3-3 Studies on Countermeasures for Thwarting Spoofing Attacks — Cases of IP Address Spoofing and Web Spoofing —

MIYAMOTO Daisuke, HAZEYAMA Hiroaki, and KADOBAYASHI Youki

This article intends to give case studies for of thwarting spoofing attack. Spoofing is widely used when attackers attempt to increase the success rate of their cybercrimes. In the context of Denial of Service (DoS) attacks, IP address spoofing is employed to camouflage the attackers' location. In the context of social engineering, Web spoofing is used to persuade victims into giving away personal information. A Web spoofing attacker creates a convincing but false copy of the legitimate enterprises' web sites. The forged websites are also known as phishing sites.

Our research group developed the algorithms, systems, and practices, all of which analyze cybercrimes that employ spoofing techniques. In order to thwart DoS attacks, we show the deployment scenario for IP traceback systems. IP traceback aims to locate attack source, regardless of the spoofed source IP addresses. Unfortunately, IP traceback requires that its systems are widely deployed across the Internet. We argue the practical deployment scenario within Internets of China, Japan, and South Korea.

We also develop a detection method for phishing sites. Currently, one of the most important research agenda to counter phishing is improving the accuracy for detecting phishing sites. Our approach, named HumanBoost, aims at improving the detection accuracy by utilizing Web users' past trust decisions. Based on our subject experiments, we analyze the average detection accuracy of both HumanBoost and CANTINA.

Keywords
IP spoofing, Web spoofing, Internet emulation, IP traceback, Machine learning

1 Introduction

DoS attacks exhaust the resources of remote hosts or networks that are otherwise accessible to legitimate users. Especially, a flooding attack is the typical example of DoS attacks. In the case of the flooding attack, the attackers often used the source IP address spoofing technique. IP address spoofing can be defined as the intentional misrepresentation of the source IP address in an IP packet in order to conceal the sender of the packet or to impersonate another computing system. Therefore, it is difficult to identify the actual source of the attack packets using traditional countermeasures. IP traceback aims to locate attack sources, regardless of the spoofed source IP addresses. Several IP traceback methods have been proposed [1]-[3]; especially Source Path Isolation Engine (SPIE)[3] is a feasible solution for tracing individual attack packets. However, SPIE requires that its systems are widely deployed across the Internet for enhancing traceability. Traceability would decrease to a minimum if there were only a few routers that support SPIE.

Web spoofing, also known as phishing, is a form of identity theft in which the targets are users rather than computer systems. A phishing attacker attracts victims to a spoofed website, a so-called phishing site, and attempts to persuade them to provide their personal information. To deal with phishing attacks, a heuristics-based detection method has begun to garner attention. A heuristic is an algorithm to identify phishing sites based on users' experience, and checks whether a site appears to be a phishing site. Based on the detection result from each heuristic, the heuristic-based solution calculates the likelihood of a site being a phishing site and compares the likelihood with the defined discrimination threshold. However, current heuristic solutions are far from suitable use due to the inaccuracy of detection.

In this paper, we describe our two contributions for thwarting IP address spoofing and Web spoofing, respectively. Chapter **2** describes the deployment scenario for IP traceback systems. Chapter **3** figures out a detection method of phishing sites which aims at improving the detection accuracy. Chapter **4** concludes our findings.

2 Deployment scenario for IP traceback systems

2.1 Background

Several IP traceback methods have been proposed [1]-[3]. Especially, Source Path Isolation Engine (SPIE)[3] is a feasible solution for tracing individual attack packets, however it requires large-scale deployment.

Several researchers[4]-[6] have proposed autonomous system (AS)-level deployment to facilitate global deployment of IP traceback systems (IP-TBSs). In this case, it is necessary to deploy an IP-TBS into each AS instead of implementing the SPIE in each router. Since the IP-TBS monitors the traffic between the AS border routers and exchanges information for tracing packets, the traceback client can identify the source AS of the packets.

However, the traceability can be easily affected by the types of network topology and/or the deployment scenario. Gong et al. simulated traceability by using three types of network topologies[4], but their deployment scenario was the random placement; they selected ASes in a random manner. Castelucio et al. mentioned that IP-TBS should be deployed along with intent[5]. In their proposed "strategic placement", IP-TBSs should be deployed in order of BGP neighbors. Hazeyama et al. proposed to emulate the Internet topology[6] that resembles the current Internet topology observed by CAIDA[7]. Hazeyama et al. also introduced four types of deployment scenario and estimated the traceability in the case of Japanese Internet topology[8].

Herein, we evaluated the traceability in China, Japan, and South Korea Internet using AS-level deployment. In our simulation, we created three types of emulated network topologies that resemble China, Japan, and South Korea, respectively. We also prepare four types of deployment scenario, namely, deployment in core ASes, leaf ASes, middle-class ASes, and deployment in a random manner.

2.2 Simulation of traceback deployment

Deployment of the IP-TBS should be considered along with the type of network topology. Let us assume that a network has a star topology and that the IP-TBS is deployed in the central node. In this case, all ASes and AS links can be traced.

In this section, we measure the traceability with deployment simulation. First, we explain the two classes of traceability used in our simulation. We then introduce three types of outfitted Internet topologies, i.e., emulated inter-AS topologies in China, Japan, and South Korea. We also introduce four types of deployment scenarios.

2.2.1 Metrics

We selected traceability as a performance metric. There are two principal classes of traceability: ***packet traceability*** and ***path traceability***. Traceability in the first class is that the system can specify the AS number where the issued IP packet is generated. The second class, path traceability, is that the system can designate the datalink of the AS border.

To calculate the traceability, we refer to the deployment case of previous study[8]. In

[8], the traceability had been defined in Equation (1), where N_S denotes the number of strict ASes, N_L denotes the number of loose ASes, and N denotes the amount number of ASes in the network topology.

$$T_{packet} = \frac{(N_S + N_L)}{N} \quad (1)$$

A strict AS is an AS where an IP-TBS is deployed. A loose AS is an AS where the IP-TBS is not deployed but the neighboring AS is a strict AS. Because of border tracking in typical IP-TBS[9], Hazeyama et al. recognized that a loose AS can be traced within the traceback architecture.

Furthermore, the path traceability is shown in Equation (2) where L_S denotes the number of strict AS links, L_L denotes the number of loose AS links, and L denotes the amount number of AS links in the network topology.

$$T_{link} = \frac{(L_S + L_L)}{L} \quad (2)$$

In a strict AS link, both peered ASes deploy the IP-TBS. In a loose AS link, on the other hand, an AS that deploy an IP-TBS is interconnected to another AS that does not deploy an IP-TBS.

2.2.2 Network topology

We employ the emulated network topologies for several regions. Basically, every traceback method can be used to construct attack paths. Hence, with the use of such traceback methods, communication privacy may be affected. Because of diverse legal interpretations of privacy, deployment across country border may not be easy. As the first step in deployment simulation, we selected the emulated topologies of China, Japan, and South Korea.

We have developed several techniques, including Internet emulation[6] to construct the emulated topologies. Internet emulation involves outfitting an Inter-AS topology to a network emulation testbed for carrying out a realistic performance test. For this study, we used the Region Based Filtering (RBF) algorithm to construct a subgraph of each network region.

In our simulation, we employ the snapshot of CAIDA AS Relationship Database (ASRD) published on November 22, 2008. The dataset can be summarized as shown in Table 1. Because there are loose ASes located outside of each region, the number of deployment target AS and traceback target AS are different. Note that CAIDA extensively surveys AS relationships, however, some types of BGP peering styles such as private peering hinder the creation of a perfect ASRD.

2.2.3 Simulation scenarios

We consider four types of deployment scenarios as follows.

S1: Deployment in order of core ASes

In the ideal scenario, IP-TBSs are deployed into the core ASes. Since the core ASes are interconnected to many BGP neighbors, the traceback system can handle many ASes and AS links. Hence, traceability is expected to be high even if the number of deployed traceback system is low.

Although various criteria need to be satisfied for identifying the network core, we used the number of BGP peers as a metric. In this scenario, the traceback system is deployed to ASes in the decreasing order of the number of established BGP peers.

S2: Deployment in order of leaf ASes

In this scenario, IP-TBSs are deployed to ASes in the increasing order of the number of established BGP peers. Since the IP-TBSs will trace fewer ASes and AS links in this case, traceability will be low. However, attacker

Table 1 Numbers of deployment target and traceback target

	Japan	China	South Korea
Deployment Target (Number of ASes)	500	196	640
Traceback Target (Number of ASes)	768	308	755
Traceback Target (Number of Links)	1589	529	1375

nodes often exist in the leaf ASes. The major ISPs (core ASes) are prone to DoS attacks. Hence, it is reasonable to assume that these types of AS installed defense schemes against DoS attacks, such as Ingress Filtering[10].

S3: Deployment in middle-class ASes

We assumed that the traceability observed with deployment into the core AS to be comparable to that reported by Hazeyama[8]. However, deployment in the core AS might be difficult due to the number of AS border routers. Unless hash-based IP-TBSs are used to network traffic among the AS border routers, the cost involved for deployment into core ASes would be high.

In this scenario, IP-TBSs are deployed to ASes in the decreasing order of the number of established BGP peers, except for core ASes. We assumed that the number of core AS will be estimated by the power-law, referring to the Barabasi-Albert Model[11]. For example, the number of ASes in Japan was 500 as shown in Table 1. The number of core AS is roughly 22 ($\approx\sqrt{500}$), and hence, we measure the traceability by deploying IP-TBSs to the remaining ASes.

S4: Deployment in a random manner

Similar to the simulation performed by Gong et al.[4], IP-TBSs are deployed in a random manner in this scenario. To eliminate bias, we repeated trial experiments 10 times and calculated the average of the traceability values obtained for 1 AS through 50 ASes.

2.3 Simulation results

First, we calculated the packet traceability for the Japanese network topology and summarized in Fig. 1(a), where x axis denoted the number of ASes which deployed IP-TBS, y axis denoted the packet traceability (T_{packet}). If IP-TBS were deployed in 15 AS, the highest T_{packet} was observed in the case of S1 (86.3%), followed by S3 (18.5%), S4 (15.4%), and S2 (3.4%). We also calculated path traceability as shown in Fig. 1(b), where x axis denoted the number of ASes which deployed IP-TBS, y axis denoted the packet traceability (T_{path}). Given the number of deployed ASes (N) = 15, the highest T_{path} was 69.0% in the case of S1, followed by S3 (11.6%), S4 (3.6%), and S2 (0.9%).

We then measured the traceability in the case of the Chinese network topology and the results were shown in Fig. 2(a) and Fig. 2(b). Given N = 15, we observed that the highest T_{packet} was in the case of S1 (74.8%), followed by S3 (27.3%), S4 (21.7%), and S2 (8.1%). The highest T_{path} was 74.9% in the case of S1, followed by S3 (22.9%), S4 (13.0%), and S2 (2.8%).

Finally, we simulated the case of the South Korean network topology and the results were shown in Fig. 3(a) and Fig. 3(b). The results indicated that S1 performed better than others. Given N = 15, the highest T_{packet} was 92.6% in the case of S1, followed by S4 (8.8%), S3 (4.5%), and S2 (3.1%). The highest T_{path} was 93.4% in the case of S1, followed by S3 (5.0%), S4 (2.7%), and S2 (1.1%).

In all cases, the highest T_{packet} and the highest T_{path} were observed in the case of S1. Notably, in the South Korean network topology, traceability in the case of S1 outperformed that in the other cases. We assumed that many ASes in the South Korea network topology were interconnected to a few core ASes.

However, the efficiency of deployment in the core AS was not significantly high in the Chinese network topology. The pair of traceability (T_{packet}, T_{path}) was (27.3%, 22.9%) in the case of S3, higher than that in the other network topologies. We considered there are two reasons. One is the number of deployment target. As shown in Table 1, the number of deployment target was 196 in China. The other one is the geographical restrictions in China; we considered that the core ASes were distributed due to the country size of China. We, therefore, assumed middle-class and/or leaf ASes have established BGP peers with each other.

We found that the South Korean network topology was "concentrated" type while the Chinese network topology was "distributed"

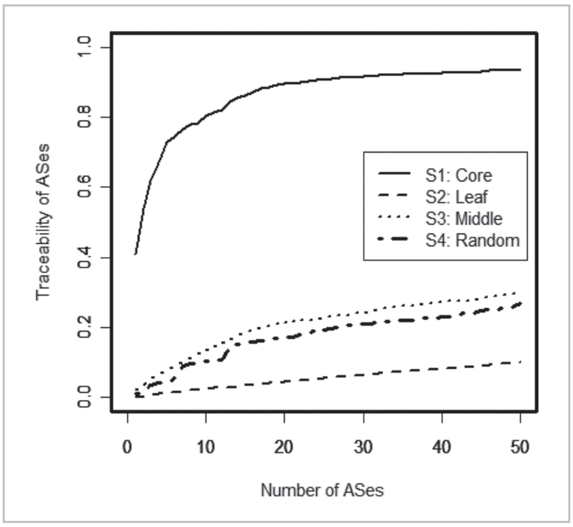

Fig.1(a) *Packet traceability in Japan*

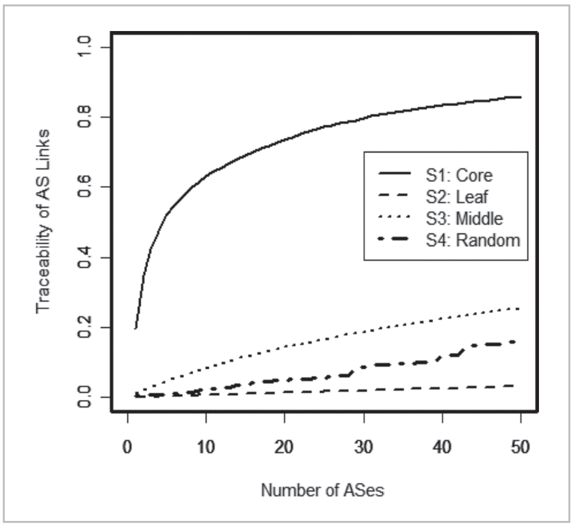

Fig.1(b) *Path traceability in Japan*

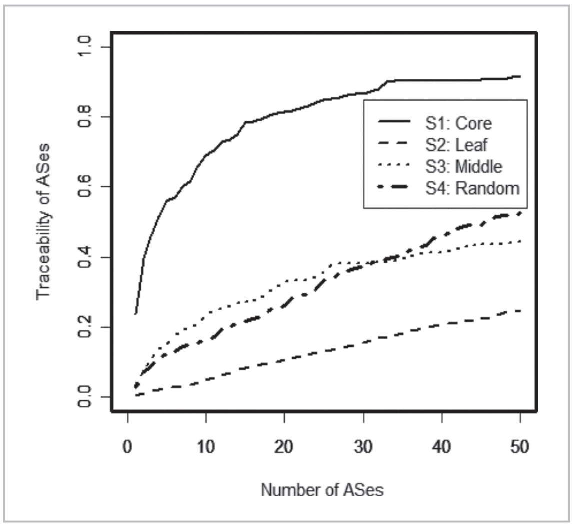

Fig.2(a) *Packet traceability in China*

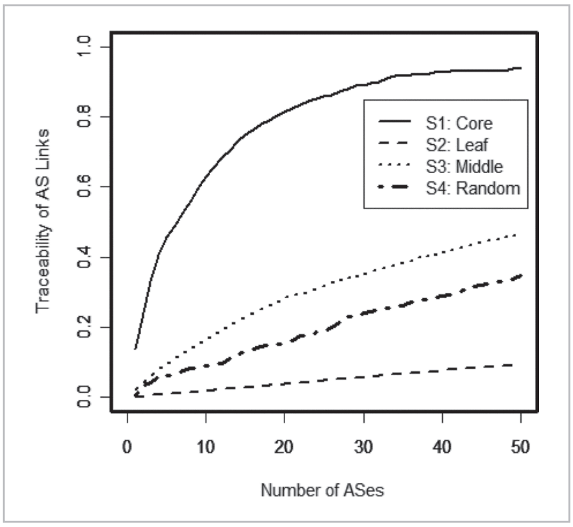

Fig.2(b) *Path traceability in China*

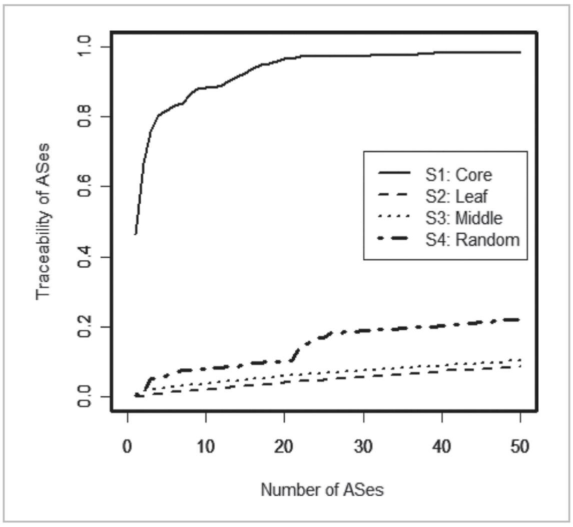

Fig.3(a) *Packet traceability in South Korea*

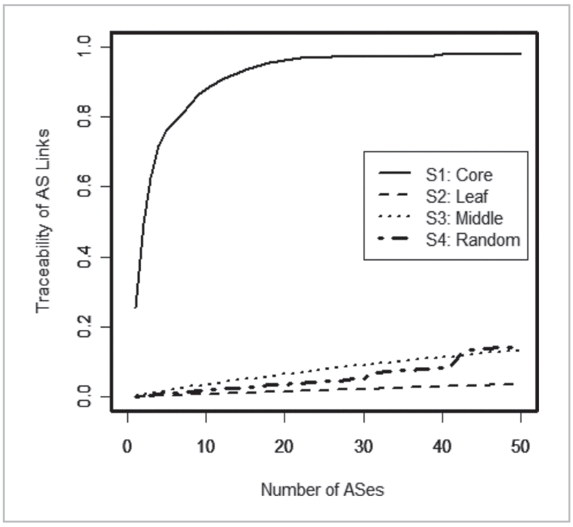

Fig.3(b) *Path traceability in South Korea* type. The characteristics of the Japanese network topology were found to be intermediate between South Korean and Chinese network topologies. However the path traceability in the Japanese network topology was not very high. As shown in Table 1, the number of AS links in the Japanese network topology (1589) was higher than that in the South Korean network topology (1378); however, the number of deployment target in the Japanese network topology (500) was lower than in the South Korean network topology (640). We assumed that middle-class and/or leaf ASes have established BGP peers with both core ASes and other ASes.

3 Detection methods for phishing sites by utilization of past trust decisions

3.1 Background

There are two distinct approaches for identifying phishing sites. One is URL filtering. It detects phishing sites by comparing the URL of a site where a user visits with a URL blacklist, which is composed of the URLs of phishing sites. Unfortunately, the effectiveness of URL filtering is limited. In 2007, the detection accuracy of URL blacklist-based systems was roughly 70%[12]. In 2009, Sheng et al. reported[13] that URL blacklists were ineffective when protecting users initially, as most of them caught less than 20% of phishing sites at hour zero. The rapid increase of phishing sites hinders URL filtering to work sufficiently due to the difficulty of building a perfect blacklist.

The other approach is a heuristic-based method. A heuristic is an algorithm to identify phishing sites based on users' experience, and checks whether a site appears to be a phishing site or not. Checking the life time of a registered website is well-known heuristic as most phishing sites' URL expires in short time span. Based on the detection result from each heuristic, the heuristic-based solution calculates the likelihood of a site being a phishing site and compares the likelihood with the defined discrimination threshold. The detection accuracy of existing heuristic-based solutions is, however, far from suitable for practical use. Zhang et al.[12] mentioned that SpoofGuard[14], which is one of the heuristics-based solutions, identified more than 90% of phishing sites correctly, but incorrectly identified 42% of legitimate sites as phishing. Our previous work[15] proposed to employ machine learning techniques for detection of phishing sites. By comparing with the traditional method and nine types of machine learning-based methods, we found that machine learning-based methods performed better than the traditional methods in almost all of evaluation results. The highest performance was observed in the case of the AdaBoost-based detection method.

A current challenge of the heuristics-based solutions is improving the detection accuracy. In our study, we proposed HumanBoost, which aims at improving AdaBoost-based detection methods. The key concept of HumanBoost is utilizing Web users' past trust decisions (PTDs). Basically, humans have the potential to identify phishing sites, even if existing heuristics cannot detect them. If we can construct a database of PTDs for each Web user, we can use the record of the user's trust decisions as a feature vector for detecting phishing sites. HumanBoost also involves the idea of adjusting the detection for each Web user. If a user is a security expert, the most predominant factor on detecting phishing sites would be his/her trust decisions. Conversely, the existing heuristic will have a strong effect on detection when the user is a novice and his/her PTD has often failed.

3.2 Experiments and results

To check the availability of PTDs, we invited participants and performed a phishing IQ test to construct PTDs, in November 2007, in March 2010, and July 2010. This section describes our first test and explains the dataset description of the phishing IQ test, introduces the heuristics that we used, and then explains our experimental design and finally show the results.

3.2.1 Dataset description

Similar to the typical phishing IQ tests performed by Dhamija et al.[16], we prepared 14 simulated phishing sites and six legitimate ones, all of which contained Web forms in which users could input their personal information such as user ID and password. The conditions of the sites are shown in Table 2. The detailed explanation of phishing tricks is available in [17].

3.2.2 Heuristics

Our experiment employs eight types of heuristics, all of which were employed by CANTINA[18]. To the best of our knowledge, CANTINA is the most successful tool for combining heuristics, since it has achieved high accuracy in detecting phishing sites without using the URL blacklist.

3.2.3 Experimental design

We used a within-subjects design, where every participant saw every website and judged whether or not it appeared to be a phishing site. In our test we asked 10 participants to freely browse the websites. Each participant’s PC was equipped with Windows XP and Internet Explorer (IE) version 6.0 as the browser. Other

Table 2 *Conditions of each website*

#	Website	Real / Spoof	Lang	Description
1	Live.com	real	EN	URL (*login.live.com*)
2	Tokyo-Mitsubishi UFJ	spoof	JP	URL (*www-bk-mufg.jp*), similar to the legitimate URL (*www.bk.mufg.jp*)
3	PayPal	spoof	EN	URL (www.paypal.com.%73%69 ... %6f%6d) (URL Encoding Abuse)
4	Goldman Sachs	real	EN	URL (*webid2.gs.com*), SSL
5	Natwest Bank	spoof	EN	URL (*onlinesession-0815.natwest.com.esb6eyond.gz.cn*), derived from PhishTank.com
6	Bank of the West	spoof	EN	URL (*www.bankofthevvest.com*), similar to the legitimate URL (*www.bankofthewest.com*)
7	Nanto Bank	real	JP	URL (*www2.paweb.anser.or.jp*), SSL, third party URL
8	Bank of America	spoof	EN	URL (*bankofamerica.com@index.jsp-login-page.com*) (URL Scheme Abuse)
9	PayPal	spoof	EN	URL (*www.paypal.com*), first “a’’ letter is a Cyrillic small letter “a’’ (U+430) (IDN Abuse)
10	Citibank	spoof	EN	URL (IP address) (IP Address Abuse)
11	Amazon	spoof	EN	URL (*www.importen.se*), contains “amazon’’ in its path, derived from PhishTank.com
12	Xanga	real	EN	URL (*www.xanga.com*)
13	Morgan Stanley	real	EN	URL (*www.morganstanleyclientserv.com*), SSL
14	Yahoo	spoof	EN	URL (IP address) (IP Address Abuse)
15	U.S.D. of the Treasury	spoof	EN	URL (*www.tarekfayed.com*), derived from PhishTank.com
16	Sumitomo Mitsui Card	spoof	JP	URL (*www.smcb-card.com*), similar to the legitimate URL (*www.smbc-card.com*)
17	eBay	spoof	EN	URL (*secuirty.ebayonlineregist.com*)
18	Citibank	spoof	EN	URL (*シテイバンク.com*), is pronounced “Shi Tee Ban Ku’’, look-alike “Citibank’’ in Japanese Letter (IDN Abuse)
19	Apple	real	EN	URL (*connect.apple.com*), SSL, popup warning by accessing non-SSL content
20	PayPal	spoof	EN	URL (*www.paypal.com@verisign-registered.com*), (URL Scheme Abuse)

than configuring IE to display Internationalized Domain Names, we installed no security software and/or anti-phishing toolbars. We also did not prohibit participants from accessing websites not listed in Table 2. Some participants therefore inputted several terms into Google and compared the URL of the site with the URLs of those listed in Google's search results.

In this experiment, we used the average error rate as a performance metric. To average the outcome of each test, we performed 4-fold cross validation and repeated 10 times.

3.2.4 Experiment results

First, we invited 10 participants, all Japanese males, from the Nara Institute of Science and Technology. Three had completed their master's degree in engineering within the last five years, and the others were master's degree students. We let participants to label the websites described in Table 2.

Next, we determined the detection accuracy of the AdaBoost-based detection method along with our experimental designs as mentioned in Section ***3.2.3***. We used eight heuristics and outputted a binary variable representing phishing or not-phishing. The detection results by each heuristic are shown in [17].

Finally, we measured the detection accuracy of HumanBoost. We constructed 10 PTD databases. In other words, we made ten types of 20 * 9 binary vectors. Under the same conditions described above, we calculated the average error rate for each case of HumanBoost.

The results are summarized in Fig. 4, where the gray bars denote the error rate of each participant, the white bar denotes the average error rate of the AdaBoost-based detection method, and the black bars denote

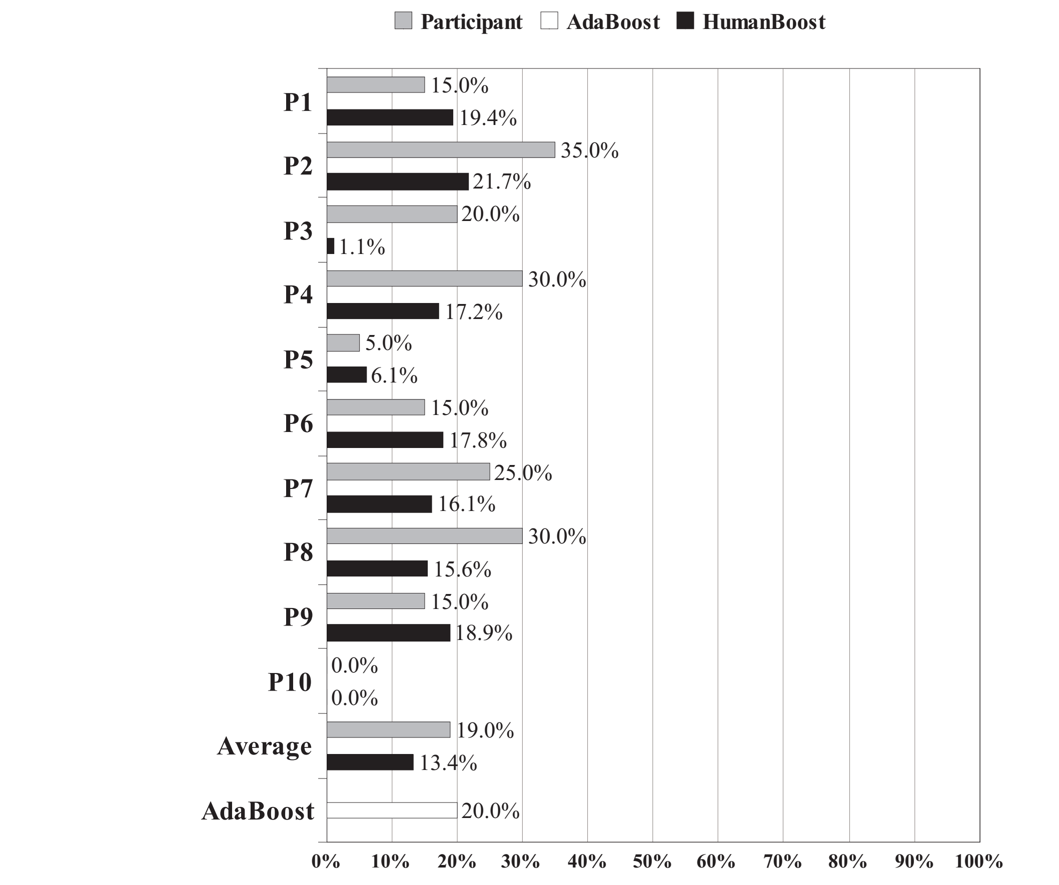

Fig.4 Average error rates of each participant, AdaBoost-based detection method, and HumanBoost in the pilot study, in November 2007

that of HumanBoost. The average error rate for HumanBoost was 13.4%, 19.0% for the participants and 20.0% for the AdaBoost-based detection method. The lowest false positive rate was 19.6% for HumanBoost, followed by 28.1% for AdaBoost and 29.7% for the participants. The lowest false negative rate was 8.5% for HumanBoost, followed by 13.5% for AdaBoost, 14.0% for the participants.

We found that the average error rate of some participants increased by employing HumanBoost. We analyzed the assigned weights and found that some heuristics were assigned higher weights than such users' trust decision. For instance, participant 9 had labeled three legitimate sites as phishing sites, whereas the existing heuristics had labeled these three sites correctly. His trust decision was therefore inferior to that of existing heuristics and we assumed that this is the reason for the increase in error rate.

3.3 Follow-up study

Increasing the number of participants essentially enables us to generalize the outcome of HumanBoost. In this section, we explain the two cases of the follow-up studies performed in 2010. Note that the pilot study was performed in November 2007 and the follow-up studies were performed in March 2010 and July 2010, therefore there may be difference based on the demographics of the participants and substantial media coverage about phishing.

3.3.1 A case of the follow-up study in March 2010

Our follow-up study had 11 new participants, aged 23 to 30. All were from the Japan Advanced Institute of Science and Technology. All were Japanese males, two had completed their master's degree in engineering within the last five years, and the others were master's degree students.

Before conducting the follow-up study, we modified the dataset described in Table 2. Due to the renewal of PayPal's website during 2007–2010, we updated websites 9 and 20 to mimic the current PayPal login pages. Particularly, Nanto Bank, website 6 in Table 2, had changed both the URL and the content of its login page. Nanto Bank is also not well-known in Ishikawa Prefecture, where the participants of the follow-up study lived. We therefore changed website 6 to Hokuriku Bank (another Japanese regional bank in Ishikawa). The domain name of Hokuriku Bank is *www2.paweb.answer.or.jp*, the same as Nanto Bank.

In March 2010, we invited 11 participants and asked them to label 20 websites as legitimate or phishing. Different from the pilot study described in Section **3.2**, we prepared printed documents to expedite this experiment. Instead of operating a browser, participants looked at 20 screen shots of a browser that had just finished rendering each website. These screen shots were taken on Windows Vista and IE 8.0 because IE 6.0 was out of date in March 2010. Additionally, showing a browser screen shot is often used for phishing IQ tests.

The results are shown in Fig. 5, where the gray bars denote the error rate of each participant, the white bar denotes the average error rate of the AdaBoost-based detection method, and the black bars denote that of HumanBoost. The lowest error rate was 10.7% for HumanBoost, followed by 12.0% for AdaBoost and 31.4% for the participants. The lowest false positive rate was 15.4% for AdaBoost, followed by 18.1% for HumanBoost and 39.9% for the participants. The lowest false negative rate was 6.1% for HumanBoost, followed by 8.4% for AdaBoost and 25.9% for the participants. In comparison to the pilot study, the average error rate in participants increased due to the difference in the experimental design; the pilot study allowed participants to operate a browser but the follow-up study did not. However, we observed that HumanBoost achieved higher detection accuracy.

3.3.2 A case of the follow-up study in July 2010

In order to collect more users' PTDs, we recruited participants via Internet research company. In this section, we summarize the results briefly.

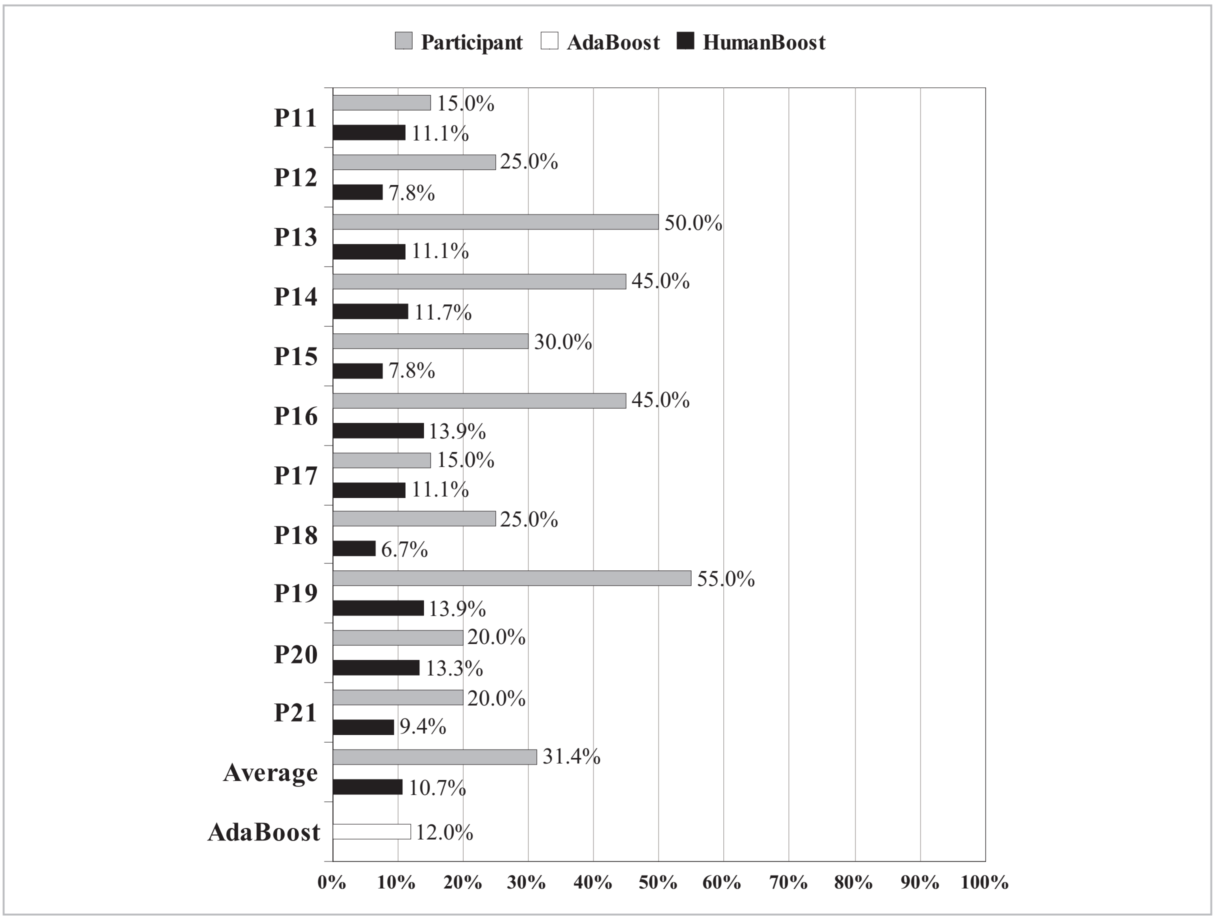

Fig.5 *Average error rates of each participant, AdaBoost-based detection method, and HumanBoost in the follow-up study, in March 2010*

Of the recruited 309 participants, 42.4% (131) were male and 57.6% (178) were female. Age ranged from 16 to 77 years old. 48.2% of participants (149) were office workers, and 19.7% (61) were households and 5.8% (18) were students. Of the students, 66.7% (12) were Bachelors, 11.1% (2) were high school students, 5.6% (1) was a master's degree student. They mainly lived around Tokyo area. We therefore changed website 6 to Tokyo Tomin Bank (another Japanese regional bank in Tokyo). The domain name of Tokyo Tomin Bank is also *www2.paweb.answer.or.jp*. The other conditions of this study are the same as the follow-up study described in Section ***3.3.1***. In July 2010, recruited 309 participants looked at 20 screen shots and judged whether the site seems to be phishing or legitimate.

Based on the detection results, we also calculated the average error rate for each participant, the AdaBoost-based detection method, and HumanBoost. The lowest error rate was 9.7% for HumanBoost, followed by 10.5% for AdaBoost and 40.5% for the participants. The lowest false positive rate was 18.3% for AdaBoost, followed by 19.5% for HumanBoost and 57.4% for the participants. The lowest false negative rate was 5.5% for HumanBoost, followed by 7.1% for AdaBoost and 33.2% for the participants.

4 Conclusion

We tackled two types of deception, namely IP address spoofing and Web spoofing. For tracing spoofed IP address, practical deployment of IP traceback system (IP-TBS) is necessary. We simulated the traceability by using our strategy for deployment of IP-TBS into Autonomous Systems (ASes). We used two types of traceabilities — packet traceability and path traceability — as performance metrics in our simulation. Generally, traceability was affected by the types of network topology and the deployment scenario. For practical simulations, we used emulated Chinese, Japanese, and South Korean network topologies. We also introduced four types of deployment scenario, namely, deployment in core ASes, leaf ASes, middle-class ASes, and deployment in a random manner.

Our simulation results showed that the traceability obtained for deployment into core ASes outperformed those numbers obtained for the other scenarios, regardless of the type of network topology. When the number of ASes that deployed IP-TBS was 15, the pair of packet traceability and path traceability was (86.3%, 69.0%) in the case of Japan, (74.8%, 74.9%) in the case of China, and (92.6%, 93.4%) in the case of South Korea. Deployment for middle-classes was the second highest in almost of all cases, however, the pair of traceability was (18.5%, 11.6%) in the case of Japan, (27.3%, 22.9%) in the case of China, and (4.5%, 5.0%) in the case of South Korea.

The results also revealed the characteristics of three network topologies. In the Chinese network topology, middle-class ASes and/or leaf ASes were interconnected. On the contrary, in the South Korean network topology, many ASes established BGP peers with a few core ASes. By comparing these two regions, Japanese network topology was intermediate between South Korea and China.

For thwarting Web spoofing, a sophisticated detection method for phishing sites is desired. We presented an approach called HumanBoost to improve the accuracy of detecting phishing sites. The key concept was utilizing users' past trust decisions (PTDs). Since Web users may be required to make trust decisions whenever they input their personal information into websites, we considered recording these trust decisions for learning purposes. We simply assumed that the record can be described by a binary variable, representing phishing or not-phishing, and found that the record was similar to the output of the existing heuristics.

As our pilot study, in November 2007, we invited 10 participants and performed a subject experiment. The participants browsed 14 simulated phishing sites and six legitimate sites, and judge whether or not the site appeared to be a phishing site. We utilized participants' trust decisions as a new heuristic and we let AdaBoost incorporate it into eight existing heuristics.

The results showed that the average error rate for HumanBoost was 13.4%, whereas that of participants was 19.0% and that for AdaBoost was 20.0%. We also conducted the follow-up study in March 2010. This study invited 11 participants, and was performed in the same fashion of the pilot study. The results showed that the average error for HumanBoost was 10.7%, whereas that of participants was 31.4%, and that for AdaBoost was 12.0%. Finally, we invited 309 participants and performed the follow-up study in July 2010. The results showed that the average error rate for HumanBoost was 9.7%, whereas that of participants was 40.5% and for AdaBoost was 10.5%. We therefore concluded that PTDs are available as new heuristics and HumanBoost has the potential to improve detection accuracy for Web user.

As future work, our research items are summarized as follows. In the case of IP traceback, we plan to estimate the traceability when IP-TBSs that deployed in China, Japan, and South Korea are interconnected. Although there are several legal interpretations of privacy in communication, the IP-TBSs should be capable of exchanging traceback queries; this is because DoS attacks often originate regardless of the regions. We will also perform simulation studies using emulated network topologies derived from other network regions.

In the case of HumanBoost, we perform a field test in a large-scale manner. Removing bias is generally important for a participant-based test. Though we used cross validation, the presence of bias can still be assumed due to the biased dataset and/or biased samples.

A field test is possible by distributing it as browser extension with some form of data collection and getting a large population of users to agree to use it.

References

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

2 S. Savage, D. Wetherall, A. R. Karlin, and T. E. Anderson, "Practical network support for IP traceback," Proceedings of the ACM SIGCOMM 2000 Conference on Applications, Technologies, Architectures, and Protocols for computer communications, pp. 295–306, Aug. 2000.

3 A. C. Snoeren, C. Partridge, L. A. Sanches, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Stayer, "Hash-based IP traceback," Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for computer communications, pp. 3–14, Aug. 2001.

4 C. Gong, T. Le, T. Korkmaz, and K. Sarac, "Single Packet IP Traceback in AS-level Partial Deployment Scenario," Proceedings of the IEEE Global Telecommunications Conference, Nov. 2005.

5 A. O. Castelucio, Ronaldo M. Salles, and A. Ziviani, "Evaluating the partial deployment of an AS-level IP traceback system," Proceedings of the ACM symposium on Applied computing, pp. 2069–2073, Mar. 2008.

6 H. Hazeyama, M. Suzuki, S. Miwa, D. Miyamoto, and Y. Kadobayashi, "Outfitting an Inter-AS Topology to a Network Emulation TestBed for Realistic Performance Tests of DDoS Countermeasures," Proceedings of the Workshop on Cyber Security and Test, Jul. 2008.

7 The CAIDA Web Site, "CAIDA: cooperative association for internet data analysis," Available at: http://www.caida.org/

8 H. Hazeyama, K. Wakasa, and Y. Kadobayashi, "A consideration on deployment scenarios on a filed test of IP traceback in Japan," IEICE technical report, Internet Architecture, pp. 25–30, Jul. 2008. (in Japanese)

9 H. Hazeyama, Y. Kadobayashi, D. Miyamoto, and M. Oe, "An Autonomous Architecture for Inter-Domain Traceback across the Borders of Network Operation," Proceedings of the IEEE Symposium on Computers and Communications, Jun. 2006.

10 B. R. Greene, C. Morrow, and B. W. Gemberling, "Tutorial: ISP Security - Real World Techniques II," Available at: http://www.nanog.org/meetings/nanog23/

11 A. Barabasi and R. Albert, "Emergence of Scaling in Random Networks," Science, Vol. 286, pp. 509–512, 1999.

12 Y. Zhang, S. Egelman, L. Cranor, and J. Hong, "Phinding Phish: Evaluating Anti-Phishing Tools," Proceedings of the 14th Annual Network and Distributed System Security Symposium, Feb. 2007.

13 S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An Empirical Analysis of Phishing Blacklists," Proceedings of the 6th Conference on Email and Anti-Spam, Jul. 2009.

14 N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C. Mitchell, "Client-side defense against web-based identity theft," Proceedings of the 11th Annual Network and Distributed System Security Symposium, Feb. 2004.

15 Daisuke Miyamoto, Hiroaki Hazeyama, and Youki Kadobayashi. "An Evaluation of Machine Learning-based Methods for Detection of Phishing Sites," Australian Journal of Intelligent Information Processing Systems, Vol. 10, No. 2, pp. 54–63, Nov. 2008.

16 R. Dhamija, J. D. Tygar, and M. A. Hearst, “Why Phishing Works,” Proceedings of Conference on Human Factors in Computing Systems, Apr. 2006.

17 D. Miyamoto, H. Hazeyama, and Y. Kadobayashi, “HumanBoost: Utilization of Users' Past Trust Decision for Identifying Fraudulent Websites,” Journal of Intelligent Learning Systems and Applications, Vol. 2, No. 4, pp. 190–199, Scientific Research Publishing, Dec. 2010.

18 Y. Zhang, J. Hong, and L. Cranor, “CANTINA: A Content-Based Approach to Detecting Phishing Web Sites,” Proceedings of the 16th World Wide Web Conference, May 2007.

(Accepted June 15, 2011)

MIYAMOTO Daisuke, *Ph.D.*

Assistant Professor, Information Technology Center, University of Tokyo

Network Security

HAZEYAMA Hiroaki, *Ph.D.*

Assistant Professor, The Graduate School of Information Science, Nara Institute of Science and Technology

IP Traceback, Testbed

KADOBAYASHI Youki, *Ph.D.*

Guest Expert Researcher, Network Security Research Institute/Associate Professor, The Graduate School of Information Science, Nara Institute of Science and Technology

Cybersecurity, Internet Engineering