



Contribution ID: 179

Type: not specified

Reduction of network traffic to point images for the analysis of its behavioral structure

Tuesday, 4 July 2017 16:30 (15 minutes)

In Cisco Guard XT technology under the protection against DDoS attacks, along with filtering and active verification, uses anomaly detection. In this case, all traffic that is not stopped by the filtering and active verification modules is monitored, and this traffic is matched against the basic behavior recorded for a certain period of time.

In this paper, we propose an approach based on the reduction of numerous parameters of network traffic into point images that form the corresponding time trajectories in 3D and 2D spaces. Initial parameters of the network traffic are obtained from the information generated by the NetFlow protocol (Cisco). In the future, the resulting trajectories can be easily used both at the learning stage and at the stage of anomalies recognizing of network traffic, since it becomes possible both for visual and automatic marking of 3D and 2D spaces to normal and abnormal areas.

Examples of visualization of network traffic are presented, which simplify the analysis of its behavioral structure.

Keywords: network traffic, DDoS-attack, parameters, reduction, point images, learning, recognition, behavioral structure.

Редукция сетевого трафика в точечные образы для анализа его поведенческой структуры

Боков Д.Ю., Краснов А.Е., Никольский Д.Н., Репин Д.С.

Аннотация.

В технологии Cisco Guard XT при защите от DDoS атак наряду с фильтрацией и активной верификацией используется распознавание аномалий. При этом выполняется мониторинг всего трафика, который не был остановлен модулями фильтрации и активной верификации, и этот трафик сопоставляется с базовым поведением, зафиксированным в течение определенного периода времени.

В настоящей работе предлагается подход, основанный на редукции многочисленных параметров сетевого трафика в точечные образы, формирующие соответствующие временные траектории в 3D и 2D пространствах. При этом исходные параметры сетевого трафика получают из информации, формируемой протоколом NetFlow (Cisco). В дальнейшем получаемые траектории легко использовать как на стадии обучения, так и на стадии распознавания аномалий сетевого трафика, поскольку появляется возможность как визуальной, так и автоматической разметки 3D и 2D пространств на нормальные и аномальные области.

Приведены примеры образной визуализации сетевого трафика, упрощающие анализ его поведенческой структуры.

Ключевые слова: сетевой трафик, DDoS-атака, параметры, редукция, точечные образы, обучение, распознавание, поведенческая структура.

Primary author: Dr REPIN, Dmitry (State Institute of Information Technologies and Telecommunications «Informika»)

Co-authors: Prof. KRASNOV, Andrey (State Institute of Information Technologies and Telecommunications «Informika»); Dr BOKOV, D (State Institute of Information Technologies and Telecommunications «Informika»); Dr NIKOL'SKII, Dmitry (State Institute of Information Technologies and Telecommunications «Informika»)

Presenter: Dr REPIN, Dmitry (State Institute of Information Technologies and Telecommunications «Informika»)

Session Classification: Mathematical methods and application software for modeling complex systems and engineering (II)