электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.453

ShadowWalker: анонимная peer-to-peer коммуникация с использованием топологий с избыточной структурой

***Денисов И.А.**, студент*
Россия, 111024, г. Москва, МТУСИ,
кафедра «Информационная безопасность и автоматизация»
Dr.espio@yandex.ru

Научный руководитель: В.А. Алешин, к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э.Баумана,
кафедра «Информационная безопасность»
v.aleshin@bmstu.net

Анонимная коммуникация (АК) – ключевая, направленная на повышение конфиденциальности технология, которая обрела широкую популярность в эру распространенной слежки. АК скрывает личности ее участников от третьих лиц или скрывает личность пользователя от удаленного перехвата. Сеть Tor, разработанная в 2003, сейчас обслуживает сотни тысяч пользователей и обрабатывает терабайты трафика ежедневно. Изначально экспериментальная сеть, используемая частными энтузиастами, сегодня используется практически повсеместно: недавняя атака показала, как много иностранных консульств использовали Tor, чтобы избежать слежки своих стран.

Объемы Tor уже на исходе, и для поддержки растущего числа пользователей может пригодиться технология P2P, т.к. P2P сети позволяют изменять размер сети в соответствии с количеством пользователей. Действительно, некоторые идеи и предложения по использованию P2P сетей были продвинуты вперед. Однако, несколько недавних результатов показали, что даже лучшие из предлагаемых систем уязвимы к нарушению конфиденциальности, побуждая к разработке новых систем анонимной P2P коммуникации.

Главная идея состоит в созданий *узлов-теней* (или *теневых узлов*), которые избыточно проверяют корректность таблицы соседей заданного узла и удостоверяют ее как корректную. Подобные сертификаты могут быть задействованы в проверке шагов случайного прохода; используя подобные сертификаты вместо онлайн-проверок, возможно избежать утечки информации.

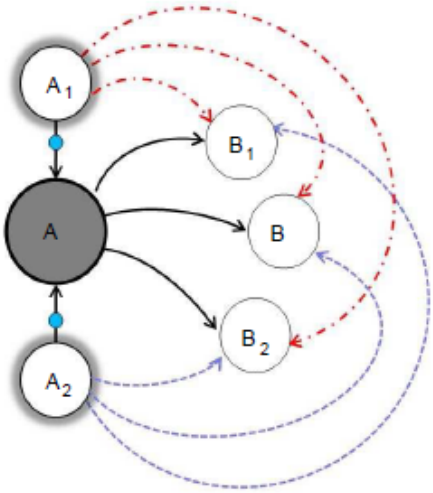

Рис. 1. Топология со случайной структурой

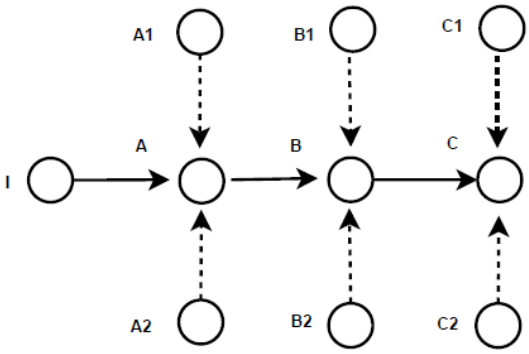

Рис. 2. Построение цепочек

Вначале введем понятие *тени*. Каждый узел A имеет несколько теней, и каждая из них должна независимо поддерживать информацию по соседям для A. Тени обеспечивают эту информацию как способ проверить, что A не пытается реализовать атаку захвата пути. Для избыточного параметра r узлы-тени A обозначаются как A_1, A_2,…, A_r. Взаимодействие теней между собой – детерминистическое, проверяемое, которое может быть вычислено применением математических формул к идентификатору узла. В качестве примера, для r=2 тени для узла A могут определяться как преемник и предшественник. Для общего r они могут быть определены как $\left[\frac{r}{2}\right]$ предшественников и $\left[\frac{r}{2}\right]$ преемников в PXT.

Авторы используют структурированные P2P топологии, такие как Chord или Pastry (также известные как распределенные хэш-таблицы, или PXT) как основу для анонимной P2P коммуникации[1]. Каждому узлу в структурированной P2P топологии соответствует некое количество соседей, также известных как пальцы. Отношения между ними определены математической формулой, основанной на идентификаторах узла. Это позволяет проверять эти взаимодействия внешне, оставляя меньше возможностей для атаки. Узел содержит таблицу маршрутизации, которая состоит из IP-адресов и открытых ключей пальцев.

Используя отношения теней, можно определить преобразование, которое сделает любую P2P топологию избыточной:

Свойство 1: В дополнение к пальцам, узел A содержит защищенную информацию о теневых узлах пальцев. Это означает, что если A→B – это ребро в структурированной

топологии, $A \rightarrow B_j$ также является ребром в топологии с избыточной структурой, справедливо для j = 1,2,…, r (r теней B).

Свойство 2: Если узел A_j – тень узла A, он содержит копию пальцев (также как и теней пальцев) A. Другими словами, если $A \rightarrow B$ – ребро в структурированной топологии, то $A_j \rightarrow B$ и $A_j \rightarrow B_k$ – также ребра в топологии с избыточной структурой, справедливо для j = 1,2,…, r и k = 1,2,…, r.

Рисунок 1 показывает преобразование ребра $A \rightarrow B$ в топологию с избыточной структурой с параметром избыточности r=2. Danezis проанализировал использование случайных путей вдоль ограниченной топологии для «смеси» сетей и предложил использовать топологии с высоким расширением, дабы обеспечить логарифмический характер роста максимальной анонимности сугубо с ростом количества узлов в сети[2].

Borisov[3] проанализировал случайные проходы по P2P топологиям и предложил использование топологии де Брёйна[4], чтобы обеспечить анонимность малыми длинами путей. Эта топология используется в ShadowWalker. Узлы должны быть способны содержать указатели на топологию с избыточной структурой защищенным образом.

Авторы используют тени узла A, чтобы проверить информацию, переданную A в течение постройки цепочки. Инициатор I не может общаться с тенями напрямую, так как тени могут узнать, что он создавал цепочку через A. I может использовать цепочку, которую он установил с A, чтобы общаться с A_j, также как MorphMix общается со своими узлами-очевидцами. Но это все же позволяет узлу A_j знать, что цепочка строится через узел A.

Можно полностью избежать этой утечки информации, указывая каждой тени A_j снабжать цифровой подписью свою версию таблицы маршрутизации A и передавать эту подпись ему. После того, как инициатору становятся известны открытые ключи теней (по свойству 1), он может заверить подписи, не вступая в контакт с тенями никоим образом. Таким образом становится возможным проверять информацию, предоставляемую A, без контакта с другим узлом. Далее описывается символический код протокола защищенного случайного прохода, основанного на топологиях с избыточной структурой (листинг 1).

I.настройка цепочки(I)
Пусть A – случайный палец I
Пусть A_j – тени of A, ∀j = 1..r
Пусть Pub(A_j) – открытый ключ A_j , ∀j = 1..r
Создать цепочку между I и A
цикл: для count = 1 до I − 1 выполнить

Пусть B – случайный палец A с индексом i

Пусть Pub(B) – открытый ключ B

/* Случайный палец выбран I*/

Пусть B_k – тени B, $\forall k = 1..r$

Пусть $Pub(B_k)$ – открытый ключ B_k, $\forall k = 1..r$

Пусть $Signature_j$ – сигнатура, выданная A_j для состояния маршрутизации A.

I получает B, Pub(B), все Bk, $Pub(B_k)$, и

все $Signature_j$ от A через созданную цепочку.

условие: если B, Pub(B), и все Bk, Pub(Bk) заверены всеми

$Signature_j$ тогда

расширить цепочку до B

$A = B$

$A_j = B_j$, $\forall j = 1..r$

$Pub(A_j) = Pub(B_j)$, $\forall j = 1..r$

иначе

прекратить

конец условия

конец цикла

Листинг 1. Символический код протокола защищенного случайного прохода

Инициатор I сначала устанавливает цепочку к случайному пальцу A. Далее он запрашивает узел A по пальцу B со случайным индексом I (i-ая запись в таблице маршрутизации). A возвращает следующую информацию I:

1. IP-адрес и открытый ключ B и B_k для k=1,2,…, r.
2. Сигнатуры вышеуказанной информации от A_j, j=1,2,…, r.

Тогда инициатор I проверяет, что сигнатуры всех A_j правильны. Так как A – палец I, A_j также содержится в I (свойство 1). Таким образом I узнает об открытых ключах всех A_j и может подтвердить сигнатуры. Если сигнатуры верны, I может расширить цепочку к узлу B. Теперь I может запросить B о пальце C со случайным индексом i', заверить его, используя сигнатуры с B_k, и повторить процесс. Выше представлен пример на рисунке 2. Если сигнатуры не совпадают, построение цепочки прерывается.

Существующие методы защищенного поиска, используемые Halo[5] и Castro и другими[6], эффективно обеспечивают следующее: в качестве результата поиск вернет ближайший к выбранному идентификатору узел. Однако в контексте топологий с избыточной структурой эти механизмы не очень эффективны. Например, в подобной

топологии узел должен содержать тени своих пальцев. Дабы достичь этого, вышеупомянутые протоколы поиска должны быть выполнены множество раз подряд для каждого теневого узла, и затраты на это весьма значительны. Авторы предлагают протокол защищенного поиска, который создан специально для работы в топологиях с избыточной структурой.

Скажем, узел I хочет найти защищенным образом идентификатор ID. Пусть A – ближайший предшествующий узел для ID в таблицу пальцев I. Следуя повторяющейся стратегии маршрутизации, I запросит A по его пальцу B, который есть ближайший предшествующий узел к ID. Так как I известны все тени A, I может заверить эту информацию с их помощью. В этом случае I узнает правильную сущность B так же, как и всех его теней. Теперь он может действовать итеративно, спрашивая B и его тени насчет следующего ближайшего предшествующего пальца к ID. Пока один узел между A и его тенями остается нескомпрометированным, I узнает настоящую сущность B; в случае противоречащих ответов, I должен выбрать ближайший к ID (для анонимного поиска все узлы должны согласовать поиск для выполнения. В ином случае, однако, I может заверить существование B напрямую, предотвращая получение ответов злоумышленниками от фальшивых узлов). Таким образом, поиск успешен, если существует хотя бы один нескомпрометированный узел на каждом шаге поиска.

Важным результатом представленного протокола защищенного поиска является то, что наряду с узлами, соответствующими выбранному ID, поиск также возвращает в качестве результата их тени. Это значительно уменьшает затраты на коммуникацию протокола, поскольку устраняет надобность в выполнении множества защищенных поисков теней пальцев.

Регулирование текучести узлов – главная проблема в P2P системах. Существующие PXT-разработки, такие как Chord, реализуют алгоритмы, которые предоставляют определенные гарантии в этом вопросе. В случае ShadowWalker, периодически использовался *протокол стабилизации*, чтобы обеспечить передачу информации о новых узлах другим узлам, находящимся поблизости. Время от времени узлы реализовывают поиск выбранных идентификаторов для обновления своих таблиц пальцев. Список преемников также поддерживается, чтобы выполнять обработку в случае отказа узлов.

Для адаптации протокола к топологиям с избыточной структурой необходимо внести следующие изменения:

1. Узел периодически реализует защищенные поиски, чтобы определить сущности узлов (например, множества S), для которого он является тенью.

2. Узел периодически реализует защищенные поиски для нахождения пальцев узлов во множестве S.

Вышеописанных шагов достаточно для поддержания топологии с избыточной структурой, поскольку защищенные поиски также находят и тени пальцев. Более того, для достижения цели АК, узел также периодически посылает сигнатуры к узлам во множестве S по соответствующим состояниям маршрутизации.

Низколатентные системы анонимности часто изучаются с точки зрения атак *компрометации путей* подсчетом скопления находящихся под угрозой цепочек. Эта метрика показывает, способны ли злоумышленники идентифицировать инициатора цепочки или нет. Однако в P2P системах могут быть проведены некоторые наблюдения, которые выдают определенную информацию об инициаторе, даже когда полная идентификация невозможна. Поэтому вместо использования двоичной концепции компрометации путей используется метрика анонимности, основанная на энтропии[7]. Эта метрика определяет распределение потенциальных инициаторов цепочки как вычисленное злоумышленниками, и вычисляет его энтропию (p - вероятность, что узел i был инициатором цепочки):

$$H(I) = -\sum_i p_i \log_2 p_i \qquad (1)$$

Также авторами в статье была создана аналитическая модель поведения ShadowWalker в зависимости от различных типов атак (а именно: *атака захвата пути, end-to-end временной анализ, атака ограниченной топологии*), а также выборочных DDoS-атак. И в качестве завершения модели было представлено сравнение с системой Salsa. Во всех случаях, как при реакции на атаки, так и при сравнении с существующими атаками, ShadowWalker показывал лучшие результаты, а некоторые негативные эффекты ввиду невозможности их полного нивелирования были в значительной мере смягчены благодаря гибким настройкам протокола.

При помощи экспериментальных результатов были успешно продемонстрированы приемлемые затраты на коммуникацию, а также наглядное смягчение ShadowWalker эффекта текучести сети и снижение вероятности отказа защищенного поиска с ростом узлов-теней.

В итоге: ShadowWalker способен эффективно защищаться против обычных атак на P2P системы и достигать уровня анонимности, превосходящего сегодняшний. В частности, когда 20% узлов находятся под угрозой, ShadowWalker обеспечивает на 4.5

бита энтропии больше, чем Salsa. Более того, вероятность end-to-end временного анализа в этом случае меньше 5%, что близко к идеальному варианту, наподобие Tor, где она составляет 4%.

Система представляет несколько компромиссов между анонимностью и затратами на производительность. Были продемонстрированы варианты, которые имеют управляемое вычисление и затраты на коммуникацию, обеспечивая при этом высокую гарантию анонимности. ShadowWalker также способен регулировать среднюю текучесть в сети. В итоге, он представляет многообещающее новое направление в P2P АК.

Разработка топологии с избыточной структурой имеет преимущества, которые могут распространяться за системы анонимности. В дальнейшем авторы планируют расширить свою разработку, которая будет включать в себя вопросы гетерогенной полосы пропускания узла и политику выхода.

Список литературы

1. P. Mittal, N. Borisov. ShadowWalker: Peer-to-peer Anonymous Communication Using Redundant Structured Topologies // CCS'09, November 9–13, 2009, Chicago, Illinois, USA.
2. G. Danezis. Mix-networks with restricted routes // In R. Dingledine, editor, Proceddings of PET, pages 1-17. Spriner-Verlag, LNCS 2760, March 2003.
3. N. Borisov. Anonymous routing in structured peer-to-peer overlays // PhD thesis, University of California at Berkeley, Berkeley, CA, USA, 2005.
4. N. de Bruijin. A combinational problem // In Proceedings of the Section of Sciences, Vol. 49, No. 7, pp. 758–764. Koninklijke Nederlandse Akademie v. Wetenschappen, 1946.
5. A. Kapadia and N. Triandopoulos. Halo: High-assurance locate for distributed hash tables // In Proceedings of NDSS, pages 61–79, February 2008.
6. M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach. Secure routing for structured peer-to-peer overlay networks // In Proceedings of OSDI, December 2002.
7. C. Diaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity // In R. Dingledine and P. Syverson, editors, Proceedings of PET, San Diego, CA, April 2002. Springer-Verlag, LNCS 2482.