УДК 502.5:004.056.53

А. А. Платонов

АВТОРИЗАЦИЯ НА ОСНОВЕ ОТКРЫТЫХ КЛЮЧЕЙ ДЛЯ ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ

Предлагается алгоритм аутентификации и авторизации на основе открытых ключей, обладающий свойством распределенности, надежности (за счет создания множественных копий списков ключей). В числе основных его применений — построение модуля регистрации пользователей в геоинформационной системе народного контроля экологического состояния городской среды.

К л ю ч е в ы е с л о в а: геоинформационная система, экологический мониторинг, аутентификация, авторизация, инфраструктура открытых ключей.

Distributed and reliable (due to creation of numerous copies of lists of key) public key based authentication and authorization algorithm is suggested. It will be used as a base for user registration subsystem of public-supported geographic information system of urban territories ecological monitoring.

K e y w o r d s: geo-information system, ecological monitoring, authentication, authorization, public key infrastructure.

При создании геоинформационной системы, позволяющей пользователям взаимодействовать с ней через интернет (например, в плане наполнения ее контентом или создания отметок (комментариев) на карте), остро встает задача создания и поддержки жизненного цикла учетных записей пользователей, также известная как проблема авторизации и аутентификации.

Развитие и интеграция информационных систем в интернет, а также совершенствование механизмов обратной связи с пользователями, хотя и делает возможным новые, улучшенные механизмы развития и наполнения систем знаниями [1], одновременно ставит перед их разработчиками ряд технически сложных задач, включая:

идентификацию и аутентификацию пользователей, предназначенную для упрощения управления коллективными правками, и в то же время достаточно простую и универсальную для того, чтобы пользователи имели как можно более низкий порог вхождения в систему;

перенос регистрационных данных пользователей (например, пары логин-хеш пароля) между системами, чтобы исключить необходимость повторного прохождения процедуры проверки подлинности;

обеспечение безопасности обмена, позволяющего:

а) исключить или снизить возможность перехвата регистрационных данных, в том числе при их многократном использовании в системах разной степени защищенности;

б) снизить возможность незаконного копирования контента пользователями и самим владельцем информационной системы, а также его перехвата при передаче через сети общего пользования;

в) позволить распределенный одноранговый (p2p) обмен информацией между пользователями [2, 3].

Рассмотрим основные способы решения этих задач. Во многих системах, требующих проверки подлинности, достаточно давно [4] используется инфраструктура открытых ключей. Она строится на предположении, что имеется третья доверенная сторона, являющаяся посредником между пользовате-

лем и сервером и выдающая первому или обоим цифровой сертификат. Другой подход к решению данного вопроса состоит в использовании систем с единой точкой входа [5, 6], представляющих программные интерфейсы для подтверждения подлинности внешним системам. Широко распространенным примером такой реализации является OpenID. Несмотря на то, что такой подход упрощает процедуру первичной регистрации пользователя, он обладает существенными недостатками. Во-первых, пользователь вынужден привязывать свои реальные данные, используемые в другой системе, к текущему профилю, что не всегда является приемлемым. Во-вторых, и это имеет даже большее значение для владельца ИС, на надежность системы начинает влиять третья сторона (удостоверяющий центр или ID-провайдер).

Таким образом, вместо решения второй задачи, существующие решения просто переносят процедуру проверки подлинности на внешние сервисы, доступные через интернет.

В инфраструктуре открытых ключей проблема перехвата отсутствует, поскольку закрытый ключ не покидает систему его владельца [7]. В системах типа OpenID или OAuth периодически находятся разнообразные уязвимости [8].

Задача защиты контента от владельца ИС, как правило, не ставится, поскольку концепция Web 2.0 [1, 9] подразумевает безграничное использование пользовательской информации в коммерческих целях.

Несмотря на то, что одноранговые пиринговые сети зарекомендовали себя как надежный и очень эффективный способ передачи больших объемов информации, их развитие сдерживается причинами, описанными в предыдущем пункте.

Суммируя вышесказанное, видно, что в настоящий момент не существует единой системы проверки подлинности, обеспечивающей решение хотя бы большей части основных задач, приобретающих все большую значимость по мере развития веб-технологий.

В то же время, довольно давно известны и получили определенное распространение системы шифрования на основе открытых ключей, позволяющие решить значительную часть описанных выше проблем. В классическом виде такая система представляет собой 3 компонента — источник и приемник информации, а также (необязательное) хранилище открытых ключей. Каждый из участников обмена обладает собственной парой ключей (открытым и закрытым), первый из которых используется для шифрования, а второй — для расшифровки [10] (рис. 1).

Рис. 1

В такой форме данный алгоритм позволяет, с одной стороны, защитить информацию от перехвата (поскольку дешифрование может осуществляться только соответствующим открытому закрытым ключом), а с другой — осуществлять взаимную проверку подлинности (если, например, первый пользователь шифрует некое уникальное значение, второй расшифровывает его и, вновь зашифровав уже открытым ключом отправителя, отправляет обратно).

Рассмотрим модифицированную схему этого метода для осуществления безопасного обмена между пользователями А и Б. Для ее реализации введем третью сторону, обладающую собственной парой ключей — общий ресурс (ОР), одинаково доступный всем пользователям системы. ОР имеет два основных раздела: общедоступный (доступный на чтение всем пользователям и позволяющий добавлять в него новые записи, но не удалять их — аналог стандартной «гостевой книги» сайта) и закрытый, в котором размещаются записи, шифрованные открытыми ключами соответствующих пользователей.

Пусть теперь пользователь А решит безопасно обмениваться с Б конфиденциальной информацией. Для этого:

А инициирует создание пользователем Б пары ключей, например, путем отправки ему ссылки на общедоступный раздел ОР с инструкциями по их получению;

Б создает пару ключей стандартными средствами, например, OpenPGP [11];

Б размещает свой открытый ключ в общедоступном разделе ОР вместе с уникальным идентификатором (например, хэшем этого ключа [12]);

сообщает этот идентификатор пользователю А;

А шифрует информацию и размещает ее в общедоступном разделе вместе с уникальным идентификатором и отправляет ссылку;

Б расшифровывает информацию своим закрытым ключом.

При этом очевидно, что информация не может быть перехвачена третьей стороной, в том числе и самим ОР. Единственный способ для ОР завладеть информацией — изменить идентификатор, привязанный к ключу Б, однако данную возможность можно устранить путем введения дополнительного подтверждения ключа между А и Б.

Рассмотрим теперь безопасный обмен между А и Б таким образом, чтобы ОР тоже имел доступ к информации (рис. 2). Это можно использовать, например, для массовых публикаций информации ОР, доступной всем пользователям.

ОР, как и любой другой участник обмена, может создать свою пару ключей и разместить открытый ключ в своем общедоступном разделе. Далее информация может шифроваться, например, А при помощи данного ключа и после расшифровки ОР зашифровываться им для каждого получателя при помощи соответствующего открытого ключа.

На рис. 2 сплошными линиями показано направление передачи ключей, пунктирными — возможные варианты информационного обмена.

Интересной особенностью предлагаемого метода является то, что открытый раздел в общем случае можно переносить без каких-либо изменений на другие ОР (другие сайты). При этом копируется только база открытых ключей, и все пользователи, включая владельца исходного ОР, могут получить доступ к ресурсам другого ОР, используя свои собственные закрытые ключи.

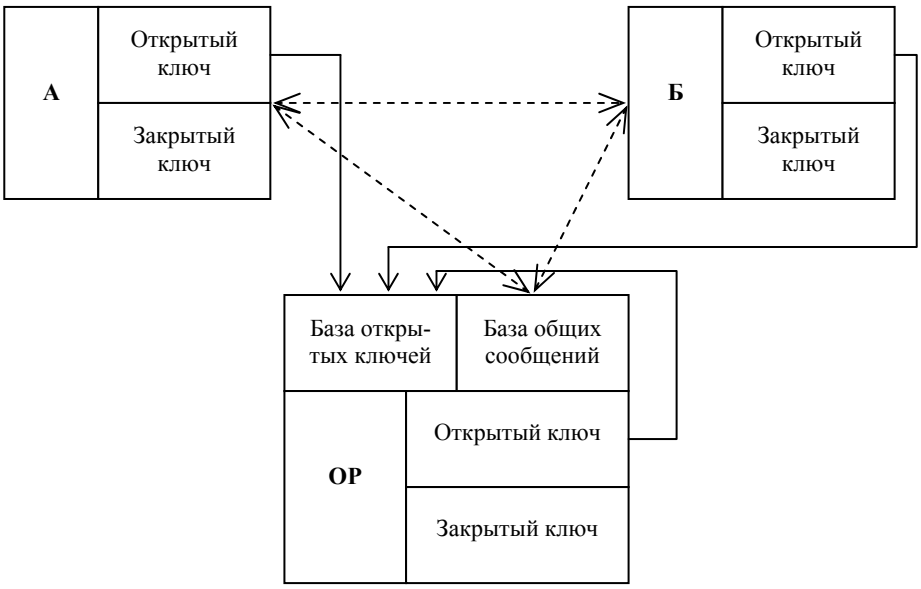

Рис. 2

К потенциальным недостаткам можно отнести невозможность восстановления учетных записей пользователей (поскольку закрытые ключи создаются самими пользователями и никогда не передаются на сервер). Эту особенность можно обойти путем применения дополнительных сервисов облачного хранения типа DropBox или GogleDrive [13], предварительно шифруя ключи любым стандартным способом, например, GnuPG.

Таким образом, предложена эффективная схема аутентификации и авторизации на основе открытых ключей, обладающая свойством распределенности, надежности (за счет создания множественных копий списков ключей) и позволяющая решать следующие основные задачи:

защита контента пользователя от перехвата сторонними лицами, в том числе и владельцем ресурса общего доступа (если это требуется);

копирование базы аутентификационных данных на другие ресурсы общего доступа без возможности их утечки;

предоставление возможности прямого (однорангового) обмена информацией между пользователями.

В числе основных применений алгоритма можно выделить его использование в качестве основы для построения системы регистрации пользователей в геоинформационной системе народного контроля экологического состояния городской среды.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Musser J., O'Reilly T.* Web 2.0: Principles and best practices. Sebastopol, CA : O'Reilly Media, 2007.

2. *Санжапов Б. Х., Садовникова Н. П.* Согласование целей при эколого-экономическом обосновании градостроительного проекта с учетом ограничений на значения характеристик, входящих в систему средств, в условиях нечеткой информации // Вестник ВолгГАСУ. Сер.: Стр-во и архит. 2011. Вып. 21(40). С. 151—159.

3. *Castillo J. A. R.*, *Jilveseu A., Caragea D., Pathok J., Honavar V. U.* Information extraction and integration from heterogeneous, distributed, autonomous information sources-a federated ontology-driven query-centric approach // Information Reuse and Integration, 2003. IRI 2003. IEEE International Conference on. IEEE, 2003. Pp. 183—191. doi: 10.1109/IRI.2003.1251412.

4. *Aiello L. M., Milanesio M., Ruffo U., Schifanella R.* Tempering Kademlia with a Robust Identity Based System // Peer-to-Peer Computing, 2008. P2P'08. Eighth International Conference on. IEEE, 2008. Pp. 30—39. doi: 10.1109/P2P.2008.40.

5. *Lesueur F., Mé L., Tong V. V. T.* An efficient distributed PKI for structured P2P networks // Peer-to-Peer Computing, 2009. P2P'09. IEEE Ninth International Conference on. IEEE, 2009. Pp. 1—10. doi: 10.1109/P2P.2009.5284491.

6. *Lesueur F., Mé L., Tong V. V. T.* A Sybil-Resistant Admission Control Coupling SybilGuard with Distributed Certification // Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2008. WETICE'08. IEEE 17th. IEEE, 2008. Pp. 105—110.

7. *Sit E., Morris R.* Security Considerations for Peer-to-Peer Distributed Hash Tables // Peer-to-Peer Systems. Springer Berlin Heidelberg, 2002. Pp. 261—269.

8. *Balfanz D., Smetters D. K., Stewart P., Wong H. Ch.* Talking to Strangers: Authentication in Ad-Hoc Wireless Networks // NDSS. 2002.

9. *Alnemr R., Meinel C.* Getting more from reputation systems: A Context-aware reputation framework based on trust Centers and agent lists // Computing in the Global Information Technology, 2008. ICCGI'08. The Third International Multi-Conference on. IEEE, 2008. Pp. 137—142. doi: 10.1109/ICCGI.2008.45.

10. *Lioy A., Marian M., Moltchanova N., Pala M.* PKI past, present and future // International Journal of Information Security. 2006. Vol. 5. Issue 1. Pp. 18—29. doi: 10.1007/S10207-005-0077-9.

11. *Yu B., Singh M. P., Sycara K.* Developing trust in large-scale peer-to-peer systems // Multi-Agent Security and Survivability, 2004 IEEE First Symposium on. IEEE, 2004. Pp. 1—10.

12. *Wallach D. S.* A survey of peer-to-peer security issues // Software Security — Theories and Systems. Springer Berlin Heidelberg, 2003. Pp. 42—57.

13. *Vobugari S., Somayajulu D. V. L. N., Subraya B. M., Srinivasan M. K.* A Roadmap on Improved Performance-centric Cloud Storage Estimation Approach for Database System Deployment in Cloud Environment // Mobile Data Management (MDM), 2013 IEEE 14th International Conference on. IEEE, 2013. Vol. 2. Pp. 182—187. doi: 10.1109/MDM.2013.91.

1. *Musser J., O'Reilly T.* Web 2.0: Principles and best practices. Sebastopol, CA : O'Reilly Media, 2007.

2. *Sanzhapov B. Kh., Sadovnikova N. P.* Soglasovanie tselei pri ekologo-ekonomicheskom obosnovanii gradostroitel'nogo proekta s uchetom ogranichenii na znacheniya kharakteristik, vkhodyashchikh v sistemu sredstv, v usloviyakh nechetkoi informatsii // Vestnik Volgogradskogo gosudarstvennogo arhitekturno-stroitel'nogo universiteta. Seriya: Stroitel'stvo i arhitektura. 2011. Vyp. 21(40). S. 151—159.

3. *Castillo J. A. R., Jilveseu A., Caragea D., Pathok J., Honavar V. U.* Information extraction and integration from heterogeneous, distributed, autonomous information sources-a federated ontology-driven query-centric approach // Information Reuse and Integration, 2003. IRI 2003. IEEE International Conference on. IEEE, 2003. Pp. 183—191. doi: 10.1109/IRI.2003.1251412.

4. *Aiello L. M., Milanesio M., Ruffo U., Schifanella R.* Tempering Kademlia with a Robust Identity Based System // Peer-to-Peer Computing, 2008. P2P'08. Eighth International Conference on. IEEE, 2008. Pp. 30—39. doi: 10.1109/P2P.2008.40.

5. *Lesueur F., Mé L., Tong V. V. T.* An efficient distributed PKI for structured P2P networks // Peer-to-Peer Computing, 2009. P2P'09. IEEE Ninth International Conference on. IEEE, 2009. Pp. 1—10. doi: 10.1109/P2P.2009.5284491.

6. *Lesueur F., Mé L., Tong V. V. T.* A Sybil-Resistant Admission Control Coupling SybilGuard with Distributed Certification // Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2008. WETICE'08. IEEE 17th. IEEE, 2008. Pp. 105—110.

7. *Sit E., Morris R.* Security Considerations for Peer-to-Peer Distributed Hash Tables // Peer-to-Peer Systems. Springer Berlin Heidelberg, 2002. Pp. 261—269.

8. *Balfanz D., Smetters D. K., Stewart P., Wong H. Ch.* Talking to Strangers: Authentication in Ad-Hoc Wireless Networks // NDSS. 2002.

9. *Alnemr R., Meinel C.* Getting more from reputation systems: A Context-aware reputation framework based on trust Centers and agent lists // Computing in the Global Information Technology, 2008. ICCGI'08. The Third International Multi-Conference on. IEEE, 2008. Pp. 137—142. doi: 10.1109/ICCGI.2008.45.

10. *Lioy A., Marian M., Moltchanova N., Pala M.* PKI past, present and future // International Journal of Information Security. 2006. Vol. 5. Issue 1. Pp. 18—29. doi: 10.1007/S10207-005-0077-9.

11. *Yu B., Singh M. P., Sycara K.* Developing trust in large-scale peer-to-peer systems // Multi-Agent Security and Survivability, 2004 IEEE First Symposium on. IEEE, 2004. Pp. 1—10.

12. *Wallach D. S.* A survey of peer-to-peer security issues // Software Security — Theories and Systems. Springer Berlin Heidelberg, 2003. Pp. 42—57.

13. *Vobugari S., Somayajulu D. V. L. N., Subraya B. M., Srinivasan M. K.* A Roadmap on Improved Performance-centric Cloud Storage Estimation Approach for Database System Deployment in Cloud Environment // Mobile Data Management (MDM), 2013 IEEE 14th International Conference on. IEEE, 2013. Vol. 2. Pp. 182—187. doi: 10.1109/MDM.2013.91.

Поступила в редакцию
в мае 2014 г.

Ссылка для цитирования:

Платонов А. А. Авторизация на основе открытых ключей для геоинформационной системы // Интернет-вестник ВолгГАСУ. Сер.: Строительная информатика. 2014. Вып. 11(32). Ст. 3. Режим доступа: http://www.vestnik.vgasu.ru/

For citation:

Platonov A. A. [Public key based authorization for a geographic information system]. *Internet-Vestnik VolgGASU*, 2014, no. 11(32), paper 3. (In Russ.). Available at: http://www.vestnik.vgasu.ru/