Taxonomical Approach to the Deployment of Traceback Mechanisms

Takeshi Takahashi*, Hiroaki Hazeyama†, Daisuke Miyamoto*, Youki Kadobayashi*†
* National Institute of Information and Communications Technology, Tokyo, Japan
Email: takeshi_takahashi@ieee.org
† Nara Institute of Science and Technology, Nara, Japan

***Abstract*—The development of cyber society has fostered the emergence of e-commerce, which is active with business and private transactions. Nevertheless, it also emboldened malicious activities that damage users' profit in the society. Among these activities, Distributed Denial of Services (DDoS), which imposes an excessive workload on network entities such as hosts, is one of the most devastating form of attacks and can cause complete malfunctioning of cyber society's infrastructure. In order to counter DDoS and facilitate secure and reliable functioning of cyber societies, various types of traceback mechanisms have been proposed that trace the entire attack path or partial attack path of the attacks. In the future, networks will need to accommodate such traceback functionalities. This paper proposes a taxonomy of traceback mechanisms and describes their characteristics. It also discusses issues toward the deployment of the mechanisms over the Internet.**

I. Introduction

In the wake of vast development of Internet technologies, one can easily communicate with anybody around the world. This has contributed to the development of cyber society and e-commerce, which plays host to huge amount of business and private transactions. The modern-day Internet is not a mere communication tool but an indispensable instrument for the present cyber society era.

Nevertheless, this has also emboldened the range of malicious activities, which damage users' profit in the society, and the number of cyber crimes is on the rise. Internet security largely lags behind cyber threats since the development process prioritizes usability over security. Among the various types of cyber attacks, Distributed Denial of Service (DDoS) is one of the most severe, and can completely halt functioning of the Internet [1]. It sends a massive amount of unwanted traffic, with which the entire network's functioning is forced down. In order to protect network infrastructure against DDoS, attack traffic should be blocked at the most upstream router, i.e., the edge router of the attacker, or at one of the upstream routers en route from the attacker to the victim. Apart from DDoS, many forms of attacks impair the profit of cyber society users, and many of the attacks may cause the damages with a couple of packets. In order to claim compensation from the attackers, attacks need to be traced as evidence.

In order to identify the attack paths and the origin of attacks, traceback mechanisms have been researched and proposed. The term "traceback" refers to a technical and/or administrative process for reliably identifying the source of IP packets that may be spoofed by the sender and the paths or parts of paths used for attacks. A traceback mechanism is in fact used to identify the hackers' physical and logical location in real time at the time of the attack with the help of network elements such as a router or the hosts in the network. If the source address cannot be disguised, we may no longer need traceback mechanisms. By applying ingress filtering and related technologies [2–4], a network may be configured to ban the disguise of the source address. Albeit such technologies advance the security of the network, current networks still allow attackers to disguise source addresses.

Nevertheless, traceback mechanisms have not been widely deployed over the Internet. To advance their practical implementation, this paper introduces a taxonomy of traceback mechanisms. Since characteristics and applicability differ depending on the type of the mechanisms, the paper describes their usability and applicability. Based on the taxonomy, the paper also discusses issues toward traceback system deployment, particularly on the Internet.

The rest of this paper is organized as follows: Section II defines the scope of IP traceback, Section III introduces related works, Section IV proposes the taxonomy of traceback mechanisms and elaborates each type of mechanism, Section V discusses the applicability of traceback mechanisms to the Internet, Section VI discusses essential issues toward their practicality and deployability on the Internet, and Section VII concludes the paper.

II. Scope of IP Traceback

This paper uses the term "traceback" as a general term referring to technologies for tracing the source of an attack from the victim's location. Depending on the layer that runs the traceback mechanism, traceback mechanisms are classified into three: Ethernet traceback, IP traceback, and application traceback. An Ethernet traceback runs its mechanisms in the Ethernet layers, thus its applicability is limited within the Ethernet. Major schemes are found in [5–9]. Application traceback [10], [11] runs its mechanisms in the application layers. Therefore, regardless of the structure and architecture of the lower layers, it can trace the attack path though its applicability is limited to specific applications such as HTTP communication. An IP traceback runs its mechanisms in the IP layer. Therefore it traces attacks beyond routers and can generally be applied to Internet communication.

For the purpose of deployment of traceback mechanisms over the Internet, this paper focuses on IP traceback since the applicability of Ethernet and application tracebacks is rather limited. IP traceback mechanisms naturally investigates attack paths hop-by-hop. Many of them start from the router closest to the victim and interactively test its upstream links until they determine which is used to carry the attacker's traffic. Ideally, this procedure is repeated recursively on the upstream routers until the source is reached. This technique assumes that an attack remains active until the completion of a trace and is therefore inappropriate for attacks that are detected after the fact, occur intermittently, or modulate their behavior in response to a traceback.

Although such investigation operations are already taken by many ISPs inside their own administrative domains, they are usually conducted manually and are time-consuming. This paper focuses on IP traceback mechanisms that enable hosts and/or routers to automatically exchange necessary traceback information.

III. Related Works

There exist some taxonomies and surveys of traceback mechanisms. The proposed taxonomy is designed to be able to classify major traceback mechanisms and is able to classify all the traceback mechanisms introduced by the surveys [12–14].

Prior to the proposed taxonomy, Mirkovic et al. proposed a taxonomy of DDoS attack and DDoS Defense Mechanisms [15]. They discuss traceback as parts of DDoS attack prevention mechanisms. Different from [15], the proposed taxonomy particularly focuses on traceback mechanisms.

Santhanam et al. [16] provides a comprehensive taxonomy of IP traceback. The taxonomy provides various useful viewpoints that are also utilized as a basis of the proposed taxonomy. Different from the taxonomy, the proposed taxonomy was built from the viewpoint of deploying traceback mechanisms. For instance, traceback systems considering the different administration policies of Autonomous Systems (ASes) are needed to consider the deployment scenarios of traceback mechanisms over the Internet.

Based on the taxonomy, this paper describes the usability and applicability of different types of traceback mechanisms, and then leads the discussion of such deployments and their hurdles.

IV. Taxonomy of IP Traceback Mechanisms

This section proposes the taxonomy of IP traceback mechanisms as shown in Table I. The taxonomy classifies IP traceback mechanisms into Intra-AS traceback and Inter-AS traceback from the viewpoint of the administrative domain. The former assumes that the entire network is under control while the latter assume that an AS may have different administrative policies regarding traceback system implementation. Note, Intra-AS traceback mechanisms can be used as a basis of Inter-AS traceback mechanisms, and some may be applied to Inter-AS traceback systems without any significant modification.

The taxonomy further classifies Intra-AS traceback mechanisms into Traffic Monitoring type and Packet Monitoring type from the viewpoint of the target of analysis. The former analyzes the traffic/stream of an attack while the latter analyzes each packet.

The taxonomy further classifies the Traffic Monitoring type into Controlled Flooding type and Pattern Analysis type. The former controls traffic volume, detects anomalies and traces the attack source while the latter analyzes traffic pattern, identifies anomalies and traces the attack source.

The taxonomy also classifies the Packet Monitoring type further into Verbatim Routing type and Modified Routing type from the viewpoint of packet routing. The former inspects packets on the routers on the attack paths while the latter forwards packets to a certain point on a network, where they are inspected.

The taxonomy further classifies the Verbatim Routing type into Packet Marking type, Messaging type, Packet Logging type and Hybrid type from the viewpoint of routers' behaviors. The Packet Marking type modifies, appends, and/or encapsulates packets at routers in order to mark them. The modified packets are analyzed at the host node that is usually a victim node. The Messaging type sends messages from routers to victims, be it either deterministically or probabilistically. The Packet Logging type stores audit logs of forwarded packets at routers. This type is designed to identify the true source of even a single particular IP packet, and require the intermediate routers to log the passage of IP packets. The Hybrid type selectively does either storing audit logs of forwarded packets, marking packets, or sending messages.

Each category of traceback mechanism mentioned above is detailed in the following sections.

A. Controlled Flooding Type

This type is one subtype of Traffic Monitoring type that monitors traffic and/or streams instead of individual packets. It controls traffic volume and detects anomalies for each of the links between routers, and traces the attack source. One prominent scheme proposed by Burch et al. [17] loads the links of the suspected path and observes the drop of the attack traffic rate. If a drop is observed, the loaded link is judged as a path of the attack. The underlying assumption is that DDoS attacks heavily load the links on the attack path.

This type of scheme enjoys higher confidentiality of information than the Packet Monitoring type since it does not investigate packet contents. However, it is only applicable to traffic-consuming attacks such as DDoS and not to any non-traffic-consuming attacks. Moreover, loading unnecessary traffic is not preferred, especially in a large network.

B. Pattern Analysis Type

This type of scheme is, as with Controlled Flooding type, one subtype of Traffic Monitoring type. It analyzes traffic pattern to identify anomalies, with which it traces the source of attacks. Albeit concrete traceback mechanisms of this type is still under study, by applying the traffic pattern analysis

TABLE I
TAXONOMY OF TRACEBACK MECHANISMS

Categories				Characteristics	Prominent proposals
Intra-AS traceback	Traffic Monitoring	Controlled Flooding		controls traffic volume and detects anomalies	[17]
		Pattern Analysis		analyzes traffic pattern to identify anomalies	[18], [19]
	Packet Monitoring	Verbatim Routing	Packet Marking	Inserts traceback information into the IP header at routers	[20–36]
			Messaging	Sends messages including traceback information at routers	[37], [38]
			Packet Logging	Logs packets at routers and check whether specific packets have traversed the routers	[39–45]
			Hybrid	Marks packets or sends messages while logging packets	[46–49]
		Modified Routing		Forwards packets to specific point in the network for inspection	[50–53]
Inter-AS traceback				Exchanges traceback information between ASes while allowing them to implement their own traceback mechanisms within their networks	[54–60]

schemes [18], [19], they should be possible to trace the attack source.

Due to the nature of Traffic Monitoring type, this type enjoys higher confidentiality of information than the Packet Monitoring type with the limited applicability problem, as with Controlled Flooding type. Different from Controlled Flooding type, this type does not have to load unnecessary traffic in the network.

C. Packet Marking type

This type of scheme modifies, appends, and/or encapsulates packets at routers in order to mark the packets. The modified packets are analyzed at the host node that is usually a victim node.

One major scheme is Probabilistic Packet Marking (PPM) [20], [25], which marks packets probabilistically as shown in Figure 1. It inserts router information into a packet on the routers along the attack connection chain so that the victim node can construct the attack connection chain using the inserted information, even if an attacker uses a spoofed IP address.

Although this scheme is useful under certain conditions, it changes the header information, i.e., IP identification field necessary for IPsec AH header authentication. Therefore, in order to run the scheme, we need to ensure that the IPsec AH header authentication is not used or that some mechanisms compensating the header information change are implemented. The same difficulties apply not only to the IPv4 environment but also to the IPv6 environment. The scheme is therefore used within controllable networks, e.g., within an AS, and cannot be globally used on the Internet.

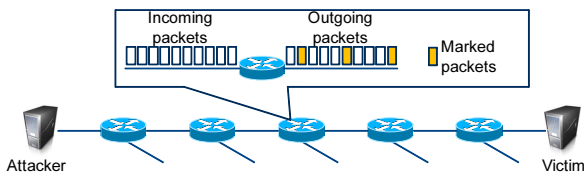

Fig. 1. Concept of PPM

Based on the PPM, some modifications have been proposed [26–28]. Dean et al. [26] utilized algebraic techniques. More specifically, their scheme encodes path information as points on polynomials. It then uses algebraic methods from coding theory to reconstruct the polynomials at the victim. Yaar et al. [27] preserved the advantages of PPM and can perform traceback even after a very small number of attack packets with minimal processing overhead. This is achieved through an approach for upstream router map reconstruction, a one-bit field to measure up to 32 hops to the distance to the marking router, node-based instead of edge-based marking, and a fast scheme to identify the marking router. Goodlich [28] used large checksum cords to ”link” message fragments in a highly scalable manner, for the checksums to serve both as associative addresses and data integrity verifiers. Lu et al. [31] introduced Random Packet Marking (RPM), which uses network topological information and reduces computational cost and difficulties. In order to enable incremental deployment, Castelucio et al. [34] and Muthuprasanna et al. [35] introduce overlay network.

Different from PPM and its variants, Yaar et al. proposed a deterministic scheme called a Path Identifier (Pi), a packet marking mechanism in which a path fingerprint is embedded in each packet [32], [33]. This is a per-packet deterministic mechanism and allows the victim to take a proactive role in defending against DDoS attacks by using the Pi mark to filter out packets matching the attackers' identifiers on a per packet basis.

Instead of modifying the packet header, some schemes mark packets by encapsulating them. Chang et al. proposed Deciduous [30], which is based on an assumption that the complete network topology is known to the system, and used IPSec packet encapsulation in order to mark packets. The underlying principle is that if there is an IPSec security association between an arbitrary router and the victim, and the attack packets detected are authenticated by the association, the attack originates on some device further than this router. If the packets of the attack are not authenticated by this security association, the attack originates on some device between the router and the victim. By establishing these security associations, it is possible to identify a single router or group of routers from which the attack was initiated.

On the other hand, hybrid schemes of logging type mentioned below and marking type are also proposed in [46–49]. Albeit such schemes enjoy the routers' ability to trace single

packet as the one of logging type and reduces the amount of storage required in the router by marking packets, they still render the packet header information and cause the routing problem of Packet Marking types such as the IPsec and VPN problems.

D. Messaging type

This type of scheme sends messages including traceback information from routers to victims. Similar to PPM, most of the schemes let routers probabilistically send such messages, which is best described by ICMP Traceback (iTrace) [37].

The concept of iTrace is described in Figure 2. iTrace lets the router residing in the connection chain create one ICMP packet for a certain number of packets passing through it on the way to a victim node. The ICMP packet generated is then forwarded to the victim node. All the gathered ICMP packets are used to determine the connection chain to the victim node at the destination node. The ICMP packet works as an iTrace message, which includes traceback information such as the IP address of a router residing in the connection chain in the ICMP payload.

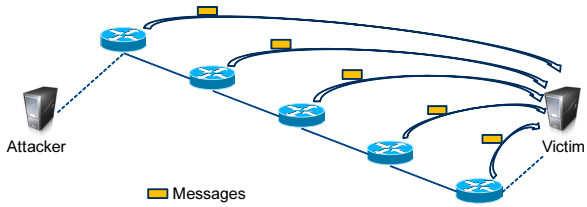

Fig. 2. Concept of iTrace

Based on iTrace, a modification was proposed by Mankin et al. [38], who described a simple enhancement that introduces an extra bit in the routing and forwarding process. With the new ”intention-bit”, ICMP messages are created. By meticulously setting up the policy to put the ”intention-bit” on, the number of ICMP messages is significantly reduced.

The schemes of this type, however, are not developed further except the aforementioned major works due to the two main reasons. First reason is that the schemes increase the traffic volume since it newly create ICMP messages even if any attacks do not actually take place and the amount of increased traffic is still nonnegligible. Second reason is that many routers and firewalls are configured to drop ICMP messages for security reasons, thus this scheme is incompatible with the routers with such configurations.

E. Packet Logging type

This type of scheme stores audit logs of forwarded packets at routers probabilistically or deterministically in order to support tracing of attack flows. They are designed to identify the true source of a particular IP packet, and require the intermediate routers to log the passage of IP packets. Victims consult upstream routers to reconstruct attack paths in a hop-by-hop manner.

Many packet logging schemes have been proposed for monitoring traffic at routers [61–63]. Some of them are already implemented in the routers; For instance, sflow [61] is already implemented in the routers from Foundry Networks, Inc. (currently Brocade Communications Systems, Inc.) and ALAXALA Networks Corporation while netflow [62] is already implemented in the routers from Cisco Systems, Inc. Conventionally, operators can manually trace the source of attacks based on the logged data.

A great deal of research has been conducted on reducing the storage size and human operations. One major outcome is Hash-based IP traceback [39], [40], [43], a scheme officially called a Source Path Isolation Engine (SPIE). In hash-based traceback, every router captures partial packet information of every packet that passes through the router in order to in the future determine if that packet passed through it. In this scheme such routers are called data generation agents (DGAs), and DGA functionality is implemented on the routers. The network is logically divided into regions. In every region SPIE collection and reduction agents (SCARs) connect to all DGAs, and are able to query them for necessary information. The SPIE traceback manager (STM) is a central management unit that communicates to Intrusion Detection Systems (IDSs) of the victims and SCARs.

As packets traverse the network, packet digests get stored in the DGAs. In this scheme, constant fields from the IP header and the first eight bytes of the payload of each packet are hashed by several hash functions to produce several digests. The digests are stored in a space-efficient data structure called a bloom filter [64], which reduces storage requirements by several orders of magnitude. When a given bloom filter is about 70 % full, it is archived for later querying, and another one is used.

Some modification proposals also exist. Sung et. al. [41] introduced a more scalable scheme that samples and logs a small percentage of packets.

Different from the above schemes, Duffield et al. proposed Trajectory sampling [42], which samples packets on the routers residing on the potential attack paths instead of on every router. Zhang et al. [44] proposed a scheme using bloom-filter with modifications reducing the false positive problems.

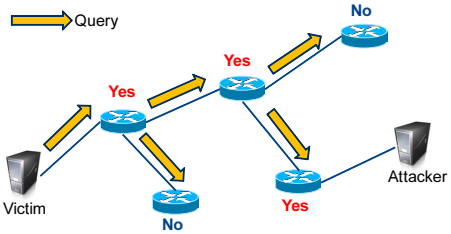

Fig. 3. Concept of hash-based logging scheme

F. Hybrid type

This type of scheme hybrids the mechanisms of Packet Marking type, Messaging type, and Packet Logging type.

Albeit several types of such hybrids are logically available, only the ones of Packet Marking type and Packet Logging type are developed further practically since the Messaging type is regarded as impractical as discussed in IV-D. For instance, Gong et al. [46] proposed a hybrid scheme that records network path information partially at routers and partially in packets. Depending on the availability of free space in the marking field of the forwarded packets, routers decide where to record network path information. If there is free space available in the marking field, routers write their identification information into the packets; otherwise, routers compute and record the packet digests and then clear the marking field. Compared to the Packet Logging type, the needed storage on routers are reduced though it inherits the disadvantage of Packet Marking type.

G. Modified Routing type

This type of scheme forwards packets to a certain network point, where the packets are inspected. These are useful only inside a controllable network domain, and cannot be deployed on an Internet-wide scale. Major schemes in this category are Shunt routing, Sinkhole routing, and Blackhole routing.

Shunt routing forwards packets to a certain point in the network, where they are inspected. One prominent such mechanism is CenterTrack [50], an overlay network-based traceback mechanism, which introduces a Tracking Router (TR), a special type of router connected with the edge router physically or virtually with an IP tunnel, called generic route encapsulation (GRE), in a network. All TRs should also be connected to a central TR via IP tunnels, resulting in creating a total overlay network. If an attack is detected, a victim node sends the relevant traceback information to a TR. The TR uses the information to analyze and block unwanted traffic, identify the origin of attacks, and construct the attack connection chain. Similar to CenterTrack, Arbor Networks provide a service called ”Peakflow” [51], which collects all the incident information at the server of Arbor Networks and analyzes network incidents.

Similar to Shunt routing is Sinkhole routing, which forwards packets to a certain point on the network to inspect them, but it discards the packets there instead of delivering them to the destination.

Different from Sinkhole routing, Blackhole routing forwards packets to /dev/null instead of certain network inspection points at the border routers. In this way, routers can save CPU resources. One prominent scheme is [52], which describes an operational technique that utilizes a sinkhole tunnel, which is implemented at all possible entry points from which attacks can pass into the destination/attacked AS. Using the Border Gateway Protocol (BGP) community technique, traffic destined for the attacked/targeted host could be re-routed to a special path (tunnel) where a sniffer could capture it for analysis. After being analyzed, traffic exits the tunnel and is routed normally to the destination host. In other words, the traffic will pass through the network to a sniffer without altering the next hop information of the destination network. All routers within the destination/attacked AS iBGP domain will have the proper next hop address, and only the entry point router will have the altered next hop information. Through the analysis, the edge routers within the destination/attacked AS from which the attack emanates are revealed.

Note, though Sinkhole and Blackhole routing identifies partial attack path, they focus on DDoS countermeasures rather than tracing back the attack source at this moment.

H. Inter-AS traceback

In order to deploy an Internet-wide traceback system, differing administration policies and regulation among countries and organizations need to be considered. Albeit an Inter-AS traceback mechanism may work in a network environments, it is hard to assume that all ASes adopt and deploy the same, single traceback mechanism. Moreover, some ASes may wish to conceal which traceback mechanism they deploy inside their own AS.

Inter-AS traceback mechanisms are considered for addressing such issues. They define the communication between ASes, and allow them to implement arbitrary traceback mechanisms inside their own networks following their security policies. With this type of mechanisms, ASes are not required to implement a traceback mechanism on all the routers provided one representative router implement the scheme, and the ASes may internally implement their own traceback mechanisms that are concealed from outside.

Gong et al. applied the concept of AS on SPIE and proposed the communication scheme between ASes [54], [55]. The scheme utilizes BGP attribute to understand the network topology. When a victim traces the attack path back to the attack source, it dispatches queries to the routers implementing the traceback mechanism level-by-level. Note, this scheme has a capability of incremental implementation.

Hazeyama et al. introduced InterTrack, which proposes communication between ASes based on BGP [56–58]. InterTrack records the hashes of the IP headers and the first 16 bytes of payload [65]. InterTrack with basic mode traces attack paths hop-by-hop, thus it does not require the network topological information. Note, it has another mode enabling incremental implementation mode. The test implementation over ISP networks are introduced in [66], [67]. The implementation of the scheme is found in [68].

Castelucio et al. [59] introduced an Inter-AS traceback mechanism based on the packet marking scheme. It uses the BGP, particularly the Community Attribute of BGP Update Message [69] in order to discover which ASes have the proposed traceback system deployed and to allow partial deployment.

Moriarty also argued the need for Inter-AS communication and, apart from the traceback mechanisms themselves, defined a standard RID message format so that the traceback information can be exchanged on a timely basis [60].

V. Applicability to the Internet

As discussed in Section IV, there exist assorted types of traceback mechanisms. Nevertheless, the applicability and

usability of such mechanisms differ depending on the purpose and environment. This section discusses the applicability of traceback mechanisms to the Internet.

In order to deploy traceback mechanisms on the Internet, Inter-AS traceback mechanisms enabling each AS to deploy its own security policy inside its network are needed as discussed in IV-H. Although Inter-AS traceback mechanisms can be based on arbitrary Intra-AS traceback mechanisms, the Packet Logging types are suitable due to the following reasons;

- Modified Routing type cannot be deployed on the uncontrollable network: the routing of the Internet cannot be changed, thus this type can not be deployed over the Internet.
- Packet Marking type may affect the proper transaction of packets that use IPsec.
- Messaging type may not work with many firewalls and routers since they ignore ICMP messages. Moreover, this type may incur non-trivial extra traffic.
- Controlled Flooding type may work over the Internet. However, it floods excessive amount of unwanted traffic over the network.
- Traffic Analysis type is still immature for implementation. Also, this type has difficulties to trace non-traffic-consuming attacks.

In addition to the Packet Logging type, well-tuned hybrid of Marking and Packet Logging types may work correctly if it only marks packets that do not cause any problem by marking them. The Hybrid type is flexible enough not to mark packets and log the digest of the packets instead. For instance, it logs packets that use IPsec while it otherwise marks packets. In this way, the disadvantage of Packet Marking type can be avoided.

On the other hand, although the importance of tracing DDoS attacks still remain high, other attacks that use only a few packets need to be traced in the future. In order to trace such attacks, single packet needs to be traced, and thus Packet Logging type including its hybrids is one of the suitable mechanisms.

Hence, Inter-AS traceback mechanisms based on logging type including its hybrid seem to be appropriate for the deployment over the Internet.

VI. Issues Toward Practical Implementation

This section discusses the issues toward practical implementation of logging-type Inter-AS traceback mechanisms on the Internet. This section begins discussion from the viewpoint of technical enhancement, especially packet buffering capabilities, and continues it from the perspective of legal restrictions, privacy concerns, deployment feasibility, and security of traceback systems.

A. Packet Buffering Capabilities

The traceback mechanisms mentioned in Section IV-H buffer packets at the transient routers, which are required to have sufficient storage and computational power. The needed storage size will increase following the development of network bandwidth and speed. The system must cope with much faster network traffic following the development of network technologies. While we may store only the hashes of the headers and 16 bytes of sampled packets, we still need to have a surplus of storage. Albeit hardware implementation of the algorithm and implementation of high-performance computers would help in coping with this issue, they depend on the amount of allowed investment for this system. This buffering size issue cannot be solved simply by hardware implementation.

To handle this issue, traceback mechanisms may utilize packet sampling functions. The difficulties here is to choose a proper sampling rate; the rate can be low to cope with DDoS attacks while it needs to be as high as possible in order for routers not to miss any important information for coping with non-DDoS attacks such as private information leakage theft.

Two directions of future research on this sampling issue are dynamic change of sampling rate and selective buffering. The former enables routers to change the sampling rate dynamically depending on the context of the network and/or the type of attacks; when the network seems to be unsafe, the sampling rate needs to be higher. Selective buffering enables routers to buffer packets selectively; only potentially malicious packets need to be buffered instead of all the sampled packets.

At the same time, the number of packets used for the inquiry needs to be aggregated in order to improve the success rate of tracing back. Performing such aggregation improves the success rate of tracing back. Hence, $H \propto b, H \propto f$, where H denotes traceback success rate, b does the bulk number, f does the sampling frequency. Since H is dependent on the value b and f, the traceback success rate H can be denoted as $H(b, f)$. Proper schemes to choose suitable values of b and f need to be further researched.

Apart from sampling functions, we may consider the Hybrid type that selectively either logs or marks packets. By meticulously controlling the number of logged packets, the amount of needed storage can be reduced though the proper control of such scheme still needs further research.

B. Legal Restrictions

Traceback mechanisms can be applied to many systems. For instance, they can be applied to e-commerce systems to provide evidence of malicious activities in cyber societies. Albeit these mechanisms are still under development, they can be already applied to specific applications.

Nevertheless, the mechanisms' applicability from a legal restriction standpoint is still disputable. As a nature of cyber society, threats come from beyond national borders; and therefore applying laws across cyber society is extremely complicated. Packets traversing over countries A and B are subject to different laws. The differences of those laws are sometimes crucial in performing traceback mechanisms.

One such issue is privacy law. Some countries see traceback mechanisms as a violation of this law since they access the message contents. The information that traceback mechanisms may utilize without violating privacy laws may differ from one country to another. For instance, some countries allow

traceback mechanisms to use the first several bits of the payload of the IP packet while others only allow usage of the IP packet header. However, it is disputable whether traceback mechanisms can work effectively if they use no information from the IP packet payload.

Another such issue is national security. Tracebacks tend to be considered as an issue related to national security; thus it needs to be clarified to what extent traceback mechanisms can work without violating such security.

Traceback systems cannot work beyond national borders unless they tackle such legal issues. Although the importance of such systems is acknowledged by many countries, modification and adaptation of laws are required to deploy them.

C. Privacy Concerns

Privacy concerns are another issue facing traceback mechanisms. Hash-based traceback systems need to use part of the packet's raw data, which needs to be exchanged between routers and sometimes between ASes. Users may resultantly be reluctant to use the mechanisms since the query itself leaks unfavorable information outside the users' organizations.

Hence, schemes to exchange traceback information without unveiling the contents of the information are needed. One expected scheme is privacy preserving protocol [70], which enables information queries with only hash information. Apart from this scheme, [71] provides a scheme to retrieve information from bloom filters without unveiling the contents by using a group cipher though this scheme requires a trustable third party. In utilizing such schemes, no one but the contents holder needs to know the contents of packets.

D. Deployment Feasibility

Traceback mechanisms need to be widely implemented over the Internet in order to secure their practicality, and the penetration rate is one of the most important indicators. Without a high penetration rate, traceback mechanisms cannot work effectively.

From the viewpoint of organization with a network, such as an Internet Service Provider (ISP), traceback systems need to be installed in its own network. In terms of practicality, traceback software needs to be installed at the interfaces of routers that are connected to external networks. For large organizations, the routers have many interfaces, and each needs to install such software. Despite the implementation difficulties, the motivation of implementing such software is currently rather low. An organization implementing a traceback can gain very little merit unless neighboring organizations do the same since the traceback mechanisms may not work effectively without their wide deployment.

Indeed, a fairly high penetration rate is needed in order to let traceback mechanisms work practically. Even if one organization implements the system, most of the traceback mechanisms cannot provide any useful information unless neighboring organizations also implement one. Miyamoto et al. [72] addressed the effectiveness of traceback systems based on the penetration rate. Although the required penetration rate for sufficient effectiveness of the traceback system differs depending on the network topology, a fairly high penetration rate is always required.

Some schemes considering the incremental implementation increases their effectiveness regardless of low penetration rate. For instance, Castelucio et al. [59] argues that their incremental scheme may work efficiently with relatively low penetration rate if the scheme is strategically deployed over the network.

In order to deploy traceback mechanisms over the Internet, such scheme enabling incremental deployment and providing fairly high success rate of tracing back the attack path with rather low penetration rate need to be considered.

E. Traceback System Security

In order to deploy a traceback system on an Internet-wide scale, it is necessary to consider the vulnerabilities and threats that the system itself exposes. For instance, an attacker may set up a router that confuses the traceback mechanisms in the network or conceals malicious activities from the mechanisms.

Abuse of traceback systems also needs to be considered. For instance, an attacker may intentionally create a DDoS attack from third-party network by using a bot net and sue for compensatory damages with the traceback information as evidence.

The usage of traceback information also needs to be considered. Since the information itself may contain sensitive information, caution is required. It would be appropriate for an industry association and/or international authority to build some guidelines for this and based on these, proper adjustment of laws and regulations needs to be considered in each country.

VII. Conclusion

This paper proposed a taxonomy of traceback mechanisms. Based on the taxonomy, it detailed individual types of traceback mechanisms, and clarified their applicability. With that foundation, the paper discussed the issues toward the deployment of such mechanisms over the Internet. The issues include not only technical matters but also legal restrictions, privacy concerns, penetration rate, and the security of the traceback system itself. As the development of traceback mechanisms move forward, society needs to begin preparing the adoption and adaption of traceback systems.

References

[1] D. McPherson, *et al.*, "WorldWide Infrastructure Security Report Volume V," Arbor Networks, Sep. 2010.

[2] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," Internet Engineering Task Force, RFC 2267, Jan. 1998.

[3] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," Internet Engineering Task Force, RFC 2827, May 2000.

[4] F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," Internet Engineering Task Force, RFC 3704, Mar. 2004.

[5] Cisco Systems Inc., "Catalyst 6500 Series Command Reference, 8.7 - format to ping ethernet," *http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/command/reference/ghi_cmd.html#wp1030529*.

[6] H. Hazeyama, H. Matsumoto, and Y. Kadobayashi, "Design of an FDB based Intra-domain Packet Traceback System," in *ARES*, 2008.

[7] H. Hazeyama, M. Oe, and Y. KADOBAYASHI, "A layer-2 extension to hash-based ip traceback," *IEICE transactions on information and systems*, Nov. 2003.

[8] M. Andreou and A. van Moorsel, "COTraSE: Connection Oriented Traceback in Switched Ethernet," *Journal of Information Assurance and Security*, 2009.

[9] M. Snow and J. Park, "Link-Layer Traceback in Ethernet Networks," *IEEE LANMAN*, 2007.

[10] D. Miyamoto, H. Hazeyama, and Y. Kadobayashi, "Detecting Methods of Virus Email based on Mail Header and Encoding Anomaly," in *ICONIP*, Nov. 2008.

[11] K. Takemori, *et al.*, "Host-based traceback; tracking bot and C & C server," in *ICUIMC*, 2009.

[12] S. Vincent and J. I. J. Raja, "A survey of ip traceback mechanisms to overcome denial-of-service attacks," 2010.

[13] A.John and T. Sivakumar, "Ddos: Survey of traceback methods," in *IJRTE*, 2009.

[14] A. Belenky and N. Ansari, "On IP traceback," *IEEE Communications magazine*, July 2003.

[15] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, April 2004.

[16] L. Santhanam, A. Kumar, and D. Agrawal, "Taxonomy of IP traceback," *Journal of Information Assurance and Security*, 2006.

[17] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in *USENIX*, 2000.

[18] M. S. Kim, *et al.*, "A wavelet-based approach to detect shared congestion," in *SIGCOMM*, 2004.

[19] A. Magnaghi, T. Hamada, and T. Katsuyama, "A wavelet-based framework for proactive detection of network misconfigurations," in *NetT*, 2004.

[20] S. Savage, *et al.*, "Network Support for IP Traceback," *IEEE/ACM Trans. Networking*, June 2001.

[21] A. Belenky and N. Ansari, "Tracing multiple attackers with deterministic packet marking (dpm)," 2003.

[22] V. Bhaskaran, A. Natarajan, and S. Sivanandam, "A new promising IP traceback approach and its comparison with existing approaches," *Inform. Technol. J*, 2007.

[23] T. W. Doeppner, P. N. Klein, and A. Koyfman, "Using router stamping to identify the source of IP packets," in *CCS*, 2000.

[24] H. Alwis, *et al.*, "Topology based packet marking for IP traceback," in *ATNAC*, 2006.

[25] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Scheme for IP Traceback," *IEEE INFOCOM*, 2001.

[26] D. Dean, M. Franklin, and A. Stubblefield, "An Algebraic Approach to IP Traceback," *ACM Transactions on Information and System Security*, May 2002.

[27] A. Yaar, A. Perrig, and D. Song, "Fit: fast internet traceback," *INFOCOM*, Mar. 2005.

[28] M. T. Goodrich, "Probabilistic packet marking for large-scale IP traceback," *IEEE/ACM Trans. Netw.*, 2008.

[29] M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," in *CCS*, 2002.

[30] H. Y. Chang, *et al.*, "Deciduous : Decentralized Source Identification for Network-based Intrusions," in *IFIP/IEEE IM*, 1999.

[31] L. Lu, M. C. Chan, and E.-C. Chang, "A general model of probabilistic packet marking for ip traceback," in *ASIACCS*, 2008.

[32] A. Yaar, A. Perrig, and D. Song, "Pi: a path identification mechanism to defend against ddos attacks," in *Symposium on Security and Privacy*, may. 2003.

[33] A. Yaar, A. Perrig, and D. Song, "Stackpi: New packet marking and filtering mechanisms for ddos and ip spoofing defense," *Selected Areas in Communications, IEEE Journal on*, oct. 2006.

[34] A. Castelucio, *et al.*, "Intra-domain ip traceback using ospf," in *LANOMS*, 2009.

[35] M. Muthuprasanna, *et al.*, "Coloring the internet: Ip traceback," in *ICPADS*, 2006.

[36] Y. Xiang, W. Zhou, and M. Guo, "Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks," *Parallel and Distributed Systems, IEEE Transactions on*, 2009.

[37] S. Bellovin, M. Leech, and T. Taylor, "ICMP Traceback Message," Feb. 2003, IETF, Internet Draft, draft-ietf-itrace-04.txt.

[38] A. Mankin, *et al.*, "On Design and Evaluation of "Intention-Driven" ICMP Traceback," in *ICCCN*, Oct. 2001.

[39] A. C. Snoeren, "Hash-based ip traceback," in *SIGCOMM*, 2001.

[40] A. C. Snoeren, *et al.*, "Single-Packet IP Traceback," *IEEE/ACM Trans. Networking*, Dec. 2002.

[41] M. Sung, *et al.*, "Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation," *IEEE/ACM Trans. Networking*, Dec. 2008.

[42] N. Duffield and M. Grossglauser, "Trajectory sampling with unreliable reporting," *IEEE/ACM Trans. Netw.*, 2008.

[43] W. Strayer, *et al.*, "Spie-ipv6: single ipv6 packet traceback," nov. 2004.

[44] L. Zhang and Y. Guan, "Topo: A topology-aware single packet attack traceback scheme," in *Securecomm and Workshops*, sept. 2006.

[45] S. Matsuda, *et al.*, "Design and implementation of unauthorized access tracing system," 2002.

[46] C. Gong and K. Sarac, "A more practical approach for single-packet ip traceback using packet logging and marking," *IEEE Trans. Parallel Distrib. Syst.*, October 2008.

[47] B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for ip traceback," *IEEE Trans. Parallel Distrib. Syst.*, May 2006.

[48] S. Malliga and A. Tamilarasi, "A hybrid scheme using packet marking and logging for ip traceback," *Int. J. Internet Protoc. Technol.*, April 2010.

[49] K. Choi and H. Dai, "A marking scheme using huffman codes for ip traceback," in *I-SPAN*, May 2004.

[50] R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," in *USENIX*, Aug. 2000.

[51] Arbor Network, "peakflow," *http://arbornetworks.com*.

[52] D. Turk, "Configuring BGP to Block Denial-of-Service Attacks," Internet Engineering Task Force, RFC 3882, Sept. 2004.

[53] W. Kumari and D. McPherson, "Remote triggered black hole filtering with unicast reverse path forwarding (urpf)," Aug. 2009, RFC 5635.

[54] T. Korkmaz, *et al.*, "Single packet ip traceback in as-level partial deployment scenario," *Int. J. Secur. Netw.*, 2007.

[55] C. Gong, *et al.*, "Single packet ip traceback in as-level partial deployment scenario," in *GLOBECOM*, 2005.

[56] H. Hazeyama, *et al.*, "Intertrack: A federation of ip traceback systems across borders of network operation domains," in *ACSAC, Technology Blitz Session*, 2005.

[57] H. Hazeyama, *et al.*, "An autonomous architecture for inter-domain traceback across the borders of network operation," in *ISCC*, 2006.

[58] H. Hazeyama, Y. Matsumoto, and Y. Kadobayashi, "Message Forwarding Strategies for Inter-AS Packet Traceback Network," in *JWIS*, August 2007.

[59] A. Castelucio, A. Ziviani, and R. Salles, "An as-level overlay network for ip traceback," *Network, IEEE*, 2009.

[60] K. Moriarty, "Real-time Inter-network Defense (RID)," Internet Engineering Task Force, RFC 6045, Nov. 2010.

[61] P. Phaal, S. Panchen, and N. McKee, "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks," Internet Engineering Task Force, RFC 3176, Sept. 2001.

[62] B. Claise, "Cisco Systems NetFlow Services Export Version 9," Internet Engineering Task Force, RFC 3954, Oct. 2004.

[63] B. Trammell, *et al.*, "Specification of the ip flow information export (ipfix) file format," Oct. 2009, rFC 5655.

[64] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, 1970.

[65] T. Kai, A. Hashiguchi, and H. Nakatani, "Proposal for and evaluation of improved method of hash-based ip traceback system," in *CSA*, 2009.

[66] K. Wakasa, *et al.*, "Demonstration Experiments Towards Practical IP Traceback on the Internet," in *IEEE-CCNC*, January 2010.

[67] K. Wakasa, *et al.*, "Large Scale Demonstration Experiments Towards Acheiving Practical Traceback on the Internet," in *WAIS*, Febrary 2010.

[68] http://intertrack.naist.jp/, "Ip traceback - research iplab - naist iplab," 2010.

[69] R. Chandra, P. Traina, and T. Li, "BGP Communities Attribute," Internet Engineering Task Force, RFC 1997, Aug. 1996.

[70] R. Nojima and Y. Kadobayashi, "Cryptographically secure bloom-filters," *Transactions on Data Privacy*, 2009.

[71] S. M. Bellovin and W. R. Cheswick, "Privacy-enhanced searches using encrypted bloom filters," 2004.

[72] D. Miyamoto, H. Hazeyama, and Y. Kadobayashi, "A Comparative Evaluation of Traceability in CJK Internet," in *JWIS*, Aug. 2009.