PLENARY TALKS

СЕТЕВАЯ БЕЗОПАСНОСТЬ СРЕДСТВАМИ МАРШРУТИЗАЦИИ: ПРОБЛЕМЫ И РЕШЕНИЯ

А.В. Лемешко, М.А. Евдокименко, А.С. Еременко
Харьковский национальный университет радиоэлектроники, Харьков, Украина
e-mail: oleksandr.lemeshko@nure.ua, marina.ievdokymenko@nure.ua,
oleksandra.yeremenko@nure.ua

Обеспечение информационной безопасности страны является важной государственной проблемой, решение которой требует максимальной концентрации сил и средств на всех этапах, связанных с формированием, передачей/приемом, хранением, обработкой, отображением и даже уничтожением информации. В последнее время все больше внимания уделяется именно проблематике обеспечения сетевой безопасности, когда объектом атак и компрометации передаваемых сообщений становится коммуникационное оборудование [3], [5]. Именно разнотипные и взаимодополняющие организационные, социальные, технические (аппаратные и программные) меры и средства должны обеспечить надлежащий уровень безопасности информации, передаваемой в современных телекоммуникационных сетях (ТКС).

Достаточно действенным средством обеспечения сетевой безопасности в ТКС являются протоколы маршрутизации. Именно они должны обеспечить проактивную и реактивную защиту сети на основе сбора и анализа информации о ее состоянии. В то же время протоколы безопасной маршрутизации, кроме привычных данных о состоянии сети, должны прогнозировать и оценивать значение ключевых показателей безопасности коммутационного и серверного оборудования ТКС, уровени их уязвимости и компрометации. С этой целью математическое и алгоритмическое обеспечение протоколов маршрутизации в ТКС должно быть усовершенствовано и расширено под новые условия и задачи, связанные с обеспечением заданного уровня сетевой безопасности.

В зависимости от перечня и содержания требований, которые предъявляются к уровням сетевой безопасности и QoS, маршрутизирующие решения могут достаточно сильно различаться [1]-[7]. Первая большая группа решений посвящена маршрутизации конфиденциальных сообщений (КС) с использованием, например, механизма SPREAD (Secure Protocol for Reliable dAta Delivery) [2]. В его основу положен принцип порогового разделения КС в соответствии с выбранной схемой Шамира на отдельные фрагменты (части), которые в дальнейшем передаются в ТКС к получателю по множеству непересекающихся путей. В работе [6] предложены решения по усовершенствованию механизма SPREAD, в рамках которых допускается определенный характер пересечения путей в ТКС, что сопровождается улучшением показателей сетевой безопасности при передаче КС. Закон (схема) разделения

сообщения на фрагменты в общем случае может быть известна злоумышленнику, но скомпрометировать конфиденциальное сообщение он сможет только тогда, когда скомпрометирует все используемые пути. Поэтому уровень сетевой безопасности в этом случае полностью зависит от количества и безопасности путей, используемых для доставки фрагментов КС.

Вторая группа решений по безопасной маршрутизации [4], [7] основана на использовании соответствующих маршрутных метрик, которые, в общем случае, должны учитывать множество показателей сетевой безопасности (Network Security, NS) каналов связи и маршрутизаторов ТКС. Так, в работе [7] для расчета маршрутных метрик используются выражения, характеризующие риск информационной безопасности элементов ТКС в соответствии с рекомендациями NIST, учитывая убытки от нарушения конфиденциальности и целостности информации, доступности сетевого ресурса в случае использования имеющихся уязвимостей, а также показатели сложности использования уязвимостей на узлах сети и доступа к сетевым элементам и сети в целом вследствие использования указанных уязвимостей. Метрический подход используется и при организации безопасной маршрутизации мультимедийных потоков пакетов, т.е. когда, например, необходимо обеспечить для передаваемой в ТКС аудиовизуальной информации высокий уровень и качества обслуживания (Quality of Service, QoS), и сетевой безопасности. Основной научной и прикладной задачей тогда становится поиск моделей композитного учета показателей NS/QoS [4].

Третья группа решений, касающаяся маршрутизации потоков пакетов с целью повышения показателей NS/QoS, основана на реализации принципов Traffic Engineering (TE) [1]. При этом балансировка нагрузки в ТКС происходит с учетом не только сетевых параметров, которые характеризуют уровень ее качества обслуживания, например, пропускную способность, но и уровень сетевой безопасности – вероятность компрометации узлов и каналов сети. В рамках решений Secure TE заложена возможность регулировать чувствительность потоков пакетов к показателям NS/QoS, так как нередко повышение уровня сетевой безопасности отрицательно сказывается на показателях QoS.

Таким образом, в зависимости от особенностей структурно-функционально построения ТКС, ее состояния и загруженности, требований относительно уровней NS и QoS на практике могут использоваться различные подходы к организации процессов безопасной маршрутизации. Разнотипные математические модели и методы безопасной маршрутизации могут быть положены в основу алгоритмическо-программного обеспечения маршрутизаторов традиционных IP/MPLS-сетей, серверов или контроллеров маршрутов в программно-конфигурируемых сетях, реализуясь в форме перспективных протоколов маршрутизации.

Ключевые слова: сетевая безопасность, маршрутизация, балансировка нагрузки, телекоммуникационная сеть, уязвимость, метрика.

Литература

1. Lemeshko O., Shapovalova A., Al- Dulaimi A.M.K., Yeremenko O., Yevdokymenko M. (2020), Flow-Based Routing Model With Load Balancing Under Network Security Parameters, Information and Telecommunication Sciences, No. 2, pp. 44-50.
2. Lou W., Liu W., Fang Y. (2004), SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks", INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, China, 7–11 March, P. 2404-2413.
3. Santos O., Kampanakis P., Woland A. (2016), Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP, 1st edition, Cisco Press, 368 p.
4. Snihurov A., Chakrian V. (2015), Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters, Scholars Journal of Engineering and Technology, No. 3(8), P. 707-714.
5. Stallings W. (2016), Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 768 p.
6. Yeremenko O., Lemeshko O., Persikov A. (2018), Secure Routing in Reliable Networks: Proactive and Reactive Approach, Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, No. 689, Springer, Cham, P. 631–655.
7. Yevdokymenko M., Yeremenko O., Shapovalova A., Shapoval M., Porokhniak V., Rogovaya N. Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment. Workshop Proceedings of the MoMLeT+DS 2021: 3rd International Workshop on Modern Machine Learning Technologies and Data Science, June 5, 2021, Lviv-Shatsk, Ukraine. pp. 207-217.

Network security by routing means: problems and solutions

An overview of the main solutions related to secure routing in telecommunication networks is carried out. The review covers theoretical approaches based on optimizing secure routing processes associated with implementing the SPREAD mechanism, the metric approach, and the principles of Secure Traffic Engineering. The analyzed solutions can form the basis of promising routing protocols in traditional and software-defined networks.