网络安全可视化综述

袁 斌, 邹德清, 金 海

华中科技大学 服务计算技术与系统教育部重点实验室 集群与网格计算湖北省重点实验室 武汉 中国 430074

摘要 随着互联网技术的发展, 网络渗入到人们生活的方方面面。一方面, 电子商务、社交网络、线上娱乐、信息化办公等各种网络应用为人们的生活带来了诸多便利; 另一方面, 网络与人们生活的不可分割性为网络攻击和网络犯罪提供了可乘之机。攻击者通过各种各样的网络攻击获取他人隐私, 牟取非法利益。近年来, 网络攻击的数量越来越多, 攻击的规模越来越大, 攻击的复杂度也越来越高。因此, 网络安全比以往任何时期都显得重要。然而传统的网络安全保障机制, 如入侵检测, 防御系统, 网络防火墙等, 因其智能性、动态性、全局性等的缺乏, 都不足以应对越发复杂和高强度的网络攻击。因此, 网络安全可视化应运而生, 成为近年来网络安全研究的一个热点。与传统网络安全保障机制不同, 网络安全可视化技术不仅能有效处理海量网络数据信息, 捕获网络的全局态势, 而且能通过对图形图像模式的分析帮助网络管理人员快速识别潜在的攻击和异常事件, 即时预测安全事件, 甚至是发现新的攻击类型。可视化技术为网络安全研究方法带来了变革, 优秀的网络安全可视化方案层出不穷。网络安全可视化建立在对网络数据分析的基础之上, 网络数据对网络安全分析十分重要, 而大数据时代的到来进一步凸显了数据的重要性。因此, 本文从数据角度出发, 根据所处理的网络数据的类型, 对网络安全可视化工作进行系统的整理、分类和对比。此外, 本文还深入分析网络安全可视化研究面临的挑战并探讨未来该领域的研究方向。

关键词 可视化技术; 网络安全; 安全可视化
中图法分类号 TN915.08 DOI 号 10.19363/j.cnki.cn10-1380/tn.2016.03.002

Network Security Visualization: A Survey

YUAN Bin, ZOU Deqing, JIN Hai

Cluster and Grid Computing Lab, Services Computing Technology and System Lab, Huazhong University of Science and Technology, Wuhan, 430074, China

Abstract The developing of Internet techniques has brought many convenience into our daily life, such as on-line shopping, on-line entertainment, social network, etc. However, cyber-attack and cyber-crime have also become more and more common since Internet provides so many potential profits, which makes cyber security more and more important. Unfortunately, traditional cyber security approaches, such as firewall, IDS and IPS, are not efficient because they lack the feature of intelligence, dynamic nature and global view. As such, network security visualization is proposed. Visualization is not only efficient but also very effective at communicating information. Based on the analysis of network data, network security visualization transfers the invisible, unexpressed and abstract network data into visual images to provide a high-level view of security events to analysts for more timely and informed decisions. Visualization brings revolution to the network security research area and has developed very fast. In this paper, we provide a thorough survey of network security visualization, categorizing the related work based on the type of network data (since network data is the basis of network security visualization). Further, we analyze the issues and challenges regarding network security visualization and provide guidelines and directions for future work.

Key words visualization techniques; network security; security visualization

1 引言

随着互联网技术的发展和普及, 网络渗入到了人们生活的方方面面。电子商务、社交网络、线上娱乐、信息化办公等各种网络应用为人们的生活带来了诸多便利。与此同时, 网络在人们日常生活的全面渗透为恶意网络用户提供了可乘之机。近年来, 网络攻击和网络犯罪层出不穷。攻击者通过各种不同的攻击方式, 获取隐私信息、造成网络公共设施瘫痪、牟取非法利益。更严重的是, 随着技术的发展和普及, 网络攻击的门槛越来越低, 攻击数量越来越多, 攻击强度也越来越大。网络攻击不仅能够造成巨

通讯作者: 金海, 博士, 华中科技大学教授, Email: hjin@hust.edu.cn。
本课题得到 973 国家重点基础研究发展计划(2014CB340600)资助。
收稿日期: 2016-06-21; 修改日期: 2016-06-29; 定稿日期: 2016-07-01

大的经济损失, 甚至能威胁到国防安全。因此, 网络安全已经成为信息基础建设的重要组成部分, 不仅关系到民众生活, 而且关系到社会稳定, 国家存亡。

然而, 传统网络安全保障机制存在诸多不足, 难以应付日趋复杂的网络攻击。如, 杀毒软件不能抵御网络攻击; 防火墙技术缺乏动态性, 且无法处理来自内部网络的攻击; 入侵检测与防御系统则有着高误报率等缺陷[1]。此外, 传统网络安全保障机制还存在缺乏全局视角、交互性差、无法提前预测等不足。

在这种情况下, 网络安全可视化应运而生。与传统网络安全保障机制不同, 网络安全可视化技术不仅能有效处理海量网络数据信息, 捕获网络的全局态势, 而且能帮助网络管理人员通过对图形图像的分析来快速识别潜在的攻击和异常事件, 即时预测安全事件, 甚至发现新的攻击类型。例如, 网络入侵检测通常会产生大量的警报信息, 对这些警报信息的传统分析方法需要耗费管理员大量的精力, 且容易出错。而可视化技术可以把不可见的抽象的警报信息转换成直观的便于理解的图像信息, 极大地方便管理员对警报信息的分析, 从而快速掌握网络动态, 识别网络异常。

网络安全可视化系统的处理流程通常可以分为: 网络数据源选取; 数据分析处理; 图形化显示; 用户交互等步骤。网络安全可视化系统在选取数据源并对数据进行分析的基础上, 将抽象的网络数据以图形的方式展现出来, 从而帮助分析人员更直观、准确地分析网络状况, 识别网络异常并预测网络发展趋势。

网络安全可视化是可视化技术在网络安全领域的应用, 因其在全局性、高交互性、智能性等方面的优势, 迅速成为了网络安全研究的热点之一。然而, 网络安全可视化是一个新型的尚处在发展阶段的研究领域, 在关键技术和基础理论的研究上还有很多问题亟待解决。

因此, 本文从数据角度--网络安全可视化技术的基础--出发, 根据所处理的网络数据源的类型, 对网络安全可视化工作进行系统的整理、分类和对比。此外, 本文还深入分析网络安全可视化研究面临的挑战并探讨未来该领域的研究方向。笔者希望通过对现有工作的系统的整理和对未来研究方向的探讨, 来吸引更多的学者参与该领域的研究, 共同促进网络安全可视化的发展, 进一步丰富网络安全研究内容, 强化网络安全保障。

2 网络数据源

网络安全可视化的第一步是选取合适的网络数据源并对网络数据进行分析, 在此基础上, 来完成后续的图形展示和交互操作。因此, 网络数据源是网络安全可视化的基础。

另一方面, 目前的网络安全可视化系统有着很多不同的目标, 如态势感知、网络取证、主机异常行为检测、BGP 异常检测等。有着不同目标的系统需要对不同的网络事件、网络行为、网络属性等进行分析。而不同类型的网络数据源则为这些系统提供了不同的网络信息。正是丰富的网络数据源类型使得网络安全可视化系统有着多方面的应用。

目前网络安全可视化系统中常用的网络数据源可分为以下几种:

1) **网络流量数据**。网络流量数据通常包含完整的网络数据包, 可以通过 TCPDUMP[3], WIRESHARK [4]等软件进行获取。

2) **NetFlow**。NetFlow 由思科提出, 能提供网络流量的会话级视图。它虽然不提供网络流量的完整记录, 但具有更有易于管理和易读的优势。

3) **日志**。几乎网络中的所有设备都能提供日志数据。因此, 基于日志数据的分析的网络安全可视化系统十分常见。

4) **网络中间设备的输出数据**。网络中间设备在网络中广泛部署, 其输出数据也是网络安全可视化系统的重要的数据来源之一, 如入侵检测系统的警报信息等。

5) **其他数据**。除了上述数据源外, 还有如网络拓扑信息, AS 属性与关系信息, BGP/IGP 信息等数据源。这些数据也常被网络安全可视化系统使用来协助网络管理员分析网络。

3 网络安全可视化工作分类

网络安全可视化离不开网络数据, 没有网络数据, 网络安全的可视化就无法进行。因此, 网络数据源在网络安全可视化的流程中, 起着基石的作用。一方面, 如第 2 章所述, 不同类型的网络数据包含了不同的网络信息, 为网络安全可视化在不同方面的应用提供了基础。另一方面, 随着大数据时代的到来, 数据在信息行业显得越来越重要。必然, 网络数据在网络安全可视化中也会愈发显得重要。因此, 下文将从数据角度出发, 以所使用的网络数据源的类型为分类依据, 来回顾现有网络安全可视化工作, 阐述网络安全可视化的研究现状。

3.1 网络流量数据

Keim 等人[5]提出 Radial Traffic Analyzer 系统来对网络流量进行可视化分析。如图 1 所示, 该系统通

过同心圆的方式对网络流量的源/目的 IP 地址和源/目的端口进行可视化, 从而协助分析人员监控网络流量, 捕捉网络通信模式并识别流量类型。此外, 通过使用时间轴, 该系统还能展示网络流量随时间变化的趋势。

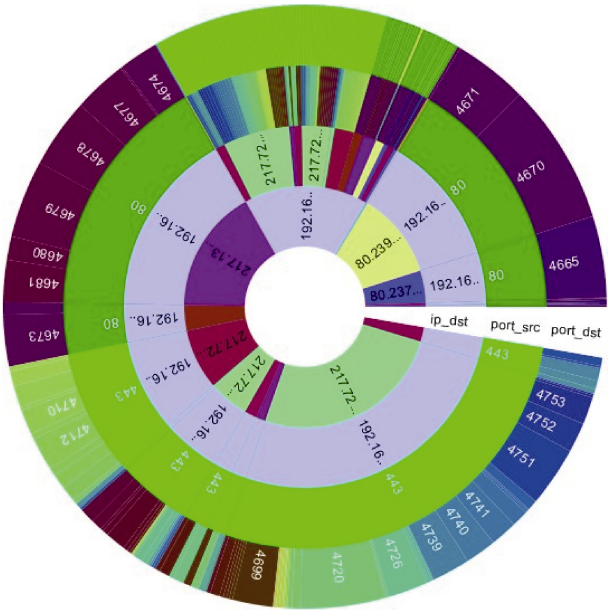


图 1 Radial Traffic Analyzer[5], 用 4 层同心圆对源 IP 地址, 目的 IP 地址, 源端口, 目的端口进行可视化

VISUAL[6]系统被设计用来监控内部网络。在该系统中, 内部节点用网格的方式来表示, 网格中的每一个方格表示一个内部主机; 外部资源则在网格外部用方块表示; 用连接内部方格和外部方块的直线表示访问行为; 外部方块的大小指示访问行为的强度。通过这种可视化, VISUAL 系统可以非常有效地展示当前内部监控网络和外部资源之间的访问模式, 帮助分析人员快速直观地理解所监控网络内发生的网络事件。

Xiao[7]等人把网络流量可视化与陈述式知识表达法相结合, 通过迭代的方式, 来发现网络攻击模式。如图 2 所示, 系统分析分为 3 步。首先, 用基于可视化的已知知识来发现网络数据中的模式; 一旦发现了某种模式, 分析人员为该模式建立一个模型; 然后把该模型添加到知识库完成知识库的更新以便在以后的分析中利用该新模型。

Mansmann[8]等人提出一个可交互的具有 TreeMap 布局的网络地图可视化系统。在实际中, 往往在单个任务中无法一次查看整个 IP 地址空间。因此, 该系统对 IP 地址空间进行分层处理。这种对 IP 地址的前缀(如 AS 域, 国家, 大陆等)进行分层的处理使得大规模网络的可视化成为可能, 从而可以很直观方便地对感兴趣的流量数据进行分析。

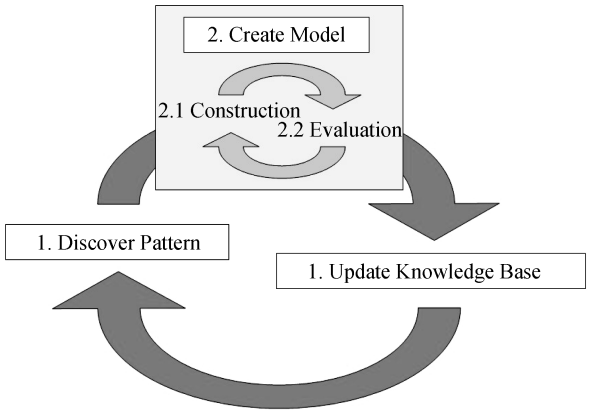


图 2 系统[7]的迭代式分析步骤。

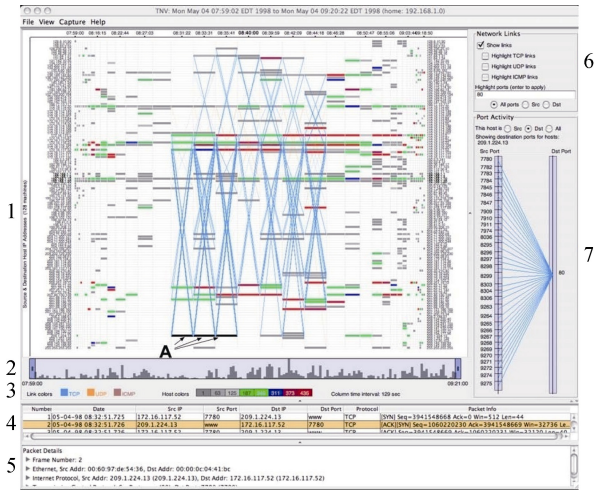


图 3 TNV[9]系统用 7 个显示区域对约 90 分钟内的 50000 个数据包进行可视化

Goodall 等人[9]认为在网络数据包级别进行入侵检测时, 分析人员往往因为过分关注底层细节而缺少全局考虑。为了避免这种上下文信息的缺失, 系统 TNV[9]被设计用来进行基于时序的网络流量分析。如图 3 所示, TNV 系统主要包含 7 个显示区域: 1)矩形主窗口; 2)基于数据统计的导航; 3)图中各图标的意义; 4)选定主机(图中主机 A)的所有数据包的列表; 5)从区域 4)中选定行的数据包的细节描述; 6)过滤面板; 7)端口活动统计。

Cappers 等人[10]指出仅仅基于对上层网络流相关属性分析的网络流量分析系统不足以应付针对目标网络进行过专门设计的攻击, 如 APT 攻击。要检测这类攻击, 深度数据包检查和异常检测必不可少。为了协助安全分析人员判断消息层的异常是否会威胁到网络层的安全, Cappers 等人提出 SNAPS 系统。如图 4 所示, 在该系统中, 安全分析人员使用总况信息图表来对其感兴趣部分进行检测警报。检测到警

报后，分析人员可以根据其位置和取值来获取更多信息。基于警报的取值和属性的情况，分析人员评估该警报的严重程度，然后做出决定，如忽略该警报，重新修改分类器以不再显示该警报等。

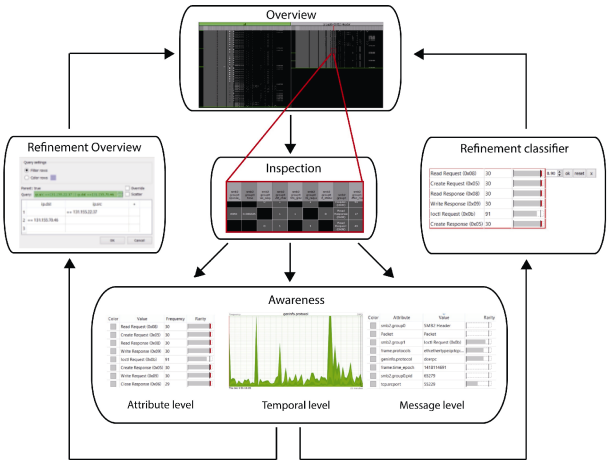


图 4　SNAPS[10]工作流程。

3.2　NetFlow

NVisionIP[11]系统使用 NetFLow 数据在单一屏幕上对 B 类网络的流量进行可视化来增强分析人员对网络的态势感知。该系统用一个 256x256 的矩阵来表示整个 B 类网络，矩阵的每个单元表示相关网络主机的交互。如图 5 所示，系统还提供放大功能，让用户对感兴趣的部分进行放大，通过柱状图等来进一步提供相关信息，如端口活动状态等。

NetBytes Viewer[12]系统利用 NetFLow 数据来帮助分析人员对单个主机行为进行详细的检查。NetBytes Viewer 系统通过对每个端口的流量随时间变化情况的展示，使得分析人员能基于非正常的端口使用或流量大小的变化等信息来判断主机行为的变化，进而识别入侵行为。

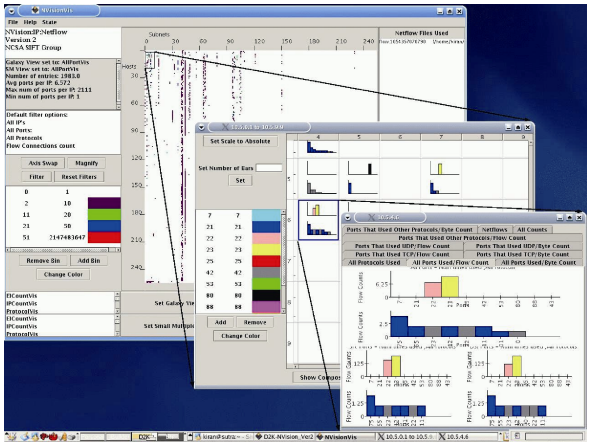


图 5　NVisionIP[11]的放大功能。

VizFlowConnect[13]系统借助平行轴来对内部主机和外部主机之间的流量进行可视化。如图 6 所示，系统中主窗口中包含 3 条平行轴：中间的轴线表示内部主机；左边轴线表示向内部主机发送数据的机器；右边轴线表示内部主机发送数据的目的机器。轴线上的点表示一个主机，而点之间的连线表示主机之间的通讯连接。VizFlowConnect 系统能有效地协助网络管理人员发现内部机器与外部机器之间的异常流量。

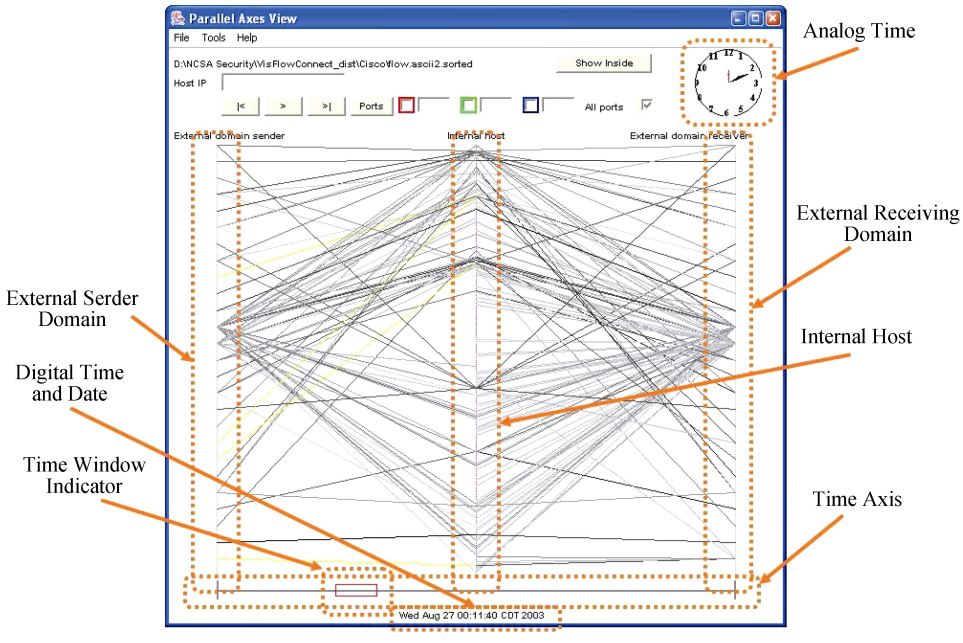


图 6　VizFloeConnect[13]的放大功能。

NFLowVis[14]系统使用一个关系数据库系统来分析 NetFlow 数据, 其设计目标是快速对通信模式进行可视化。NFLowVis 采用 TreeMap 来对所监控的网络进行映射。该系统能帮助安全分析人员评估警报信息之间的相关性、发现大规模分布式攻击以及分析网络内部相关服务的使用情况。

PortVis[15]系统利用不同颜色的网格来把网络活动映射到对应的方格。该系统用一个 256x256 的网格来表示 65536 个可能的端口。每个方格的颜色变化表示对应的端口活动的变化情况。黑色表示没有变化, 蓝色表示较小的变化, 红色表示较大的变化而白色表示极大的变化。此外, 每个网格还能被放大来显示更多的相关信息。该系统能很直观地显示端口的活动变化情况, 然而其不足之处在于, 当异常的端口周围都是正常且变化较大的端口时, 该异常端口将很难被发现。

3.3 日志

Tudumi[16]是较早的利用日志数据对网络安全进行可视化的系统之一。如图 7 所示, Tudumi 系统采用 3D 可视化技术, 用 3D 图符表示系统节点, 用线条表示连接, 不同的线形表示不同的连接模式, 如粗虚线表示终端服务而细虚线表示文件传输等。

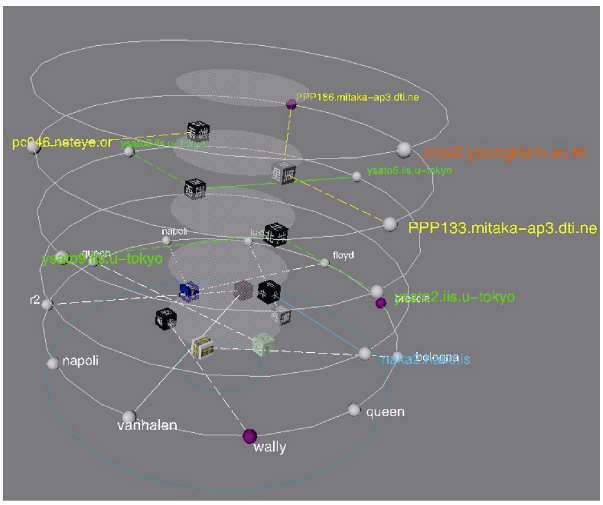


图 7 Tudumi[16]系统的 3D 可视化。

Erbacher 等人[17]也设计了基于日志数据的网络安全可视化系统。在其系统中, 主机被 5 个同心圆包围(所监控的服务在最中间)。由不同节点构成的圆环表示其与所监控系统的 IP 地址的差异。此外, 系统还附加了许多其他可视化属性来表征网络信息, 如不同的线形表示不同类型的连接, 连接线的数目表示所连接的用户数目等。

ELVIS 系统[18]是一个能支持多种日志类型的网络安全可视化系统。如图 8 所示, ELVIS 系统能导入多个不同类型的日志数据文件, 为安全分析人员提供充分的信息展示。即使是没有任何可视化技术背景的分析人员, 也能很好地利用该系统进行安全性分析。

图 8 基于所选字段, ELVIS [18]自动选取多种表征。

为了更好的了解针对 Web 服务器的攻击, Alsaleh 等人[19]设计了一个开源的对基于 PHP 的 Web 应用进行入侵检测和保护的系统。该系统把 PHPIDS 日志与相应的 Web 服务器的日志联合起来, 对网络安全事件进行可视化。系统利用多种视图, 如树形视图, 环状视图以及条形视图等, 从不同角度对安全事件进行可视化展示, 向网络管理人员提供细粒度的可视化查询功能, 以协助其发现网络攻击。

CORGI[20]是一个面向安全的日志可视化工具。使用该工具, 安全分析人员可以通过相关性表述和全局过滤来把多个或多种日志数据连接在一起进而发现安全事件。通过在一个日志文件中指定感兴趣的内容, 该工具能协助分析人员在其他日志文件中检查相关内容, 使得分析人员能更好的了解攻击事件的相关性甚至是重构攻击场景。

CORGI 系统[21]通过处理多种网络日志文件(如 IPS 日志, 主机状态日志等)来帮助网络安全分析人员快速获取网络状态信息。导入数据后, CORGI 系统能在多维度上进行网络状态的可视化展示, 如瞬时网络状态, IP 连接状态等。此外, 如图 9 所示, 分析人员能利用该系统获取其他分析人员发现的结论或上传自己发现的结论。系统所提供的相互协作的功

能可以帮助安全分析人员有效的发现微小的网络安全事件以及多步骤的网络安全攻击。

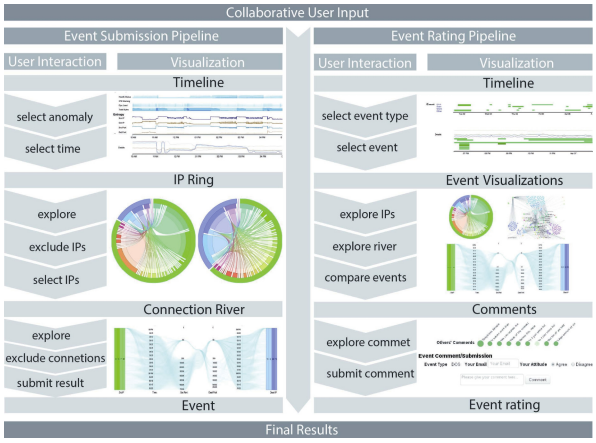


图 9　CORGI [21]系统工作流程。

网络日志文件往往包含很多行数，这使得查看网络日志时候的导航、概况描述以及快速进行模式识别变得十分复杂，尤其是人工处理时。因此，Stange 等人提出 Visual Filter 系统。如图 10 所示，该系统能对整个网络日志文件进行总况展示，同时提供可视化过滤接口和导航，从而帮助安全分析人员快速过滤和定位感兴趣的网络事件，进而快速识别网络模式和网络异常事件。

3.4　网络中间设备的输出数据

网络入侵检测设备被广泛应用在网络中，其检测结果能被用来分析网络安全状态。NIVA[23]系统就通过对多个入侵检测设备的检测结果数据进行分析，利用不同颜色和连接线来对网络攻击进行可视化。如图 11 所示, NIVA 系统由一个 3D 渲染窗口和图形交互界面组成。3D 渲染窗口中，根据 IP 地址决定图元的位置，而其连线的不同颜色表示不同的强度的攻击。

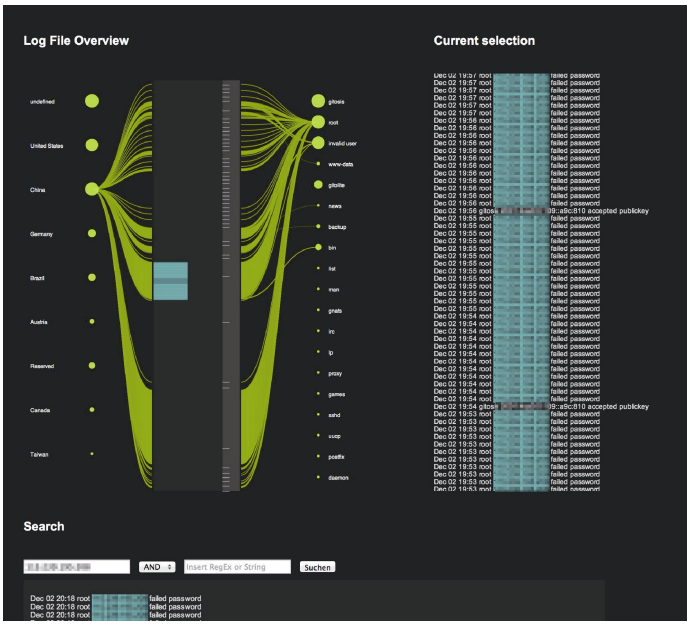


图 10　Visual Filter[22]：选定 IP 的所有出现情况。

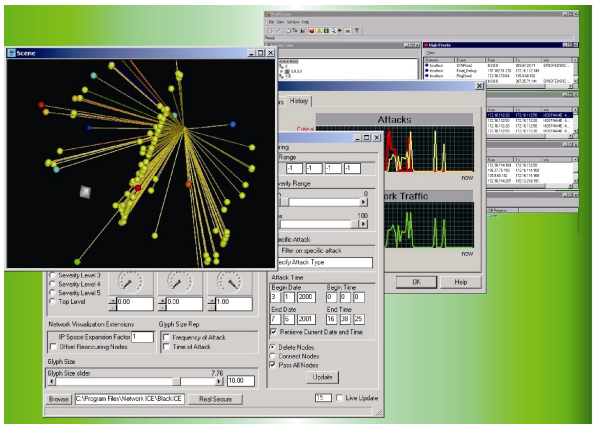


图 11　NIVA[23]: 3D 渲染窗口与交互界面。

为了展示网络攻击中攻击者的 IP 地址, Koike 等人设计了 IP Matrix[24]系统。在该系统中，作者使用两个 256x256 的矩阵来(分别在 Internet 级和本地级)表示攻击者的 IP 地址。通过读取入侵检测器的检测结果，把每一个警报信息都映射到矩阵中对应方格的像素，再对像素进行颜色编码来表示攻击的不同属性。

在大型网络中，入侵检测系统往往会产生超大量的警报信息。网络管理员在人工分析这些信息时往往会漏掉某些重要的细节或是难以从全局角度获取网络的状态信息。为了解决该问题, Abdullah 等人

设计了 IDS RainStorm[25]系统。该系统把警报信息以总况表的方式进行可视化展示，使得网络管理员能很好地掌握网络的全局状态并发现攻击。此外，系统提供的缩放功能，可以让网络管理人员进一步获取相关网络事件的详尽信息。

Livnat[26]等人认为网络警报信息包含 3 个方面的属性：何种，何时，何地。作者从这 3 个属性出发，对网络警报进行可视化展示和对比。在该可视化系统中，本地网络拓扑可视化区域的中间进行展示，外围的同心圆表示各种不同的警报。同心圆的深度表示不同的时间，不同的类型的警报用不同的颜色标记，警报与本地主机之间的连线表示该主机上触发了该警报，较细的线表示较多数量的同类型的警报，而内部节点越大则表示该节点上触发了与其他节点不同的类型的警报。图 12 是用该系统对多个主机遭受多种攻击的情况的可视化结果。

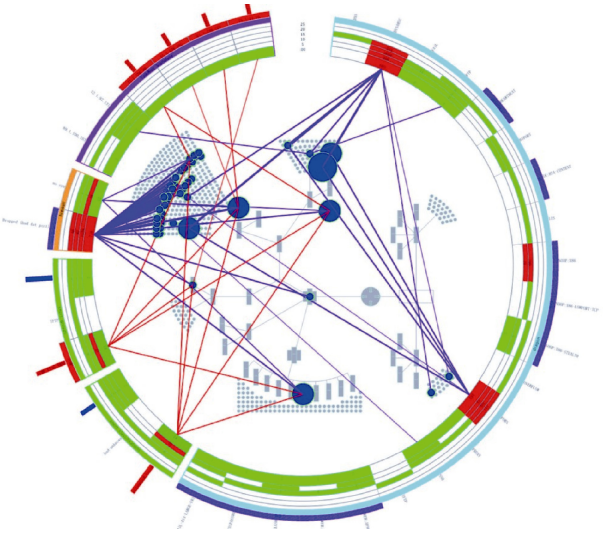


图 12　对警报信息的可视化[26]

网络中间设备被广泛部署在网络中，完成网络监控、状态管理、功能实现等不同功能。因此，其输出数据包含了网络的很多方面的信息。故其在网络安全分析中起着非常重要的作用。正因如此，网络中间设备数据被广泛应用在网络安全可视化系统中，如 Avisa[27], SnortView[28], Spiralview[29]等。网络管理员利用这些系统能更方便快速得完成获取网络状态，分析网络安全威胁，识别网络异常等任务。

3.5　其他数据源

除了上述 4 种典型网络数据源之外，许多其他网络数据也被网络安全可视化系统使用，来从不同角度对网络安全进行可视化分析。

Ren[30]等人主要关注 DNS 协议相关的网络攻击，因此在其设计的系统中，DNS 流量数据被用来进行可视化和网络安全分析。

网络的路由行为是网络事件分析的重点之一。在路由行为的可视化分析中，BGP 相关的数据被广泛采用，如 BGPlay[31], BGP Eye[32], LinkRank[33], BGPfuse[36]等。

此外, AS 属性与关系信息数据、网络拓扑信息数据、电子商务数据以及互联网路由注册信息数据等也在诸多网络安全可视化系统[34], [35], [37]中被应用。

3.6　多数据源

网络是一个包含各种各样不同设备的复杂系统，不同的设备能提供不同的网络数据。因此，越来越多的网络安全可视化系统不再仅仅使用单一的数据源来进行分析，使用多数据源的系统越来越多。利用多数据源，能有效发现不同设备之间行为的相关性，这对发现复杂的，多步骤的，长潜伏期的网络攻击，如 APT 攻击，十分有用。

Ocelot[38]系统使用 NetFlow、警报数据以及健康状态数据来帮助安全分析人员进行快速有效的决策制定和评估网络威胁; PERCIVAL[39]系统综合利用系统事件记录数据、日志以及警报信息数据等评估系统应对安全攻击的能力; Legg[40]则利用用户行为记录数据、检测结果等来进行内部威胁的检测; NStreamAware[41]通过对 NetFlow、数据流、系统日志消息等分析来协助网络管理员进行网络态势感知; Hao[42]也通过对 NetFlow、Snort 警报数据等的分析来帮助网络管理员进行安全事件的调查。

4　网络安全可视化面临的挑战与未来研究方向

网络安全可视化将网络安全分析与可视化技术结合起来，将不可见的抽象的网络数据以图形图像的方式展现出来，并提供交互操作接口，从而协助网络安全分析员更直观快速且准确地获取网络状态信息并识别网络异常事件。网络安全可视化是一个新型的尚处在发展阶段的研究方向，虽然目前已经取得了不错的研究成果，但是面对越来越复杂的网络环境，越来越庞大的网络数据和越来越高明的攻击手段，其在关键技术和基础理论的研究上还有很多问题亟待解决。下文将从理论基础、数据处理、应用多样性、概念延伸等四个方面分析网络安全可视化研究面临的挑战并探讨未来研究方向。

4.1　设计规范与理论基础

目前，网络安全可视化系统缺乏统一的设计指

导规范和理论基础。不同系统的设计者仅仅是根据自己对网络安全可视化需求的理解进行系统的设计, 这就导致了五花八门的网络安全可视化系统。对网络安全可视化系统的整体设计而言, 这种系统的杂乱性会带来诸多问题:

1) **易用性**。网络安全可视化系统需要在网络数据的各种属性与图形元素之间建立映射关系, 且图形元素的不同属性, 如颜色、大小、位置等, 还需要表达对应网络数据属性的不同特征。由于缺乏设计规范, 不同系统采用了不同映射关系以及属性表达方式, 这就使得用户在不同系统之间的切换变得十分困难。用户往往需要很长时间才能熟悉和掌握一个新系统的使用。亦即, 目前网络安全可视化系统的易用性不佳, 需要提高。

2) **扩展性**。网络安全可视化系统需要在有限的区域内(如显示屏范围内)进行图形图像的展示。通常而言, 显示范围是有限且相对固定的, 而网络规模以及要展示的网络数据属性的数量则是动态变化的。目前的网络安全可视化系统的可扩展性较差: 当需要展示的图形元素增多时, 往往会造成图像拥挤, 层叠甚至是无法完全显示的后果。这不仅会严重影响用户体验, 而且会增加分析人员获取相关网络信息的耗时, 不便于网络状态的即时获取。因此, 建立设计规范和理论来指导网络安全可视化系统的设计来解决可扩展性问题也十分重要。

3) **交互性**。设计规范的缺失使得不同网络安全可视化系统的交互设计也不尽相同。不同的交互设计同样会带来易用性不佳的问题, 更重要的是, 网络安全分析员通过与系统的交互来完成对网络数据的理解和分析, 交互性差的系统将严重影响安全分析员的工作效率。而现阶段的网络安全可视化系统往往是根据系统设计者的理解进行交互操作设计, 缺乏对用户需求的全面了解。不同的用户对网络安全有不同的侧重点, 这就意味着需要不同的交互操作来调取不同的网络数据进行分析。因此, 规范化且全面的交互设计在网络安全可视化系统的设计中也是必不可少的。

4) **评估方法**。目前为止, 网络安全可视化系统的评估方法仅仅靠少量用户的使用反馈来进行。这样的评估方法具有极强的主观性, 其可信度和可靠性都不高。网络安全可视化要继续发展, 就必须要有系统的统一的评估方法和衡量指标。只有这样, 才能对网络安全可视化系统进行客观的评价, 有了客观的评估结果, 才能推动系统设计朝着更好的方向发展。

设计规范和理论基础的缺失导致了网络安全可视化系统在易用性、扩展性、交互设计和评估方法等方面的诸多不足。这些不足使得网络安全可视化系统还不足以在真实环境中广泛部署和使用。因此, 网络安全可视化要继续发展, 在未来的研究工作中就必须要探讨如何建立设计规范和理论基础。

4.2 数据处理

网络安全可视化以分析网络数据为基础。因此, 数据的处理在网络安全可视化中显得至关重要。网络安全可视化系统的不同目标对数据的处理提出了不同的要求, 而大数据时代的到来又对数据的高效处理提出了新的挑战。因此, 在网络安全可视化系统中, 一个综合的数据处理平台(负责数据的采集、存储、传输以及分析等工作)十分必要。下文将从数据的预处理、数据的正确性、数据处理与可视化的耦合度等几方面进行讨论。

1) **数据预处理**。如前文所述(第 2 章), 网络安全可视化需要处理许多不同种类的网络数据。目前的系统通常只能处理某一个或某一类网络数据。然而, 网络安全可视化系统要想在实际生产环境中得到广泛部署和应用就必须能处理各种不同种类的网络数据。亦即需要对数据进行预处理, 实现对各种数据的格式转换、降低维度等处理, 以便于后续分析和可视化呈现。

2) **数据的正确性**。目前, 几乎所有的研究工作都没有考虑其所使用的网络数据源是否正确可靠的问题。一旦所使用的数据源是错误的, 那么之后的安全分析以及可视化结果都将是错误的。而攻击者完全有能力对网络数据源进行篡改, 如数据包截获与修改、回滚攻击、篡改审计日志等等[2]。因此, 在未来研究中, 必须对网络数据源的正确性进行验证和保护。

3) **数据处理与可视化的耦合度**。目前的网络安全可视化系统中, 数据处理和可视化过程没有明显的界限, 耦合度较高。为了提高数据处理效率, 便于系统更新, 一种更高效的处理方式是对数据处理和可视化进行解耦。由数据处理平台统一进行数据的处理, 再向可视化过程提供标准接口以完成图形显示和交互操作。这种解耦操作能带来高效处理的同时, 还可以让网络安全人员更关注安全数据处理而让可视化技术人员更关注可视化设计, 充分发挥各自的优势。

网络数据处理是网络安全可视化的第一步, 也是其基础。而不同的数据类型、不同的应用环境以及数据本身的高维度等特性对数据网络安全可视化

中的数据处理提出了很多挑战。尤其是在大数据时代到来后, 数据和数据的有效处理愈显重要。因此, 搭建统一高效的、可解耦的数据处理平台(如, 把大数据处理平台整合到网络安全可视化系统中)是提高网络安全可视化系统能力的有效手段之一。

4.3 应用多样性

网络的复杂性以及其在人们日常生活中的全面渗透使得网络安全可视化有着很多方面的应用。目前, 各个独立的系统往往有着明确的子应用。而不同应用对网络安全可视化系统提出了不同的要求。

具体而言, 以网络态势感知为目标的应用要求网络安全可视化系统具有极高的实时性; 当网络安全可视化被用于犯罪取证时, 分析结果的正确性取代了实时性成为最为重要的要求; 当在特定类型的网络(如智能电网, 无线传感网络等)里进行安全可视化时, 则必须要满足该特性类型的网络的要求, 如无线传感网络的各节点的处理能力有限等; 此外, 几乎目前所有的网络安全可视化系统都需要人工介入, 这与信息产业的自动化趋势相违背。因此, 如何解决该矛盾也对网络安全可视化提出了新要求。

应用的多样性必然导致对网络安全可视化系统的要求多样性和复杂性。如何满足各种不同要求, 整合多种应用, 是网络安全可视化研究的必不可少的环节。

4.4 网络安全可视化的概念延伸

目前的网络安全可视化研究工作大都关注如何协助网络安全分析人员更快速地识别网络攻击。因此, 系统往往是对与安全相关的事件的属性, 如端口访问记录、IP 地址、警告类型等, 进行可视化展示。然后, 对于没有专业背景知识的普通用户而言, 这样的可视化程度还不够, 他们不足以从中感知到当前自己所处网络的安全态势。

因此, 网络安全可视化的概念可以延伸到**可感知的网络安全**。即, 既为网络安全分析人员进行相关数据的图形展示, 协助其分析网络, 又能使普通用户感知到自己所处的网络面临什么样的网络威胁和受到了哪些安全保障服务。

可感知的网络安全是对网络安全可视化概念的进一步延伸, 除了应该涵盖现有网络安全可视化系统的功能外, 还包括网络脆弱性评估、网络整体安全保障服务展示、网络中软件的安全性评估等功能。可感知的网络安全将进一步提升用户(包括网络安全分析人员和普通用户)对网络安全状态的认知, 是对目前网络安全可视化工作的一个很好的扩展和补充。

5 结语

网络安全可视化将可视化技术整合到网络安全研究中来, 把高维度的不可见的抽象的网络数据以图形图像的方式展示出来, 协助网络安全分析人员感知网络状态, 发现网络异常。本文从数据角度出发, 以所使用的网络数据源的类型为分类依据, 回顾现有网络安全可视化工作。在此基础上, 对网络安全可视化研究的挑战进行分析, 并展望未来研究方向。

参考文献

[1] 吕良福. DDoS 攻击的检测及网络安全可视化研究.[博士学位论文]. 天津大学, 2008.

[2] B.R. Waters, D. Balfanz, G. Durfee and D.K. Smetters, “Building an Encrypted and Searchable Audit Log,” in Proc. ISOC Network and Distributed System Security Symposium (NDSS’04), pp. 5-6, 2004.

[3] “TCPDUMP”, http://www.tcpdump.org

[4] “WIRESHARK”, https://www.wireshark.org

[5] D. A. Keim, F. Mansmann, J. Schneidewind and T. Schreck, “Monitoring Network Traffic with Radial Traffic Analyzer,” in Proc. IEEE Symposium. Visual Analytics Science and Technology, pp. 123-128, 2006.

[6] R. Ball, G.A. Fink, and C. North, “Home-Centric Visualization of Network Traffic for Security Administration,” in Proc. ACM Workshop Visualization and Data Mining for Computer Security, pp. 55-64, 2004.

[7] L. Xiao, J. Gerth, and P. Hanrahan, “Enhancing Visual Analysis of Network Traffic Using a Knowledge Representation,” in Proc. IEEE Symp. Visual Analytics Science and Technology, pp. 107-114, 2006.

[8] F. Mansmann, D. Keim, S. North, B. Rexroad, and D. Sheleheda, “Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats,” IEEE Trans. Visualization and Computer Graphics, vol. 13, no. 6, pp. 1105-1112, Nov./Dec. 2007.

[9] K. Lakkaraju, W. Yurcik, and A. Lee, “NVisionIP: Netflow Visualizations of System State for Security Situational Awareness,” in Proc. ACM Workshop Visualization and Data Mining for Computer Security, vol. 29, pp. 65-72, 2004.

[10] B. C. M. Cappers and J.J. van Wijk, “SNAPS: Semantic Network traffic Analysis through Projection and Selection,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’15), pp. 1-8, 2015.

[11] K. Lakkaraju, W. Yurcik, and A. Lee, “NVisionIP: Netflow Visualizations of System State for Security Situational Awareness,” in Proc. ACM Workshop Visualization and Data Mining for Com-

puter Security, vol. 29, pp. 65-72, 2004.

[12] T. Taylor, S. Brooks, and J. McHugh, “Netbytes Viewer: An Entitybased Netflow Visualization Utility for Identifying Intrusive Behavior,” in Proc. Workshop Visualization for Computer Security (VizSEC ’07), pp. 101-114, 2008.

[13] X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju, “Visflowconnect: Netflow Visualizations of Link Relationships for Security Situational Awareness,” in Proc. ACM Workshop Visualization and Data Mining for Computer Security, pp. 26-34, 2004.

[14] F. Fischer, F. Mansmann, D.A. Keim, S. Pietzko, and M. Waldvogel, “Large-Scale Network Monitoring for Visual Analysis of Attacks,” in Proc. Workshop Visualization for Computer Security (VizSEC ’08), pp. 111-118, 2008.

[15] J. McPherson, K. Ma, P. Krystosk, T. Bartoletti, and M. Christensen, “PortVis: A Tool for Port-Based Detection of Security Events,” in Proc. the ACM Workshop Visualization and Data Mining for Computer Security, pp. 73-81, 2004.

[16] T. Takada and H. Koike, “Tudumi: Information Visualization System for Monitoring and Auditing Computer Logs,” in Proc. Int’l Conf. Information Visualization, pp. 570-576, 2002.

[17] R. Erbacher, “Intrusion Behavior Detection through Visualization,” in Proc. IEEE Int’l Conf. Systems, Man and Cybernetics, pp. 2507-2513, 2003.

[18] C. Humphries, N. Prigent, C. Bidan and F. Majorczyk, “ELVIS: Extensible Log VISualization,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’13), pp. 9-16, 2013.

[19] M. Alsaleh, A. Alqahtani, A. Alarifi and A. Al-Salman, “Visualizing PHPIDS Log Files for Better Understanding of Web Server Attacks,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’13), pp. 1-8, 2013.

[20] C. Humphries, N. Prigent, C. Bidan and F. Majorczyk, “CORGI: combination, organization and reconstruction through graphical interactions,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’14), pp. 57-64, 2014.

[21] S. Chen, C. Guo, X. Yuan, F. Merkle, H. Schaefer and T. Ertl, “OCEANS: online collaborative explorative analysis on network security,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’14), pp. 1-8, 2014.

[22] J. Stange, M. Dörk, J. Landstorfer and R. Wettach, “Visual filter: graphical exploration of network security log files,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’14), pp. 41-48, 2014.

[23] K. Nyarko, T. Capers, C. Scott, and K. Ladeji-Osias, “Network Intrusion Visualization with niva, an Intrusion Detection Visual Analyzer with Haptic Integration,” in Proc. Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems (HAPTICS’02), pp. 277 -284, 2002.

[24] H. Koike, K. Ohno, and K. Koizumi, “Visualizing Cyber Attacks Using ip Matrix,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’05), pp. 91-98, 2005.

[25] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko, “Ids Rainstorm: Visualizing ids Alarms,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’05), pp. 1-10, 2005.

[26] S. Foresti, J. Agutter, Y. Livnat, S. Moon, and R. Erbacher, “Visual Correlation of Network Alerts,” IEEE Computer Graphics and Applications, vol. 26, no. 2, pp. 48-59, Mar./Apr. 2006.

[27] H. Shiravi, A. Shiravi, and A. Ghorbani, “IDS Alert Visualization and Monitoring through Heuristic Host Selection,” in Proc. Int’l Conf. Information and Comm. Security(ICICS’10), pp. 445-458, 2010.

[28] H. Koike and K. Ohno, “SnortView: Visualization System of Snort Logs,” in Proc. ACM Workshop Visualization and Data Mining for Computer Security, vol. 29, pp. 143-147, 2004.

[29] E. Bertini, P. Hertzog, and D. Lalanne, “Spiralview: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms,” in Proc. IEEE Symp. Visual Analytics Science and Technology, pp. 139-146, 2007.

[30] P. Ren, J. Kristoff, and B. Gooch, “Visualizing DNS Traffic,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’06), pp. 23-30, 2006.

[31] L. Colitti, G. Di Battista, F. Mariani, M. Patrignani, and M. Pizzonia, “Visualizing Interdomain Routing with BGPlay,” Journal of Graph Algorithms and Applications, vol. 9, pp. 117-148, 2005.

[32] S.T. Teoh, S. Ranjan, A. Nucci, and C.-N. Chuah, “BGP Eye: A New Visualization Tool for Real-Time Detection and Analysis of bgp Anomalies,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’06), pp. 81-90, 2006.

[33] M. Lad, D. Massey, and L. Zhang, “Visualizing Internet Routing Changes,” IEEE Trans. Visualization and Computer Graphics, vol. 12, no. 6, pp. 1450-1460, Nov./Dec. 2006.

[34] J. J. Fowler, T. Johnson and P. Simonetto, “IMap: Visualizing Network Activity over Internet Maps,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’14), pp. 80-87 , 2014.

[35] C. C. Gray, P. D. Ritsos and J. C. Roberts, “Contextual network navigation to provide situational awareness for network administrators,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’15), pp. 1-8, 2015.

[36] S. Papadopoulos, G. Theodoridis and D. Tzovaras, “CBGPfuse: Using visual feature fusion for the detection and attribution of BGP anomalies,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’13), pp. 57-64, 2013.

[37] K. Webga and A. Lu, “Discovery of rating fraud with real-time streaming visual analytics,” in Proc. IEEE Workshop Visualization

for Computer Security (VizSEC'15), pp. 1-8, 2015.

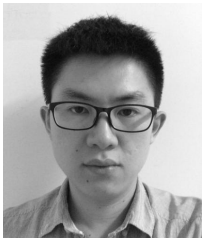
[38] D. L. Arendt, R. Burtner, D. M. Best and M. D. Bos, "Ocelot: User-Centered Design of a Decision Support Visualization for Network Quarantine," in Proc. IEEE Workshop Visualization for Computer Security (VizSEC'15), pp. 1-8, 2015.

[39] M. Angelini, N. Prigent and G. Santucci, "PERCIVAL: Proactive and rEactive attack and Response assessment for Cyber Incidents using Visual AnaLytics," in Proc. IEEE Workshop Visualization for Computer Security (VizSEC'15), pp. 1-8, 2015.

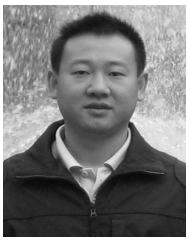
[40] P. A. Legg, "Visualizing the Insider Threat: Challenges and tools for identifying malicious user activity," in Proc. IEEE Workshop Visualization for Computer Security (VizSEC'15), pp. 1-8, 2015.

[41] F. Fischer and D. A. Keim, "NStreamAware: real-time visual analytics for data streams to enhance situational awareness," in Proc. IEEE Workshop Visualization for Computer Security (VizSEC'14), pp. 65-72, 2014.

[42] L. Hao, C. G. Healey and S. E. Hutchinson, "Flexible web visualization for alert-based network security analytics," in Proc. IEEE Workshop Visualization for Computer Security (VizSEC'13), pp. , 2013.



袁斌 于 2013 年在华中科技大学获得计算机科学与技术专业学士学位。现在华中科技大学计算机科学与技术学院攻读博士学位。研究领域包括: 网络安全、软件定义网络、大数据隐私保护等。Email: yuanbin@hust.edu.cn



邹德清 于 2004 年在华中科技大学获得博士学位。现任华中科技大学计算机科学与技术学院教授。主要研究领域为虚拟化技术, 可信计算, 系统安全, 安全评估, 网格计算以及集群与高性能计算。Email: deqingzou@hust.edu.cn

金海 于 1994 年在华中科技大学获得博士学位。现任华中科技大学计算机科学与技术学院教授。主要研究领域为计算机系统结构, 虚拟化技术, 集群计算, 网格计算, 并行与分布式计算, 对等计算, 普适计算, 语义网, 存储与安全。Email: hjin@hust.edu.cn