МОДЕЛЬ РЕКОНФИГУРИРУЕМОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ СОЦИАЛЬНОЙ СЕТИ

Ашот Хачатуров
Государственный Инженерный Университет Армении
Ереван, Армения
e-mail: ashotian@gmail.com

АННОТАЦИЯ

Показана идея построения реконфигурируемой стеганографической системы на основе социальной сети, которая может быть применена для обеспечения длительного хранения секретной информации. Предложена математическая модель подобной системы для оценки устойчивости к атакам и показаны эффективность хранения секретной информации в социальных сетях.

Ключевые слова. Стеганография, сокрытие данных, разделение секрета, обновления данных, социальная сеть.

1. ВВЕДЕНИЕ

Современные стеганографические системы позволяют скрыть секретную информацию в изображениях или инных цифровых объектах [1]. Один из таких методов предстовляет сабой пороговую стеганографию, посредством которой секретная информация "разделяется" многократно таким образом, что несанкционированное раскрытие секретной информации требует раскрытия всех частей разделенной информации [2]. Подобный подход, возможно, встретить в схемах разделения ключей. Но тут возникает вопрос. Как такие методы должны использоваться в реальном мире, чтобы, например, пользователи не обязаны были вносить какие-либо оплаты за обслуживание и не должны были бы доверять никому, кому они уже не доверяют? В статье предложено в качестве хранилища использовать социальные сети, которые в настоящее время получили широкое распространение. Пользователи используют возможности тех или иных сетей, которым они доверяют в своих интересах, чтобы обеспечить сокрытие разделеных частей секретной информации, и таким образом повысить степень безопасности.

2. ОСНОВНЫЕ ПОНЯТИЯ

Схема реконфигурируемой стеганографической системы состоит из:

- *алгоритма разделения информации,* который в качестве исходного параметра берет информацию M которую необходимо разделить и на выходе выдает разделенные части информации ($M_1,...,M_n$);
- *алгоритм периодического обновления скрываемой информации,* который периодически собирает разделенные части секретной информации, восстанавливает первоначальную информацию и снова разделяет эту информацию на множество независимых друг от друга частей;
- *алгоритм проверки,* который берет в качестве исходного параметра сообщение m_i, и определяет, была ли изменена это часть информации.

Пороговая схема разделения информации основана на методе известном, как пороговое разделение секрета; самый популярный пример которого представлен у Шамира [3]. Секретная схема разделения (m,n) "разделяет" секретные данные M на n частей $M_1,...,M_n$ таким образом, чтобы получить M, по крайней мере, необходимы m части. Такой метод определено увеличивает безопасность M во время его хранения.

3. МОДЕЛЬ СИСТЕМЫ

Допустим $G = (V,E)$ будет ненаправленным графом, где V набор узлов или вершин и E - набор краев. Для любого $u, v \in V$, есть одна и только одна связь между ними. deg (v,G), что обозначает степень узла v в G.

Рассмотрим ряд пользователей V, где у каждого $u \in V$ есть контейнеры со скрытой в них информацией. Рассмотрим тип социальных сетей которые могут быть смоделированы как ненаправленный граф G = (V;E), где каждый узел или вершина $u \in V$ представляют пользователя, и $(u;v) \in V$ означает, что u связано с v в социальной сети. Другими словами, остальные контейнеры находятся в профайлах пользователей из доверенной группы данного пользователя.

Рассматриваеться противник, который может поставить под угрозу пользовательские профайлы, и таким образом секретную информацию, которая хранится в контейнерах данного профайла. Это очевидно, потому что существующие шифровальные методы достаточны для того, чтобы противостоять любому вероятному противнику в полиномиальное-время, который применяет атаки типа криптоанализа контейнеров, но противник может относительно легко поставить под угрозу профайлы, чтобы получить информацию, сохраненную на них. Мы предполагаем, что противник управляет всеми скомпроментированными или оказавшимися под угрозой узлами (то есть, контейнерами), и знает топологию социальных сетей. Так как первичная цель противника, это заполучить скрытую информацию, то разумно предположить, что он будет совершать атаку таким образом, чтобы не выдавать себя, то есть, не будет изменять секретную информацию, или удалять ее (что может послужить сигналом об атаке).

Системы исследуются по двум мерам, называемые *устойчивость к атакам* и *доступность*, которые независимы от криптосистем и могут быть приняты в конкретной реализации. (Другие меры, такие как

производительность, конечно важны, но они зависят от принятых криптосистем).

Прежде, чем определить две меры, следует обсудить объяснение определений. Естественно допустить захват доступности, некоторым образом, т.е. насколько доступны части секретной информации. Это относится к делу из-за природы соединения равноправных узлов социальных сетей.

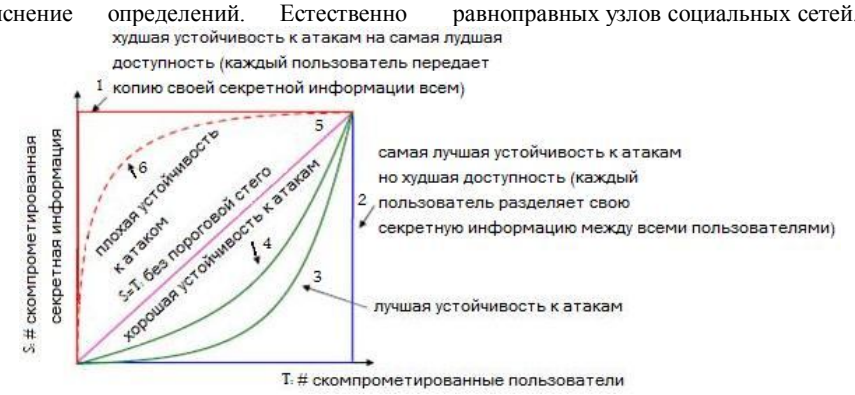

Рис. 1 устойчивость к атакам и доступность

Компрометация контейнеров T может вызвать компрометацию $S \geq T$ скрытых данных. Так как пользователь может быть связан с другими держателями частей секретной информации, и таким образом компроментирование узла может способствовать компроментированию многих частей секретной информации. "Точкой отсчета" является состояние, когда каждый пользователь держит у себя одну часть секретной информации, то компроментация узлов T вызывает компроментацию S=T частей секретной информации (линия номер 5 на рис. 1). Поэтому, важно отметить, что устойчивость к атаком выше при большом количестве скомпрометированых узлов не содержащих секретную информацию (S-T).

Следует отметить, что устойчивость к атаком и пригодность часто имеют разногласия друг с другом. Для наглядности, рассмотрим особый случай, когда социальная сеть является полным графом, что означает, что каждый пользователь связан со всеми. С одной стороны, когда каждый пользователь u связан со всеми пользователями и использует (|V|; |V|) секретную схему разделения (линия номер 2 на рис. 1) предлагает лучшую устойчивость к атаком. Для того, чтобы скомпрометировать любую скрытую информацию, нападавший должен поставить под угрозу все |V| контейнеры. Однако, у этой модели плохая пригодность, потому что для восстановления сообщения необходима каждая часть секретной информации. С другой стороны, проектирование модели, когда каждый узел u передает копию M_u всем другим узлам (линия номер 6 на рис. 1) приводит к наилучшей доступность, потому что один любой единственный узел в состоянии восстановить сообщение. Однако, эта модель предлагает худшую устойчивость к атаком, потому что компроментация любого единственного контейнера вызывает компроментацию всей скрытой информации.

В результате вышеупомянутое обсуждение предлагает следующее: меры должны быть определены таким образом, что хорошая модель должна обеспечить устойчивость к атаком, которая лучше чем та, предлагаемая в соответствии с эталонной схемой (например, кривые под номерами 3,4 на рис. 1), и плохая модель приведет к кривой под номером 1 в рис. 1. Теперь мы представляем формальные определения.

Определение 1. *(устойчивость к атакам) Обозначим G' набор всех возможных социальных сетей. Для данной социальной сети G = (V; E), где у каждого узла $u \in V$ есть контейнеры со скрытой в них информацией. Обозначим D' набор возможных моделей (которые определены параметрами конфигурации) определяющих, как пользователи держат разделеные части информации независемо друг от друга, и A' набор всех возможных нападений (например, стратегии анализа контейнеров, чтобы скомпроминтировать их). Допустим $S(G,D,A,T): G' \times D' \times A' \times N' \to N$ это функция, которая возвращает число скомпрометированных скрытых данных, когда $0 \leq T \leq |V|$ узлы оказались под угрозой согласно $A \in A'$. Обозначим D^* эталоном упомянутой выше модели (то есть, контейнеры не содержат разделеные части информации друг друга), тогда это ясно что S(G; D*; A; T) = T для любого $A \in A'$. Для любой модели $D \in D'$, его устойчивость при атаке A определена таким образом, чтобы*

$$AR(G,D,A) = \frac{\frac{1}{V}\sum_{0<T\leq|V|}\left(S(G,D^*,A,T) - S(G,D,A,T)\right)}{(|V|-1)/2} = \frac{2}{|V|(|V|-1)}\sum_{0<T\leq|V|}(T - S(G,D,A,T))$$

Теперь некоторые проблемы которые заслуживают специального упоминания. Строго говоря, определение захватило среднее расстояние между линией S(G; D*; A; T) = T и кривая S(G,D,A,T). "Среднее число" мотивировано для того, чтобы приспособить следующее: защитник никогда не знает заранее число скомпроминтированных контейнеров. Кроме того, устойчивость к атаком преднамеренно нормализована таким образом, чтобы $0 \leq AR(G,D,A) \leq 1$. Действительно, эталонная схема соответствует $AR(G,D^*,A) = 0$, и вышеупомянутая модель, когда каждый узел u разделяет M_u используя схему (|V|; |V|, секретный метод разделения соответствует $AR(G,D^*,A) = 1$. Заключение о вышеупомянутом определении, то, что проект D "хороший" если $AR(G,D,A) > 0$ и "плохой" в остальных случаех. Это также илюстрирует то, что при большом положительном значение $AR(G,D,A)$, обеспечивается лучшая устойчивость к атаком.

Определение 2. *(доступность) Как прежде, обозначим G' набор всех возможных социальных сетей,*

и $D^{'}$ набор возможных моделей определяющих, как пользователи держат разделеные части информации независимо друг от друга. Обозначим $L^{'}$ набор возможной продолжительности работы узла и распределений времени простоя, и $R^{'+}$ время системы (со временем инициализации системы, будучи нолем). Пригодность проекта $D \in D^{'}$ относительно социальной сети $G \in G^{'}$ и продолжительности работы узла и распределения времени простоя $L \in L^{'}$ во время t>0 определена так, что функция $AV : G^{'} \times D^{'} \times L^{'} \times R^{'+} \to [0,1]$ таким образом, что $AV(G,D,L,t) = \frac{\sum_{u \in V} R_u(G,D,L,t)}{|V|}$ где $R_u(G,D,L,t)$,

вероятность, что сокрытая информация M_u доступна во время t.

В особом случае $Ru(G,D,L,t) = 1$ для любого $u \in V$ и любой t, а именно, когда каждый узел включен, у нас есть $AV(G,D,L,t) = 1$. Однако, $0 < Ru(G,D,L,t) < 1$ из-за природы соединения равноправных узлов социальных сетей.

3.1. МОДЕЛЬ УСТОЙЧИВОСТИ К АТАКОМ

Предположим, $0 < \alpha < 1$ является параметром всей системы. Было бы естественно для пользователя u разделить свои секретные данные M_u через $(\lceil \alpha \cdot (\deg(u,G)+1) \rceil, \deg(u,G)+1)$, разделение секрета, а именно, для того чтобы распределить свою информацию между теми пользователями, которым он доверяет, и непосредственно собой. Однако, эта модель может не всегда быть желательной. Чтобы убедиться в этом, рассмотрим простой случай |V| = 3 и α=0,5, где каждый узел доверяет другим, и таким образом разделяет свою информацию между всеми этими тремя узлами, используя (2,3) секретное разделение. В этом случае, захват любых двух узлов немедленно вызывает компроментацию всех трех частей информации (то есть, получающаяся безопасность хуже чем, предлагаемая в соответствии с эталонной схемой). Чтобы избежать этого недостатка, мы рекомендуем следующую модель D основанную на двухъярусном секретном методе разделения.

* *Инициализация*: A(2,2), используется метод порогового разделение секрета, для того, чтобы разделить секретную информацию M_u на две части M_{u1} и M_{u2}. Тогда, $(\lceil \alpha \cdot \deg(u,G) \rceil, \deg(u,G))$, используется метод порогового разделения секрета, чтобы разделить M_{u2} на $\deg(u,G)$ частей $(M_{u2,1},..., M_{u2,\deg(u,G)})$. В результате *u* держат M_{u1}, и стирает M_u так же как M_{u2}, и сосед *i*-ого *u* держит $M_{u2,i}$ (который получен от *u* по частному каналу).
* *Операция*: частная функция разделения, соответствующая M_u, выполнена через участие *u* так же как по крайней мере $\lceil \alpha \cdot \deg(u,G) \rceil$ ее друзей. Это сделано, не восстановливая значение M_u.

Отметим, что много пороговых схем для разделения секрета могут быть приспособлены, для реализации вышеупомянутого двухъярусного секретного метода разделения.

ЗАКЛЮЧЕНИЕ

Таким образом, в статье в качестве хранилища секретной информации предложено использовать различного вида социальные сети для длительного хранения секретной информации. Прежде чем построить реконфигурируемую стеганографическую систему предложена математическая модель системы, оценивающая степень противостояния различным видом атак.

ЛИТЕРАТУРА

[1] E. Cole, *Hiding in Plain Sight: Steganography and the Art of Covert Communication*. New York: John Wiley & Sons, 2003. - 353 p.

[2] P. Gemmell, *An introduction to threshold cryptography,* Crypto-Bytes, Technical Newsletter of RSA Laboratories, Volume 2 , Issue 3, Winter 1997, 7-12

[3] A. Shamir, *How to Share a Secret*, Communications of the ACM, Volume 22 , Issue 11, November 1979, 612-613

[4] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. *Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults*. In Proceeding 26th Annual Symposium on the Foundations of Computer Science, pages 383-395. IEEE, 1985.

[5] P. Feldman. A *Practical Scheme for Non-Interactive Verifiable Secret Sharing*. In Proc. 28th Annual Symp. on Foundations of Computer Science, pages 427-437. IEEE, 1987.