

Взаимосвязь понятий репутации и риска при разработке формальной модели доверия

П.К. Шиверов^а, В.П. Цветов^а, С.С. Яковлев^а

^а Самарский национальный исследовательский университет имени академика С.П. Королёва, 443086, Московское шоссе, 34, Самара, Россия

Аннотация

В данной статье предлагается к рассмотрению формальное представление понятий репутации и риска в процессе разработки модели доверия в контексте защиты информации, а также понятие опыта, как следствия из процесса выработки доверия.

Ключевые слова: информационная безопасность; доверие; репутация; опыт; риск; важность

1. 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:[1,2,3]. Вместе с тем, определение и структура понятия доверия в области информационной безопасности не представлены.

В предложенной статье будет дана попытка определить такие важные составляющие доверия, как репутация и риск и рассмотреть их взаимосвязь в контексте количественной оценки доверия.

2. Предпосылки изучения репутации и риска

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

Доверие - это субъективная вероятность со стороны А выполнения данного действия стороной В, которое А ещё не может наблюдать и которое влияет на действия А. Действие В повлияет на благосостояние А и его выгоду [4].

Это определение хорошо показывает взаимную связь доверия и рисков субъекта доверия.

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

Именно это описательное определение структуры понятия доверия позволяет максимально точно составить математическую модель его оценки, а также, выделить такие важные понятия, как репутация объекта и риск субъекта доверия.

3. Формальная оценка репутации объекта доверия

Одним из основных факторов, влияющих на уровень доверия, является **репутация**, роль которой сводится к накоплению знаний об оцениваемом объекте [5].

Репутация - это знание об агенте, сложившееся на основе его прошлых действий, о его намерениях и нормах, накопленное в некотором сообществе абонентов [6].

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 абонентов), в то время, как значение доверия персонально (каждый субъект формирует своё значение доверия по отношению к каждому объекту, исходя из репутации и личного опыта). Однако, именно репутация позволяет абоненту сделать выбор в пользу того или иного объекта, фактически, выполняя рекомендательную роль.

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.

Обобщая всё вышесказанное, можно заключить, что репутация - это статистическая характеристика объекта, 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);

- своевременность оценки текущих взаимодействий (значение параметра репутации должно корректироваться в соответствии с новым полученным знанием об объекте);
- накопление знаний об объекте (оценки предыдущих взаимодействий должны учитываться при общей оценке репутации, если они вообще были получены).

Обобщая всё вышесказанное, можно заключить, что репутация - это статистическая характеристика объекта.

$$pd = \frac{\sum_{i=1}^n q_i}{n} \quad (1)$$

где n - общее количество взаимодействий с объектом внутри сообщества абонентов,

$$q_i = \begin{cases} 1, & \text{если на } i \text{ - ом взаимодействии не произошло обмана} \\ 0, & \text{если на } i \text{ - ом взаимодействии произошёл обман} \end{cases}$$

4. Формальная оценка риска субъекта 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.

Согласно стоимостной мере риска (*Value at Risk*), оценка производится по формуле:

$$R = I \times P \quad (2)$$

где R - это риск;

P - это вероятность реализации угроз субъекту от объекта взаимодействия и от сторонних объектов (злоумышленников, вероятность существования которых нельзя исключать);

I - это стоимость возможного ущерба, который может получить субъект в случае реализации угроз.

5. Взаимосвязь понятий репутации и риска

Субъекту доверия всегда приходится принимать на себя риски, связанные с возможной ошибкой в выборе на основе оценки репутации доверенного объекта.

Существует несколько исходов взаимодействия субъекта и объекта.

Пусть из общего количества n сеансов связи в m случаях собеседник не обманул субъекта о своих намерениях, то есть, оказался тем, за кого себя выдавал. В таком случае возможны два исхода:

1. объект оказался честен, однако, атака на субъект всё равно произошла (пусть количество таких исходов равно p_1);
2. объект оказался честен и впоследствии в процессе взаимодействия субъект не был атакован (количество таких исходов равно $m - p_1$).

Очевидно, в $n - m$ случаях объект обманул субъекта, то есть выдал себя за того, кем он на самом деле не является. В данном случае также существует два исхода:

1. объект совершил обман и произвёл атаку на субъект (пусть количество таких исходов равно p_2);
2. объект совершил обман, однако, атака не была совершена. Здесь рассматривается случай пассивной атаки, при которой злоумышленник получает несанкционированный доступ к информации, не предназначенной для него, не осуществляя видимых изменений в структуре субъекта (количество таких исходов равно $n - m - p_2$).

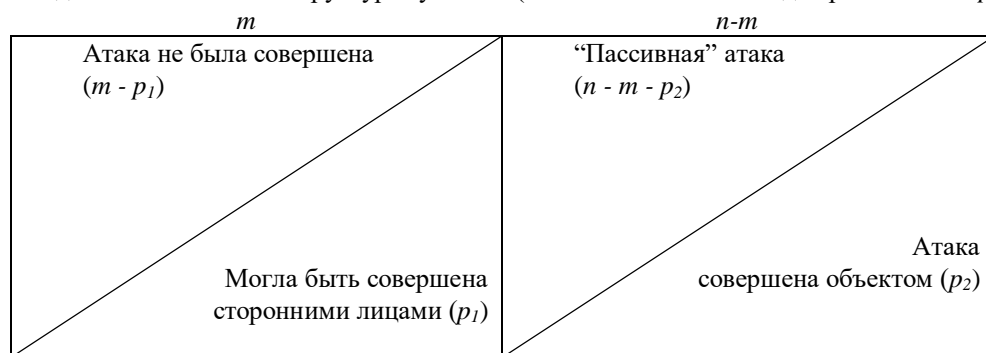


Рис. 1. Возможные исходы взаимодействия субъекта и объекта доверия.

Таким образом, из Рис.1 видно, что вероятность атаки (реализации угроз), используемой при оценке рисков, на субъект доверия описывается формулой, которая включает в себя параметры репутации:

$$P = \frac{n - m + p_1}{n} \quad (3)$$

Полученная формула является динамической, то есть от одного взаимодействия до другого её значение должно меняться, поскольку меняется количество взаимодействий, а с ним и статистическое знание. Таким образом, значение риска работы с объектом также может быть пересчитано.

В данном случае, при непосредственном общении субъекта и объекта вступает в силу понятие не только репутации, но и опыта, которое задаёт последующие статистические данные, полученные субъектом в результате личного общения с объектом.

Иными словами, после выбора объекта доверия субъект начинает взаимодействие с ним. В данном случае, репутация, то есть общее мнение, начинает уходить на второй план, поскольку появляется личный опыт взаимодействия или, по-другому, индивидуальная репутация, опираясь на которую, субъект всегда может изменить предварительно выработанное отношение к объекту.

6. Формальное описание понятия опыта

По своей сути, опыт представляет из себя репутацию, собранную не сообществом абонентов, а одним единственным субъектом доверия, который уже принял решение о взаимодействии с объектом и начал накапливать знания о поведении второго.

Иными словами, опыт можно представить аналогично репутации:

$$\theta = \frac{\sum_{n+1}^{n+t} q_i}{t} \quad (4)$$

где t - общее количество личных взаимодействий субъекта с объектом доверия,

$$q_i = \begin{cases} 1, & \text{если на } i \text{ - ом взаимодействии не произошло обмана} \\ 0, & \text{если на } i \text{ - ом взаимодействии произошёл обман} \end{cases}$$

Правильно учтённый опыт позволяет обеспечить своевременность оценки текущих взаимодействий, поскольку репутация формируется из опыта различных абонентов одного сообщества.

7. Заключение

В данной работе были представлены формализованные записи таких понятий, как репутация, риск и опыт в контексте количественной оценки понятия доверия и их взаимосвязь.

Полученные результаты позволяют получить достаточно точное представление об указанных терминах и использовать их в расчётах, связанных с оценочными проблемами информационной безопасности.

Однако, разработки, описанные в данной статье, являются лишь малой частью от той работы, которую необходимо провести и описать в контексте количественной оценки доверия.

Так, необходимо определить вхождение параметров опыта в расчёт вероятности реализации угрозы. Необходимо рассмотреть понятие стоимости возможного ущерба (важность), из которого будет получено ещё одно важное понятие – минимальный порог доверия, отвечающее за принятие субъектом решения о допустимости взаимодействия с объектом на основе репутационных данных. 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].

Понятие минимального порога доверия также должно играть важную роль во взаимосвязи с личным опытом субъекта. Оценивая индивидуальную репутацию и периодически сравнивая её с порогом доверия, субъект может принять решение о прекращении взаимодействия с объектом, исходя из личных предпосылок, таких, как стоимость собственной информации и опыт взаимодействия.

Литература

- [1] Полянская, О.Ю. Инфраструктуры открытых ключей: учебное пособие / О.Ю. Полянская, В.С. Горбатов. – М.: Издательство «Открытые системы», 2007. – 370с.
- [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 криптография: учебное пособие / А.Л. Чмора – М.: Ирдательство «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.