УДК 004.738.2

Проблемы сокрытия трафика в анонимной сети и факторы, влияющие на анонимность

© Н.Г. Ершов, Н.Ю. Рязанова

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Рассмотрены проблемы разработки анонимных сетей, позволяющих сделать контакты в глобальной сети невидимыми для посторонних наблюдателей. Все факторы, влияющие на уязвимость анонимной сети, классифицированы: выявлены уязвимости, возникающие на уровне узлов сети, а также на уровне сообщений, передаваемых по сети. Показано, что для обеспечения анонимности на уровне узлов сети, необходимо скрыть топологию узлов, обеспечить живучесть сети и исключить подмену сообщений. Продемонстрирована эффективность стратегии перемешивания узлов для решения этих задач. Проанализированы известные в настоящее время схемы нарушения анонимности сетей и типы атак на анонимные сети. Показано, как может быть нарушена анонимность при перехвате сообщения на промежуточном узле, определении шаблона коммуникации в сети, анализе сообщений по времени передачи. На основе проведенных исследований определены расширенные требования к реализации анонимных сетей и показаны направления их развития.

***Ключевые слова*:** *сеть, узел, сообщение, анонимная сеть, анонимный узел, сетевая атака, перемешивание узлов.*

Введение. В настоящее время обычной практикой является передача по глобальной сети корпоративных или личных данных, в том числе содержащих коммерческую или научную тайну. При этом оказывается недостаточным просто зашифровать данные, если партнеры желают скрыть сам факт контакта, который может привлечь внимание и раскрыть круг заинтересованных лиц. Сделать контакты невидимыми можно с помощью анонимных сетей.

Под анонимными сетями понимают системы, которые обеспечивают анонимное сетевое соединение, сохраняющие конфиденциальность передачи данных и секретность коммуникации. Обеспечение анонимности является многоаспектной задачей и требует комплексных решений. Передача информации по сети осуществляется посредством сообщений, которые проходят в процессе транспортировки определенные узлы сети. Таким образом, для обеспечения анонимности, во-первых, необходимо скрыть сам факт передачи сообщений между узлами, а во-вторых, скрыть топологию сети: последовательность узлов, через которые проходит сообщение.

Обеспечение анонимности на уровне узлов заключается в создании таких условий передачи сообщений, при которых невозможно или достаточно трудно выявить узлы, участвующие в передаче сооб-

щений, и таким образом скрыть топологию сети. Безопасность на уровне сообщений обеспечивается системой защиты сообщений, которая служит препятствием для целенаправленного перехвата данных, если топология сети раскрыта.

Обеспечение анонимности на уровне узлов. Анонимность сети на уровне узлов обеспечивается путем создания надежного алгоритма передачи и аппаратных методов защиты. При этом необходимо следующее [1, 2].

1. Создать условия для сокрытия топологии сети. Ни один промежуточный узел не должен обладать информацией об отправителе и получателе. Определение отправителя и получателя должно быть невозможно даже при частичной компрометации сети.

2. Создать условия, исключающие подмену сообщений.

3. Обеспечить «живучесть» сети. Анонимная сеть должна быть устойчива к выходу узлов из строя, способна к самоорганизации и достаточно быстрому перестроению, даже если злоумышленник намеренно разрушает или блокирует узел. Для обеспечения самоорганизации в сети должны всегда оставаться узлы, способные обеспечить ее полную функциональность. Для этого важно свести специализацию узлов к минимуму.

Способом, решающим эти задачи является так называемое перемешивание узлов [1]. Сама концепция перемешивания не была ориентирована на системы реального времени, однако показала высокую скорость работы на практике и применяется для таких критичных по времени операций, как отображение веб-страниц [3, 4].

Для реализации перемешивания узлов выполняются следующие действия:

1) сообщение отправляется через ряд узлов согласно заранее определенной (или сгенерированной) последовательности. Такая последовательность узлов называется туннелем;

2) пользователь открытым ключом узла сначала зашифровывает сообщение, затем его результат и т. д. Полученное сообщение отправляется на узел;

3) на каждом узле сообщение дешифруется, открывая доступ к следующему зашифрованному слою;

4) транзит осуществляется до последнего узла в туннеле, который является получателем, или конечным шлюзом.

В настоящее время определено несколько алгоритмов создания туннеля из перемешиваемых узлов [2, 5–8]:

каскадный алгоритм, когда маршрут следования сообщений не изменяется и не перестраивается. В этом случае злоумышленник может узнать отправителя и получателя сообщений, а также транзитные узлы. Данный алгоритм прост в реализации, но позволяет легко анализировать передаваемый трафик;

алгоритм случайного пути, при котором маршрут следования сообщений составляется случайным образом. Данный алгоритм обычно используется в реализациях анонимных сетей;

другие способы создания туннеля, например: фиксация части узлов, выбор маршрута случайным образом, но из заранее определенных «доверенных» узлов или из случайных узлов, но с некоторыми ограничениями (например, строго в различных подсетях).

Эффективность обеспечения анонимности сети на основе перемешанных узлов базируется на сложности определения случайного пути, который зависит от степени связности в графе, формирующемся исходя из структуры сети. Даже с учетом того, что сеть ограничена, а маршрут может быть построен только с использованием путей текущей топологии, подобная структура эффективна при расширении. Это следует из леммы о перемешивании: для любых двух подмножеств S и T вершин графа G, число ребер между S и T с вероятностью d/n равно числу ребер в случайном d-регулярном графе, где d — степень регулярности графа. Таким образом, эффективная в подграфе сеть будет также эффективна при ее расширении [9, 10].

Обеспечение анонимности на уровне сообщений. Помимо разработки средств, создающих и поддерживающих туннель, важнейшей задачей является обеспечение анонимности сети на уровне сообщений. Для решения этой задачи важно определить, каким атакам подвергаются информационные сети и каковы действия злоумышленников при попытке определить отправителя, получателя или раскрыть содержимое сообщения [5, 6, 11].

Перехват сообщения на промежуточном узле. Перехват сообщения на промежуточном узле может полностью скомпрометировать анонимную сеть, поскольку злоумышленник сам является одним из узлов сети и имеет прямой доступ к сообщениям. Для обеспечения анонимности и секретности сеть должна быть построена таким образом, чтобы промежуточный узел не имел доступа к информации о конечных узлах и содержании сообщения.

Особенно это важно для сетей с аутентификацией [7, 12]. В этом случае злоумышленник может перехватить сообщение с данными для аутентификации (например, с логином и паролем) от доверенного узла к серверу аутентификации и использовать его повторно. Даже если сообщения шифруются и перехватчик не имеет доступа к ключам, он может отправить перехваченное сообщение от своего имени на следующий узел в сети и сам успешно пройти аутентификацию.

Атака по времени. Одной из задач анонимной сети является сокрытие факта передачи сообщения. Поэтому реализация анонимной сети должна затруднять ассоциацию передаваемого сообщения с конкретной рабочей станцией и с конкретным туннелем. Злоумышленник

может отправлять по сети сообщения через определенные интервалы времени, а затем анализировать перехваченный трафик. Если на каком-либо узле будут обнаружены пакеты, пришедшие с таким же интервалом времени, можно утверждать, что эти пакеты отправлены злоумышленником. Данный вид атаки называется атакой по времени (*Timing Attack*) [2, 13]. Для этого вида атаки не требуется проведение сложных математических вычислений и она осуществима даже с одного узла при отправке сообщения самому себе.

Атака по времени способна раскрыть топологию сети и типичные маршруты в ней. Это дает возможность для осуществления целенаправленного перехвата сообщений между двумя конкретными рабочими станциями. Алгоритм, реализующий защиту от атаки по времени, должен обеспечить также и секретность топологии сети.

Определение шаблона коммуникации в сети. При наличии у злоумышленника времени для наблюдения за трафиком в сети, топология сети может быть раскрыта при пассивном наблюдении. Если один из узлов только отправляет сообщения, а другой — только принимает их в конкретный момент времени, то можно достоверно определить источник и приемник сообщений. При достаточно долгом наблюдении можно выявить неслучайный характер смены направления передачи сообщений и определить шаблон коммуникации в сети (*Communication Pattern*).

Как правило, пользователи поддерживают общение с небольшим числом участников сети, запрашивают в разных сессиях одни и те же веб-сайты. Таким образом, запросы пользователя не случайны и также поддаются анализу. Правильно определенный злоумышленником шаблон коммуникации значительно уменьшает объем данных для анализа и ускоряет расшифровку.

Для защиты от подобной атаки необходимы специальные встраеваемые в сеть средства, нарушающие шаблонность коммуникации. Данная проблема особенно актуальна в небольших сетях, где мало число пользователей (следовательно, и контактов между ними) и есть возможность поставить под наблюдение всю сеть целиком. Дополнительные проблемы возникают с передачей больших объемов данных. Такие данные передаются по сети в течение длительного времени, и поток их передачи однонаправленный.

«Бомбардировка» узлов пакетами. Для исследования всех возможных путей следования сообщения применятся «бомбардировка» узлов пакетами или атака грубой силы (*Brute Force Attack*) [2, 14, 15]. Идея атаки заключается в следующем: злоумышленник сначала отправляет сообщение первому узлу в системе перемешивания, а затем всем остальным известным узлам. Если сеть плохо спроектирована и состоит из небольшого числа узлов, есть риск, что пакеты сообщений

злоумышленника пройдут через все узлы сети. Таким образом, могут быть обнаружены все возможные отправители и получатели. Кроме того, если все сообщения проходят через один узел или принимаются только одним узлом, то именно его нужно контролировать, чтобы целиком скомпрометировать сеть.

Возможность анализа трафика исходя из длины пакетов. Чтобы изучить топологию сети и скомпрометировать туннель, злоумышленник может внедриться в сеть и отправить сообщение строго определенной длины. При перехвате трафика, анализируя длину сообщений, приходящих на каждый узел, можно установить полный маршрут следования сообщения, определить отправителя и получателя.

Кроме того, если большие объемы данных отправляются единым блоком без разбиения, это также дает возможность легко оценить маршрут их следования по сети. Необходимо найти способ, затрудняющий сопоставление реальной длины сообщений с длиной передаваемых по сети сообщений.

Заключение. На основе проведенного анализа большего числа известных в настоящее время атак определены факторы, влияющие на надежность сокрытия факта контакта. Кроме того, расширены требования, предъявляемые к анонимной сети:

обеспечение секретности топологии сети как на уровне узлов, так и на уровне сообщений;

устойчивость сети к выходу некоторых узлов из строя — способность к самоорганизации;

невозможность определения конечных узлов туннеля (источника и приемника);

организация передачи сообщений таким образом, чтобы их подмена была затруднена;

невозможность анализа сообщения по его содержимому;

невозможность сопоставления сообщений по их длине и времени отправки;

ограничение числа передаваемых сообщений и равномерное их распределение по структуре сети;

наличие инструментов по сокрытию «шаблона коммуникации».

Анонимная сеть, соответствующая перечисленным требованиям, будет в определенной степени неуязвима. Однако следует отметить, что создание все более надежных средств анонимной передачи информации приводит к появлению новых факторов риска, которые необходимо постоянно отслеживать и анализировать в целях последующей нейтрализации.

Все факторы риска можно разделить на внешние и внутренние. Анонимная сеть должна включать в себя комплексную защиту от всевозможных факторов. Наибольшую трудность создают внутренние

факторы. Защита от нарушения анонимности внутренним элементом, находящимся в составе сети, сильно затруднена. Причем пользователь сети может нарушать свою анонимность и анонимность других участников непреднамеренно. Разработка эффективных средств защиты от подобных факторов риска является одним из ключевых направлений дальнейших исследований.

Важнейшим направлением развития анонимных сетей является также анализ новых внешних атак. Необходимо реализовать протоколы, обеспечивающие защиту от новых факторов, нарушающих анонимность. Анализ мирового опыта показывает, что для комплексного решения данной задачи используются методы распознавания изображений и математического анализа топологий сетей.

Важным фактором, влияющим на разработку анонимных сетей, является соблюдение баланса между временем подготовки сообщения к передаче, скоростью его передачи и защищенностью.

ЛИТЕРАТУРА

[1] Chaum D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 1981, no. 2 (24), pp. 84–90.

[2] Raymond J. Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science*, 2001, pp. 10–29.

[3] Rennhard M., Rafaeli S., Mathy L. Design, Implementation and Analysis of an Anonymity Network for Web Browsing. *Technical Report*, 2002, no. 129, 17 p.

[4] Bhatia S., Motiwala M., Valancius V. *Hosting Virtual Networks on Commodity Hardware*. URL: http://www.cs.princeton.edu/~jrex/papers/trellis07.pdf (дата обращения 16.11.2014).

[5] Rennhard M., Rafaeli S., Mathy L. An Architecture for an Anonymity Network. *Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2001, pp.165–170.

[6] Berthold O., Standtke R., Pfitzmann A. The Disadvantages of free MIX routes and how to overcome them. *International workshop on Designing privacy enhancing technologies*, New York, 2001, pp. 30–45.

[7] Rannenberg K., Iachello G. Protection Profiles for Remailer Mixes. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science*, 2009, pp. 181–230.

[8] Goldschlag D., Reed M., Syverson P. Hiding Routing Information. *Workshop on Information Hiding*, Cambridge, 1996, 14 p.

[9] Danezis G., Mix-Networks with Restricted Routes. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science,* 2003, pp. 1–17.

[10] Serjantov A., Danezis G. Towards an Information Theoretic Metric for Anonymity. *Proceedings of the 2nd International Conference on Privacy Enhancing Technologies,* 2003, pp. 41–53.

[11] Chaum D. L. The Dining Cryptographers Problem: Unconditional Sender and Receiver Untraceability. *Journal of Cryptology*, 1988, no. 1 (1), pp. 66–75.

[12] Berthold O., Federrath H., Kopsell S. WebMIXes: A System for Anonymous and Unobservable Internet Access. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science*, 2009, pp. 115–129.

[13] Syverson P., Tsudik G., Reed M., Landwehr C. Towards an Analysis of Onion Routing Security. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science,* 2009, pp. 96–114.

[14] Wiangsripanawan R., Susilo W., Safavi-Naini R. Design Principles for Low Latency Anonymous Network Systems Secure Against Timing Attacks. *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers*, 2007, no. 68, pp. 183–191.

[15] *Tor. Anonymity Online*. URL: https://www.torproject.org/index.html.en (дата обращения 22.06.2014).

Статья поступила в редакцию 21.10.2014

Ссылку на эту статью просим оформлять следующим образом:

Ершов Н.Г, Рязанова Н.Ю. Проблемы сокрытия трафика в анонимной сети и факторы, влияющие на анонимность. *Инженерный журнал: наука и инновации*, 2014, вып. 12.

URL: http://engjournal.ru/catalog/it/security/1331.html

Ершов Никита Георгиевич родился в 1991 г., студент кафедры «Программное обеспечение ЭВМ и информационные технологии» МГТУ им. Н.Э. Баумана. Область научных интересов: защита информации, сетевая обработка данных, программирование драйверов. e-mail: yershov.n@mail.ru

Рязанова Наталья Юрьевна родилась в 1951 г., окончила МИЭМ в 1973 г. Канд. техн. наук, доцент кафедры «Программное обеспечение ЭВМ и информационные технологии» МГТУ им. Н.Э. Баумана. Автор 38 печатных работ. Область научных интересов: разработка системного программного обеспечения, алгоритмы машинной графики. e-mail: ryaz_nu@mail.ru

The problem of traffic hiding in anonymous networks and the factors affecting anonymity

© N.G. Yershov, N.Y. Ryazanova

Bauman Moscow State Technical University, Moscow, 105005, Russia

The article considers the problems of the development of anonymous networks, allowing you to make contacts in the global network invisible to outside observers. All factors affecting the vulnerability of the anonymous network are classified: vulnerabilities that arise at the level of network nodes and at the level of messages sent over the network. It is shown that to ensure anonymity at the level of nodes in the network, it is necessary to hide the topology of the nodes to ensure network survivability and exclude substitution messages. Effectiveness of the strategy of mixing nodes to solve these problems is demonstrated. We analyzed currently known schemes of violating anonymity networks and types of attacks on anonymous networks. We show how anonymity can be violated when intercepting the message at the intermediate node, when identifying the communication template of the network, analyzing the message transmission time. On the basis of the conducted researches we formulated extended requirements for the implementation and development of anonymous networks.

Keywords: *network, node, message, anonymous network, anonymous site, network attack, mixing nodes.*

REFERENCES

[1] Chaum D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 1981, no. 2 (24), pp. 84–90.

[2] Raymond J. Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science*, 2001, pp. 10–29.

[3] Rennhard M., Rafaeli S., Mathy L. Design, Implementation and Analysis of an Anonymity Network for Web Browsing. *Technical Report*, 2002, no. 129, 17 p.

[4] Bhatia S., Motiwala M., Valancius V. *Hosting Virtual Networks on Commodity Hardware*. Available at: http://www.cs.princeton.edu/~jrex/papers/trellis07.pdf (accessed on 16.11.2014).

[5] Rennhard M., Rafaeli S., Mathy L. Architecture for an Anonymity Network. *Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2001, pp. 165–170.

[6] Berthold O., Standtke R., Pfitzmann A. The Disadvantages of free MIX routes and how to overcome them. *International workshop on Designing privacy enhancing technologies*, New York, 2001, pp. 30–45.

[7] Rannenberg K., Iachello G. Protection Profiles for Remailer Mixes. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science*, 2009, pp. 181–230.

[8] Goldschlag D., Reed M., Syverson P. Hiding Routing Information. *Workshop on Information Hiding*, Cambridge, 1996, 14 p.

[9] Danezis G., Mix-Networks with Restricted Routes. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science,* 2003, pp. 1–17.

[10] Serjantov A., Danezis G. Towards an Information Theoretic Metric for Anonymity. *Proceedings of the 2nd International Conference on Privacy Enhancing Technologies,* 2003, pp. 41–53.

[11] Chaum D. L. The Dining Cryptographers Problem: Unconditional Sender and Receiver Untraceability. *Journal of Cryptology*, 1988, no. 1 (1), pp. 66–75.

[12] Berthold O., Federrath H., Kopsell S. WebMIXes: A System for Anonymous and Unobservable Internet Access. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science*, 2009, pp. 115–129.

[13] Syverson P., Tsudik G., Reed M., Landwehr C. Towards an Analysis of Onion Routing Security. *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science,* 2009, pp. 96–114.

[14] Wiangsripanawan R., Susilo W., Safavi-Naini R. Design Principles for Low Latency Anonymous Network Systems Secure Against Timing Attacks. *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers*, 2007, no. 68, pp. 183–191.

[15] *Tor. Anonymity Online*. Available at: https://www.torproject.org/index.html.en (accessed on 22.06.2014).

Yershov N.G., (b. 1991) a student of the Software and Information Technologies Department at Bauman Moscow State Technical University. The fields of research are information security, processing network information, drivers development. e-mail: yershov.n@mail.ru

Ryazanova N.Yu. (b. 1951) graduated from the Moscow Institute of Electronics and Mathematics in 1973. Ph.D., assoc. professor of the Software and Information Technologies Department at Bauman Moscow State Technical University. Author of over 38 scientific and educational works in the field of the system programming and computer graphics. e-mail: ryaz_nu@mail.ru