$$q_i * l^{n-1} = \frac{Q * r_i^{n+1}}{n * \left(\left(\overrightarrow{[\vec{R} - (R_e)]} + \overrightarrow{r_i} \right) \right)^2}$$

Аппроксимируем потенциал для дыры (рис. 1):

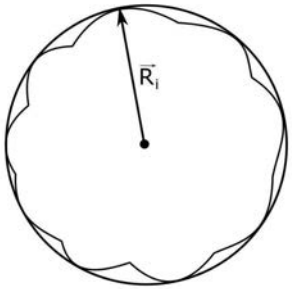

Рис. 1

Приближение при n = 2 обладает наилучшими свойствами.

Литература

1. Newman M. E. J. The structure and function of complex networks //SIAM review. – 2003. – Т. 45. – №. 2. – С. 167-256.

2. Krioukov D. et al. On compact routing for the Internet //ACM SIGCOMM Computer Communication Review. – 2007. – Т. 37. – №. 3. – С. 41-52.

3. Mahadevan P. et al. Systematic topology analysis and generation using degree correlations //ACM SIGCOMM Computer Communication Review. – ACM, 2006. – Т. 36. – №. 4. – С. 135-146.

4. Porter M. A., Onnela J. P., Mucha P. J. Communities in networks //Notices of the AMS. – 2009. – Т. 56. – №. 9. – С. 1082-1097.

5. Carbone L. et al. The spectrum of internet performance //Pasive and Active Measurements (PAM2003). – 2003. – С. 75-88.

Р.В. Чигирь

СИСТЕМА АУТЕНТИФИКАЦИИ В РАСПРЕДЕЛЁННЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

(Поволжский государственный университет телекоммуникаций и информатики)

Развитие систем телекоммуникаций и повсеместное их внедрение практически во все сферы жизнедеятельности человека ведёт к росту доступности различных информационных ресурсов. В свою очередь это способствует тому, что помимо открытых сетевых ресурсов более доступны становятся и источни-

ки с конфиденциальной информацией. Обеспечение безопасности и разграничение прав доступа к данными источникам становится всё более сложной задачей, так как количество уязвимостей с ростом их доступности также становится больше. Многие системы, обеспечивающие безопасность ресурсов, становятся менее эффективными в подобных условиях эксплуатации, а использование отдельных систем становится и вовсе не целесообразным из-за особенностей их функционирования.

Соответственно, системы обеспечения безопасности передачи данных должны учитывать особенности функционирования архитектуры сети и быть гибкими и оперативными во взаимодействии с ними. Одним из важнейших аспектов систем безопасности является процедура аутентификации пользователей, так как именно благодаря ей система может определять всех адресатов передачи данных, их права доступа во взаимодействия и создавать возможность безопасного обмена информацией.

Системы аутентификации пользователей можно условно разделить на две группы: стационарные и мобильные. Данное разделение лежит в различии первоначальных задач, стоявших перед этими системами.

Стационарные системы изначально разрабатывались для функционирования на фиксированных локальных вычислительных сетях. Они должны были обеспечивать идентификацию пользователей, жёстко привязанных за географическими и, возможно, несколькими логическими локациями. В данных системах точки терминации пользователей известны заранее, и остаётся только обеспечить процедуру авторизации пользователей для определения их прав доступа во взаимодействии с ресурсами и другими пользователями. Подобные системы обеспечивали весьма хорошие показатели защищённости передачи информации по каналам передачи данных [1].

Типичным и наиболее ярким представителем таких систем является протокол аутентификации Kerberos [2]. В настоящий момент его активной версией является Kerberos 5, в нём, по сравнению с предыдущими, был расширен список используемых криптографических протоколов, усовершенствованы процедуры постановки и проверки Электронной Цифровой Подписи.

Недостатком данной системы является централизация управления процедурами аутентификации, где каждые из сторон являются зависимыми от решающего центра – так называемого «арбитра», который проводит проверку подлинности пользователей и управляет их правами доступа. Данный элемент ввиду логической распределённости сетей передачи данных может быть скомпрометирован злоумышленниками, что подрывает безопасность передачи информации в таких системах. Подтверждением опасности этой уязвимости служат известные факты об утечке пользовательских данных с крупных сетевых ресурсов в начале 2010 годов [3;4].

Мобильные системы аутентификации разрабатывались для обеспечения мобильного доступа в сеть пользователя независимо от его географического местоположения, и гарантированного предоставления ему сервисов согласно его прав доступа. Данные системы имеют высокие показатели гибкости сопро-

вождения пользователя как в физических так и логических локациях, способны гарантировано определять участников передачи информации при процедуре аутентификации.

Основным же недостатком данной системы является меньшая по сравнению со стационарными системами криптостойкостью канала. Данный недостаток был связан в первую очередь с недостаточной ресурсной мощностью клиентских терминалов для обеспечения функционирования более развитых систем обеспечения безопасности. Недостаток криптостойкости каналов в мобильных системах аутентификации так и не был устранён, несмотря на прогресс в области клиентских терминалов, к тому же уже длительное время на рынке технологий не появляются новые разработки в этом направлении. Подтверждением факта уязвимости мобильных систем служит международный скандал июня 2015 года, связанный с прослушкой немецких политических деятелей через средства мобильной связи.

На сегодняшний день проблема вычислительной мощности клиентских терминалов фактически осталась в прошлом. Современные клиентские терминалы представляют из себя портативные ЭВМ с достаточной производительностью, для решения задач различной степени сложности.

Проводя анализ ситуации в сфере телекоммуникационной безопасности, можно сделать вывод, что для обеспечения максимальных показателей эффективности защиты ресурсов требуются системы с достаточной автономностью и самодостаточностью в работе элементов, а также возможностью адаптации под внешние условия и оперативной реакцией на их изменения.

Такой системой, отвечающей обозначенным требованиям, является система независимой аутентификации с интеллектуальным распределением ключей безопасности в открытых сетях передачи данных.

Стороны взаимодействия наделены всем необходимым функционалом для проведения автономной проверки подлинности второй стороны, а также для подтверждения собственной аутентичности. Это позволяет исключить из взаимодействия третьи стороны с решающим голосом, тем самым убирая возможность их компрометации, а также делая стороны взаимодействия более универсальными. Также это позволяет более гибко и оперативно настраивать политики доступа в сети.

Инициатором открытия сессии служит клиент, отправивший запрос на доступ к ресурсу. Система безопасности ресурса должна подтвердить свою подлинность, а также предоставить данные по параметрам взаимодействия. Затем запрошенный ресурс запрашивает клиента на подтверждение подлинности. На основании полученных данных определяется права доступа. После успешного взаимного подтверждения подлинности участвующих сторон и согласования параметров взаимодействия вырабатывается сеансовый ключ, и сессия считается установленной. После завершения сессии вся информация по взаимодействию удаляется и при новом подключении уже генерируется новая техническая информация.

Переход на симметричное шифрование проводится для ускорения процесса передачи и обработки данных между клиентом и облаком с целью увеличить производительность системы и уменьшить нагрузку на аппаратно-программное обеспечение сторон. Если же в дальнейшем нет необходимости подтверждать авторство передаваемых сообщений, то можно отключить модуль цифровой подписи при передаче данных по симметричному каналу.

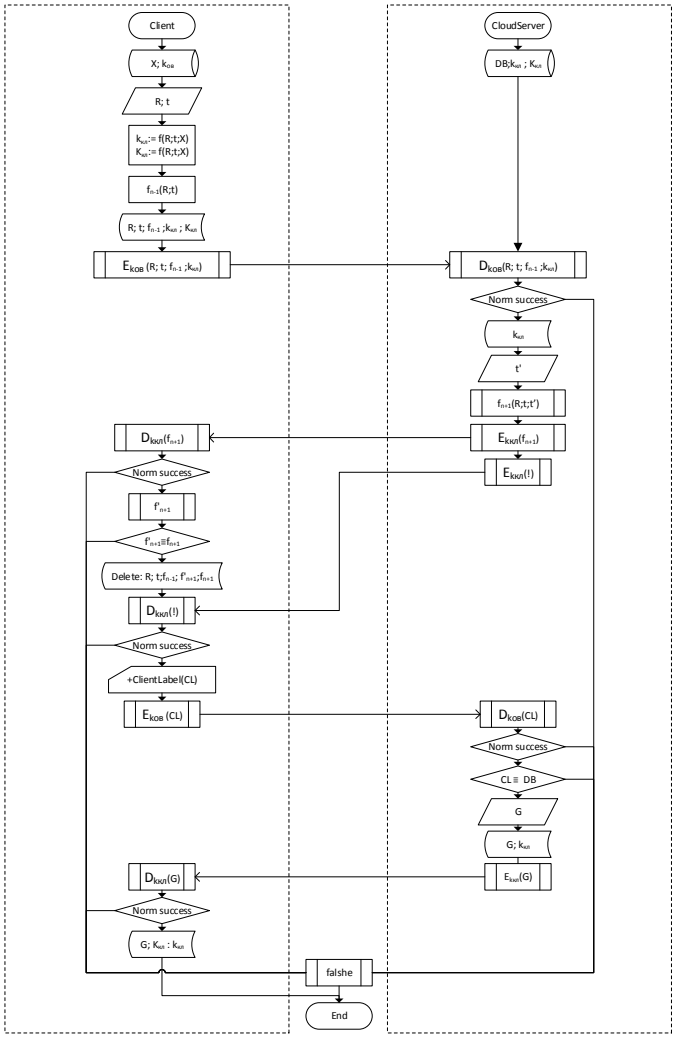

Рис.1 Алгоритм аутентификации в распределённых сетях передачи данных

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].