Автономное управление разрывом канала передачи по закрытому расписанию, как метод повышения информационной безопасности

Я.А. Мостовой[а,б], И.И. Слепушов[б]

[а] *Самарский национальный исследовательский университет имени академика С.П. Королёва, 443086, Московское шоссе д. 34, Самара, Россия*

[б] *Поволжский государственный университет телекоммуникаций и информатики, 443010, ул. Льва Толстого д.23, Самара, Россия*

Аннотация

Рассматривается метод противодействия угрозам информационной безопасности путём автономного управления физическим разрывом канала передачи данных по защищенному расписанию. Метод применим для многих компьютеризированных систем, для которых достаточно эпизодических связей с сетевыми структурными элементами или пользователями услуг. В этом случае доступ узла к сети необходим и достаточен в определенные и ограниченные интервалы времени, между которыми доступ может отсутствовать. Предлагаемый метод имеет самостоятельное значение, как ещё один эшелон обороны, но одновременно повышает эффективность применения других методов эшелонированной обороны, вероятность преодоления которых зависит от времени нахождения защищаемого узла под возможными атаками или наблюдением. Проведена оценка эффективности рассматриваемого метода. Для реализации данного метода написано клиент-серверное программное обеспечение на C#.

Ключевые слова: защита информации; эшелонированная оборона; вероятность преодоления защиты; закрытое расписание; время нахождения под наблюдением

1. Введение

В арсенале современных средств обеспечения информационной безопасности имеется множество эффективных IT-инструментов: управление доступом, системы идентификации/аутентификации, шифрование данных, установка сетевых и межсетевых экранов, мощное антивирусное ПО, системы раннего обнаружения вторжений IDS, каскадные фильтры и прокси и т.п. [1]

Ни один из перечисленных инструментов не может считаться «главным» или самым непреодолимым или надежным – преодолеть можно фактически любую защиту. Именно поэтому стратегия информационной безопасности – стратегия «эшелонированной обороны», основанная на использовании целого комплекса разнородных средств защиты [2]. В случае прорыва одного из эшелонов безопасности, появления в нем уязвимости или выхода его из строя, «избыточная» многоуровневая защита выполнит свою задачу.

Такой подход позволяет справляться с разнонаправленными и постоянно «мутирующими» угрозами, а также повысить надежность средств защиты с учетом некоторой неуверенности в их достаточной эффективности через некоторое время эксплуатации.

Основной поток информационных угроз поступает из сети Интернет - нарушения конфиденциальности информации, ее кража или намеренное искажение, сбои и обрушения работающих систем. Обычно такие разрушительные атаки требуют определённого времени для подготовки с целью доступа к атакуемому сегменту информации – узлу сети (сканирование, поиск уязвимостей, взлом защиты, внедрение вирусов, атаки на операционную систему и программное обеспечение). [3]

Кардинальный метод защиты от потока этих угроз – отключение защищаемого узла от сети. Это способно предотвратить реализацию угроз, но приводит к прекращению обмена информацией с удаленными узлами и структурными сегментами системы. Однако, это не беда в тех случаях, когда в процессе работы, компьютеризированные системы требуют только периодического выхода во внешнюю Сеть.

В этом случае интернет-подключение и доступ к сетям может быть организован в режиме определенного по времени и продолжительности сеанса. В остальное время узел может быть просто отключен от сети и работать в автономном режиме.

2. Разрыв сетевого канала по защищенному расписанию

Исходя из вышеизложенного, в работе рассмотрен эффективный способ улучшения информационной безопасности – автономное управление разрывом сетевого канала передачи информации в соответствии с расписанием, представляющим секрет.

Сеансовое подключение к сетям защищаемого узла строго по расписанию позволяет существенно снизить угрозу несанкционированного доступа к данным. Конечно, если само расписание будет секретом, доступным только ограниченному кругу лиц, участвующих в организации связи.

Составление самого расписания подключения (доступа) защищаемых узлов к сетям может быть сделано автоматизированным, управляться соответствующим ПО и передаваться по защищенным каналам с шифрованием. Причем, чем меньше времени защищаемый узел будет соединен с сетью, тем выше будет эффективность такой защиты, которая создаст еще один эшелон безопасности.

Предлагаемый метод имеет самостоятельное значение, как ещё один эшелон обороны, но при этом повышает эффективность применения других защитных барьеров эшелонированной обороны, вероятность преодоления которых зависит от времени нахождения защищаемого узла под возможными атаками или наблюдением.

Примеры таких угроз:

1. Подбор паролей. Требуется определённое время на поиск и попытки войти в защищенные узлы. [4-6]
2. Разведка в Сети. Получение и анализ данных об атакуемой системе, аппаратных устройствах и ПО, средствах и сложности защиты будет затруднена при малом времени доступа к защищаемому узлу. [4-6]
3. Вирусы и сетевые черви. Для их внедрения и распространения требуется определённое время. [4-6]
4. Отказ в обслуживании (DDoS). Прерываемый доступ к информационным ресурсам уменьшает время воздействия и не позволяет прорвать системы защиты. [4-6]

3. Эффективность управляемого разрыва сетевого канала (доступа к защищаемому узлу из / в сети)

Эффективность защиты i-го барьера (Q_i) определяется как вероятность его непреодоления (P_i) за определенное время

$$Q_i = 1 - P_i \tag{1}$$

На рис. 1 представлена схема защиты при эшелонированной обороне.

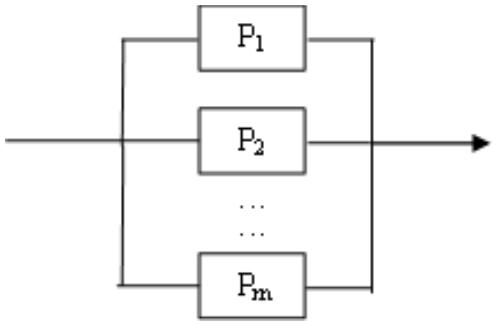

Рис. 1. Схема эшелонированной защиты.

Система будет взломана, если будут преодолены все m параллельные защитные эшелоны (i=1…m):

$$Q_\Sigma = \prod_{i=1}^{m} Q_i = \prod_{i=1}^{m} (1 - P_i) \tag{2}$$

Таким образом, вероятность непреодоления системы безопасности (надежность защиты) P_Σ:

$$P_\Sigma = 1 - \prod_{i=1}^{m} (1 - P_i) \tag{3}$$

Будем классифицировать защитные барьеры – уровни защиты на три вида:

1) Уровни защиты, вероятность взлома которых не зависит от времени (t), в течении которого узлы подключены к сети и могут подвергаться атакам. Пусть число таких уровней защиты - n
2) Уровни защиты, вероятность взлома которых зависит от времени подключения узла к сети. Пусть число таких уровней - k.
3) Дополнительно вводимый уровень защиты - управляемое отключение узла от сети и подключение по закрытому расписанию. Пусть такое расписание содержит в себе относительное время подключения к сети.

$$\gamma = \frac{t_{подкл.сост.}}{t} \tag{4}$$

При этом γ – это ни что иное, как вероятность взлома дополнительного уровня защиты Q_3, а $t_{подкл.\ сост.}$ - время пребывания узла подключенным к сети. Чем меньше время нахождения узла в подключенном состоянии, тем меньше вероятность реализации угрозы. В этом случае схема расчета вероятности непреодоления системы безопасности будет выглядеть как на рис. 2.

Если учесть влияние времени отключения ПК от сети на общую надёжность системы, получим:

$$Q_\Sigma = \prod_{i=1}^{n} Q_{1i} \cdot \prod_{i=1}^{k} (Q_{2i} \cdot \gamma) \cdot \gamma = \prod_{i=1}^{n+k} Q_i \cdot \gamma^{k+1} \tag{5}$$

$$P_\Sigma = 1 - (\prod_{i=1}^{n+k} Q_i) \cdot \gamma^{k+1} \tag{6}$$

То есть, если γ - достаточно мало (0.001), можно серьезно увеличивать P_Σ (т.е., уменьшить Q_Σ) в случаях, когда k> 2.

При предельном значении k=0, получим:

$$P_{\Sigma} = 1 - (\prod_{i=1}^{n} Q_i) \cdot \gamma \qquad (7)$$

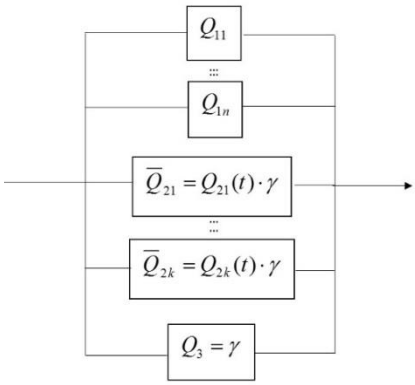

Рис. 2. Схема эшелонированной защиты с управляемым отключением от сети.

Если обозначить α повышение эффективности защиты всей системы от использования дополнительного эшелона защиты через управляемое автономное отключение узла от сетевого канала, как отношение вероятности преодоления защиты после применения метода к вероятности преодоления защиты до применения метода и то получим:

$$\alpha = \frac{\prod_{i=1}^{n} Q_{1i} \cdot \prod_{i=1}^{k} Q_{2i} \cdot \gamma^{k+1}}{\prod_{i=1}^{n} Q_{1i} \cdot \prod_{i=1}^{k} Q_{2i}} = \gamma^{k+1} \qquad (8)$$

Если γ=0,1 и k=4, то угроза взлома системы снижается в 10^5 (Рис. 3).

Дополнительный уровень защиты отчасти уязвим при подключении узла к сети. Однако сложность такого взлома практически идентична сложности взлома других уровней безопасности. Кроме того, время доступа к нему ограничено, что дает преимущества перед другими защитными инструментами.

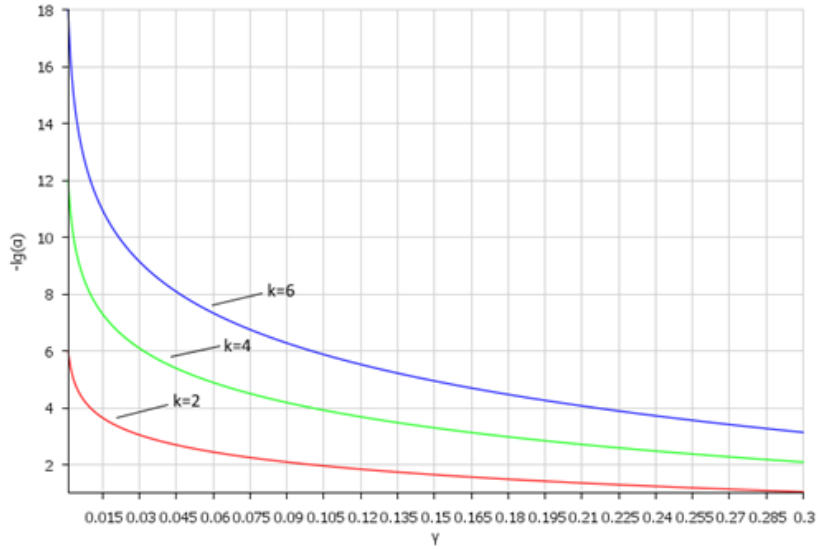

Рис. 3. Изменения эффективности защиты α от относительного времени подключения защищаемого узла к сети γ.

4. Работа ПО и аварийная защита

Для реализации способа защиты информации с помощью управляемого отключения ПК от сети, создано специализированное программное обеспечение [7]. Оно рассчитано на автономную работу защищаемых узлов-клиентов, успешно создает проблемы для злоумышленников и затрудняет их попытки взлома информационных систем (Рис. 4).

В случае необходимости поддержания двунаправленной связи для группы клиентов при подключении к серверу каждый клиент получает согласованные и зашифрованные расписания своих подключений, вне которых он отключается от сети.

Хранится и передается информация о расписании подключений в зашифрованном виде (например, алгоритм Triple DES), а любая работа с ней и редактирование расписаний выполняется только администратором с помощью специального программного модуля.

В случае технического сбоя или отсутствия связи ПК с сервером в установленное по расписанию время, программа будет пытаться восстановить связь и продолжить функционирование. Для этого разработана специальная автоматизированная сервисная служба, устраняющая неполадки в работе программы-клиента. Если заданное время подключения истекло, а связь отсутствует, служба принудительно удалит старое расписание подключений клиента, оставив клиента до выяснения причин в подключенном к сети состоянии.

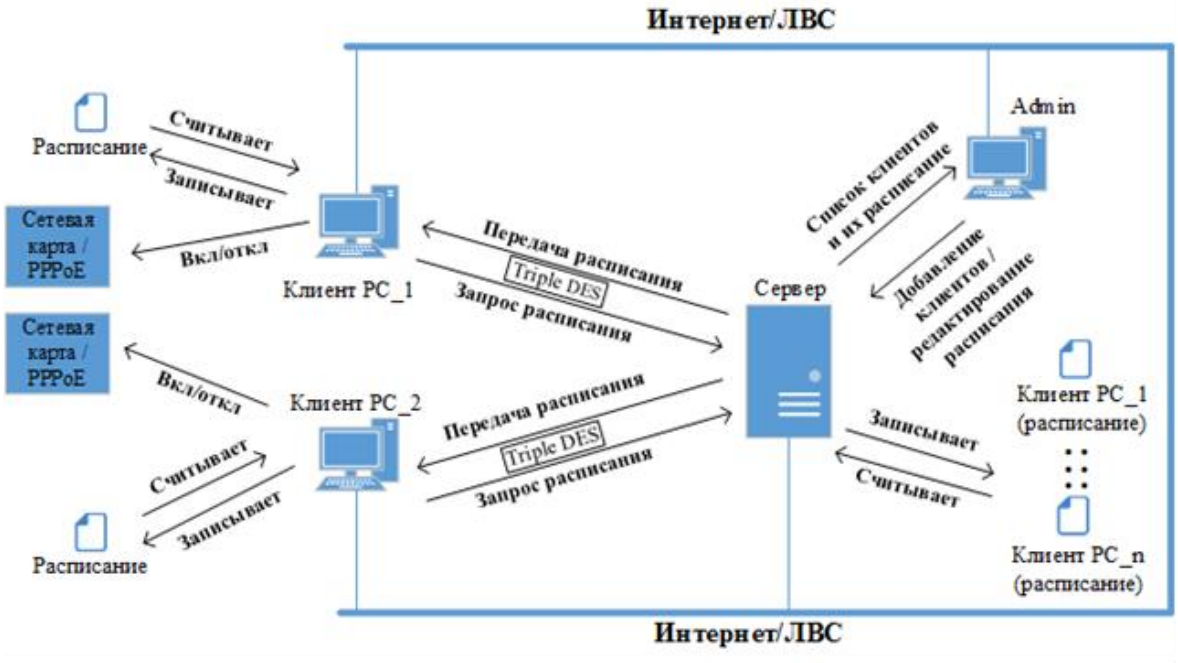

Рис. 4. Схема работы ПО, реализующего рассмотренный метод.

5. Заключение

1. Многие системные ЦВМ и автономные компьютерные сети способны эффективно работать в автономном режиме и нуждаются лишь в периодическом подключении к сети Интернет. В таких случаях предпочтительным для безопасности системы будет сеансовый режим подключений узлов к сети, т.е., включения их в сеть в определенное время и на определенный период времени.
2. Чтобы улучшить защиту информации необходимо использовать способ управляемого разрыва связи по автономным внутренним расписания подключений защищаемого узла к сетевому каналу передачи. Расписания должны представлять секрет и передаваться в защищаемый узел по защищённому каналу.
3. Для улучшения эффективности рассматриваемого метода защиты с управляемым разрывом подключения используется специализированное программное обеспечение, которое позволяет централизованным образом задавать и передавать расписания по защищённым каналам в защищаемые узлы, которые в автоматическом режиме управляют своими подключениями к сети, согласно этим расписаниям.
4. Управляемый разрыв подключения ПК к сети является самостоятельный уровнем защиты и существенно увеличивает надежность и эффективность работы уже имеющихся средств безопасности, вероятность преодоления которых зависит от времени работы сети

Литература

[1] Хорев, А.А. Угрозы безопасности информации // Специальная техника. – 2010. – № 1(67) – С. 50-63.

[2] Мостовой, Я.А., Слепушов, И.И. Повышение информационной безопасности путем управления физическим разрывом канала передачи // Материалы XXIII Российской научн. конф. ППС, НС и аспирантов. ПГУТИ, 2016. – С. 264-265.

[3] Исаев, А.Б. Современные технические методы и средства защиты информации: учебное пособие – М., РУДН, 2008., - С. 258-259.

[4] Барышников, А.А. Моделирование вероятности взлома системы информационной безопасности Исаев // Горный информационно-аналитический бюллетень. – М.: 2010. – № 5 – С. 152-155.

[5] Singer, P.W. Cybersecurity and Cyberwar: What Everyone Needs to Know / P.W. Singer, Allan Friedman. // Oxford University Press, 2014. – 101 p.

[6] John, Fay. Contemporary Security Management, Third Edition. Butterworth-Heinemann, 2010. – 56 p.

[7] Мостовой, Я.А. Программа управления доступом компьютеров к сети в сеансах связи по изменяемому закрытому расписанию / Я.А. Мостовой, И.И. Слепушов // Свидетельство о регистрации программы на ЭВМ. № 2016662289, 2016.