Характерной особенностью этого алгоритма является модульный принцип построения элементов процедуры аутентификации, позволяющий использовать любые, как уже известные элементы, так и оперативно внедрять новые, только разрабатываемые. В отличие от имеющегося программного обеспечения, которое также позволяет по модульному принципу выбирать процедурные элементы, данный алгоритм отличается большей мобильностью сторон, а также автоматизацией создания временной служебной информации.

Автоматизация создания, использования и удаления клиентских ключей безопасности приводит к повышению степени защищённости организуемого канала передачи данных, так как данные ключи, имея достаточную длину и время жизни равную продолжительности сеанса связи, фактически ставят задачу их перехвата в разряд нереальной. Также имеется возможность организации автоматического обновления и настройки элементов системы аутентификации, оперативного внесения изменений в его работу.

По средством данного алгоритма обеспечивается должный уровень защищённости как ресурсов, так и самих пользователей от стороннего вредоносного воздействия. Снижается степень влияния уязвимостей в работе открытых телекоммуникационных сетей. За подобные системами стоит будущее в обеспечении сетевой безопасности.

Литература

1. Сергей Панасенко // Протоколы аутентификации // «BYTE Россия», №4 (80), апрель 2005 (http://www.bytemag.ru/articles/detail.php?ID=9059)

2. Станислав Коротыгин // Протокол сетевой аутентификации Kerberos 5// «iXBT.com», 10 января 2001 (http://www.ixbt.com/comm/kerberos5.shtml)

3. Михаил Кондрашин // Безопасность облачных вычислений // //“Storage News” № 1 (41), 2010 (http://www.pcmag.ru/solutions/detail.php?ID=38248)

4. Шон Дьюби // Kerberos: пациент скорее мертв, чем жив?// «Windows IT Pro», № 03, 2014 (http://www.osp.ru/win2000/2014/03/13039732/)

П.К. Шиверов, В.В. Бондаренко

СОСТАВЛЯЮЩИЕ ЭЛЕМЕНТЫ МОДЕЛИ ДОВЕРИЯ

(Самарский национальный исследовательский университе
имени академика С.П. Королёва)

Введение

Анализ стойкости систем защиты информации, во многом, зависит от возможности установить наличие доверия между двумя или более общающимися абонентами сети. Отсюда вытекает задача получения механизма оценки доверия.

Составляющие доверия

Доверие, являясь одним из основополагающих понятий в психологии, социологии, экономике, информационной безопасности и т.д., само включает в себя несколько различных элементов. Ниже будут рассмотрены основные понятия и элементы доверия.

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 [1].

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

В общем случае, репутация - это сформировавшееся общественное мнение о качествах, достоинствах и недостатках того или иного индивида [1].

Более функциональное определение репутации выглядит так.

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

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

Значение репутации в определении доверия настолько велико, что некоторые модели расчёта фактически отождествляют эти два понятия. Однако, этот подход нельзя считать вполне верным. 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).

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.

Источниками информации для расчёта репутации обычно выступают непосредственный опыт субъекта, косвенная (от свидетелей) или социологическая информация [3].

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).

Немаловажной составляющей доверия является среда взаимодействия участников, в которой реализуются механизмы репутации и доверия. В виду того, что методики оценки доверия решают в первую очередь технические задачи, в качестве среды взаимодействия обычно рассматриваются электронные рынки, пиринговые сети, каналы передачи данных и т.д.

По своей сути, основной характеристикой среды взаимодействия является надёжность выбранного канала взаимодействия (отсутствие возможности искажения, раскрытия конфиденциальности и отказа доступа к информации). Вместе с тем, в большинстве существующих методов оценки доверия среда взаимодействия рассматривается, как контекст для выбора той или иной модели.

Однако, контекстная зависимость имеет более широкую сферу применения. Она определяет предметную область, в которой будет происходить оценка. Существуют и многоконтекстные модели, в которых каждому пользователю ставится в соответствие несколько различных моделей доверия, что значительно усложняет производимую оценку доверия. В связи с этим, большинство моделей доверия работает в одноконтекстном режиме и рассматривает ограниченные, конкретные задачи.

Анализ существующих базовых формальных подходов к оценке доверия

Среди множества существующих вычислительных моделей (метрик) оценки доверия можно выделить примитивные или базовые модели, отвечающие основным требованиям к расчёту значений доверия.

Существующие базовые системы, используют по отдельности такие механизмы, как:

- взятие среднего арифметического значения репутации, без дальнейшего расчёта доверия (eBay);

- расчёт доверия в диапазоне (-1; 1), с учётом невозможности достижения крайних значений (Marsh);

- использование понятия риска на основе таких понятий, как субъективные полезность и важность ситуации (Marsh);

- введение понятия порога доверия, когда возможность доверия зависит от некоторого минимально допустимого значения, при дополнительном введении понятия взаимности, влияющем на рассчётное значение доверия (Marsh);

- обязательное введение априори доверенных объектов - ядра доверия, влияющего на последующее формирование цепей (потоков) доверенных объектов (Advogato Trust Metric) [4].

Все указанные механизмы являются очевидно целесообразными и активно развиваются (Marsh) [4]. Однако, необходимо отметить тот факт, что использование этих механизмов может быть гораздо более объективным и точным при их использовании в совокупности. Так указанный ранее Marsh не учитывает расчёта репутации, а Advogato Trust Metric нуждается в обязательном выборе непоколебимо доверенных объектов, что продиктовано его целевым применением в социальных сетях и блогах для защиты от спама и нежелательных сообщений.

Литература

1. Полянская О.Ю. Инфраструктуры открытых ключей: учебное пособие / О.Ю. Полянская, В.С. Горбатов. – М.: Издательство «Открытые системы», 2007. – 370 с.

2. 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

3. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие – М.: Издательский центр «Академия», 2009. – 272 с.

4. Marsh S. Formalising Trust as a Computational Concept. 1994. Ph.D. dissertation, University of Stirling.

И.М. Янников [1], М.В. Телегина[1], В.А. Куделькин [2]

АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ ОБСЛУЖИВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ И ПОТЕНЦИАЛЬНО ОПАСНЫХ ОБЪЕКТОВ

([1]Ижевский государственный технический университет имени М.Т. Калашникова, г. Ижевск, [2] Консорциум «Интегра-С», г. Самара)

В настоящее время тенденции развития современных систем физической защиты (СФЗ) критически важных для национальной безопасности (КВО) и потенциально опасных объектов (ПОО) связаны с использованием новейших разработок технических средств контроля и охраны и переходом к интегрированным системам безопасности, представляющим собой сложные территориально распределённые автоматизированные системы сбора и обработки информации