УДК 004.056
DOI: 10.17586/0021-3454-2016-59-10-807-812

МЕТОДИКА ВИЗУАЛИЗАЦИИ ТОПОЛОГИИ КОМПЬЮТЕРНОЙ СЕТИ ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ

М. В. Коломеец, А. А. Чечулин, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук, 199178, Санкт-Петербург, Россия
E-mail: kolomeec@comsec.spb.ru

Разработана методика визуализации данных топологии компьютерной сети для мониторинга безопасности, применяемого в SIEM-системах, а также системах мониторинга компьютерных сетей и сетевой активности. Методика основана на использовании соотношения эффективности восприятия и информативности отображаемых данных. Методика учитывает возможные модели визуализации, которые могут быть применены для отображения данных мониторинга безопасности, особенности когнитивного аппарата оператора, которые были рассмотрены коллективом авторов в предыдущих работах. Методика включает в себя все этапы процесса визуализации, что позволяет рассматривать отдельные компоненты системы визуализации данных безопасности на уровне архитектуры разрабатываемого или анализируемого программного средства. Представленные результаты могут быть использованы при разработке систем визуализации, для повышения эффективности уже реализованных систем, а также для оценки их эффективности. Приводится пример использования методики для повышения эффективности визуализации топологии компьютерных сетей с использованием древовидных и графовых структур.

Ключевые слова: *методика визуализации, визуализация топологии компьютерной сети, мониторинг безопасности компьютерной сети, SIEM-системы, компьютерная безопасность*

Целью представленного исследования являлась разработка обобщенной методики визуального представления разнородных данных и демонстрация возможности ее использования для визуализации компьютерной сети при помощи древовидных и графовых структур. Эта методика предназначена для мониторинга безопасности, применяемого в комплексах систем управления событиями безопасности и информационной безопасностью (Security Information and Event Management, SIEM).

Классическим представлением модели визуализации компьютерной сети является граф, в котором под узлами понимаются хосты сети, а дугами обозначаются связи между хостами. В работах [1, 2] рассмотрен подход, согласно которому изображения вершины графа представлены различными метриками защищенности [3, 4] соответствующих хостов. Благодаря развитию подхода [5] у пользователя появляется возможность видеть как текущие, так и предыдущие значения метрик безопасности. В работах [6, 7] рассмотрены основные графические модели и способы отображения данных, а также методы их оценки и эффективного применения в зависимости от сценария использования [8].

Такой подход основан на моделях визуализации [6], что позволяет комбинировать отдельные компоненты системы, в то же время он обеспечивает учет особенностей когнитивного аппарата оператора [9], благодаря чему повышается эффективность визуального анализа отображаемой информации.

Качество работы системы визуализации зависит от того, насколько эффективно пользователь воспринимает информацию при анализе изображений, предоставляемых системой, и от того, насколько эти изображения информативны. Очевидно, что графические модели,

которые лежат в основе систем визуализации, обладают различным соотношением „эффективность—информативность“. При этом часто повышение информативности отрицательно сказывается на эффективности восприятия, и наоборот. Примеры информативной, но неэффективной таблицы и неинформативного, но хорошо воспринимаемого (эффективного) символа тревоги приведены на рис. 1, *а* и *б* соответственно.

а)

Input Packet Length	Input Rate	Input Media Overhead (Ethernet)	Total Input Port bytes	MAC removed bytes (including CRC)	Other PP/MAC/FRAMER removed bytes	PP Packet add bytes (to fabric and peer PP)	Switch Port Packet Size	Switch Port effective Input Rate
64	1.00E+10	20	84	24	0	12	72	8.57E+09
128	1.00E+10	20	148	24	0	12	136	9.19E+09
256	1.00E+10	20	276	24	0	12	264	9.57E+09
1500	1.00E+10	20	1520	24	0	12	1508	9.92E+09

б)

Рис. 1

Для повышения эффективности систем визуализации разрабатывают и внедряют модели визуализации, которые можно охарактеризовать как концептуальные графические модели. Однако при этом разработка и внедрение новых графических моделей должны производиться согласно методике, которая может обеспечить необходимое соотношение „эффективность—информативность“ в соответствии со сценарием использования системы визуализации.

В статье [6] представлены основные графические модели, которые применяются в системах визуализации, а также описываются параметры этих моделей, влияющие на отношение „эффективность—информативность“. Информативность визуализации зависит от детализации собранных агрегированных и корректированных данных и от графических моделей, отображающих эти данные (графики, графы карты деревьев, географические карты, матрицы, гистограммы, трилинейные координаты, параллельные координаты).

При использовании классических графических моделей для наглядного представления данных применяются некоторые визуальные приемы, такие как расположение объекта в пространстве, кодирование информации при помощи формы, размера и цвета этого объекта [6].

Необходимого соотношения „эффективность—информативность“ также можно достичь при использовании в графической модели дополнительных инструментов, таких как „рыбий глаз“ [10], „множественный взгляд“, „семантическое масштабирование“ [11], „небольшие различия“ [12] и др. Важно также предоставить пользователю возможность получить исчерпывающую информацию о выбранном объекте при помощи инструментов поиска [13].

Таким образом, формируемое изображение не должно „выходить за рамки“ возможностей когнитивного аппарата человека [9]. На эффективность восприятия информации при визуальном анализе влияют основные особенности когнитивного аппарата человека. В предыдущей работе авторов [7] были рассмотрены шаблон визуального поиска, учет когнитивного аппарата человека, соответствие данных и их представления, контроль информационного шума, наличие в модели прямых манипуляций, применяемый в модели концепт графического дизайна.

При этом отношение „эффективность—информативность“ зависит и от способа сбора и анализа данных, подлежащих визуализации.

Процесс визуализации топологии компьютерной сети включает шесть этапов.

Этап 1. Выбор источников данных. На этом этапе необходимо определить системы, ответственные за сбор данных, с учетом сценария использования системы визуализации. Так как каждая система сбора предоставляет данные в уникальном формате, необходимо разработать парсеры для модуля сбора данных и определить интерфейсы взаимодействия систем сбора с системой визуализации, а также разработать алгоритмы нормализации для преобразования данных к единой структуре.

Этап 2. Выбор алгоритмов агрегации и корреляции. С использованием определенной последовательности выбранных алгоритмов происходит анализ данных, их объединение и формирование непосредственно для отображения. Этот этап является самым значимым, так как на основе сформированных данных выбирается графическая модель для визуализации.

Этап 3. Формирование списка графических моделей. На этом этапе выбираются графические модели, которые позволят визуализировать полученные на предыдущем этапе данные. Критериями для выбора могут быть: степень детализации данных, возможность единовременного отображения всего объема данных, отношение количества характеристик данных к количеству метрик, поддерживаемых графической моделью и т.д. При выборе графической модели также должен учитываться сценарий использования системы визуализации.

Этап 4. Изменение графических моделей для обеспечения необходимого соотношения „эффективность—информативность“. Для каждой выбранной на предыдущем этапе графической модели необходимо проверить, насколько она соответствует сценарию использования системы визуализации, удалить избыточные элементы из графической модели или добавить новые. Изменения должны обеспечить максимальную эффективность восприятия для конкретного сценария использования системы визуализации. В то же время изменения не должны негативно сказаться на информативности, а также нивелировать преимущества графической модели, выбранной на третьем этапе.

Этап 5. Добавление инструментов (для дополнительной корректировки соотношения „эффективность—информативность“) к графической модели (например, „рыбий глаз“, „множественный взгляд“). При добавлении следует учитывать ограничения, описанные для этапа 4.

Этап 6. Создание информационной панели. На заключительном этапе производится объединение графических моделей, инструментов для работы с ними, с модулями сбора и анализа данных в единую систему визуализации.

В соответствии с предложенной методикой сначала необходимо обеспечить сбор данных. Для визуализации топологии и параметров сети наиболее важны физические источники информации, например, могут использоваться активные и пассивные средства сбора информации о компьютерной сети: Nmap [14] и Wireshark [15].

Затем необходимо проанализировать информацию, собранную на предыдущем этапе. В том числе для визуализации безопасности, рассчитываются такие метрики, как возможный ущерб от эксплуатации уязвимости (на основе данных об уязвимостях этого хоста), критичность активов (на основе оценки данных, хранящихся на хосте) и т.д. Так как различные источники могут предоставлять одну и ту же информацию (с небольшими различиями), следует выполнить корреляцию и агрегацию данных.

На следующем этапе необходимо выбрать графические модели, которые позволяют визуализировать проанализированные данные. В большинстве систем для визуализации данных компьютерной сети используются графы, матрицы и карты деревьев. Матрицы подходят для отображения компьютерных сетей сложной топологии, где каждый хост имеет множество связей. Карты деревьев эффективны в отображении метрик сугубо иерархических сетей, графы — при визуализации небольших компьютерных сетей или сетей, хосты которых не содержат много связей. Все три указанные графические модели удовлетворяют критериям выбора (возможность отображать топологию сети и метрики хостов), однако в настоящей работе рассматривается только наиболее простая и распространенная модель — граф.

Сценарий использования графической модели предполагает визуализацию для анализа топологии сети и получение значений нескольких метрик для каждого хоста и связей между хостами. Топология сети уже представлена на графе вершинами и ребрами, для того чтобы визуализировать метрики связей между хостами, необходимо изменить способ отображения ребер графа. При помощи цвета, степени прозрачности, толщины и направления ребра могут отображаться, как минимум, 4 метрики. Необходимо отметить, что в случае двунаправленной

связи, например при клиент-серверном взаимодействии, происходит наложение ребер друга на друга, когда при помощи толщины ребра визуализируются метрики связи (рис. 2, *а*). Таким образом, использование метрик в виде длины, толщины или цвета ребра не представляется возможным, поскольку ребра накладываются друг на друга. Однако одновременное отображение всех четырех метрик связи возможно при отображении ребер, как на рис. 2, *б*. В данном случае ребра располагаются последовательно, направление связи обозначено стрелкой, а значение метрики выражается в толщине ребра.

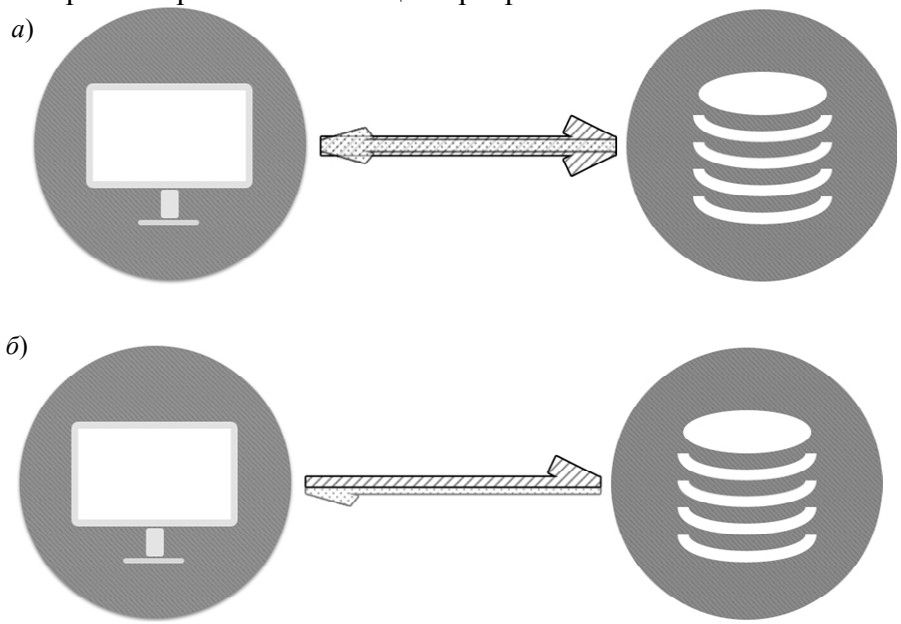

Рис. 2

Построенная таким образом графическая модель соответствует требуемому уровню „информативность—эффективность“, и применение дополнительных инструментов не требуется.

На заключительном этапе необходимо объединить все построенные графические модели и средства управления ими в единую информационную панель таким образом, чтобы выполнялась концепция множественного взгляда.

Заключение. В настоящей работе предлагается использовать соотношение эффективности восприятия данных пользователем и информативности данных визуализации с целью визуализации топологии компьютерной сети для мониторинга данных безопасности. Предложена методика визуализации, учитывающая существующие графические модели, основные когнитивные особенности человека, архитектуру системы визуализации и способ использования системы визуализации. Согласно методике поэтапно осуществляется выбор отдельных компонентов архитектуры разрабатываемой системы либо дополняются модели визуализации, вследствие чего достигается большая эффективность восприятия и повышается качество работы пользователя (оператора) с самой системой визуализации. Представленная методика может быть использована как для разработки системы визуализации топологии компьютерной сети, так и для повышения эффективности уже существующей системы или для ее оценки. В работе также продемонстрирован пример работы методики для визуализации топологии компьютерных сетей в виде графовых и древовидных структур.

Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. *Erbacher R.* Visualization design for immediate high-level situational assessment // Intern. Symp. on Visualization for Cyber Security (VizSec'12). 2012. P. 17—24.
2. *Matuszak W., DiPippo L., Lindsay Y.* Sun CyberSAVe — situational awareness visualization for cyber security of smart grid systems // Intern. Symp. on Visualization for Cyber Security (VisSec'13). 2013. P. 25—32.
3. *Котенко И. В., Новикова Е. С., Чечулин А. А.* Визуализация метрик защищенности для мониторинга безопасности и управления инцидентами // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 42—47.
4. *Kotenko I., Doynikova E., Chechulin A.* Security metrics based on attack graphs for the Olympic Games scenario // 22th Euromicro Intern. Conf. on Parallel, Distributed, and Network-Based Processing (PDP 2014). Torino, Italy, February, 2014. art. no. 1066-6192/14. DOI 10.1109/PDP.2014.113.
5. *Kotenko I. V., Novikova E. S.* Visualization of security metrics for cyber situation awareness // 9th Intern. Conf. on Availability, Reliability and Security (ARES 2014). Fribourg, Switzerland, 2014. P. 506—513.
6. *Kolomeec M., Chechulin A., Kotenko I.* Methodological primitives for phased construction of data visualization models // J. of Internet Services and Information Security (JISIS). 2015. Vol. 5, N 4. November. P. 60—84.
7. *Коломеец М. В., Чечулин А. А., Котенко И. В.* Обзор методологических примитивов для поэтапного построения модели визуализации данных // Тр. СПИИРАН. 2015. Вып. 42. С. 232—257.
8. *Kotenko I., Chechulin A.* A Cyber attack modeling and impact assessment framework // 5th Intern. Conf. on Cyber Conflict 2013 (CyCon 2013). Tallinn, Estonia, 2013. P. 119—142.
9. *Goldstein B.* Cognitive Psychology. Thomson Wadsworth, 2005.
10. *Sarkar M., Brown M.* Graphical fisheye views // Communications of the ACM. 1994. Vol. 37, N 12. P. 73—83.
11. *Watson G.* Lecture 15 — Visualisation of Abstract Information. Edinburgh Virtual Environment Centre, 2004.
12. *Wroblewski L.* Small Multiples within a User Interface // Web Form Design, 2005 [Электронный ресурс]: <http://www.uxmatters.com/mt/archives/2005/12/small-multiples-within-a-user-interface.php>.
13. *Ferebee D. and Dasgupta D.* Security visualization survey // 12th Colloquium for Information Systems Security Education. University of Texas, 2—4 June 2008. 124 p.
14. *Lyon G.* Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning, Insecure.Com, LLC, 2009.
15. *Orebaugh A., Ramirez G., Beale J.* Wireshark and Ethereal: Network Protocol Analyzer Toolkit, Syngress, 2007.

Сведения об авторах

Максим Владимирович Коломеец — Санкт-Петербургский институт информатики и автоматизации РАН, лаборатория проблем компьютерной безопасности; программист; E-mail: kolomeec@comsec.spb.ru

Андрей Алексеевич Чечулин — канд. техн. наук; Санкт-Петербургский институт информатики и автоматизации РАН, лаборатория проблем компьютерной безопасности; E-mail: chechulin@comsec.spb.ru

Игорь Витальевич Котенко — д-р техн. наук, профессор; Санкт-Петербургский институт информатики и автоматизации РАН, лаборатория проблем компьютерной безопасности; E-mail: ivkote@comsec.spb.ru

Рекомендована лабораторией проблем компьютерной безопасности

Поступила в редакцию 27.06.16 г.

Ссылка для цитирования: *Коломеец М. В., Чечулин А. А., Котенко И. В.* Методика визуализации топологии компьютерной сети для мониторинга безопасности // Изв. вузов. Приборостроение. 2016. Т. 59, № 10. С. 807—812.

TECHNIQUE OF VISUALIZATION OF COMPUTER NETWORK TOPOLOGY FOR MONITORING OF INFORMATION SECURITY

M. V. Kolomeets, A. A. Chechulin, I. V. Kotenko

St. Petersburg Institute for Informatics and Automation of the RAS,
199178, St. Petersburg, Russia
E-mail: kolomeec@comsec.spb.ru

A new visualization technique for computer network topology is developed to be used in SIEM or similar systems for information security monitoring of computer networks. The technique is based on a proposed conception and is reported to improve the effectiveness of security visualization systems. The technique considers the existing visualization models that can be used for visualization of security monitoring data. The technique takes into the account the features of cognitive apparatus of the system operator described in detail in previous papers by the authors. The proposed technique contains all stages of data visualization process and therefore allows for consideration of individual components of visualization system of information security on the architecture level. Generally, the technique unifies the approach to development of security data visualization system for computer network. The results of the study may be used in design of a new visualization system, as well as for evaluation and improvement of existing visualization system efficiency. An example of the proposed technique application to improve the efficiency of network topology visualization based on tree and graph visual model is presented.

Keywords: visualization technique, visualization of topology of computer network, security monitoring of computer network, SIEM, cyber security.

Data on authors

Maxim V. Kolomeets — St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems; Programmer; E-mail: kolomeec@comsec.spb.ru

Andrey A. Chechulin — PhD; St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems; E-mail: chechulin@comsec.spb.ru

Igor V. Kotenko — Dr. Sci., Professor; St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems; E-mail: ivkote@comsec.spb.ru

For citation: *Kolomeets M. V., Chechulin A. A., Kotenko I. V.* Technique of visualization of computer network topology for monitoring of information security // Izv. vuzov. Priborostroenie. 2016. Vol. 59, N 10. P. 807—812 (in Russian).

DOI: 10.17586/0021-3454-2016-59-10-807-812