ПОНЯТИЕ ДОВЕРИЯ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

П.К. Шиверов, В.В. Бондаренко

Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет) (СГАУ), Самара, Россия

В данной статье предлагается к рассмотрению формальное представление доверия в контексте защиты информации. Даётся определение, приводятся основные понятия и рассматриваются базовые элементы доверия.

Ключевые слова: доверие, информационная безопасность, защита информации, компьютерная безопасность, риск, репутация, базальное доверие, внешнее доверие, модель оценки доверия, канал связи.

Введение

Понятие информационной безопасности тесно связано с понятием доверия. Удостоверяющие центры, протоколы аутентификации, модели угроз и некоторые отдельные правовые аспекты защиты информации используют механизм доверия в качестве базового понятия [1-3]. Вместе с тем, определения доверия в информационной безопасности не существует.

В предложенной статье будет дана попытка определить понятие доверия в контексте информационной безопасности и рассмотреть математическую модель оценки доверия.

Определение доверия

Прежде чем рассматривать модель оценки доверия, необходимо выбрать то его определение, из которого можно будет исходить в дальнейшем.

Доверие – это субъективное ожидание агентом A будущего поведения агента B на основе истории их взаимодействий [4].

Рассмотрим основные определения доверия и свойства вытекающие из них.

Доверие — это уверенность в поступке другого человека определённым образом.

Доверие зависит от степени соблюдения оговорённых правил, а также от умения правильно действовать, достигая обозначенной цели для субъектов, даже в случаях, когда некоторые правила не оговорены [3].

Доверие может выступать в двух ролях. Во-первых, как вера в порядочность, доброжелательность другого человека или, в критических ситуациях как вера обоих агентов в принадлежность к одному и тому же сообществу, требующая от них той или иной степени солидарности. Во-вторых, доверие понимается как готовность следовать правилам игры, принятым в системе, например, отдавать долги, выполнять должностные обязанности,

следовать принятым обычаям. Эти две роли связаны между собой, но не пропорциональны друг другу.

В экономике и компьютерных науках используется следующее, более формальное, представление о доверии в рамках теоретико-игрового подхода.

Доверие - это субъективная вероятность со стороны *A* выполнения данного действия стороной *B*, которое *A* ещё не может наблюдать и которое влияет на действия *A*. Действие *B* повлияет на благосостояние *A* и его выгоду [5].

Это определение хорошо показывает взаимную связь доверия и рисков субъекта доверия (того, кто доверяет).

Однако, следует отметить, что доверие может не быть абсолютным и, в ряде случаев, оценка его значения может являться лишь способом выбора "наименьшего зла". Иными словами, доверие - это мера готовности стороны *A* положиться на кого-то или что-то в данной ситуации с некоторой относительной уверенностью, несмотря на возможные негативные последствия.

Отсюда следует, что понятие доверия включает в себя не только уверенность абонента *A* в соответствии намерений абонента *B* его заявленной роли, но и учитывает возможный ущерб, в случае обмана.

Именно это описательное определение понятия доверия позволяет максимально точно составить математическую модель его оценки.

Составляющие доверия

Ниже будут рассмотрены основные понятия и элементы доверия.

Как было отмечено выше, значительную роль в формировании доверия играет понятие **риска** (материального, экономического, репутационного и т.д.).

Субъекту доверия всегда приходится принимать на себя риски, связанные с возможной ошибкой в выборе доверенного объекта. Риск определяет возможные негативные последствия принятия решения. В ряде работ, посвящённых методам оценки доверия, вводится понятие порога "приемлемого" ущерба, который может оказаться настолько высоким, что даже при минимальной вероятности реализации соответствующей угрозы, может свести доверие к нулю [6].

Ещё одним фактором, влияющим на уровень доверия, является **репутация**, роль которой сводится к накоплению знаний об оцениваемом объекте [7].

Репутация - это восприятие об агенте, сложившееся на основе его прошлых действий, о его намерениях и нормах [5].

Особенную роль репутация играет в оценке доверия в электронной коммерции и социальных сетях, где позволяет пользователю выбирать более надёжных собеседников, поставщиков товаров или покупателей на основе отзывов других пользователей.

Иными словами, репутация - это коллективный опыт, связанный с поведением оцениваемого объекта.

Значение репутации каждого объекта глобально (оно одинаково для всех пользователей), в то время, как значение доверия персонально (каждый субъект формирует своё значение доверия по отношению к каждому объекту) [8].

Также, к различиям в расчётах доверия и репутации следует отнести следующее.

Во-первых, доверие, как правило, является более "общим" понятием, которое выводится на основании многих субъективных и объективных знаний, в то время, как репутация рассчитывается исходя исключительно из объективных знаний об объекте (поведение при конкретных событиях, транзакциях).

Во-вторых, для понятия доверия существенным является свойство транзитивности. Репутация, подразумевающая одинаковое глобальное значение для всех субъектов, не имеет такого свойства [9].

Обобщая всё вышесказанное, можно заключить, что репутация - это статистическая характеристика объекта (например, в 10 случаях из 15 результат взаимодействия был отрицательным), в то время, как доверие является субъективным отношением к нему (например, учитывая большое количество отрицательных результатов, в конкретном случае объекту всё-таки можно доверять).

Эффективность расчёта параметра репутации определяется тремя обязательными правилами:

- продолжительность жизни оцениваемого объекта (в случае, если на каждый сеанс общения вырабатывается новый объект, невозможно использовать накопленные знания о нём) [7];

- своевременность оценки текущих взаимодействий (значение параметра репутации должно корректироваться в соответствии с новым полученным знанием об объекте) [9];

- накопление знаний об объекте (оценки предыдущих взаимодействий должны учитываться при общей оценке репутации, если они вообще были получены) [10].

Немаловажной составляющей доверия является среда взаимодействия участников, в которой реализуются механизмы репутации и доверия. По своей сути, основной **характеристикой среды** взаимодействия является надёжность выбранного канала взаимодействия (отсутствие возможности искажения, раскрытия конфиденциальности и отказа доступа к информации).

Рассматривая доверие, как субъективное понятие, необходимо однозначно определить ещё два термина.

Субъект доверия - это тот, "кто доверяет" (пользователь, агент, сервис и т.д.).

Объект доверия - это то, чему доверяют. Объектами доверия могут выступать как пользователи, так и сервисы, модули, материальные, абстрактные и программные сущности [6].

При вычислении значения доверия степени ответственности объекта и субъекта также играют немаловажную роль. **Ответственность абонента** зависит от обязанностей и прав предоставленных ему в конкретном случае.

Модель оценки доверия

Для формального описания понятия доверия необходимо ввести обозначения приведённых выше параметров и рассмотреть зависимость значения доверия от них.

Исходя из вышесказанного, можно утверждать, следующее.

Во-первых, доверие *D* обратно пропорционально риску *R*.

Во-вторых, очевидно, что объект скорее поверит тому источнику, который организовал передачу, через более надёжный канал передачи данных. Иными словами, при расчёте доверия характеристика канала связи *X* оказывает прямое влияние на уровень доверия к абоненту. Конкретизировав условия задачи можно определить надёжность *X* как предварительно заданную табличную величину. Так, например, в случае взаимодействия абонентов в вычислительной сети, значение *X* будет зависеть от возможности нарушения и незаметной прослушки канала злоумышленником. Беспроводные сети являются наиболее уязвимыми, поэтому *X* будет равен 0,1. Проводные сети *Ethernet* сложнее поддаются прослушиванию, поэтому *X=0,3*. Оптоволоконные сети имеют достаточно высокий уровень защиты, отсюда *X=0,9*. Квантовый канал передачи данных наиболее надёжен, поэтому *X=1*. Значение *X* можно задать иначе, но для объективности оценки и сравнения полученных результатов, необходимо использовать одну и ту же таблицу значений.

В-третьих, преддоверие *pD* (репутация) прямо пропорционально доверию.

Зависимость доверия от роли (ответственности) μ абонента однозначно задать нельзя. Дело в том, что доверие может быть разделено на два субъектных типа: базальное (к самому себе) и внешнее (к другому абоненту).

В базальном доверии роль представляет из себя дополнительные риски для объекта. Во внешнем доверии роль предполагает дополнительные гарантии.

Из вышесказанного можно сделать вывод, что доверие описывается следующими формулами.

$$D_{баз} = \frac{pd \times X}{R + \mu} \qquad (1)$$

$$D_{внеш} = \frac{pd \times X + \mu}{R} \qquad (2)$$

В формулах (1) и (2) μ может быть нулевым в случае, если роль абонента специально не оговорена, что однако не влияет на логику процесса выработки доверия. В связи с этим μ не может учитываться в произведении.

Заключение

Таким образом, существует возможность однозначно определить понятие доверия и составить модель оценки его значения в зависимости от заданных условий.

Представленный подход позволяет количественно оценить доверие к различным системам, абонентам и защитным механизмам, что, в свою очередь, даёт возможность автоматизировать процесс выработки доверия, а также упростить выбор решений, предлагаемых в контексте заданной ситуации.

Литература

1. Полянская О.Ю. Инфраструктуры открытых ключей: учебное пособие / О.Ю. Полянская, В.С. Горбатов. – М.: Издательство «Открытые системы», 2007. – 370 с.
2. Алфёров А.П. Основы криптографии: учебное пособие / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. - М.: Издательство «Гелиос АРВ», 2002 - 480 с.
3. Чмора А.Л. Современная прикладная крип-тография: учебное пособие / А.Л. Чмора – М.: Издательство «Гелиос АРВ», 2001.– 244 с.
4. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков. - Ползуновский Вестник №2/1 2012 – С. 61-67
5. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие – М.: Издательский центр «Академия», 2009. – 272 с.
6. Marsh S. Formalising Trust as a Computational Concept. 1994. Ph.D. dissertation, University of Stirling.
7. Richardson M. Trust management for the semantic web. International Semantic Web Conference. 2003 - C. 351-368.
8. Fudenberg D. Reputation in the simultaneous play of multiple opponents. Review of Economic Studies. 1987. № 4. C. 541 – 568.
9. Beaufils B. Reputation games and the dynamics of exchange network. Lille: University of Science and Technology, 2004. – 22 с.
10. Carter J. Reputation Formalization for an Information-Sharing Multi-Agent Sytem. Computational Intelligence. C. 515-534.