ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ К ВОЗМУЩАЮЩИМ ВОЗДЕЙСТВИЯМ

Введение

В настоящий момент во всем мире назрел вопрос разработки методов защиты информации, представленной в цифровом виде, среди которых важное место занимают стеганографические методы [1].

Несмотря на то, что стеганографирование может осуществляться различными способами, общей чертой этих способов является то, что секретное сообщение, или дополнительная информация (ДИ), погружается в некоторый объект, или основное сообщение (ОС), не привлекающий внимания, который затем открыто пересылается адресату. Одной из основных проблем при этом является проблема обеспечения устойчивости таких стеганографических сообщений к возмущающим воздействиям в канале связи.

Дополнительным толчком для развития исследований в области компьютерной стеганографии в последнее время послужило появление новых областей ее применения. В качестве ОС, или контейнера, может использоваться видео, изображение, аудиозаписи и т.д. Не ограничивая общность рассуждений, для простоты изложения далее в качестве контейнера рассматривается монохромное изображение.

В настоящей работе предлагается новый метод организации пересылки и декодирования ДИ, основанный на решении систем линейных алгебраических уравнений (СЛАУ), целью которого является обеспечение повышения устойчивости стегоалгоритмов к возмущающим воздействиям; обосновываются достаточные условия нечувствительности задачи о декодировании ДИ путем решения СЛАУ к погрешностям исходных данных. В качестве инструмента исследования используется теория относительных возмущений [2].

Число обусловленности задачи - мера ее чувствительности к возмущениям входных данных

Любое монохромное изображение можно рассматривать как функцию f двух переменных x и y, областью определения которой, не ограничивая общности рассуждений, можно считать $[0,1]\times[0,1]\subset R^2$:

$$f(x,y):[0,1]\times[0,1]\to R^+. \qquad (1)$$

Пусть $f(x,y)$ является основным сообщением, используемым для встраивания в него некоторой ДИ с целью ее скрытой передачи, также рассматриваемой в виде функции $z(x,y)$ вида (1), тогда погружение секретного сообщения в контейнер равносильно получению нового изображения, т.е. построению новой сложной функции $s(x,y)=F(f(x,y),z(x,y))$ вида (1). Функцию $s(x,y)$ в дальнейшем будем называть стегосообщением.