РТК НОВЫЕ ТЕХНОЛОГИИ

Общество с ограниченной ответственностью
«РТК Новые Технологии» (ООО «РТК НТ»)
Адрес: 192289 , Россия, Санкт-Петербург,
Гаражный проезд, д.1, лит. «И»
для почты: 190000, С.-Петербург, ВОХ 2007,
тел./факс: (812) 339-45-50

Р/сч. 40702810126000751801,
К/сч. 30101810000000000920
Ст-Петербургский ф-л ПАО «Промсвязьбанк»,
г.Санкт-Петербург,
БИК 044030920, ИНН 7816485320, КПП 781601001

Исх.№ 20 от 12.05.2016 г.

К.А.Решетников

ОТЗЫВ

на автореферат диссертационной работы Ковцура Максима Михайловича по теме «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Тема диссертационной работы М. М. Ковцура является актуальной в силу роста популярности услуг IP-телефонии и видеотелефонии и, как следствие, увеличения речевого трафика в сетях. Увеличение числа пользователей услуг, а также объемов передаваемой информации способствуют росту интереса нарушителей к перехвату передаваемых данных с целью их дальнейшего использования в своих целях. Это приводит к разработке специального программного обеспечения для осуществления атак и совершенствованию механизмов реализации атак.

Обеспечение информационной безопасности (ИБ) – постоянный, непрекращающийся процесс, не сводящийся к разовому мероприятию, организационному или техническому. Обнаружение уязвимых с точки зрения ИБ мест в каналах связи, в частности, наличия нарушителей различного типа – первый, но один из самых важных этапов обеспечения ИБ.

В свете поставленной цели исследования – повышения уровня защищенности информации в сеансах IP-телефонии и сокращения времени установления защищенного соединения – автором разработаны:

- модель нарушителя для оценки защищенности системы IP-телефонии;
- методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии;
- предложения по модификации протокола распределения ключей для улучшения вероятностно-временных характеристик протокола;

- метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана;
- предложения по модификации протокола Zimmermann Real-time Transport Protocol (ZRTP) для обеспечения безопасности корреспондентов при взаимодействии без сервера в топологии клиент-клиент.

Представленные к защите результаты обладают научной новизной, а также теоретической и практической значимостью. Предложенная методика, основанная на математическом аппарате вероятностных графов и производящих функций, позволяет выполнить оценку среднего времени успешного завершения протоколов с учетом переменного таймера повторной передачи, а представленный метод повышения безопасности позволяет обнаружить активного нарушителя, реализующего атаку "человек посередине", при отсутствии общего ключевого материала между корреспондентами.

Тематика публикаций в изданиях из перечня ВАК отражает полученные результаты и содержание работы.

Вместе с тем, к автореферату имеются следующие замечания:

1. Использование вероятностных графов предполагает наличие процедур постоянной актуализации значений этих вероятностей, которые, очевидно, изменяются во времени. К сожалению, в автореферате отсутствуют описания подобных процедур;
2. Для эксперимента при проверке наличия независимых маршрутов канал связи устанавливается между двумя точками (городами), но в таблице 1 указывается только одна точка. Возможно, второй точкой является Санкт-Петербург, однако в тексте автореферата это не указано;
3. В автореферате следовало бы привести ссылки на нормативные документы, описывающие требования, предъявляемые к каналам связи для предоставления услуг IP-телефонии.

Представленные замечания не снижают ценности, практической и теоретической значимости работы, которая представляет собой законченное исследование, содержащее решение важной научно-технической задачи.

Постановка задачи, ее актуальность, качество решения, внедрение полученных результатов дают основания для признания диссертационной работы соответствующей требованиям п. 9 Положения о присуждении ученых степеней, предъявляемых к кандидатским диссертациям, а автор - Ковцур Максим Михайлович достоин присуждения ученой степени кандидата технических наук по специальности 05.13.19 – "Методы и системы защиты информации, информационная безопасность".

Ведущий специалист