Traffic Monitoring and Analysis Technologies

Junichi Murayama[†]*, Atsushi Kobayashi, Hiroshi Kurakami, Takeshi Kuwahara, Keisuke Ishibashi, and Nobuhisa Miyake*

Abstract

This article introduces trends in the development of technologies for monitoring and analyzing anomalous traffic in a multifaceted manner by utilizing traffic-flow information to solve the problem of attacks on the network.

1. Introduction

With attacks on the Internet becoming increasingly diverse, the development of countermeasures is an important issue. Distributed denial of service (DDoS) attacks have been known to bring down servers by flooding them with a huge volume of invalid packets. Other examples include the cache poisoning attack, which tampers with the content of a domain name system (DNS) by providing it with a bogus IP address pointing to a phishing site, and the route hijacking attack, which disables access to a server by supplying bogus routing information.

NTT Information Sharing Platform Laboratories is researching and developing network security technologies for monitoring and analyzing traffic in a multifaceted manner to defend against such a diversified array of attacks. In this article, we introduce technologies for countermeasures to DDoS attacks, DNS attacks, and unexpected border gateway protocol (BGP) route changes and describe trends in the development of flow quality monitoring technologies.

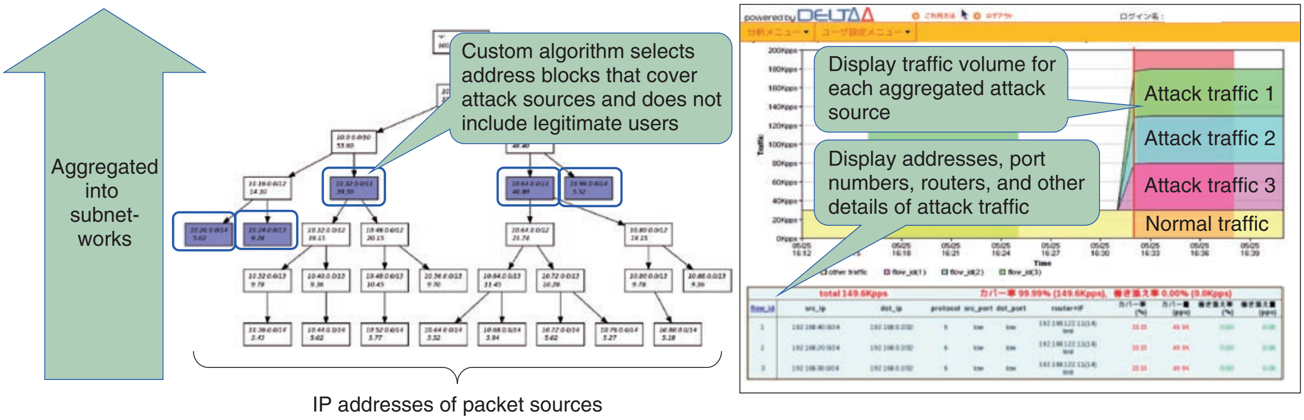
2. Technologies to counter DDoS attacks

The SAMURAI [1] traffic analysis system is an example of NTT Group technology for defending against DDoS attacks. It uses sampled flow information to analyze specific attack patterns using a signature function and to analyze anomalous increases in traffic using a baseline detection function. These analyses enable the source of an attack on specific servers to be identified and attack traffic to be filtered through the use of a router's access control list (ACL) or a Cisco Guard DDoS mitigation appliance. This technology has been put to actual use by NTT Communications. In some cases, however, there are many DDoS attack sources, which makes it difficult to set an ACL with the IP addresses of the packet-sending sources. In such a situation, the DELTAA [2] anomalous traffic identification system can be used.

The DELTAA system recognizes hosts with sharp increases in traffic as attack sources and aggregates them into subnetworks. This process involves precise calculations to avoid including legitimate users (**Fig. 1(a)**). In this way, a very large number of attack sources can be identified in terms of a small number of subnetworks, enabling attack traffic to be easily filtered by a router's ACL. This system is also equipped with functions for visualizing the attack traffic volume for each aggregated attack source, attack start time, etc. (**Fig. 1(b)**). These functions enable an operator to understand the nature of a DDoS attack clearly and quickly.

Our aim at present is to implement DELTAA in a form that links up with SAMURAI (**Fig. 2**).

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan


Aggregated into subnet-works
Custom algorithm selects address blocks that cover attack sources and does not include legitimate users
IP addresses of packet sources
powered by DELTAA
Display traffic volume for each aggregated attack source
Display addresses, port numbers, routers, and other details of attack traffic
Attack traffic 1
Attack traffic 2
Attack traffic 3
Normal traffic
Traffic
Time
total 149.6Kpps

(a) Aggregation of attack-source IP addresses by DELTAA

(b) Visualization of attack traffic by DELTAA

Fig. 1. Anomalous traffic identification by DELTAA.

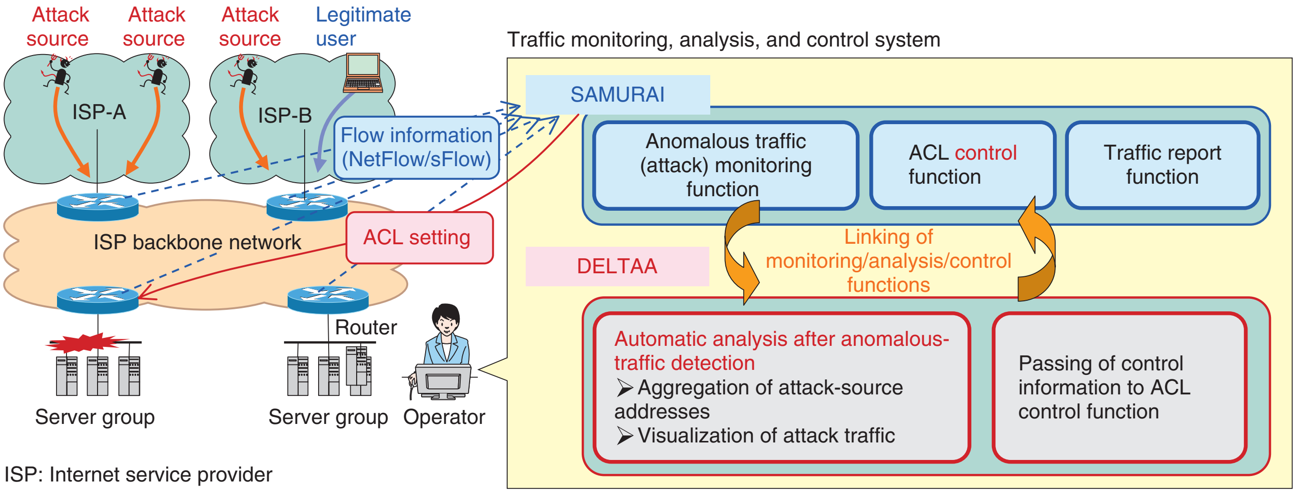

Attack source
Attack source
Attack source
Legitimate user
ISP-A
ISP-B
Flow information (NetFlow/sFlow)
ISP backbone network
ACL setting
Router
Server group
Server group
Operator
ISP: Internet service provider
Traffic monitoring, analysis, and control system
SAMURAI
Anomalous traffic (attack) monitoring function
ACL control function
Traffic report function
DELTAA
Linking of monitoring/analysis/control functions
Automatic analysis after anomalous-traffic detection
➢Aggregation of attack-source addresses
➢Visualization of attack traffic
Passing of control information to ACL control function

Fig. 2. Linking of DELTAA and SAMURAI.

3. Technology to counter DNS attacks

One type of DNS attack is the DNS cache poisoning attack, which inserts a DNS record pointing to a phishing site. Such an attack can be detected using the KOROKU DNS-attack monitoring and analysis tool, which monitors and analyzes flow information [3] exhaustively sampled from the traffic addressed to a certain DNS server.

In the case of a DNS cache poisoning attack, a large number of name-resolution response packets that do not match any queries arrive at the targeted DNS server. Such an attack can therefore be detected by monitoring and exhaustively analyzing sampled flow information (**Fig. 3**). The KOROKU tool is currently undergoing prototype testing and demonstrations using actual equipment.

4. Technology to counter unexpected BGP route changes

Unexpected or invalid BGP route changes, such as BGP-route-hijacking or misconfiguration, suddenly lead to traffic diversions. Moreover, they might lead

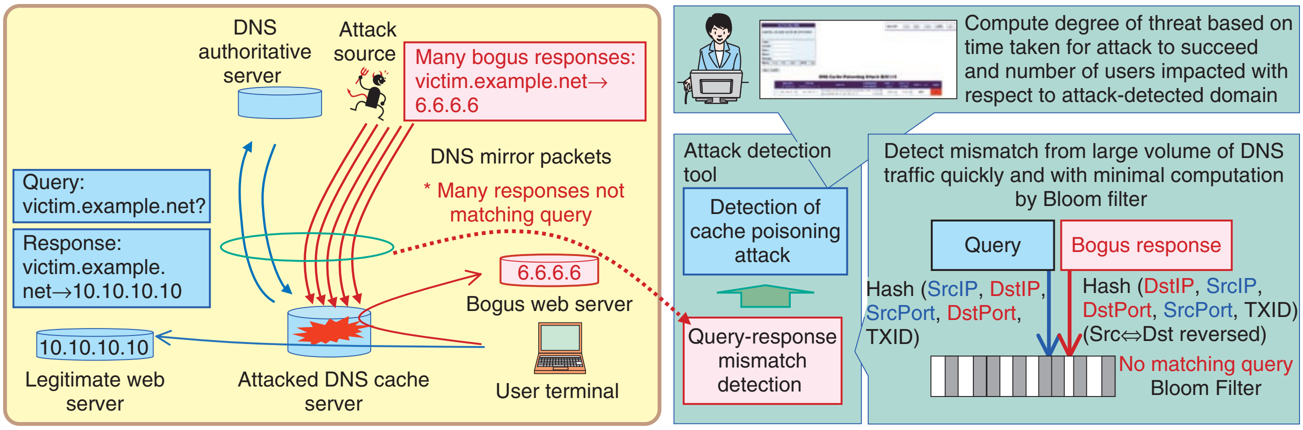

DNS authoritative server
Attack source
Many bogus responses: victim.example.net→ 6.6.6.6
DNS mirror packets
* Many responses not matching query
Query: victim.example.net?
Response: victim.example. net→10.10.10.10
6.6.6.6
Bogus web server
10.10.10.10
Legitimate web server
Attacked DNS cache server
User terminal
Compute degree of threat based on time taken for attack to succeed and number of users impacted with respect to attack-detected domain
Attack detection tool
Detection of cache poisoning attack
Query-response mismatch detection
Detect mismatch from large volume of DNS traffic quickly and with minimal computation by Bloom filter
Query
Bogus response
Hash (SrcIP, DstIP, SrcPort, DstPort, TXID)
Hash (DstIP, SrcIP, DstPort, SrcPort, TXID) (Src⇔Dst reversed)
No matching query
Bloom Filter

Fig. 3. DNS attack detection tool (KOROKU).

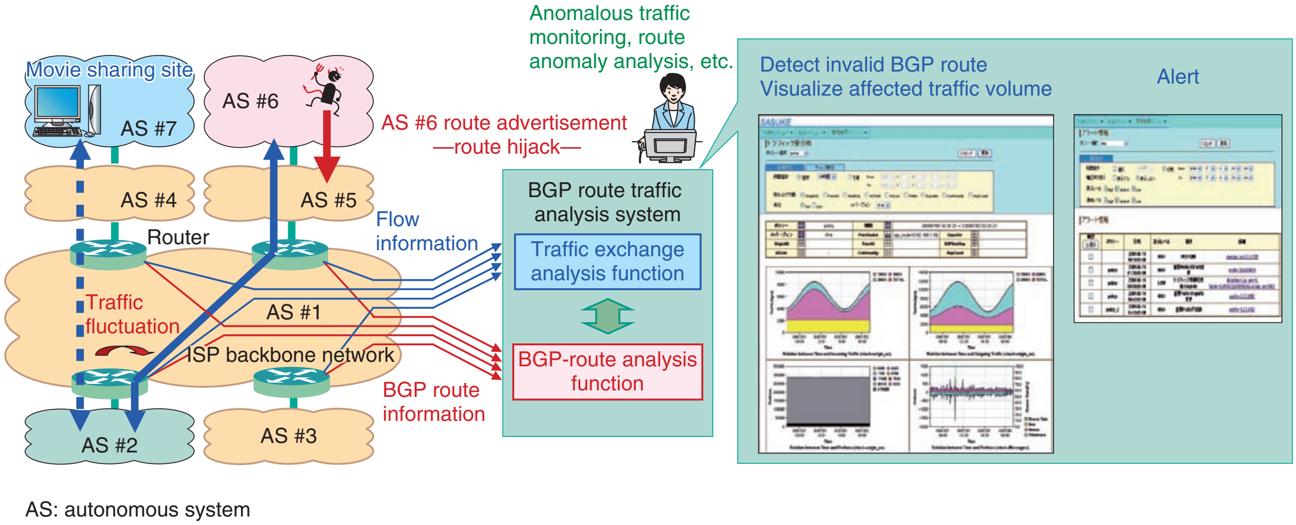

Anomalous traffic monitoring, route anomaly analysis, etc.
Movie sharing site
AS #7
AS #6
AS #6 route advertisement —route hijack—
AS #4
AS #5
Router
Flow information
Traffic fluctuation
AS #1
ISP backbone network
BGP route information
AS #2
AS #3
BGP route traffic analysis system
Traffic exchange analysis function
BGP-route analysis function
Detect invalid BGP route
Visualize affected traffic volume
Alert
AS: autonomous system

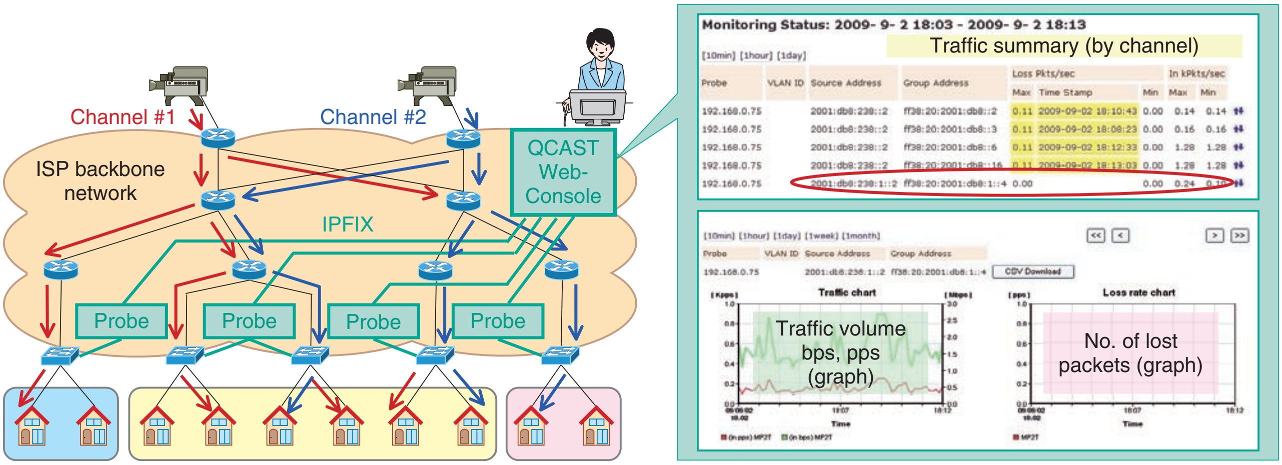
Fig. 4. BGP route traffic analysis system (SASUKE).

to traffic disruption or congestion on other backbone links.

The SASUKE BGP route traffic analysis system is used to detect traffic changes caused by unexpected BGP route changes. It collects BGP route information by direct BGP peering with BGP routers and detects unexpected or invalid BGP route changes and route fluctuations that affect traffic by monitoring for and analyzing any correlations among the flow information collected from different routers.

Since the number of BGP routes in the Internet is huge, testing each and every route for legitimacy is unrealistic. For this reason, when SASUKE detects fluctuations in BGP routes, it focuses on traffic changes for the top rank-N traffic volume and then analyzes the correlation between a traffic change and the BGP route change involved. When a traffic change caused by an invalid or unexpected route change occurs, SASUKE issues an alert and prompts the operator to investigate the cause of the route fluctuation (**Fig. 4**).

The SASUKE system is currently undergoing prototype testing and demonstrations in the field with an eye toward implementation in a form that links up with DELTAA and SAMURAI.



Monitoring Status: 2009- 9- 2 18:03 - 2009- 9- 2 18:13

[10min] [1hour] [1day]

Probe	VLAN ID	Source Address	Group Address	Loss Pkts/sec			In kPkts/sec	
				Max	Time Stamp	Min	Max	Min
192.168.0.75		2001:db8:238::2	ff38:20:2001:db8::2	0.11	2009-09-02 18:10:43	0.00	0.14	0.14
192.168.0.75		2001:db8:238::2	ff38:20:2001:db8::3	0.11	2009-09-02 18:08:23	0.00	0.16	0.16
192.168.0.75		2001:db8:238::2	ff38:20:2001:db8::6	0.11	2009-09-02 18:12:33	0.00	1.28	1.28
192.168.0.75		2001:db8:238::2	ff38:20:2001:db8::16	0.11	2009-09-02 18:13:03	0.00	1.28	1.28
192.168.0.75		2001:db8:238:1::2	ff38:20:2001:db8:1::4	0.00		0.00	0.24	0.10

[10min] [1hour] [1day] [1week] [1month]

Probe	VLAN ID	Source Address	Group Address
192.168.0.75		2001:db8:238:1::2	ff38:20:2001:db8:1::4

bps: bits per second
pps: packets per second

Fig. 5. IPTV (multicast) QoS monitoring tool (QCAST).

5. QoS monitoring technologies

With the spread of realtime applications such as IPTV (Internet protocol television) and VoIP (voice over Internet protocol), it has become increasingly difficult to troubleshoot failure points between the network and users. The monitoring of transmission quality has consequently become an important issue.

The QCAST IPTV (multicast) QoS (quality of service) monitoring tool, which consists of Probe and Web-Console, monitors the transmission quality on the network side. To monitor IPTV transmission quality, QCAST Probe measures packet loss and packet inter-arrival time fluctuations by keeping track of the sequence number of RTP (Real-time Transport Protocol) headers.

To achieve efficient measurement for multiple IPTV multicast channels on the network side, QCAST Probe uses filtering and systematic time-based sampling defined in PSAMP [3], which is suitable for keeping track of the RTP header sequence number. Accordingly, QCAST Web-Console collects this data via the IPFIX protocol [4] and then visualizes its own data. Visualization and investigation for IPTV channels on Web-Console let the operator easily check whether IPTV streams are being transmitted at an appropriate level of quality (**Fig. 5**).

There is also the voipScoop VoIP QoS monitoring tool, which monitors and analyzes VoIP transmission quality by a similar technique. voipScoop achieves signal-media-linked monitoring by first monitoring SIP (session initiation protocol) signaling information to identify the associated RTP media information and then monitoring the transmission quality of that RTP medium (**Fig. 6**).

At present, QCAST and voipScoop are undergoing prototype testing and demonstrations with actual equipment with an eye toward future implementation.

6. Multipurpose traffic monitoring technology

Since it is important for flow information to be used in various forms to cope with increasingly diverse network monitoring applications, we are researching and developing a traffic data mediation tool called ScoopFlow.

The core element of this technology is flow-based, or packet-based, traffic data mediation. This tool collects various types of traffic data from routers and distributes it to appropriate collectors (monitoring/analysis equipment). If necessary, it also controls routers that can collect the required flow- or packet-based data (**Fig. 7(a)**).

Finally, ScoopFlow deals comprehensively with diverse monitoring applications from three viewpoints: (1) monitoring all traffic by sampled flow information, (2) monitoring packet-based traffic data by focusing on specific traffic flows with ACL-based filtering, and (3) performing linked monitoring of signal and media traffic (**Fig. 7(b)**).

This traffic data mediation technology should be

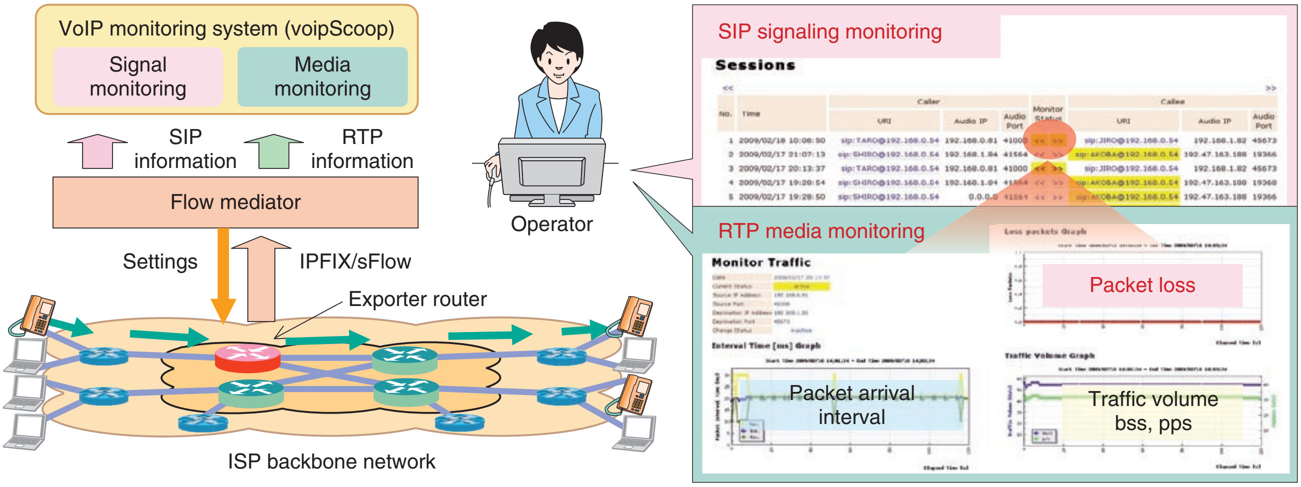
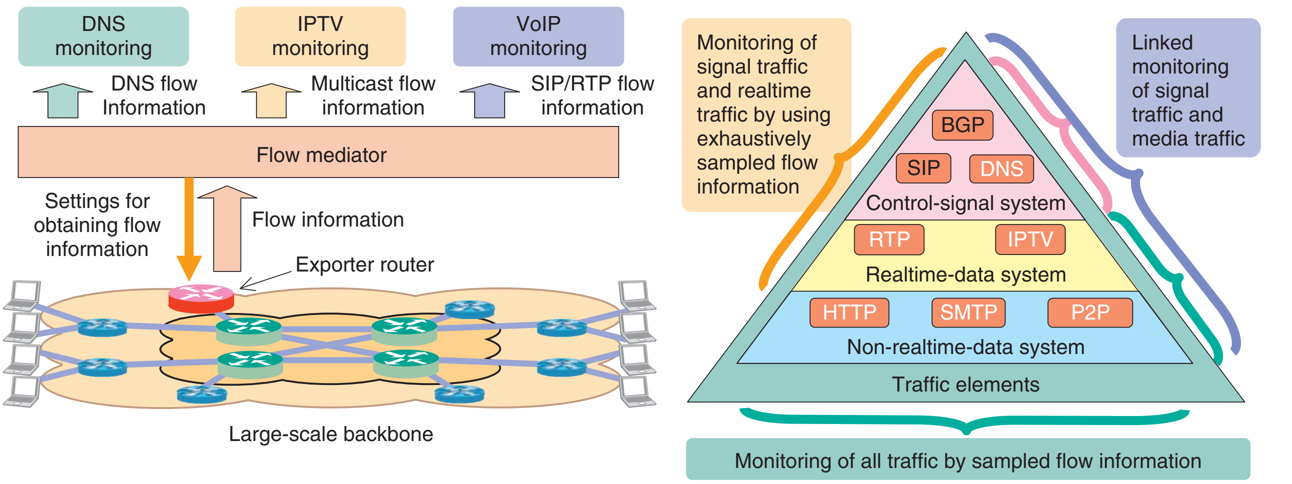


Fig. 6. VoIP quality monitoring tool (voipScoop).


DNS monitoring
IPTV monitoring
VoIP monitoring
DNS flow Information
Multicast flow information
SIP/RTP flow information
Flow mediator
Settings for obtaining flow information
Flow information
Exporter router
Large-scale backbone
Monitoring of signal traffic and realtime traffic by using exhaustively sampled flow information
Linked monitoring of signal traffic and media traffic
BGP
SIP
DNS
Control-signal system
RTP
IPTV
Realtime-data system
HTTP
SMTP
P2P
Non-realtime-data system
Traffic elements
Monitoring of all traffic by sampled flow information

(a) Distribution of diverse flow information according to monitoring purpose

(b) Comprehensive handling of diverse traffic monitoring applications

Fig. 7. Flow-mediation base technology (ScoopFlow).

deployed extensively in the network, and to that end, we are engaged in not only prototyping but also standardization activities through the IPFIX Working Group in the Internet Engineering Task Force (IEFT) [5].

7. Conclusion

Although we can expect attacks to become increasingly diversified from here on, we aim to efficiently raise the comprehensiveness of defenses by appropriately selecting and deploying the countermeasure technologies described in this article. In future research, we plan to conduct more field trials and demonstrations toward the practical deployment of these technologies.

Acknowledgment

This study was partly supported by the Ministry of Internal Affairs and Communications of Japan.

References

[1] "SAMURAI (Traffic Anomaly Detection System)". http://www.ntt.co.jp/RD/OFIS/active/2008pdfe/hot/pf/01.html

[2] T. Kondoh and K. Ishibashi, "Identifying Anomalous Traffic Using Delta Traffic," Proc. FloCon 2008, Savannah, GA, USA.

[3] T. Zseby, M. Molina, N. Duffield, S. Niccolini, and F. Raspall, "Sampling and Filtering Techniques for IP Packet Selection," RFC5475, Mar. 2009.

[4] B. Claise, S. Bryant, S. Leinen, T. Dietz, and B. Trammell, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information," RFC5101, Jan. 2008.

[5] A. Kobayashi, B. Claise, G. Muenz, and K. Ishibashi, "IPFIX Mediation: Framework," IETF Internet-Draft (Working Progress), Apr. 2010.

Junichi Murayama

Senior Research Engineer, Supervisor, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees from Waseda University, Tokyo, in 1989 and 1991, respectively. Since joining NTT in 1991, he has been engaged in R&D of ATM networks, IP VPNs, optical IP networks, and network security systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan and the Institute of Electrical Engineers of Japan.

Atsushi Kobayashi

Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

After joining NTT in 1994, he engaged in software development of the ISDN switching system and 3GPP cellular switching system. Next, he worked on MPLS backbone network designs. Once the commercial backbone network design was finished, he joined NTT Information Sharing Laboratories. He is currently studying IP traffic measurement systems.

Hiroshi Kurakami

Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in physics from Tohoku University, Miyagi, in 1991. Since joining NTT in 1991, he has been engaged in R&D of ATM networks, IP VPNs, and network security.

Takeshi Kuwahara

Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees from Waseda University, Tokyo, in 1995 and 1997, respectively. Since joining NTT in 1997, he has been engaged in R&D of IP VPNs, virtual private server systems, and network security. He is a member of IEICE.

Keisuke Ishibashi

Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.S. and M.S. degrees in mathematics from Tohoku University, Miyagi, in 1993 and 1995, respectively, and the Ph.D. degree in information science and technology from the University of Tokyo in 2005. Since joining NTT in 1995, he has been engaged in research on traffic issues in computer communication networks. He received IEICE's Young Researcher's Award in 2002, the Information Network Research Award in 2002 and 2010, and the Internet Architecture Research Award in 2009. He is a member of IEEE, IEICE, and the Operations Research Society of Japan.

Nobuhisa Miyake

Senior Research Engineer, Supervisor, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E., M.E., and Ph.D. degrees in electrical and communication engineering from Tohoku University, Miyagi, in 1985, 1987, and 1991, respectively. He joined NTT in 1991 and studied an information sharing platform including digital rights management technology. During 2001–2007, he was seconded to Internet Multifeed Co., where he developed and operated Internet data center and Internet exchange services. He has been studying technology for anomaly traffic detection and IPv6 since 2007. He received the IPSJ Industrial Achievement Award in 2008. He is a member of IEICE and the Information Processing Society of Japan.