Visual-Based Anomaly Detection for BGP Origin AS Change (OASC) Events

Soon-Tee Teoh[1], Kwan-Liu Ma[1], S. Felix Wu[1], Dan Massey[2], Xiao-Liang Zhao[2], Dan Pei[3], Lan Wang[3], Lixia Zhang[3], and Randy Bush[4]

[1] Computer Science Department, University of California
Davis, CA 95616, USA
{teoh,ma,wu}@cs.ucdavis.edu

[2] Networking Group – East (NGE), USC/ISI
Arlington, VA, 22203, USA
{masseyd, xzhao}@isi.edu

[3] Computer Science Department, UCLA
Los Angelos, CA, 90095, USA
{peidan,lanw,lixia}@cs.ucla.edu

[4] IIJ, Bainbridge Island, WA 98110, USA
randy@psg.com

Abstract. To complement machine intelligence in anomaly event analysis and correlation, in this paper, we investigate the possibility of a human-interactive visual-based anomaly detection system for faults and security attacks related to the BGP (Border Gateway Protocol) routing protocol. In particular, we have built and tested a program, based on fairly simple information visualization techniques, to navigate interactively real-life BGP OASC (Origin AS Change) events. Our initial experience demonstrates that the integration of mechanical analysis and human intelligence can effectively improve the performance of anomaly detection and alert correlation. Furthermore, while a traditional representation of OASC events provides either little or no valuable information, our program can accurately identify, correlate previously unknown BGP/OASC problems, and provide network operators with a valuable high-level abstraction about the dynamics of BGP.

1 Introduction

A statistic-based anomaly detection system is designed to detect any significant differences ***statistically*** between a long-term historical profile and a short-term behavior. We need to apply some mathematical models both to produce the long-term profiles and to compare them with short-term behaviors. On the other hand, a "visual-based" anomaly detection system is to utilize human's cognitive visualization capability to detect any significant differences ***visually*** between the particular human user's mental model [1] of the long-term behavior and his/her short-term visual observation. In

M. Brunner and A. Keller (Eds.): DSOM 2003, LNCS 2867, pp. 155-168, 2003.

short, a visual anomaly is something that catches his/her eyes. While the idea of visual-based anomaly detection is certainly not new – we have been doing it in our daily life for thousands of years, the focus here is to report our results in applying this concept to detect potential security problems due to OASC (Origin AS Change) events under the BGP routing protocol.

With the popularity of the Internet technology, unintentional faults and intentional intrusions directly on network protocols, such as routing protocols, have become a serious threat to our Internet-connected society. In 1997, a buggy BGP (Border Gateway Protocol) [2] router falsely de-aggregated thousands of network addresses which disabled the Internet in the entire US east coast for up to 12 hours. In 2001, worm attacks such as CodeRed and Nimda were spread around the Internet, while the Renesys report [3] discussed a possible correlation between worm attacks and routing protocol stability. In [4], a different interpretation of the Renesys observation indicated that the large increase in the number of BGP messages was mainly due to the behavior of the measurement points, and probably not related to the BGP routing stability.

Driven by these faulty or intrusive instances on the Internet infrastructure, many research teams have studied how to either design new protocols and/or enhance existing protocols such that the Internet can be more robust and fault/intrusion-tolerant. For instance, the Secure BGP (S-BGP) [5] protocol utilizes the PKI infrastructure to authenticate and authorize the route update messages in an inter-domain environment. In [6], a program is developed to statistically profile the "stable" BGP paths leading to critical DNS servers and to filter out "unusual" routes potentially being falsely injected by attackers or simply misbehaving BGP routers.

Another complementary approach to handle these Internet vulnerabilities is via ***an interactive process*** between network administrators/operators and network management systems with visualized network/security information. We believe that, at least in the short term, a network system with machine intelligence alone will have certain limitations in detecting and responding to novel attacks/faults targeting on the Internet infrastructure itself. For instance, given a colorful image of some BGP routing data, an experienced human operator might discover numerous facts about the Internet instantly, while an analysis program must already have the mechanisms built in to achieve the same results. One of the most difficult tasks in intrusion detection is "event correlation," but via human visualization, this task may be much more plausible. Furthermore, due to the complexity and size of the Internet, it is already a very difficult task to evaluate Internet's "health" and clearly identify the root causes of some observed symptoms. Without a comprehensive understanding of the Internet, it is not certain that some new Internet protocols, architecture, or enhancements will be effective in responding to the problems we have today.

This paper describes our design, implement, and evaluate an experimental visual anomaly detection system for BGP OASC (Origin AS Change) events. In the following section, we will describe our visualization design for the BGP/OASC events in Sections 2, 3, and 4. Then, in Section 5, we will report our results in using our visual-based anomaly system to detect non-trivial BGP/OASC problems.

2 Visualization Design

Information visualization [7] has emerged as one of the most active areas of computer science research in recent years due to the explosive growth of the World Wide Web. In contrast to scientific visualization, which is primarily about transforming numerical data defining physical structures or phenomena in three spatial dimensions into pictures, information visualization generally maps very large amount of textual, symbolic, or relational data into spatial forms that can be displayed graphically. Data visualization exploits the human vision system to help us explore and better communicate with others particular aspects of the data under study. The process of visualization is an inherently iterative one consisting of multiple steps. A standard visualization process is depicted in the following figure:

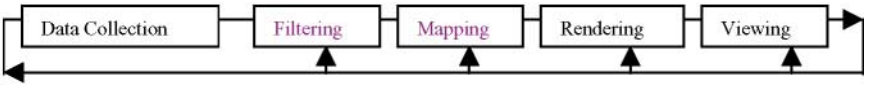


Fig. 1. a standard visualization process

In this research work, we pay special attention to the filtering and mapping steps, which prepare the collected data for rendering and viewing. Generally, the filtering step: removes "noise" from the raw data, reduces the data to a more manageable size, or enhances particular aspects of the data.

For visual anomaly detection, it extracts and organizes particular aspects of the data (e.g., the Origin AS changes in BGP routing) for the subsequent steps. The mapping step transforms the filtered data into a collection of graphics entities with appropriate properties (e.g., colors, transparency, and texture) for rendering.

To summarize, our visualization design has the following four advantages. First, our system integrates the capability of cognitive pattern matching (i.e., utilizing human's capability in recognizing special "possibly previously unknown" patterns). Second, the visual/graphical information from our program may trigger the human's intelligence and memory to reason and analyze the observed situation. A human operator will obtain experience via this process and be trained to more accurately identify the problems quickly. Third, the interactive monitoring and analysis process provides a feedback loop from the human back into our program. Finally, the human expert can provide an in depth explanation about the potential problems using the annotated images and/or animations derived. In the following section, we will demonstrate these advantages via the example of BGP/OASC.

3 OASC (Origin AS Change) Events in BGP

In this section, we very briefly describe the BGP routing protocol and the definition of OASC events.

The Internet is made of thousands of Autonomous Systems (ASes), loosely defined as a connected group of one or more IP prefixes which have a single and clearly defined routing policy. BGP (Border Gateway Protocol) [2] is the standard inter-AS

routing protocol. A BGP route lists a particular prefix (destination) and the path of ASes used to reach that prefix. The last AS in an AS path is the origin of the BGP routes (or the origin AS). The concept of origin AS is critical for the consideration of routing protocol security as it implies the ownership of the IP address prefix (destination). An OASC (Origin AS Change) event [9,10] occurs if we observe any change in the IP address ownership.

One example of OASC events, called MOAS (Multiple Origin AS), is when suddenly we observe multiple ASes simultaneously claiming the ownership of the same address prefix. More precisely, suppose prefix d is associated with AS paths $asp_1 = (p_1, p_2, \ldots, p_n)$ and $asp_2 = (q_1, q_2, \ldots, q_m)$, and p_n is not equal to q_m.

An OASC event can be either valid or invalid. The MOAS example described above is legitimate if each originating AS can directly reach the prefix. On the other hand, if one of the origin ASes cannot reach the prefix, then it is an invalid MOAS conflict and may be due to some malicious attacks. The problem of detecting invalid OASC events is further complicated by BGP operational practices. RFC1930 [8] only recommends (not requires) that each prefix originate from a single AS. In general, we have no way to determine whether an OASC event is the result of a fault, an attack, or a legitimate operational policy.

Faulty aggregation or de-aggregation may cause invalid OASC events. For instance, an AS advertises an aggregated prefix, even though some of more specific prefixes are not reachable by the AS, while there are no other more specific routes available to reach those more specific prefixes. On the other hand, as an example of de-aggregation, on April 25th, 1997, a severe Internet outage occurred when one ISP falsely de-aggregated most of the Internet routing table and advertised the prefixes as if they originated from the faulty ISP. The falsely originated prefixes resulted in many invalid OASC events, which had a serious impact on Internet routing.

For producing OASC events, we used the raw data from the Oregon Route Views server (peering with 54 BGP routers in 43 different ASes) to obtain the BGP routes and AS paths. The Oregon Route Views data is particularly attractive because it provides data from a number of different vantage points. Overall 38225 MOAS events were observed over 1279 days, and there is a significant increase from 683 events (in average) in 1998 to 1294 events (in average) in 2001 as shown in the following "traditional 2D" figure.

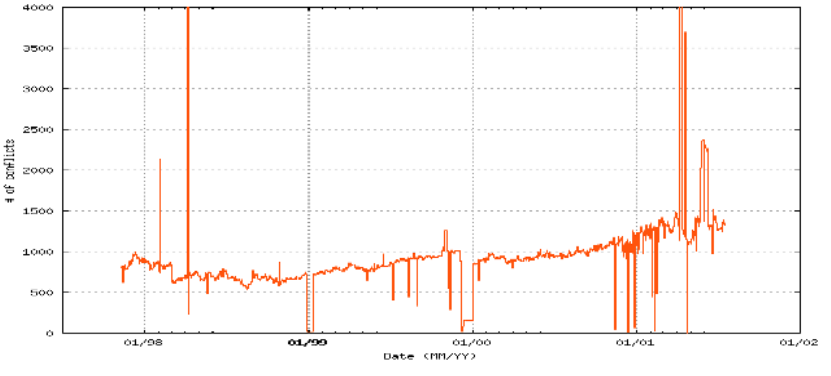


Fig. 2. MOAS events in the Internet from 1998 to 2001

Via the above 2D figure about OASC events, we can spot some event spikes/anomalies in the past. For instance, in early 2001, one single AS caused 9177 OASC events in one day. However, from the figure itself (or the raw data), it is not easy to derive more valuable information about the problem. Neither could we tell what was the response or reaction from this or other ASes after this particular BGP problem instance.

4 The Design of Our Visual-Based Anomaly Detection System

We have designed and prototyped a visualization program to support an interactive process for analyzing BGP OASC events. Via our initial experiments, we have clearly observed some great advantages in using information visualization techniques to analyze and correlate a large number of BGP/OASC events. In this section, we will first briefly describe our design. Then, in the next section, we will show a few scenarios of using our program to not only detect the problem but also quickly nail down the root cause to the detected problem.

4.1 Types of Origin AS Changes in BGP

As mentioned before, from the raw BGP data collected, we can produce a set of "Origin AS Change (OASC)" events. Each Origin AS Change (OASC) event contains the following five attributes:

Prefix	is the IP prefix whose Origin AS has changed.
AS-before	is a list of the associated AS(es) before the change.
AS-after	is a list of the associated AS(es) after the change.
Date	is the date on which the change occurred.
Type	is the type of a OASC change event.

Furthermore, OASC events are classified into 4 main types and then further classified into 8 types in total. The 4 main classes are:

B-type:	An AS announces a more specific prefix out of a larger block it already owns.
H-type:	An AS announces a more specific prefix out of a larger block belonging to another AS. In other words, this AS "punches a hole" on prefix addresses of others.
C-type:	An AS announces a prefix previously owned by another AS.
O-type:	An AS announces a prefix previously not owned (and therefore owned by ICANN by default).

The C-type and O-type changes are further classified by whether they involve Single Origin AS (SOAS) or Multiple Origin ASes (MOAS):

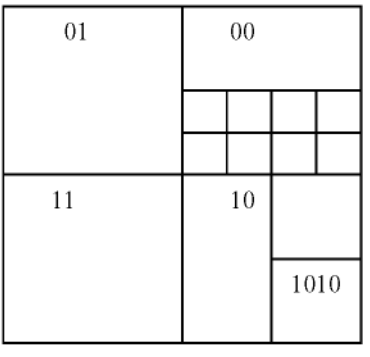
CSM:	*C*-type change from	SOAS	to MOAS
CSS:	*C*-type change from	SOAS	to SOAS
CMS:	*C*-type change from	MOAS	to SOAS

CMM:	*C*-type change from	MOAS	to MOAS
OS:	*O*-type change involving	SOAS	
OM:	*O*-type change involving	MOAS	
H:	*H*-type change always involving another AS (being punched a hole)		
B:	*B*-type change always involving itself only		

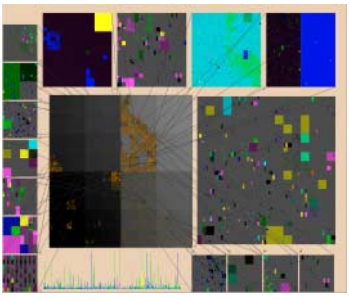
In the visualization, different colors are associated with each of the eight types. While this paper is black and white only, a colorful version of this paper can be downloaded from our web site.

4.2 Representing IP Address Prefixes

In representing BGP/OASC events, 2 key concepts are IP address prefix and Autonomous systems. We will first describe our quad-tree representation of IP address prefixes.



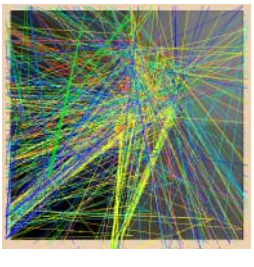
In our prototype, each IP prefix maps to one pixel on a square. The mapping is done in a traditional quad-tree manner as shown on the left. In a quad-tree, a square is repeatedly subdivided into 4 equal squares. In mapping a 32-bit prefix to a square, we start with the first two most significant bits of the address to place the IP address in one of the 4 squares in the second level of the quad-tree. We then use the next two most significant bits to place the IP prefix in the appropriate third level square within this square. We do this repeatedly until we can place the prefix in a square the size of a single pixel. The prefix is mapped to that pixel.



As an example, the following is the visualization of data for 416 days up till February 19, 2001. The main window shows the quad-tree mapping of the entire space of 32-bit IP address. A pixel is colored yellow if an Origin AS Change occurred on the current day (February 19, 2001), and colored brown to green if a change occurred on a previous day (January 1, 2000 through February 18, 2001). In the windows showing detail, a square is used to depict each change, with hue determined by the type of the change, brightness determined by how long ago the change occurred (present day data shown the brightest), and size determined by the mask of the prefix. The background of the main window is shaded according to the IP prefix the pixel represents. The brighter the pixel, the larger the IP prefix represented.

Due to the limitations of a computer screen space, we use a 512x512 pixel square to represent the entire 32-bit IP prefix space. With only 512x512 pixels, even though many IP prefixes map to the same pixel, we found that this is sufficient in spreading out the IP addresses in BGP/OASC events. IP prefixes sharing similar more significant bits would be in close proximity on the screen. With an additional level of zooming into a portion of the data, we can view individual IP prefixes as shown above. In the detail windows, each IP prefix is shown as a square or a rectangle. The size of the rectangle indicates the size of the block of IP addresses; a prefix with a smaller mask gets mapped to a larger rectangle.

4.3 Relationship Between Prefix and AS



To represent the relationship between IP address prefix and different ASes, we place 4 lines surrounding the IP square, and an AS number is mapped to a pixel on one of the 4 lines. A line is then drawn from an IP address to an AS number if there is an Origin AS change involving that IP address and that AS number. This mapping takes advantage of the user's acute ability to recognize position, orientation and length. This figure shows visually the IPAddrPrefix-AS relationship of Origin AS Changes of

“a typical day” (April 5, 2001). The color of each line represents one of the eight different OASC types.

Since there are more AS numbers than pixels, more than one AS numbers map to a single pixel. Again, we provide zooming features for the user to differentiate between AS numbers, which map to the same pixel in the main display. The lines representing changes for the AS in focus is shown with brighter and more saturated colors than other changes. This effectively highlights the AS, fading the other changes into the background.

4.4 Animation and Other Features

For the time dimension, our program shows one day's data at a time, and allows the user to animate the visualization (each frame showing consecutive day's data). With this ``movie'' display, the user can build up a mental long-term profile in his/her mind, and detect temporal patterns. To assist our memory of patterns from previous days, we allow a user-defined window of a certain number of days prior to the currently shown date. Data from these previous days are displayed, but with darker, less saturated colors, so that the current day's data stands out.

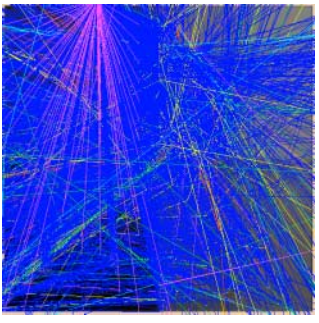
For the convenience of the user, we also provide textual display of the IP address or AS number represented by the pixel clicked by the user. Another feature for convenience is a slider bar to tell the date of the current data shown. The user can click on the bar to choose the date to show. A simple plot of the total number of changes of each type on each day is shown with the bar.

By choosing parameters like what IP prefixes to zoom in on, which AS numbers to focus on, which type of changes to view etc., the user follows an interactive process to navigate abstract information in different levels of details. Depending on the combination of chosen parameters, the user can see the overall pattern of the data, or the user can focus attention on very specific parts of the data. Different choices would reveal different anomalies and information.

5 Detecting and Analyzing OASC Anomalies Visually

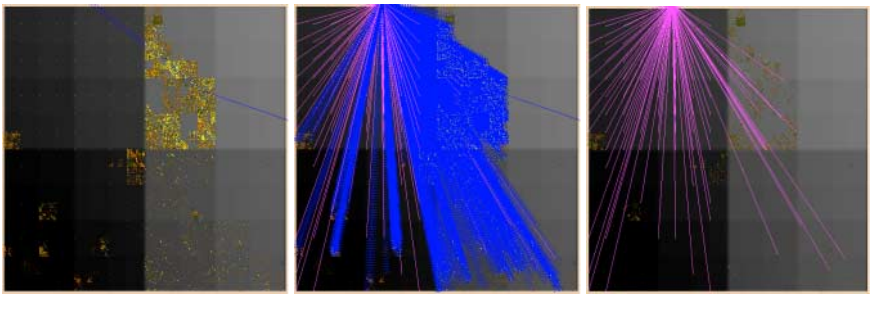
A simple “counter-based” 2D figure for historical OASC events, as shown earlier, can represent some simple OASC related anomalies. But, the value of the information is relatively inadequate to the system administrators dealing with the network instances. In this section, we present two examples of using our visualization program interactively to identify and analyze OASC problems. With our program, the system administrators can easily move deep into the data and discover critical and abstractive facts above a large set of low-level network events. In reading this part of paper, please use a color viewer or printer.

5.1 Interactive Visual Analysis: "What Went Wrong on August 14, 2000?"



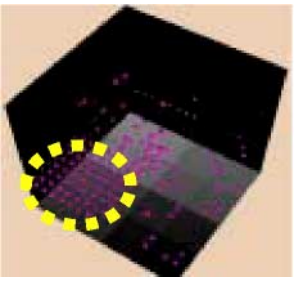
On August 14, 2000, when we turned on all eight OASC types and monitored on all ASes, we visually observed an abnormally large number of blue-colored lines (H-type OASC events). Since the amount of H type OASC events was large to catch our attention, our initial hypothesis was that, due to configuration errors possibly, one or more ASes punched a large number of holes on the IP address prefixes belonging to other innocent ASes.

Immediately, to verify our hypothesis, we used the "AS detail" feature in our program to select only one single H type OASC event and displayed the ASes being involved. The rationale is that, if a very small number of ASes are the root causes for the aggressive Hole-punching problem, selecting one of such event would lead us to one of the "trouble makers."



The figure above on the left shows that after we selected one AS randomly (AS-11724 in our example). In the same figure, the solid line connects the victim AS (AS-11724) and the prefix address (207.50.48.0/21) being hole-punched, while the dash line connects the attacking AS (AS-7777) and a subset of the prefix address (207.50.53.251/32). In other words, AS-7777 would attract all the traffic toward 207.50.53.251 from AS-11724, which supposed to be the true owner. Immediately, we know that the potential attacker (or faulty BGP router) was from AS-7777. Now, we can use the features in our program to only select the OASC events related to AS-7777, and we have the middle snapshot. In fact, after focusing on AS-7777, we can easily validate that this AS was the only AS causing H type events on August 14, 2000. However, in the rightmost picture above, we also isolated the pink-colored lines (OS type OASC events), and interestingly, it seems to us that the pattern of OS type

events was regularly distributed across a region of IP address prefixes that has never been used or allocated in Internet as in the right figure.

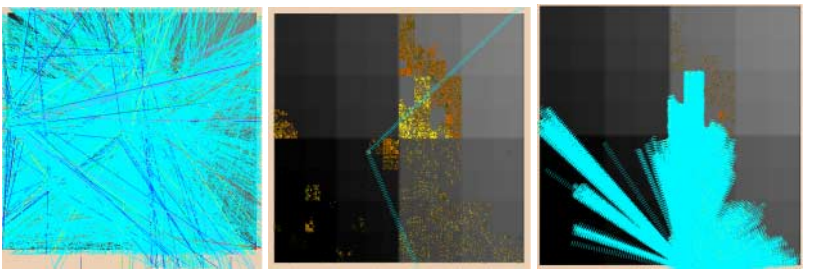


To validate further about what exactly is going on, we used our 3D representation to analyze all the OS type OASC events. With the left figure, from the left middle part (circled by a thick dash line), it is very clear and interesting that AS-7777 announced prefix addresses forming a grid in the unused IP address space. Based on the location and shape of the grid and the raw events, we concluded that AS-7777 falsely announced from 65.0.0.0/8 to 126.0.0.0/8 plus many others.

Please note that the discovery of the OS type OASC event grid is trivial by human, if the visual orientation is right. However, the same task would be very difficult for a fully automated intrusion detection system to reveal this type of facts unless the pattern matching mechanism for grids has been included in advance. Certainly, this case shows the limitation of the traditional intrusion detection systems in detecting "unknown/new/novel" attacks, while our visual-based anomaly detection system has a very good chance to catch them. In the case of August 14, 2000, with a few clicks interactively, our system not only helped detect the problem, but also, quickly nailed down the trouble source, AS-7777. Furthermore, via visualization, it even can tell the details about the errors from AS-7777.

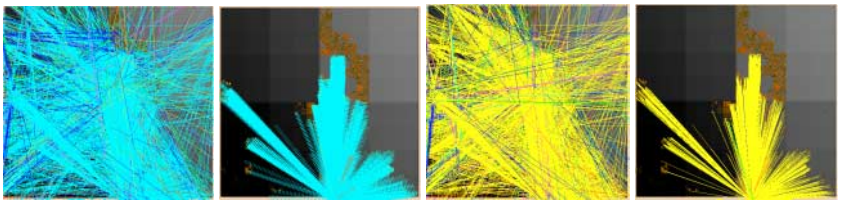
5.2 Interactive Visual Correlation: "What Was AS-15412 Doing in April 2001?"

Earlier we showed that on April 5, 2001, things looked "normal". But, on April 6, the next day, we observed an unusual amount of skyblue-colored lines (i.e., CSM-type OASC events). A CSM event indicates that a particular IP address prefix was originated by one AS the previous day, but more than one ASes are claiming it on the current day. With the possibility of multi-homing and private AS numbers, a small amount of CSM events is probably acceptable, but the snapshot on the left below is visually abnormal.



Again with a simple interactive analysis process, very quickly we identified that AS-15412 is the only AS injecting all the CSM OASC events on April 6, 2001. In the middle snapshot above, it shows that AS-15412 is conflicting with a victim AS-10132, which is the Eastar Technology Center in Hongkong. (We randomly picked one of the victims and we used the "whois" program to find out more information from the whois server, whois.radb.net.) Furthermore, after we animated the data only related to AS-15412, we found something interesting: AS-15412 not only injected thousands of CSM-type OASC events on April 6, but also, from April 7 to 12, it introduced thousands of yellow-colored lines, which are CMS-type OASC events. This indicates that, right after the CSM mistakes on April 6, 2001, the system administrator responsible for the AS-15412 problem started to "correct" the problems by withdrawing the bad announcements, which caused a storm of CMS events during next 6 days. The trouble AS was a small ISP (Internet Service Provider) called FLAG Telecom Global Internet in London, UK.

However, a few days later, on April 18, 2001 (4 days later), AS-15412 caused (at least, it seems to us visually) exactly the same mistake again, and the "shape" is exactly the same as the one on April 6 (possibly reloaded an old copy of BGP configuration file). The difference though is that this time it only took them one day to fix all the problems. The two pictures on the left below show the CSM-type OASC events on April 18, 2001, while the right two pictures are CMS-types events on April 19, 2001.



Please note that, via this example, we again observe the big advantage of integrating machine and human intelligence. From human's point of view, the correlation between CSM and CMS events is very clear. After watching the animation and interactively identifying the AS causing the problem, we will not consider, for example, the large number of CMS events on both April 12 and 19 as errors probably because we know AS-15412 over at UK was trying to fix the problems they created. On those two days (April 12 and 19 in 2001), without the right correlation as we shown here, thousands of false alarms might have been reported.

5.3 How about France Telecom?

When we first studied the instance in April 6-19, 2001, we believed, visually, that AS-15412 made "exactly" the same mistake on both April 6 and 18 of 2001 because the shapes visually look exactly the same. We reached this conclusion based on purely visual correlation. Earlier this year (2003), one of our colleagues from France Telecom came to us with their own AS numbers (AS-3215 and AS-5511). They would like to find out how many OASC events were related to their own ASes. While we quickly realized, using our Elisha BGP visualization tool, that France Telecom's ASes have been affected in relatively small number of OASC events, we also found out that France Telecom's ASes were not affected on April 6, but they were indeed part of some OASC events on April 18. This implies that, although the graphs on 6th and 18th look the same, they are different in a minor ways. It turned out that only a very small portion of ASes behave differently between 6th and 18th.

6 Remarks

In a large complex system, it is impossible to rely on any single mechanism, however powerful may it be, to detect all possible attacks or faults. It is also very difficult to pre-design and pre-implement a set of mechanisms to detect and respond to problems not being seriously considered before. However, while human intelligence (such as the security instance response team) can certainly complement an intrusion detection system, we need to have an effective interaction process to follow in order to resolve problems correctly and quickly.

With a traditional 2D representation (i.e., counting BGP/OASC events), relatively little information can be derived and we need to dig into the raw BGP data to analyze the problem instances. For the instance of August 14, we might be able to marginally spot the anomaly. But, with our visualization program, we can not only detect the H-type OASC anomaly but also go deep into the information using different representation methods with only a few clicks to identify the OS-type OASC anomaly as well. As a result, we identify the possible error made by the AS-7777. Please note that our system was designed and built BEFORE we were aware of the AS-7777 instance in August 14, 2000 or other similar instances.

In handling millions of events from a large complex distributed system such as Internet, "false alarms" and "event correlation" become two most critical issues (or technical bottlenecks). Our visual representation for the OASC events here provides a global and abstract picture about the BGP/OASC activities in the Internet. Therefore, the human operator will be given not only a huge set of events but also the context and the relations among the events graphically. An experienced human operator can then use our system to justify the validity of a reported attack instance based on his/her comprehensive awareness of the target system. On the other hand, if he/she is not certain about the situation, then the interactive process should guide him/her to navigate more information to reduce the potential false positive. Second, as demonstrated in Section 6.2, our system provides the capability of visual event correlation such that

a human operator can quickly correlate a set of reported events and provide a valid explanation about what is going on.

In the 2D counter-type figure (Figure 2 in Section 3), we can see big spikes in April 2001, but to completely understand what was going on is a very difficult task. If not correlating events correctly, the system administrator would have to digest more than tens of thousands of events over a two-week period. And, hopefully some correct abstraction of these events can be discovered. But, again, with our program's animation features, the right, short/compact, and abstractive conclusion can be drawn quickly for all these events.

Via the experience in using our programs to analyze the BGP routing data on the Internet (we have another visualization program for BGP route path stability, which has not been described in this paper), we have demonstrated the great potential in applying information visualization techniques to critical problems in fault and intrusion detection on network routing protocols such as BGP. We believe that the integration of human and machine intelligence via the technique of information visualization may provide yet another important avenue to enhance the performance, security, and fault tolerance of the Internet.

Acknowledgements

This research is supported in part by DARPA (under the FTN program) and NSF under Grant No. 0220147. We appreciate valuable information and comments regarding the OASC problem from Herve Debar (France Telecom), Jason Coit (UC Davis), and anonymous reviewers of this paper.

References

[1] Dedre Gentner and Albert L. Stevens (editors), “Mental Models”, Cognitive Science, 1983.

[2] Y. Rekher and T. Li, “A Border Gateway Protocol 4 (BGP-4)”, rfc1771, IETF.

[3] James Cowie, Andy Ogielski, BJ Premore and Yougu Yuan, “Global Routing Instabilities during Code Red II and Nimda Worm Propagation” NANOG, 09/19/2001.

[4] Lan Wang, Xiaoliang Zhao, Dan Pei, Randy Bush, Daniel Massey, Allison Mankin, S. Felix Wu, Lixia Zhang, “Observation and Analysis of BGP Behavior under Stress”, by in ACM SIGCOMM IMW (Internet Measurement Workshop), Marseille, France, November 2002.

[5] Stephen Kent, Charles Lynn, and Karen Seo, “Secure Border Gateway Protocol (Secure-BGP)” in IEEE Journal on Selected Areas in Communications Vol. 18, No. 4, April 2000, pp. 582-592.

[6] Dan Massey, Lan Wang, Xiaoliang Zhao, Dan Pei, Randy Bush, Allison Mankin, Felix Wu, Lixia Zhang, “Protecting the BGP Routes to Top Level DNS Servers” in NANOG 25, June, 2002, Toronto, Canada.

[7] Ivan Herman, Guy Melançon, M. Scott Marshall, "Graph Visualization and Navigation in Information Visualization: a Survey" in IEEE Transactions on Visualization and Computer Graphics, Vol. 6, No. 1, pp. 24-43, 2000.

[8] John Hawkinson and Tony Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)" rfc1930, IETF.

[9] X. Zhao, D. Pei, L. Wang, L. Zhang, D. Massey, A. Mankin, S. F. Wu, "Detection of Invalid Route Announcement in the Internet" in International Conference on Dependable Systems & Networks, 2002.

[10] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S.F.Wu, L. Zhang, "An Analysis of BGP Multiple Origin AS (MOAS) Conflict" in ACM SIGCOMM Internet Measurement Workshop, pp.31-35, November 1-2, 2001, San Francisco.