Sender Authentication Technology Implementation Status and Standardization Trends

In this volume we report on analysis results incorporating the 52 weeks' worth of data from week 14 of 2013 to week 13 of 2014, while referencing data from IIR Vol.1.

In our discussion of email technology, we also report on changes to the SPF sender authentication technology.

2.1 Introduction

In this report we discuss the latest trends in spam and email-related technologies, and examine a variety of anti-spam measures in which IIJ is involved. We presented ongoing reports between IIR Vol.1 and Vol.19, but in the future we are planning to present irregular reports about once a year. In this volume our report focuses on data from week 1 of 2014 (December 30, 2013 to January 5, 2014) to week 13 (March 24 to March 30, 2014), which corresponds to the fourth quarter of FY2013 in Japan. We also examine analysis results that include 52 weeks of data for the period of about a year since the last report (Vol.19), covering week 14 of 2013 (April 1 to April 7, 2013) to week 13 of 2014. Additionally, we reference the 304 weeks' worth of data since IIR Vol.1, covering almost six years, as necessary. In our discussion of email technologies, we examine the implementation status of the sender authentication technology that we have discussed to date, and report on changes to the SPF sender authentication technology that is currently undergoing standardization.

2.2 Spam Trends

In this section, we will report on spam trends, focusing on historical ratios of spam detected by the Spam Filter provided through IIJ's email services and the results of our analysis concerning spam sources. In this report, we show transitions in the ratios from IIR Vol.1 (June 2, 2008) in Figure 1, to examine long-term changes in spam ratios.

2.2.1 Ratios Have Declined Since Around the Middle of 2010

In 2008 and 2009, average spam ratios for the year came to 82.3% and 81.8%, respectively, indicating that the majority of email received was spam. This situation changed from the second quarter of 2010 (June 28 to October 3, 2010), when ratios started to gradually decline. The average ratio for 2010 was 79.4%, with the ratio of over 80% for the first quarter of 2010 dropping to 78.7% in the second quarter, falling below 80% for the first time since we began these surveys. The ratio subsequently continued to decline, and has remained in the 40% range since the second quarter of 2011.

As we have already reported a number of times in this IIR, the drop in spam ratios and actual spam volumes is estimated to be due to a decline in the botnet activity from which spam originates.

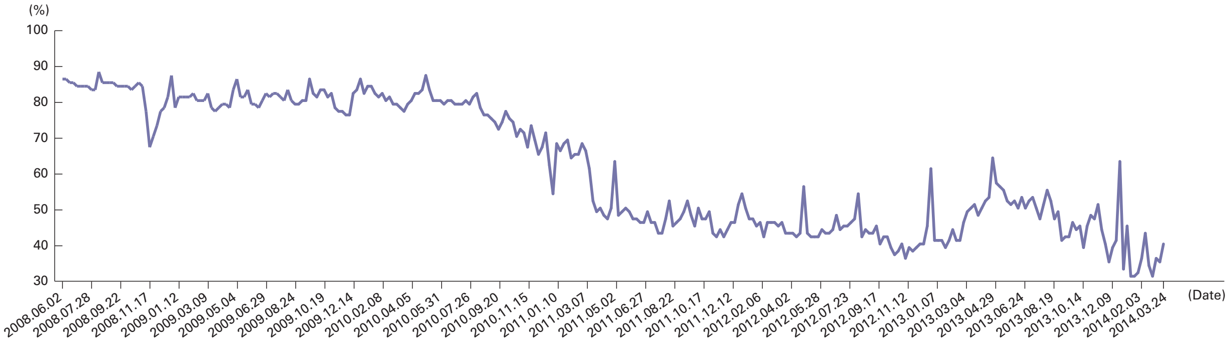

Figure 1: Spam Ratio Trends

PCs that have been infected with malicious software*1 and are being controlled from outside are called bots. Collectively these bots are known as botnets, and the servers that control them are referred to as C&C servers*2. One effective method of stopping botnet activity is to shut down these C&C servers to prevent commands being sent to a botnet. It is said that government agencies in various countries suppressing botnet activity by forcing the shutdown of these C&C servers using legal means led to a decrease in spam volumes. There is also information about the appearance of P2P (Peer-to-Peer) botnets that do not have specific C&C servers, so continued vigilance is necessary.

2.2.2 Recent Spam Ratios on the Decrease

In the fourth quarter of FY2013, from week 1 of 2014 (December 30, 2013 to January 5, 2014) to week 13 (March 24 to March 30, 2014), the average spam ratio was 38.5%. The average for the same period the previous year (the fourth quarter of FY2012) was 45.5%, so this represents a drop of 7%. During this period, the spam ratio was highest in week 1 of 2014, at 63.5%. The volume of spam during this period was also quite high, but because it was the year-end and New Year holiday period, the volume of normal mail was low, increasing the relative spam ratio. The only other weeks with an average ratio of over 40% were week 3, week 8, and week 13.

2.2.3 An Increase in Threats Triggered by Email

The ratio of spam among email received, as well as spam volumes, are both significantly lower than previous levels. However, the level of threat resulting from spam seems to be increasing. In the past email was mostly used as an advertising tool for some kind of product (including illegal ones), but recently there have been more and more cases in which it is suspected that email was used as a route for compromising PCs within an organization.

For example, a report*3 published by the National Police Agency on January 30, 2014 indicated there were 1,315 incidents of illegal remittance in 2013, reaching an unprecedented total of approximately 1.406 billion yen in damages. Furthermore, it has been reported that incidents in which users were redirected to phishing sites via email are on the rise. In other words, it could be said that spam is transforming from something that is simply a nuisance due to the time it takes to delete, to something more dangerous that can trigger incidents of financial crime. Considering that this kind of online banking crime is currently occurring, we believe it is also likely that the same techniques are being used to steal a variety of IDs and passwords. This stolen information includes IDs and passwords for sending email, and there have been many incidents in which legitimate mail servers were used as stepping stones to send spam.

2.2.4 Trends in the Regional Sources of Spam

Figure 2 shows our analysis results of regional sources of spam in the fourth quarter of FY2013. The data used in this analysis does not cover all the email services IIJ provides, so not all the sources of spam shown in Figure 1 are targeted. Because of this, note that there may be slight differences.

China (CN) was the number one source of spam for this survey period, accounting for 19.1% of total spam. China has remained the most common source of spam since IIR Vol.11 (the fourth quarter of FY2010). Japan (JP) was second at 13.4%. Japan has also held the second place since IIR Vol.16 (the first quarter of FY2012), and regularly appeared in the upper rankings from about a year before that. These regions have been practically fixed in the upper rankings since the ratio of spam to overall received email declined around the middle of 2010 (see Figure 1), so we believe it likely they are static sources not affected much by the drop in botnet activity.

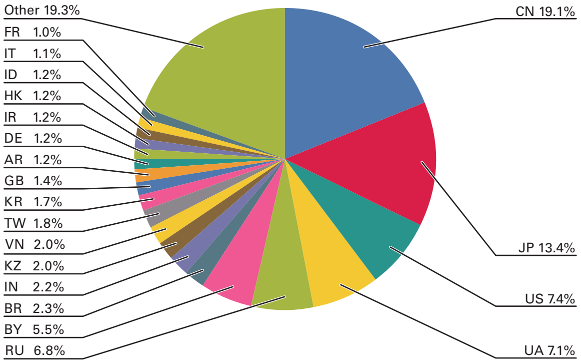

Figure 2: Regional Sources of Spam

[1] Software created for certain malicious purposes, such as the sending of spam, is sometimes called malicious software or malware to differentiate it from the more widely-used term “viruses.”

[2] C&C server (Command & Control Server).

[3] Status of Incidents of Illegal Remittance Related to Internet Banking in 2014 (http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf) (in Japanese).

The United States was third (US, 7.4%), and the Ukraine was fourth (UA, 7.1%), with Russia in fifth (RU, 6.8%) and Belarus in sixth (BY, 5.5%). Until now Asian regions were the main sources of spam, but from the results this time we identified that regions in Eastern Europe and Central Asia (Kazakhstan (KZ) was ninth) are also on the rise.

Figure 3 shows trends for the top six regions (CN, JP, US, UA, RU, BY) over 65 weeks, including this survey period and the year before it. This graph demonstrates that the top two regions (CN, JP) maintained a high ratio throughout. Additionally, changes in the ratios for China (CN) and Japan (JP) seem to be linked in the most recent results (the fourth quarter of FY2013). Japan has been involved in spam sent from China in the past, as demonstrated by the Takumi Tsushin arrests in 2007, and this relationship may have deepened.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. This time we report the implementation status of sender authentication technology, which shows promise as an anti-spam measure. Additionally, when technology is standardized and used widely, it becomes more effective. We cover trends in standardization later in this section.

2.3.1 Sender Authentication Technology Adoption Rates

Sender authentication technology was made so that it could be implemented without directly affecting existing SMTP*4 email delivery systems. Emails are authenticated on the recipient side, but authentication is only possible when the sender has implemented sender authentication technology. In other words, it is possible to implement sender authentication technology based on the judgment and timing of each email sender and recipient, but authentication results are only obtained when both sender and recipient have the technology set up.

Sender authentication technologies include SPF*5, which performs authentication based on the email sender's IP address, and DKIM*6, which creates a digital signature from the email body text, and performs authentication by verifying this. Figure 4 and Figure 5 show the sender implementation status for each technology on the sender side. These recipient authentication ratios were taken from emails received on IIJ's main email services between January and March, 2014.

To implement SPF on the email sender side, you publish (configure) SPF records in the DNS TXT resource records for domains to use (or not use) for email. One great advantage of SPF is that once you have configured an SPF record, you don't need to do anything else unless the IP address for the mail server using that domain name changes.

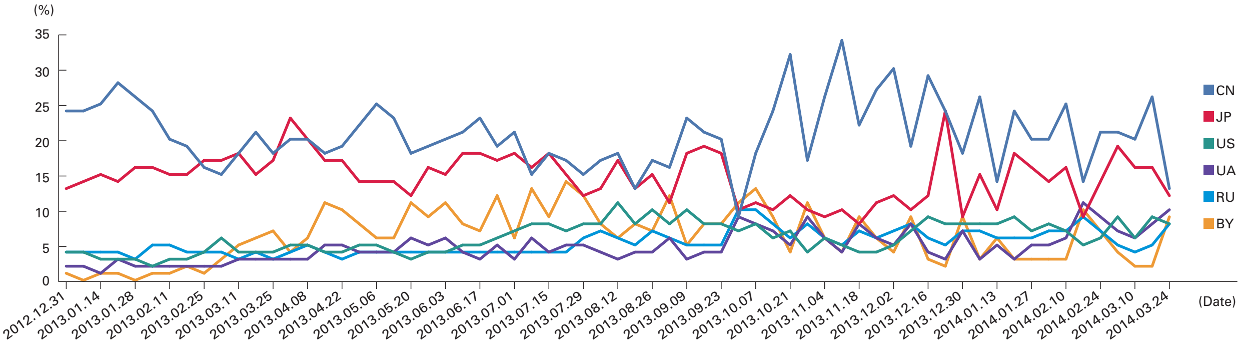

Figure 3: Trends in Ratios for the Main Regional Sources of Spam

*4 SMTP (Simple Mail Transfer Protocol) has been revised a number of times, and the latest version is available as RFC5321.

*5 SPF (Sender Policy Framework) was first published as RFC4408 in the Experimental category, and was later revised as RFC7208 (Standards Track).

*6 DKIM (DomainKeys Identified Mail) was published as RFC6376, and later became an Internet standard as STD76.

In part due to this benefit, SPF has an extremely high implementation ratio, as can be seen in Figure 4. The ratio of cases in which SPF is implemented on the sender side are those with an authentication result other than “none” (could not authenticate), and for this survey period the ratio was 73.2%. The “pass” authentication result (47.7%) indicates the ratio of email that was correctly authenticated. The “hardfail” (2.2%) and “softfail” (21.0%) results make up the ratio of authentication failures, indicating that the domain was spoofed, or that authentication failed because the delivery route changed, such as when email was forwarded.

Meanwhile, DKIM requires additional processing for each email sent, to create digital signature information from elements such as the email body text, and insert this into the email headers. This means that new functions must be added to outgoing mail servers, and a greater burden is placed upon resources due to the extra processing that signature creation involves. In other words, there are factors that make it more difficult to implement on the sender side compared to SPF, and it is believed that as a result its implementation tends to lag behind on the recipient side as well. However, it does have the benefit of authentication failures due to changes in the mail delivery route that we touched upon in the SPF authentication results almost never occurring. Additionally, because the digital signature is created from email body text, it is said to be a more robust sender authentication technology than SPF, as this enables features such as the detection of alterations to be made to body text at some point on the delivery route.

In the current survey period, DKIM authentication results showed the ratio of sender-side implementation to be 11.6%. We believe measures must be taken to increase this ratio.

2.3.2 Sender Authentication Technology Adoption Trends

Figure 6 shows trends in the ratio of SPF authentication results, and Figure 7 shows trends in the ratio of DKIM authentication results.

The SPF implementation ratio has grown steadily since we began these surveys (August 2009). Since 2013 growth in implementation has slowed, but the implementation ratio remains over 70%. Over this period, the implementation ratio has increased by a maximum of around 32.7%. DKIM implementation ratios have not increased as rapidly as SPF, but even so, its ratio is gradually growing. Over this period, its implementation ratio increased by about 11.1%.

According to data presented by Google, which provides the Gmail service, in December 2013[*7], 91.4% of email they received that was not spam could be authenticated using either SPF or DKIM. The sender authentication ratios given in this IIJ report cover all email received (including spam), so the original data has different characteristics than the Google report. This means they cannot simply be compared, but in any case the ratios were very high.

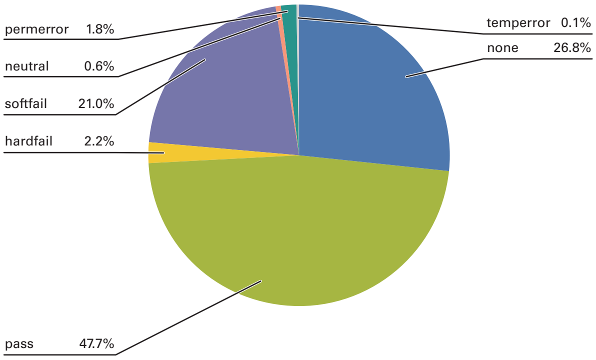

Figure 4: SPF Authentication Result Ratios

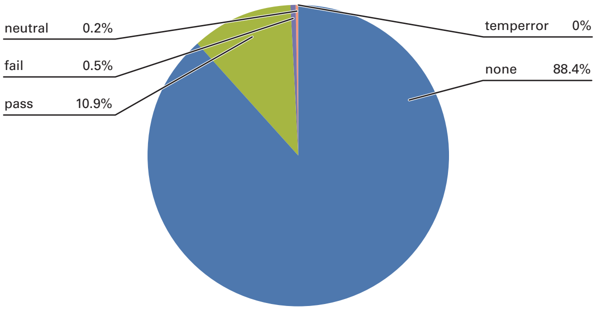

Figure 5: DKIM Authentication Result Ratios

[*7] Internet-wide efforts to fight email phishing are working (http://http://googleonlinesecurity.blogspot.sg/2013/12/internet-wide-efforts-to-fight-email.html).

The Google report states that SPF authentication was possible in 89.1% of cases, and for DKIM this ratio was 76.9%. In 74.7% of cases both SPF and DKIM authentication were possible, but domains that only implement SPF or DKIM also exist, and totaling these together apparently results in the figure of 91.4%.

Google is a company that promotes DMARC, which uses both SPF and DKIM authentication results, so by presenting high implementation ratios like these, it demonstrates that the world is already prepared for implementing DMARC. It is also reported in this document that 80,000 domains already state a policy of blocking email that cannot be authenticated using DMARC, and that every week several hundred million emails are blocked according to this policy.

Some areas of the DMARC specifications are left incompatible with the mailing list delivery methods that are currently used, so in certain cases it is difficult to advertise rejection of receipt based on the DMARC policy, and this must be taken into account.

2.3.3 SPF Standardization Trends

SPF technology is standardized as an experimental RFC. Currently, efforts are being made to revise this SPF. SPF was originally technology that underwent lengthy evaluation within the IETF's marid Working Group, with the intention to integrate it with Sender ID*8, which was also published as an experimental RFC at around the same time (April 2006). In the end, the integration fell through due to issues such as the original proposing company asserting intellectual property rights over PRA (Purported Responsible Address), which is a characteristic of Sender ID.

However, as already shown in the data, SPF is a widely prevalent sender authentication technology, so the IEFT's spfbis Working Group began discussions from November 2011 with the aim of standardization using their accumulated experience. In April 2014, SPF was published as a Proposed Standard (Standards Track) in RFC7208. Here, we will explain the differences between RFC7208 and the previous RFC4408.

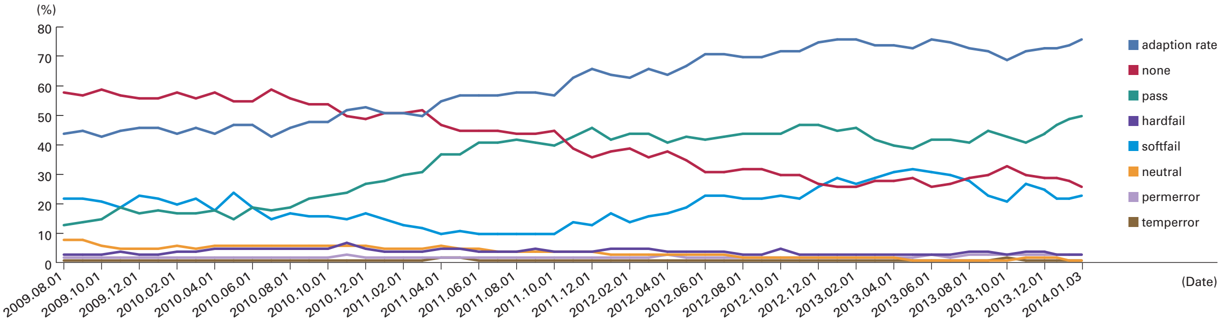

Figure 6: SPF Authentication Result Ratio Trends

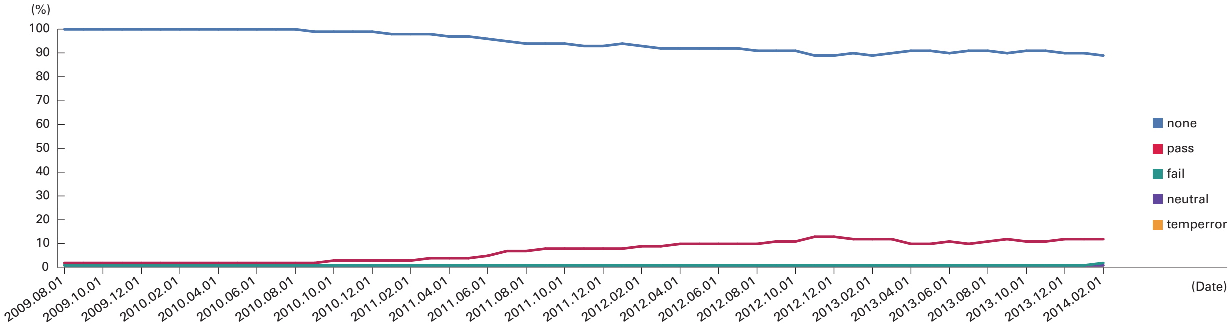

Figure 7: DKIM Authentication Result Ratio Trends

[8] Sender ID: RFC4406, RFC4407

First, as a starting point for discussion, the following views are expressed.

- SPF was successful, but Sender ID was not (so Sender ID should not be incorporated)
- The key to revising the SPF specifications is to fix errors, delete functions that are not used, and add expansions that are already widely in use, etc.
- Do not expand SPF itself or delete functions that are used

Consequently, no significant changes were added through the spfbis Working Group ID. The main changes indicated in the current ID are as follows.

1. SPF records should use TXT RR (16) rather than SPF RR type (99) on DNS
2. Authentication results should be saved to both the "Received-SPF" and "Authentication-Results" email headers

Changes other than these included fixes to minor errors, etc. In the end, it was decided that a policy for email handling when authentication fails was not specified in the RFC, and that this policy should be determined on the recipient side. Although I don't believe the SPF macro functions that enable comparatively complex formats to be written are actively used by many domains, it was decided to leave these in the specifications.

No clear measures were indicated for coping with the forwarding of email, which was an issue for SPF. Instead, proposed solutions involved rewriting the RFC5321. From (Envelope-From) when forwarding, or configuring a white list for receipt of mail at the forwarding destination. The SPF Internet-Draft was revised to Version 21, and this took a lot of time considering how few points were actually changed. SPF has a high adoption rate due to the ease of implementation on the sender side, and this standardization work is expected to further promote the utilization of SPF authentication results.

2.4 Conclusion

This is the first Messaging Technology article in a year, so we examined spam trends and sender authentication technology in more detail than usual. As mentioned in the report, although spam volumes are on the decrease, the threats that can result from spam are becoming more serious.

For example, the other day there was a commercial for a major bank on TV warning of phishing emails. We believe this indicates that the number of victims has increased to the point where it is necessary to send warnings out to the general public via media such as the television. The commercial also mentioned that the techniques used are becoming more devious. With security threats on the Internet growing, both organizations such as companies and private individuals now carry out a variety of measures. However, current email systems are one of few applications that can deliver a range of information directly to recipients. With attacks targeting these systems ongoing, there is a limit to the methods for avoiding threats based on the judgment of individual email recipients. As someone involved with email systems, every day we strive towards providing a system that identifies these major threats and prevents them from reaching email users as soon as possible.

Author:

Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Service Development Section of the Application Development Department of the IIJ Product Division. He is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He has been a member of M^{3}AAWG since its establishment. He is deputy chairperson of the Anti-Spam mail Promotion Council (ASPC), and a member of the administrative group. He is also chief examiner for the Sender Authentication Technology Workgroup, and chairperson of the LAP 10 Tokyo Committee. Additionally, he is a member of Internet Association Japan's Anti-Spam Measures Committee.