4 Pedersen, M. Tuning & Simplifying Heuristical Optimisation [Текст] /M.E.H. Pedersen. – University of Southampton, 2010. – 204 с.

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

ПОНЯТИЯ РЕПУТАЦИИ И ОПЫТА В КОНТЕКСТЕ ОЦЕНКИ РИСКОВ, СВЯЗАННЫХ С ДОВЕРИЕМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

(Самарский университет)

Введение

В процессе разработки модели количественной оценки доверия некоторые понятия выделяются в отдельные темы для изучения.

К таким понятиям относятся репутация, опыт, характеристика среды, стоимость информации и оценка рисков. В данной работе рассмотрены понятия репутации и опыта и их места в сложной структуре модели доверия.

Формальная оценка репутации объекта доверия

Одним из основных факторов, влияющих на уровень доверия, является репутация, роль которой сводится к накоплению знаний об оцениваемом объекте [1].

Репутация - это знание об агенте, сложившееся на основе его прошлых действий, о его намерениях и нормах, накопленное в некотором сообществе абонентов [2].

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 [3].

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 [4]:

- 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.

$$pd = \frac{\sum_1^n q_i}{n} \quad (1)$$

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

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

Формальная оценка опыта субъекта доверия и порог взаимодействия

Для того чтобы понять, допустимо ли взаимодействие с объектом в частных субъективных условиях, модель учитывает рейтинг объекта, основанный на опыте абонентов, которые взаимодействовали с ним ранее. Также у нас имеется порог взаимодействия, который должен перейти объект. Порог вычисляется, как среднеарифметическая нормированная важность (I) всех s блоков информации, которые хранятся в защищаемой системе.

$$\mu = \frac{\sum_1^s Ij}{s} \quad (2)$$

Поскольку в процессе сотрудничества объект может дискредитировать себя, формула расчёта репутации должна описываться функцией от времени и после каждого завершения сеанса связи её значение должно вновь сравниваться с порогом взаимодействия. Тем самым, исключается возможность длительной работы с потенциально опасной системой.

Таким образом, возникает понятие индивидуальной репутации или, иначе, личного опыта субъекта. По аналогии с репутацией, опыт можно описать следующей формулой:

$$\theta = \frac{\sum_1^z q_i}{z} \quad (3)$$

где z - общее количество личных взаимодействий субъекта с объектом.

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.

Согласно стоимостной мере риска (*ValueatRisk*) [5], оценка производится по формуле:

$$R = I \times P \quad (4)$$

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.

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 $n - m - p_2$).

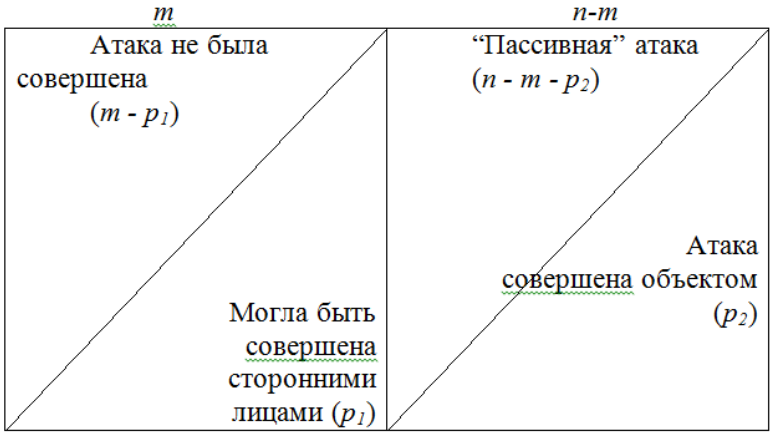

Рис. 1.Возможные исходы взаимодействия субъекта и объекта доверия.

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:

$$P = \frac{n-m+p_i}{n} \quad (5)$$

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.

$$P = \frac{n+z-(m+z\theta)+p_i}{n+z} \quad (6)$$

Выводы

В данной работе выделены фундаментальные понятия доверия в информационных системах такие, как репутация, опыт, порог взаимодействия, показана их роль в контексте оценки рисков.

Полученные результаты будут использованы в дальнейшей работе по систематизации и разработке модели количественной оценки доверия.

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 криптография: 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.

М.С. Шкиндеров, О.В. Чернов

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ПРИ НАНОСЕКУНДНЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЯХ ПО СЕТИ ЭЛЕКТРОПИТАНИЯ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ)

Система контроля и управления доступом (СКУД) – совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через специальные проходы. Увеличение функциональности СКУД, отвечающих современной концепции общественной безопасности, развитие современных технологий, привели к их широкому применению в повседневной жизни [1, 2]. Помимо увеличения функциональности СКУД появились и конструкционные различия, наряду с управляемыми преграждающими устройствами в общественных местах с фиксированным количеством посетителей, когда их идентификация не вызывает проблем (детский сад, школа и т.п.), стали использовать управляемые не преграждающие устройства. Принцип работы таких систем строится на синхронизации подсистем СКУД: датчики прохода, оповещение, фотофиксация.

Таким образом, с широким внедрением в настоящее время СКУД во все области деятельности и, так как, они отвечают за важные функции обеспечения безопасности людей, необходимы дополнительные комплексные исследования и повышение качества их функционирования при воздействие непреднамеренных (задачи помехоустойчивости) и преднамеренных электромагнитных помех (задачи информационной безопасности), в частности по наиболее опасному и вероятному пути - по сети электропитания [3, 4, 5, 6].

Интенсивность непреднамеренных электромагнитных помех связано с наличием естественных источников или с существенным увеличением количества и мощности электронных, радиотехнических и индустриальных источни-