VAST Challenge 2012: Visual Analytics for Big Data

Kristin Cook [1], Georges Grinstein [2], Mark Whiting [1], Michael Cooper [1], Paul Havig [3], Kristen Liggett [3], Bohdan Nebesh[4], Celeste Lyn Paul[4]

[1] Pacific Northwest National Laboratory
[2] University of Massachusetts Lowell
[3] Air Force Research Laboratory
[4] National Security Agency

ABSTRACT

The 2012 Visual Analytics Science and Technology (VAST) Challenge posed two challenge problems for participants to solve using a combination of visual analytics software and their own analytic reasoning abilities. Challenge 1 (C1) involved visualizing the network health of the fictitious Bank of Money to provide situation awareness and identify emerging trends that could signify network issues. Challenge 2 (C2) involved identifying the issues of concern within a region of the Bank of Money network experiencing operational difficulties utilizing the provided network logs. Participants were asked to analyze the data and provide solutions and explanations for both challenges. The data sets were downloaded by nearly 1100 people by the close of submissions. The VAST Challenge received 40 submissions with participants from 12 different countries, and 14 awards were given.

Keywords: Visual analytics, human information interaction, sense making, evaluation, metrics, contest.

Index Terms: H.5.2 [Information Interfaces & Presentations]: User Interfaces – Evaluation/methodology.

1 INTRODUCTION

The Visual Analytics Science and Technology (VAST) Challenge [1] is a series of contests that aim to advance visual analytics through competition. Started in 2006 and now in its seventh year, the VAST Challenge is designed to help researchers understand how their software would be used in a novel analytic task and determine if their data transformations, visualizations, and interactions would be beneficial for particular analytic tasks. VAST Challenge problems provide researchers with realistic tasks and data sets for evaluating their software, as well as to advance the field in solving more complex problems.

Researchers and software providers have repeatedly used the data sets from throughout the life of the VAST Challenge as benchmarks to demonstrate and test the capabilities of their systems. The ground truth embedded in the data sets has helped researchers evaluate and strengthen the utility of their visualizations.

email: {kris.cook,mark.whiting,michael.cooper}@pnnl.gov, grinstein@cs.uml.edu,{paul.havig,kristen.liggett}@wpafb.af.mil, {banebes,clpaul}@nsa.gov

2 SCOPE OF VAST CHALLENGE 2012

The goal of VAST Challenge 2012 was to provide a set of realistic computer network scenarios while pushing the boundaries of big data. The setting of the Challenge is BankWorld, a planet much like Earth, but with a very different geography. For this Challenge, the geography is one large land mass containing several different nation-states. The most important organization on BankWorld is the Bank of Money (BOM). BOM has many offices of various sizes across BankWorld. Each of these offices has many computers active throughout the day. In total, the organization operates about 895,000 machines.

Contestants were asked to focus on two general problems using a visual analytics approach. First, how do you achieve cyber situation awareness across the entire enterprise with such a large number of systems? Second, when something does go awry, can you identify it and the steps needed to resolve the problem?

2.1 Contest Problem

VAST Challenge 2012 consisted of two independent but related challenge tasks set in the fictitious BankWorld. Each challenge consisted of a data set, instructions, and questions to be answered. Unlike previous years, this year's VAST Challenge did not include an overarching Grand Challenge that tied the clues from the individual challenges together.

In previous years, the individual challenge tasks have also been referred to as mini-challenges, and they were originally posed to the participants as mini-challenges. However, given the scope and complexity of handling such gigabytes of data, it seems more appropriate to describe the individual tasks as challenges rather than mini-challenges.

Each challenge had certain constraints and business rules that contestants needed to consider for their analysis. For example, in Challenge 1, BOM offices operate during business hours 7am-6pm in their local time zone. However, the BOM enterprise spans ten time zones. Failure to properly handle the geo-temporal issues prevented proper understanding of the evolving problems across BOM.

2.1.1 Challenge 1: Situation Awareness

Challenge 1 focused directly on cyber situation awareness across BOM. Its overview and task questions read:

> The Bank of Money (BOM) Corporate Information Officer (CIO) has assigned you to create a situation awareness visualization of the entire enterprise. This is a considerable challenge, considering that BOM operates from BankWorld's coast to coast. In addition to observing the global situation, he would also would like to be able to detect operational changes outside of the norm. You are provided with two data sets that

IEEE Conference on Visual Analytics Science and Technology 2012
October 14 - 19, Seattle, WA, USA
978-1-4673-4753-2/12/$31.00 ©2012 IEEE

span two days of data for BOM. One dataset contains metadata about the bank's network. The second dataset contains periodic status reports from all computing equipment in the BOM enterprise.

MC 1.1 Create a visualization of the health and policy status of the entire Bank of Money enterprise as of 2 pm BMT (BankWorld Mean Time) on February 2. What areas of concern do you observe?

MC 1.2 Use your visualization tools to look at how the network's status changes over time. Highlight up to five potential anomalies in the network and provide a visualization of each. When did each anomaly begin and end? What might be an explanation of each anomaly?

2.1.2 Challenge 2: Operational Forensics

Challenge 2 focused on operational forensics. Its background and task questions were:

During a time period that is NOT overlapping with MC 1, a Region within the Bank of Money is experiencing operational difficulties. This becomes a challenge for the operations staff, particularly as they attempt to deploy their limited number of skilled administrators to address issues occurring in the enterprise. You will be provided with Firewall and IDS logs from one of the BOM networks of approximately 5000 machines. These are very similar to the Firewall and IDS logs you worked on during the VAST 2011 MC 2, and so the tools you used there will come in handy for this mini-challenge (and reuse is encouraged). You will also be provided with a description of the network to guide your investigation.

MC 2.1 Using your visual analytics tools, can you identify what noteworthy events took place for the time period covered in the firewall and IDS logs? Provide screen shots of your visual analytics tools that highlight the five most noteworthy events of security concern, along with explanations of each event.

MC 2.2 What security trend is apparent in the firewall and IDS logs over the course of the two days included here? Illustrate the identified trend with an informative and innovative visualization.

MC 2.3 What do you suspect is (are) the root cause(s) of the events identified in MC 2.1? Understanding that you cannot shut down the corporate network or disconnect it from the internet, what actions should the network administrators take to mitigate the root cause problem(s)?

2.2 Submission Format

Teams were asked to provide a video and a concise process description as to how they arrived at their conclusions and how the various visualizations and tools helped in the analysis.

2.3 Review Process

As in years past, the VAST Challenge Review Committee recruited reviewers from throughout the visualization and analysis communities. Subject matter experts were recruited from the pool of previous reviewers and their social networks.

Including both the visualization community reviewers and the subject matter expert reviewers, a total of 102 reviewers participated, each providing between one and five reviews. This represents a significant increase from the 56 reviewers who participated in 2011. Four to eight external reviewers, including at least one subject matter expert, reviewed each submission. Each reviewer was given the opportunity to recommend submissions for specific awards.

Reviewers were asked to rate the analytic process, the visualizations, the interactions, the clarity of explanation, and the relative novelty of the submission. In addition, reviewers rated the submission in terms of its support for dynamic situation awareness, as well as the identification of specific events of interest in the data. Reviewers provided both ratings and explanatory comments. These comments were as important as the scores in identifying award candidates.

Reviewers were also asked to evaluate the plausibility of the answers provided, rather than the accuracy of the solutions. The datasets used this year were realistically complex. Although there were certain known patterns embedded in the data, the committee recognizes the likelihood that additional patterns exist in the data that were not intended and that could reasonably be considered by the participants to be of significance. Consequently, reviewers were provided with a list of the expected patterns that were embedded in the dataset to support the scenario, but they were also instructed to accept other solutions for which the submission provided well-reasoned supporting evidence.

The VAST Challenge Review Committee held a one-day meeting to determine awards. Prior to the meeting, all of the committee members examined at least nine of the submissions in detail, with five committee members examining all 40 submissions. During the meeting, the committee reviewed and evaluated the award recommendations from the reviewers, taking the totality of the scores and reviewer comments into account. The committee also identified additional appropriate awards.

As in previous years, the awards were not pre-established. Instead, the committee identified awards recognizing the best qualities in the submissions. In addition, this year a few teams were selected to receive honorable mentions. This designation was chosen to recognize entries that demonstrated great promise but were not yet fully realized in their implementation.

3 VAST Challenge 2012 Awards

The visualizations required for the two challenges were of substantially different varieties. The geo-spatial and temporal aspects, combined with the enormous number of facilities and machines involved in C1, suggested a different approach than the increasingly odd communication patterns across approximately 5000 machines in C2.

Both C1 and C2 were significant challenges due to the data size and complexity and the difficulties of the tasks specified in each. In general, the challenge participants should be congratulated for their efforts, as reviewers found an abundance of compliments to include in their write-ups. The reviewers and the committee would have liked to have seen even more innovation in the visualizations that would work well for situation awareness. Traditional visualizations (line charts, bar charts, linear and radial graphs, colored geographic areas) were well applied, but future contestants should be encouraged to take more risks in developing new visualizations in support of cyber analytics.

Figure 1: The 2012 award winner for Outstanding Comprehensive Submission was BANKSAFE: A Visual Situation Awareness Tool for Large-Scale Computer Networks (University of Konstanz).

3.1 Comprehensive Award

One group (University of Konstanz) brought the two datasets together to enable situation awareness analytics across both challenges and was recognized for essentially tackling a Grand Challenge problem, even though there was not "official" Grand Challenge in 2012 (Figure 1).

3.2 Challenge 1 Awards

C1 asked for both a static situation awareness snapshot and a dynamic trend-oriented assessment. Two teams (Business Forensics and Charles River Associates) were recognized for visual designs that reviewers felt would work well in an operational setting. Another team (Purdue) submitted an entry that reviewers noted for its outstanding features for integrated analysis and visualization. One team caught the reviewers' attention by engaging subject matter experts in the design and testing of their toolkit (Middlesex University) and were complimented with a "Subject Matter Experts' Award." Other recognitions included Comprehensive Visualization (Stuttgart), Effective Video Presentation (Secure Decisions), Efficient Use of Visualization (City University London), Good Interaction Techniques (General Dynamics C4 Systems), and Good Support for Data Preparation, Analysis and Presentation (MTA Sztaki).

3.3 Challenge 2 Awards

In C2, participants were analyzing the effects of a growing botnet infection across a BOM region, with clues provided in the Firewall and the Intrusion Detection System logs. The geography to consider in this challenge now becomes one of a computer network that was provided in a network diagram with identification of critical systems and business rules of operation.

As for submissions, the committee appreciated that University of Buenos Aires submitted several entries to both Challenges this year. The UBA student team led by Marcos Wolff received an award for Effective Use of Commercial Software, providing a clear and effective identification of trends occurring in the data. Other notable awards included a Good Adaptation of Graph Analysis Techniques submitted by the Chinese Academy of Sciences, Central Michigan University, and Northwestern University team. Two honorable mentions were awarded in C2. Virginia Tech provided an entry illustrating Good Use of Coordinated Displays, and Central South University (China) provided an Interesting Use of Radial Visualization Techniques.

4 Discussion

4.1 Participation

VAST Challenge 2012 received 40 submissions across the two challenges. Table 1 compares the number of submissions over the life of the VAST Challenge.

Submissions	2006	2007	2008	2009	2010	2011	2012
Challenge 1	-	-	22	22	14	30	27
Challenge 2	-	-	13	17	22	8	13
Challenge 3	-	-	12	5	17	13	-
Challenge 4	-	-	20	-	-	-	-
Grand Challenge	6	7	6	5	5	5	-
Total	***6***	***7***	***73***	***49***	***58***	***56***	***40***

Table 1: Summary of VAST Challenge submissions by year

Given that this year's challenge involved only two different challenge tasks, as compared to previous years with more available tasks, the number of entries was particularly impressive. The 27 entries received for C1 is the second greatest number of entries received for any of the challenge tasks over the history of the VAST Challenge.

Again this year, the number of dataset downloads has increased. There were 703 unique downloads of the C1 data and 383 downloads of the C2 data, for a total of 1086 unique downloads by the submission closing date. Even accounting for the differences introduced by a new downloading scheme that permits downloads by individual challenge task, this still represents a substantial increase from the 671 downloads in 2011 or the 537 downloads in 2010.

In addition, this year's challenge had a good balance between student teams and non-student teams (18 of 40).

4.2 Technology

Table 2 summarizes the most commonly used technologies used in VAST Challenge 2012 submissions. This year 30% of the teams used Tableau [2] as part of their submission, which is substantially greater than in previous years. In addition, the D3 [3] and Processing [4] libraries were frequently used by teams who developed custom solutions.

Software Tool	Number of Submissions
Tableau	12
D3	7
MySQL	7
Microsoft Excel	7
Java	5
Processing	5
Postgres	5
SPSS	4
R	3
Other	65

Table 2: Most common technologies used to develop VAST Challenge 2012 submissions

4.3 VAST Papers

All contestants, not just those receiving awards, were welcome to submit a two-page summary paper for the VAST electronic proceedings. As a result 26 of 40 teams who competed this year also submitted a paper.

The following is a list of papers submitted for VAST Challenge 2012, with award titles included if applicable.

Abousalh-Neto, N. A., Kazgan, S., "Big Data Exploration through Visual Analytics."

Barcelos, Y., Aburjaile, F., Leite, L.R., Oliveira, S.T., "Combining Traditional and High-density Visualizations in a Dashboard to Network Health Monitoring."

Cao, Y., Moore, R., Mi, P., Endert, A., North, C., Marchany, R., "Dynamic Analysis of Large Datasets with Animated and Correlated Views." **Challenge 2 Honorable Mention: Good Use of Coordinated Displays.**

Chen, V.Y., Razip, A.M., Ko, S., Qian, C.Z., Ebert, D.S., "SemanticPrism: a Multi-aspect View of Large High-dimensional Data." **Challenge 1 Award: Outstanding Integrated Analysis and Visualization.**

Choudhury, S., Kodagoda, N., Nguyen, P., Rooney, C., Attfield, S., Xu, K., Zheng, Y., Wong, B.L.W., Chen, R., Mapp, G., Slabbert, L., Aiash, M., Lasebae, A., "M-Sieve: A visualisation tool for supporting network security analysts." **Challenge 1 Award: Subject Matter Expert's Award.**

Chung, H., Cho, Y.J., Self, J., North, C., "Pixel-Oriented Treemap for Multiple Displays."

Dudás, L., Fekete, Zs., Göbölös-Szabó, J., Radnai, A., Salánki, Á., Szabó, A., Szücs, G., "OWLAP - Using OLAP Approach in Anomaly Detection." **Challenge 1 Award: Good Support for the Data Preparation, Analysis, and Presentation Process.**

Fischer, F., Fuchs, J., Mansmann, F., and Keim, D.A., "BANKSAFE: A Visual Situational Awareness Tool for Large-Scale Computer Networks." **Challenge 1 and 2 Award: Outstanding Comprehensive Submission.**

Gibson, H., Vickers, P., "Network Infrastructure Visualisation Using High-Dimensional Node-Attribute Data."

Harrison, L., Laska, J., Spahn, R., Iannacone, M., Downing, E., Ferragut, E.M., Goodall, J.R., "situ: Situational Understanding and Discovery for Cyber Attacks."

Hildenbrand, J., Paval, D.I., Thapa, P., Rohrdantz, C., Mansmann, F., Bertini, E., Schreck, T., "VAST 2012 Mini-Challenge 2: Chart- and Matrix-based Approach to Network Operations Forensics."

Horn, C., Ellsworth, C., "Visual Analytics for Situation Awareness of a Large-Scale Network." **Challenge 1 Award: Effective Video Presentation.**

Jonker, D., Langevin, S., Schretlen, P., Canfield, C., "Agile Visual Analytics for Banking Cyber 'Big Data'"

Kachkaev, A., Dillingham, I., Beecham, R., Sarah Goodwin, Ahmed, N., Slingsby, A., "Monitoring the Health of Computer Networks with Visualization." **Challenge 1 Award: Efficient Use of Visualization.**

Krüger, R., Bosch, H., Koch, S., Müller, C., Reina, G., Thom, D., Ertl, T., " HIVEBEAT - A Highly Interactive Visualization Environment for Broad-Scale Exploratory Analysis and Tracing." **Challenge 1 Honorable Mention: Comprehensive Visualization Suite.**

Laberge, L. Kaul, S., Anderson, N., Agnew, C., Goldstein, D., Kolojejchick, J., "Enhancing the 'Think Loop Process' with Consistent Interactions." **Challenge 1 Honorable Mention: Good Interaction Techniques.**

Migut, G., van Wees, J., Bakker, D., de Goede, B., Steltenphol, H., Lenferink, N.O., Worring, M., "VAST Challenge 2012: Interactively Finding Anomalies in Geo-temporal Multivariate Data."

Pabst, R., "BusinessForensics HQ." **Challenge 1Award: Good Visual Design.**

Shi, L., Liao, Q., Yang, C., "Investigating Network Traffic through Compressed Graph Visualization." **Challenge 2 Award: Good Adaptation of Graph Analysis Techniques.**

Shurkhovetskyy, G., Bahey, A., Ghoniem, M., "Visual Analytics for Network Security."

Stark, R.F., Wollocko, A., Borys, M., Kierstead, M., and Farry, M., "Visualizing Large Scale Patterns and Anomalies in Geospatial Data." **Challenge 1 Honorable Mention: Good Visual Design.**

Takeda, S., Kobayashi, A., Kobayashi, H., Okubo, S., Misue, K., "Irregular Trend Finder: Visualization Tool for Analyzing Time-series Big Data."

Williams, F.C.B., Faithful, W.J., Roberts, J.C., "SitaVis - Interactive Situation Awareness Visualization of Large Datasets." **Challenge 1 Honorable Mention: Good Situation Awareness Snapshot.**

Zhang, T., Liao, Q., Shi, L., "3D Anomaly Bar Visualization for Large-scale Network."

Zhao, M., Zhong, C., Ciamaichelo, R., Konek, M., Sawant, N., Giacobe, N.A., "Federating Geovisual Analytic Tools for Cyber Security Analysis."

Zhao, Y., Zhou, F., Ronghua, S., "NetSecRadar: A Real-time Visualization System for Network Security." **Challenge 2 Honorable Mention: Interesting Use of Radial Visualization Technique.**

5 Path Forward

This year (2012) has been the "Year of the Contest" where analysis competitions have sprung up around the world, including listings in Challenge.gov, Kaggle, and CrowdAnalytix. The VAST Challenge committee is pleased to have been supporting the visual analytics community with specialized contests to support growth of the science and technology since 2006.

The VAST Challenges are never the same from year to year, but they consistently attract strong interest, both in terms of the number of submissions and the number of dataset downloads. The Challenge is an integral part of the VAST conference, and the committee also takes great pride in receiving entries from all over the world, and then meeting the team members who put so much of themselves into their work at the conference workshop each year.

This year's workshop is open so that all VisWeek participants can come learn about the Challenge, meet the participating teams, and see the solution software in action. It is hoped that this will generate even more synergy and interest in the Challenge. The committee welcomes comments and ideas from the VAST community to help make the activity increasingly beneficial to all.

Acknowledgements

The committee acknowledges the National Security Agency for supporting the VAST Challenge.

The committee also wishes to thank Wendy Cowley, Adam Roberts, Brandon Meador, Cody Tews, John Burnette, and Ian Roberts of Pacific Northwest National Laboratory; Catherine Plaisant at the University of Maryland; and John Fallon and Patrick Stickney of the University of Massachusetts, Lowell.

References

[1] VAST Challenge, http://www.cs.umd.edu/hcil/vastchallenge/.
[2] Tableau Software: http://www/tableausoftware.com
[3] Michael Bostock, Vadim Ogievetsky, and Jeffrey Heer, "D3: Data Driven Documents", IEEE Transactions on Visualization & Computer Graphics, IEEE Press, pp. 2301-2309, 2011.
[4] Casey Reas and Ben Fry, Processing: A Programming Handbook for Visual Designers and Artists, The MIT Press, Cambridge MA, 2007.
[5] Visual Analytics Benchmark Repository, http://hcil.cs.umd.edu/localphp/hcil/vast/archive/.